What's New

What's new in CCC 6?

CCC 6 offers unprecedented accountability for your backup tasks, plus a brand new file copier that's faster, smarter, and designed to adapt to Apple's fast pace of OS and filesystem innovation. Combined with a sleeker, modern interface, we think you're going to love this new version of CCC.

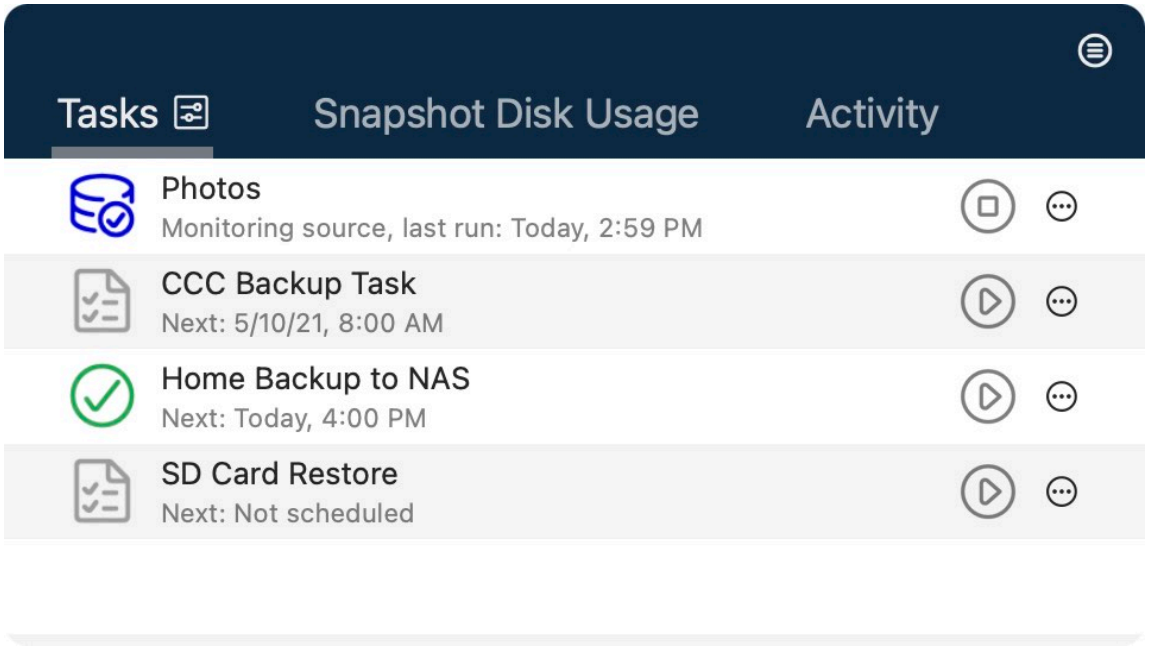
Faster backups with our next-generation file copier

We've completely rebuilt our file copier to take advantage of the performance characteristics of modern storage. Built on a multi-threaded design, our new file copier provides a foundation for many of the new features noted below, and paves the way for many new features in the future.

CCC Dashboard: The new menubar application

CCC's menubar application has gotten a complete makeover. The new "Dashboard" offers one-click access to starting, stopping and monitoring your CCC tasks, plus details about recent task activity.

The Dashboard also gives you a heads up to snapshot disk usage on the startup disk. Have you ever deleted files from the startup disk, emptied the Trash, then wondered why the space wasn't freed? Many people have been blindsided by the creation of snapshots on the startup disk – by CCC, Time Machine, and even macOS. CCC's Dashboard tracks the disk usage consumed by snapshots. If a sudden change occurs, or if disk usage is exceeding expectations, CCC raises the change to your attention so you can address the root of the matter.

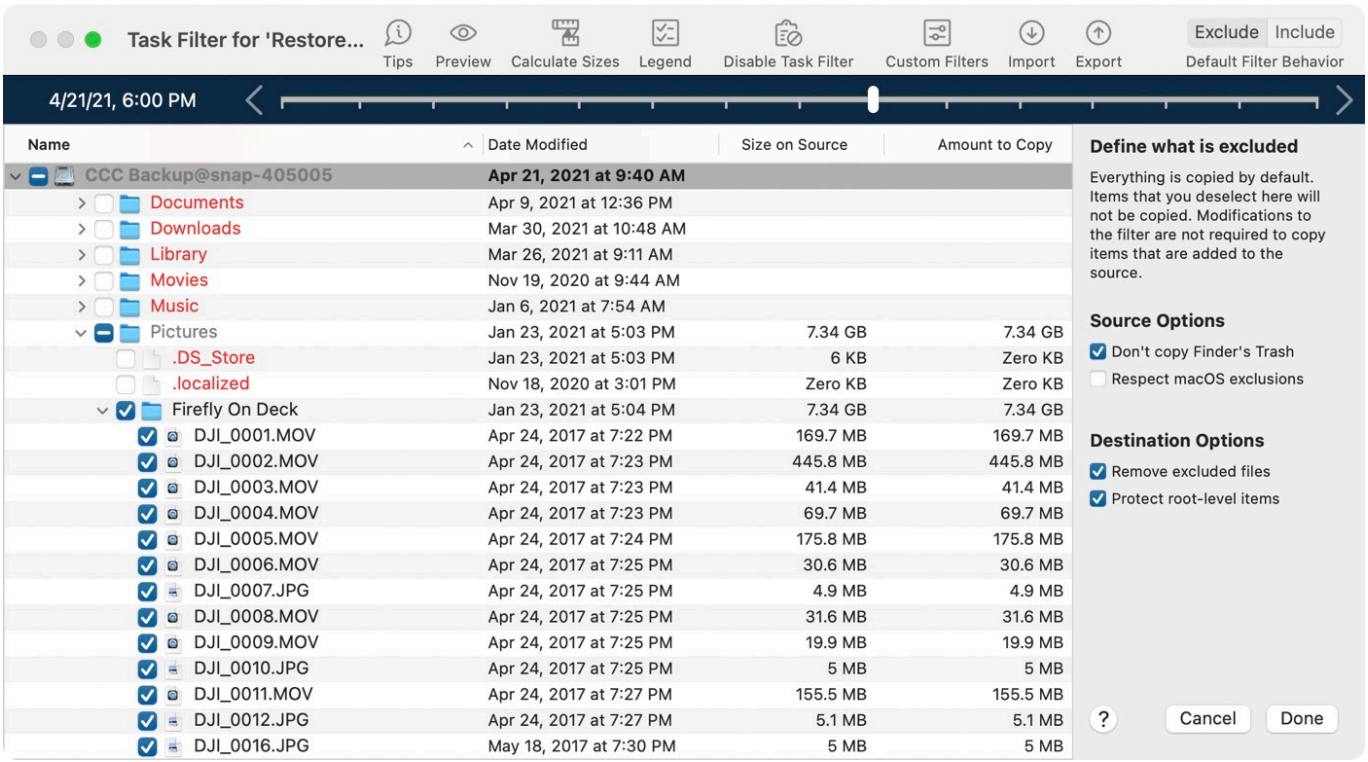


Related Documentation

- Monitoring backup tasks with the CCC Dashboard <https://bombich.com/kb/ccc6/monitoring-backup-tasks-ccc-menubar-application>

Snapshot Navigator: Easy way to explore older versions of files

Looking to restore a specific version of a file? CCC's Snapshot Navigator allows you to step through older versions of your backups and get a preview of your files as they were at specific points in time.

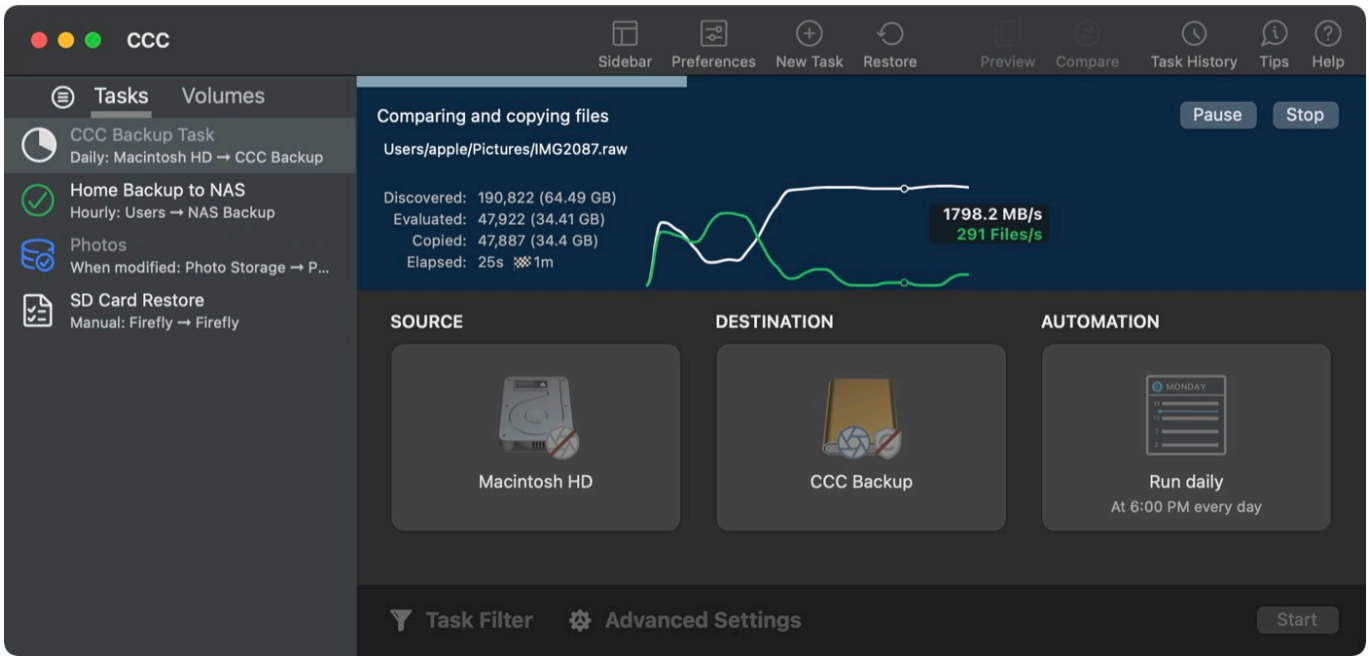


Related Documentation

- Restoring older versions of files using CCC's Snapshot Navigator <https://bombich.com/kb/ccc6/how-restore-from-your-backup#restore_snapshot>

Redesigned Interface with Dark Mode

CCC v6 includes a new, cleaner user interface. We reorganized the main window to make it smaller while making many of the controls and font sizes larger. We completely redesigned every window in CCC; revisited every button, every icon, and every color decision to offer a high quality Dark Mode experience. CCC now offers more detailed progress indication while a task is running, including a time remaining estimate. File processing and transfer rates are now charted live during backup tasks. Hover your mouse over the chart to view the current write rate (white) and files evaluated per second (green).



Quick Update: Leveraging FSEvents for super quick updates to the destination

Did you know that macOS keeps track of changes to folders? CCC 6's Quick Update taps into this service (called "FSEvents") and the result is lightning quick updates to your backups - no exhaustive scanning for changes required. When Quick Update is enabled for a task, CCC will ask the FSEvents service for a list of folders modified on the source since the last backup rather than scanning every folder for changes. The performance benefit of this feature are remarkable, we've seen up to 20X improvement to backup time, especially for tasks involving a destination network volume.

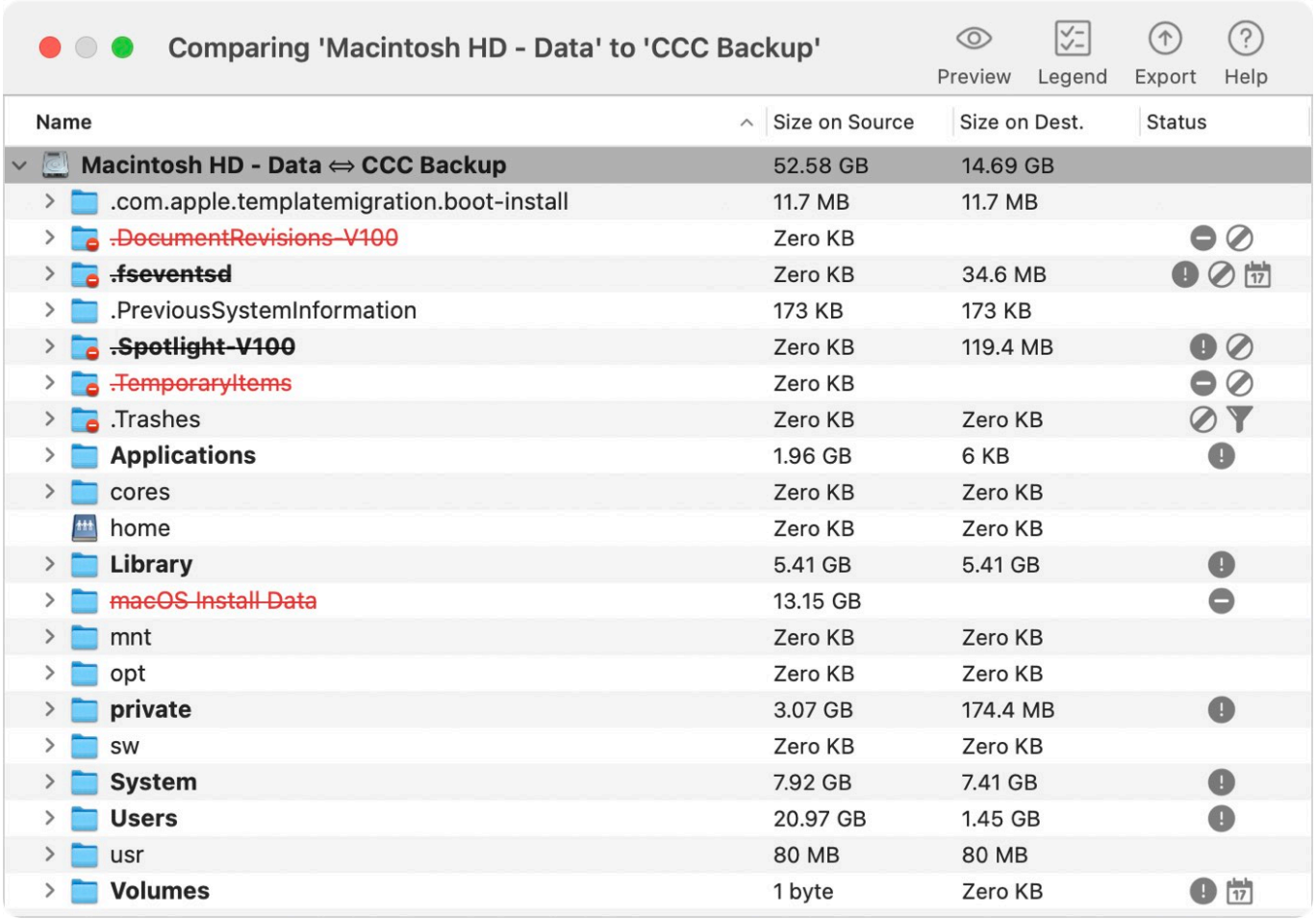
Related Documentation

- Use Quick Update when it's possible to collect a list of modified folders from macOS <https://bombich.com/kb/ccc6/advanced-settings#quickupdate>

Compare: Visual comparison of the source and destination

You've finished your backup but the source and the destination aren't exactly the same size; did CCC miss something? Probably not – the disk usage of your source and destination are usually different, but what are the specific differences?

CCC's Compare feature offers a visual comparison of your task's source and destination, and provides details if the differences are the result of a task filter. Use this feature to quickly determine if something is missing from the backup, or if folder size differences are simply the result of files sitting in the Trash.

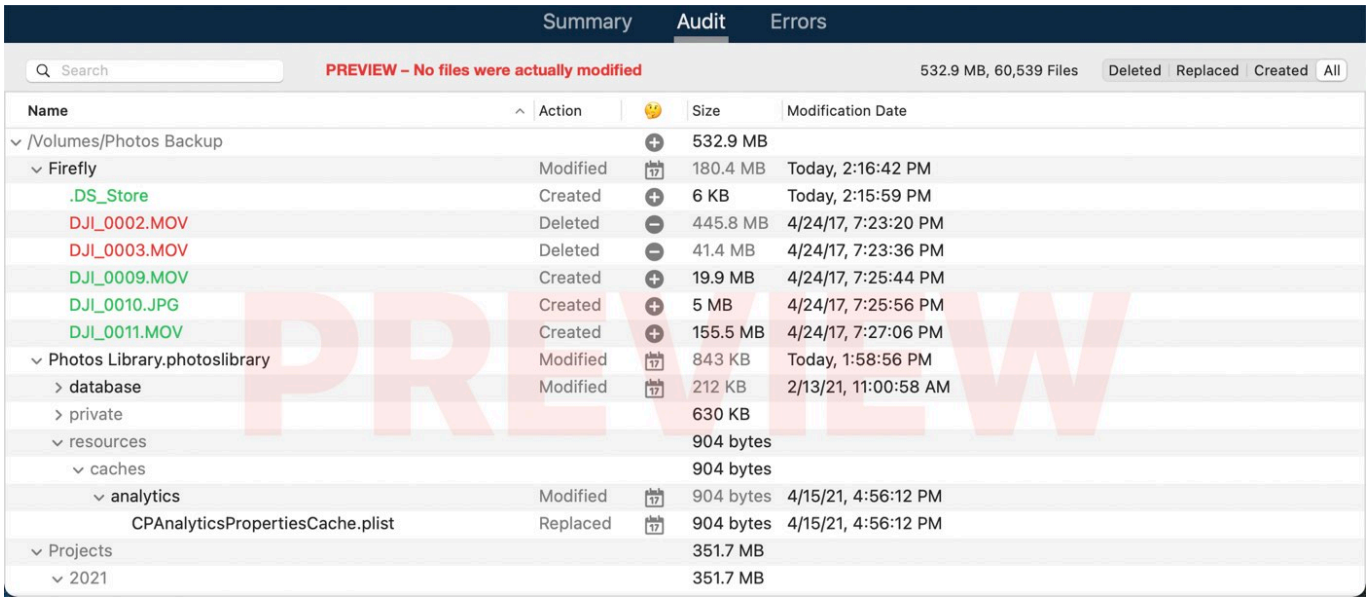


Related Documentation

- Comparing the source and destination <https://bombich.com/kb/ccc6/comparing-source-and-destination>

Task Preview: See what changes CCC is going to make before actually making them

If you've ever been nervous about what changes CCC may make on a destination volume, you can use the new Preview feature in CCC 6 to see what's going to happen before making the changes. This "Dry Run" is available via the Preview button in CCC's toolbar, and any time you save a task for which the SafetyNet feature has been disabled.

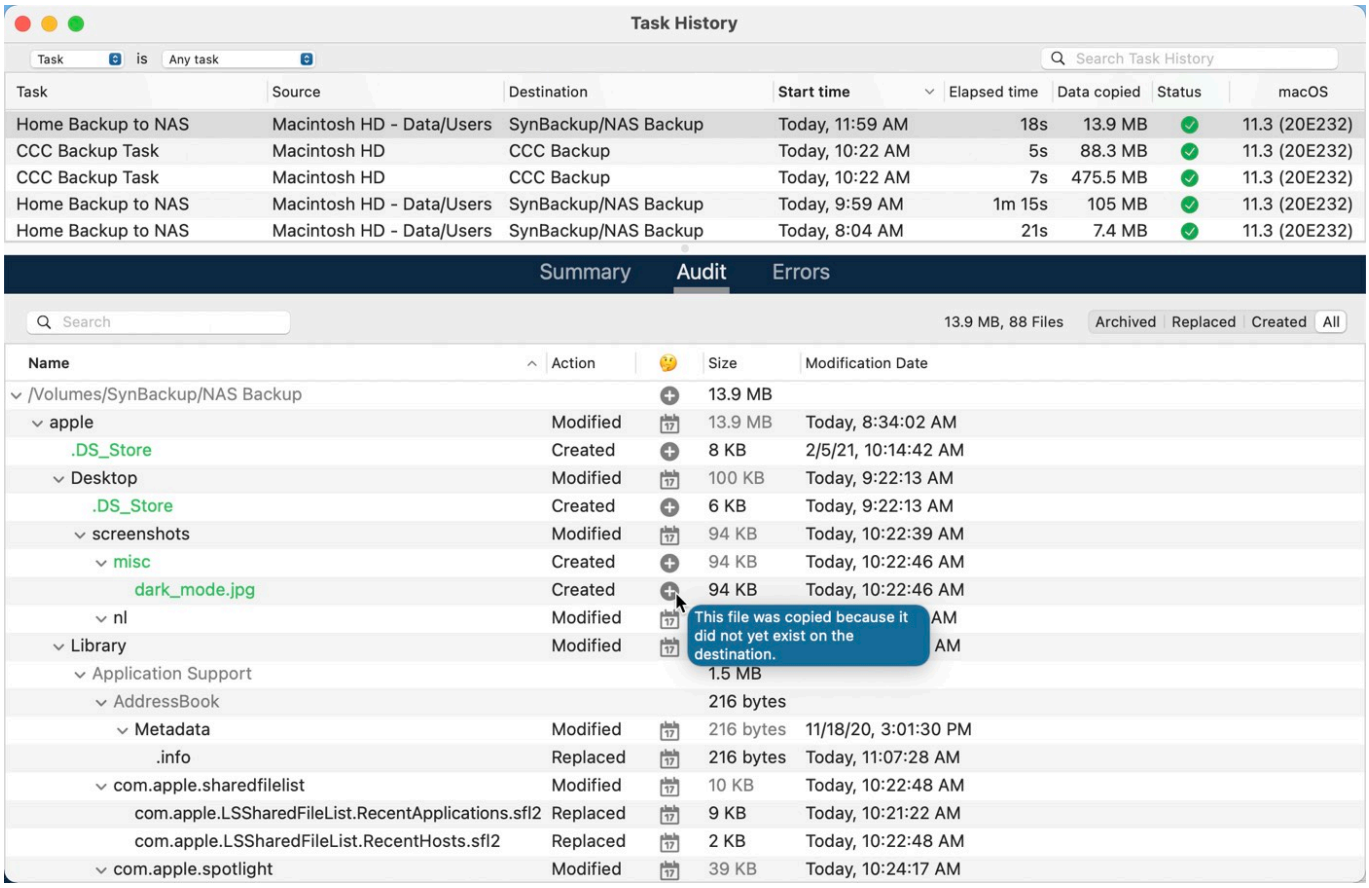


Related Documentation

- Preview: See what changes CCC will make to the destination <https://bombich.com/kb/ccc6/preview-see-what-changes-ccc-will-make-destination>

Backup Audit: Task History events include a list of transactions

What was copied, and why? You asked for this, and we're delivering it with style in CCC 6. When your tasks run, CCC will record detailed information about the transactions that occurred during the task, e.g. files copied, files updated, folders created or updated, files deleted or archived. You can view these backup audits in CCC's Task History window, and never again wonder why CCC copied a particular file.

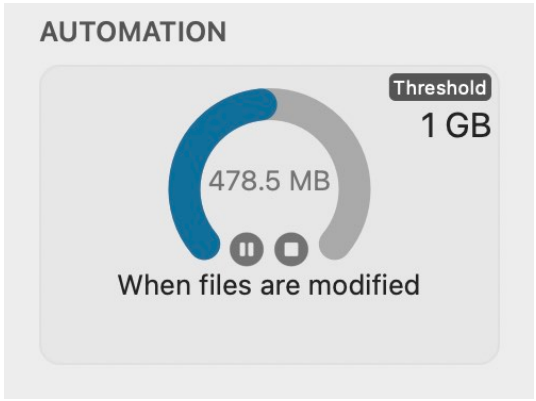


Related Documentation

- Transactions: Viewing details about the modifications made by the backup task <https://bombich.com/kb/ccc6/how-find-out-when-backup-last-ran-ccc-task-history#transactions>

New scheduling option: Run a backup task "When files are modified on the source"

Using the same underlying technology that’s used by the "Quick Update" feature, CCC 6 offers a new automation option that allows you to have a task run when a threshold of data changes have occurred at the source. So rather than hourly or daily, etc., the task will run after 5GB’s worth of data has changed (for example). You can throttle that with a time limit as well, e.g. don’t run the task more than once every 5 minutes.



Related Documentation

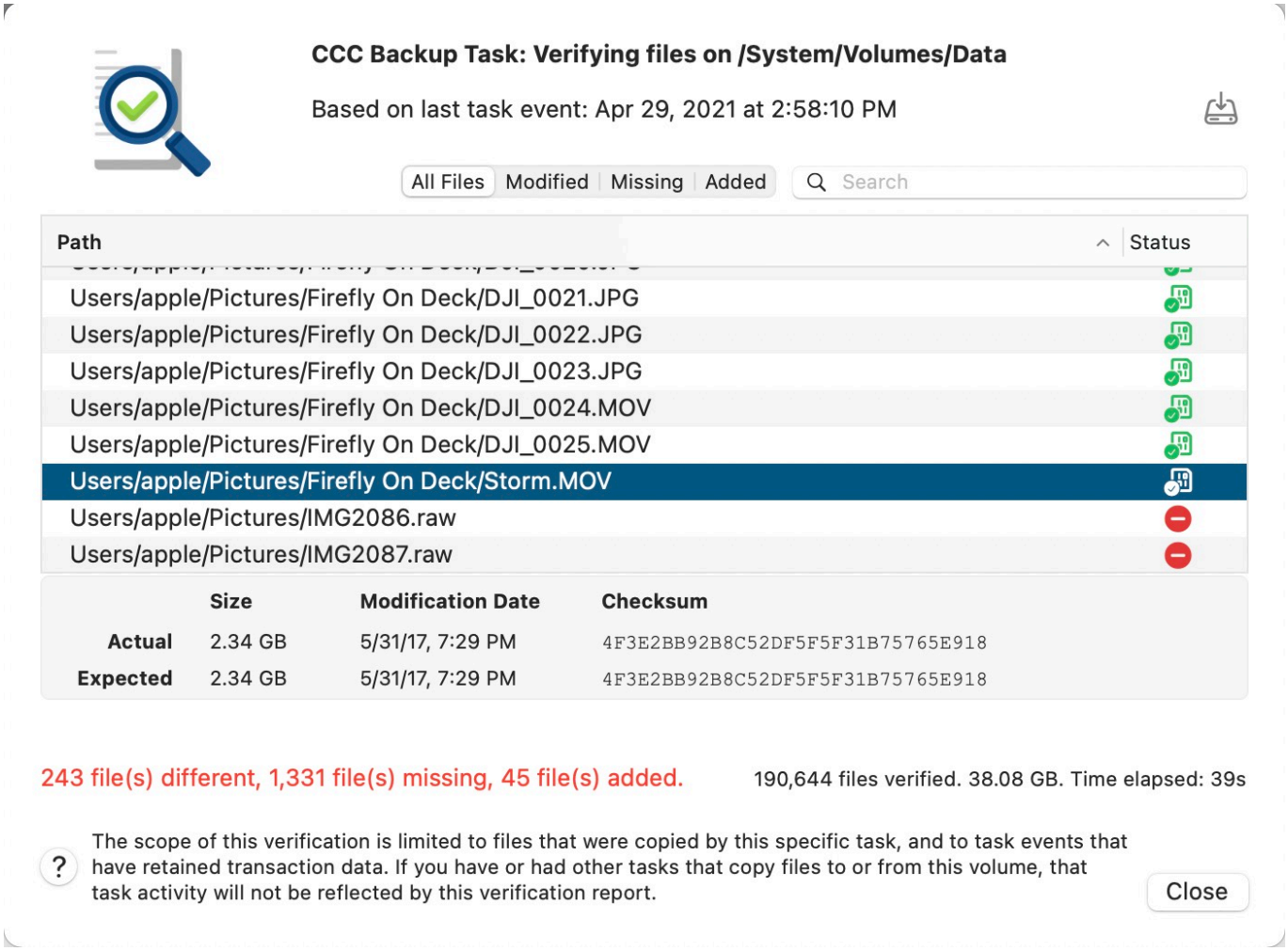
- Scheduling Option: When files are modified <https://bombich.com/kb/ccc6/advanced-scheduling-options#when_modified>

Advanced File verification

Previous versions of CCC have included the exhaustive "Find and replace corrupted files" option, but that option has a couple shortcomings that we wanted to resolve. CCC 6 can verify files at the end of the backup task, and also offers the opportunity to verify files on the source and destination, independently, against a hash that was recorded when the file was last copied.

Verifying the integrity of the source or destination

CCC 6 stores the modification date, size, and checksum of every file that was copied by a particular task. On demand, you can ask CCC to evaluate files on either the source or destination (independently of the other volume) against historical checksums. This gives you the opportunity to not only verify the integrity of the backup, but also to verify the integrity of the source.



Verification of files that were copied by the current task event

If you've ever migrated data to a new disk, you've probably wondered, "How do I know that all of the data was actually copied?" You may also not have realized that media sector failure is most often

discovered on read, not on write, which means that data corruption that occurs on the new disk isn't usually discovered until some time in the future when you try to re-read the files. This new Advanced Setting offers a new postflight task option to verify files that were written to the destination.

Related Documentation

- How to verify a backup <https://bombich.com/kb/ccc6/how-verify-or-test-your-backup>
- Re-verify the files that were copied <https://bombich.com/kb/ccc6/advanced-settings#reverify>

Other new features and improvements

Our to do list never ends, and we're constantly receiving great feedback from users on how we can improve CCC. Here are just a handful of simple improvements that we're excited to introduce in CCC v6:

- Per-task control over the file copier's CPU usage.
- You can temporarily pause a backup task.
- More information about your source and destination right at your fingertips – click on the source or destination selector to see extensive information about the selected volume.
- Refined Simple Mode – quitting and reopening CCC to switch modes is no longer necessary.
- Items that cause task errors can be excluded directly from the Task History Errors table.
- CCC's Task Filter now offers support for respecting macOS "backupd" exclusions (i.e. exclusions defined for Time Machine).

Upgrading from CCC 5

The upgrade path from CCC 5 to CCC 6 couldn't be simpler. Simply open CCC 6, and it will automatically update your CCC v5 tasks. If you kick the tires for 30 days and decide to stick with CCC 5, simply re-open CCC 5 and choose the option to downgrade. CCC 5 will then reload your original CCC v5 tasks and everything will be as it was prior to your trial of CCC v6.

Notable interface changes going from CCC v5 to v6

We use application usage metrics (see CCC's Settings > Updates for details) to determine which features of CCC get used most frequently, and which options perhaps no longer deserve the valuable real estate they've enjoyed in the past. Based on those data and user feedback, we make adjustments to the CCC user interface to make it easier to use and more approachable to new users. In CCC v6, we made the following notable adjustments:

- **File menu**: We renamed the File menu to "Task". We know this is a pretty radical idea for a macOS application, but "File" just isn't the right word. CCC is task-oriented, so we broke the mould and renamed this menu to Task.
- **SafetyNet**: The SafetyNet setting is now accessed via the Destination selector. Click on the Destination selector (i.e. the icon of your selected destination volume or folder) to access the SafetyNet options. Also note that a badge is applied to your destination icon to indicate the current SafetyNet behavior applied to that destination. When you hover your mouse over the badges a tooltip will provide a description.
- **"Copy all files"/"Copy some files" popup menu**: This popup menu is now obsolete. Click the Task Filter button at the bottom of the window to reveal your task's filter settings. If you want to retain a filter but not apply it to your task (comparable to the previous "Copy everything" setting), click the "Disable Task Filter" button in the toolbar of the Task Filter window.
- **Send Email**: Click the Advanced Settings button, then click on the Postflight tab to find this

setting.

- **Legacy bootable backups**: On macOS Big Sur (and later), CCC creates Standard Backups <https://bombich.com/kb/ccc6/cloning-macos-system-volumes-apple-software-restore#standard_backups> by default, it no longer attempts to back up Apple's proprietary System volume. You can still configure CCC to establish a bootable copy of the system, however we do not recommend making bootable copies of the system as part of a backup strategy <https://bombich.com/kb/ccc6/cloning-macos-system-volumes-apple-software-restore>. After selecting a source and destination, click on the Destination selector and choose **Legacy Bootable Copy Assistant** to configure CCC to create a bootable copy of macOS.

Related Resources

- Download CCC 6 <https://bombich.com/software/download_ccc.php?v=latest>
- Download CCC 5 <https://bombich.com/download#ccc5>

CCC 6 Release Notes

CCC 6.1.10

February 22, 2024

- Made an adjustment to the "Restore" button constraints in the Snapshots table to improve its appearance in some non-English locales. Separately, fixed an issue where this button would errantly appear on non-selected row views when scrolling.
- Fixed a layout issue in the "Grant Full Disk Access to CCC" window that was causing the French description to get cut off.
- Fixed an issue that was causing the volumes listed in the View menu to be disabled.
- Adjusted the logic for suspending deletions when a directory enumeration error is encountered during source discovery. We no longer suspend deletions when the error is specific to a DataVault (i.e. an Apple-proprietary and Apple-apps-only container).
- Fixed a condition that could lead to a "When files are modified on the source" task to repeat itself (too frequently) in cases where the task was failing in the source/destination readiness phase.
- Fixed an issue that could occasionally lead to unresponsiveness of the "Cancel" button that is presented when a CCC software update fails (e.g. because internet connectivity dropped).
- Fixed an issue where tasks that back up to or from a Remote Macintosh could go into a repeat run cycle if the remote Mac was reachable but not responsive. This appears to be restricted to cases where the remote Mac was behind a router that was responsive, but dropping traffic to the remote Mac.
- The Compare button is disabled/enabled more consistently when the source or destination is unmounted/mounted.

CCC 6.1.9

January 30, 2024

- Addressed a scenario where CCC's appearance (i.e. Light Mode vs. Dark Mode) would not track the system setting when configured to do so.
- Addressed two conditions that could lead to delays when opening CCC or connecting to its helper tool.
- Made an adjustment to how folder enumeration is approached on rotational destination volumes. This should result in fewer subtask hang events when enumerating high-file-count folders on these devices.
- Fixed an errant trial expiration issue that eventually affects Pro License users that are using a license sidecar file.
- Increased the timeout when creating or removing snapshots to accommodate slower backup devices.
- Worked around an esoteric FAT32 filesystem bug that was resulting in a file at the root level that could not be deleted.
- Implemented a more effective solution for retrieving folder lists for cloud-synced folders that were added via the web or via another Mac.
- Fixed a couple minor Voiceover issues relating to the volume attribute buttons that appear when a volume is selected in CCC's sidebar. These buttons reveal a popover, but Voiceover was failing to consistently read the content of those popovers. We also added a transparent dismissal button to that popover to make it more easily-dismissible via the Voiceover Control+Option+Space keystroke.

CCC 6.1.8

October 23, 2023

- Added a new "Cloud Storage" option to the Source selector that automates most of the steps involved in setting up a task to make a dedicated, local backup of cloud-only content <https://bombich.com/kb/ccc6/limitations-online-only-placeholder-files#temp_download_best_practice>.
- Fixed an issue in which CCC was failing to delete items that were locked on the destination.
- Addressed a performance issue in a preflight task that was leading to some errant reports that a subtask had timed out.
- Added longer timeouts when downloading really large cloud-only files.
- Fixed some minor cosmetic clipping issue (e.g. the weekday buttons in the Weekly box of the scheduler popover, the Start button in Simple Mode, and title of a volume presented in the Source/Destination contextual menus)
- The Trial window is no longer errantly presented in cases where a Pro License registration is applied via a sidecar file.
- The Quick Update Task Inactivity override threshold is now 28 days for NAS destinations (still 14 days for all other destinations).

CCC 6.1.7

September 5, 2023

This version of CCC adds official support for macOS 14 Sonoma. This update includes changes that affect all supported macOS versions, however, so we recommend this update for all CCC v6 users.

- Added support for temporarily downloading cloud-only files <https://bombich.com/kb/ccc6/limitations-online-only-placeholder-files#temp_download> from services like Dropbox, OneDrive and GoogleDrive (any cloud-backed service that uses Apple's FileProvider interface). This includes support for downloading cloud-only content from iCloud as well, with some minor caveats <https://bombich.com/kb/ccc6/limitations-online-only-placeholder-files#apple_dogfood> due to Apple's use of a proprietary, non-FileProvider cloud-syncing service (oh, the irony!). Click "Advanced Settings" at the bottom of the CCC window and select the "File Copying Settings" tab to find the new setting. Note that this setting is disabled by default and limited to Macs running macOS 12.5 or later. If you want CCC to temporarily download your cloud-only files to make a local backup, be sure to enable the new setting in Advanced Settings > File Copying Settings.
- In 6.1.6 we added a new setting to "Use the menu dialog for task restart/shutdown requests" (available in the CCC Dashboard application <https://bombich.com/kb/ccc6/monitoring-backup-tasks-ccc-menubar-application>). We enabled that setting by default, figuring it gives people a more graceful opportunity to cancel shutdown if they're in the middle of something, and no harm done if the user isn't at the system (the system performs the request after a 60-second countdown). But, apparently macOS doesn't present that dialog if the screen is locked, and doesn't perform the power management request either. The setting is still available, but now it will be disabled by default to restore the pre-6.1.6 behavior.
- Addressed an error that could occur when copying sparse files that have a negative physical file size (which is corruption of the file's filesystem entry on the source).
- Addressed a small issue affecting Quick Update tasks where some folders would errantly appear as "modified" in the Task Audit despite that they were not actually modified.
- Fixed a logic issue that was preventing the "Manage snapshots on 'Macintosh HD'" option from being presented for the startup disk (i.e. because the System volume is typically not

mounted).
- Fixed an issue in which CCC would repeatedly (and unnecessarily) prompt for NAS credentials in cases where the username or host name contained a space character.
- The dynamic performance chart is now stopped when a task is paused, and resumed when the task is resumed.
- Fixed a false-positive stall report that can occur at the end of a task that is recording millions of transactions.

CCC 6.1.6

May 23, 2023

- Now that Ventura adoption rate among CCC users is >60%, we changed all "Preferences" references to "Settings".
- Addressed a crasher that only occurs on older Macs that are running Monterey or Ventura via the "Open Core Legacy Patcher".
- Fixed a logic issue that might cause CCC to ask for NAS volume credentials when it already has them.
- Improved the experience when using the snapshot navigator with a folder selected. Previously the scroll view was scrolling back to the top, now the folder will remain selected, and the view will be scrolled to reveal as much of the folder's content as possible.
- Addressed a collection of spurious errors that would occur when restoring to the startup disk. Also resolved an issue in which iCloud might require you to log in again after restoring to the current startup disk.
- Added an option to the CCC Dashboard to use the Apple menu shutdown/restart dialog when a task makes a postflight restart/shutdown request. This gives a heads up to the action and an opportunity to cancel it. This is enabled by default and configurable in the Task tab settings.
- Fixed the color of task event status icons in the Task History window when using Dark Mode.
- Addressed a condition where CCC was throwing in the towel a bit early when the destination was running low on free space.
- Added a new "Descend into bundles" attribute for custom filter rules.

CCC 6.1.5

March 14, 2023

- When applicable, more context is presented now in cases where a task fails due to a stall at the source or destination (e.g. what specific file or folder is involved in the stall).
- At the end of a task event, CCC now sets the destination root modification date to "now", rather than preserving the source root folder modification date. The modification date of the destination root folder has more value as an indication of when CCC last made changes to the destination vs. when the user last made changes to that root folder on the source (which is typically long ago). This should offer an easy indication to the end user of "When was the last CCC backup made to this volume?".
- Errors that occur due to a disagreement between the source and (typically NAS) destination filesystems on how composed characters should be stored are now presented with more specific advice and a link to a new Kbase article <https://bombich.com/kb/ccc6/character-composition-conflicts-on-nas-volumes>.
- Network change events are now listed in the Activity tab of the CCC Dashboard application if any CCC tasks require network resources.
- Made some adjustments to the pruning of CCC's Task History database so it consumes less space.
- Fixed the behavior of the Task Filter window when working with a Remote Macintosh source.

- CCC will now run the postflight shell script (if specified on a task) in cases where the source or destination dropped offline, thus causing the task to abort. Previously we were avoiding running the script in this case (despite running that script in other error conditions), but we've since decided that there isn't any good reason for not running it.
- Made a small logic adjustment for tasks configured to run "When the source or destination is remounted" to avoid running when a staged System update is mounted (i.e. when the startup disk is the source).
- Adjusted the sidebar width when exiting full screen mode.
- Fixed a layout issue in the task plan when hiding and then revealing the sidebar (specific to Ventura).
- When a task fails because the source or destination is missing, and the user has enabled the "Don't send error notifications" (when the source or destination is missing) setting, the error will now be presented with the "cancelled by the user" icon in the Task History window, rather than an error icon.
- Fixed an issue in which a "Backup Health Check" would errantly (but harmlessly) recopy a certain class of files that did not need to be recopied.

CCC 6.1.4

November 29, 2022

- CCC will now preserve the space savings of pure "cloned" files (duplicated via the clonefile() function, e.g. duplicated in the Finder) when copying from an APFS volume to another APFS volume.
- CCC will now preserve the "Date Added" attribute on files and folders on filesystems that support that attribute.
- CCC will no longer raise concerns about dropped cloud-only placeholder files. With a minor adjustment and some additional testing of several scenarios, we have determined that there is no longer a restore concern related to dropping these placeholder files. If you previously excluded the CloudStorage folder from your backup, you may remove that exclusion. You're also welcome to leave the exclusion in place. In our tests, the cloud service providers populated the absent content just fine.
- Errors related to minor filesystem corruption in /Users/username/Library/Biome on macOS Ventura are now suppressed.
- Improved the handling of errors when free space is depleted on the destination volume.
- The "Only on the next run" and "Once a quarter" options are no longer hidden in the frequency popup menu adjacent to the "Find and replace corrupted files" setting. Same deal for the "Archives that are older than" option in the SafetyNet pruning limit popup menu in Advanced Settings > Preflight.
- The "Command+R" keyboard shortcut for starting a task now also works for starting a task group.
- Fixed an issue in which the throttling mechanism applied to "When the source or destination is reconnected" tasks was not getting applied consistently.
- Fixed an edge case in Ventura where the "Legacy Bootable Copy" method would fail with a "destination is full" error in cases where the destination was a disk image and the source was a clean install of macOS Ventura.
- Added a Ventura download link to the macOSInstaller Media Assistant.
- Added a global exclusion for a "@Recently-snapshot" folder that appears on some NAS devices. Copying each snapshot within this folder will typically overrun the capacity of the destination.
- Fixed preflight mounting and ownership enabling on Remote Mac destination volumes on Ventura+ Macs.
- When CCC is configured to copy files from a volume that lacks support for file ownership (e.g. a NAS volume, or any volume with ownership disabled), ownership of files copied to the destination (when applicable) is set to the user account that configured the CCC task. This

update fixes an issue in which numeric user account IDs larger than 32768 were getting improperly applied. This is not a common scenario; typically user account IDs start from 501, but in some corporate environments they can be much larger.

CCC 6.1.3

September 19, 2022

This version of CCC adds official support for macOS 13 Ventura. This update includes changes that affect all supported macOS versions, however, so we recommend this update for all CCC v6 users.

- The "System exclusion" is no longer applied in cases where the destination is a subfolder on the startup disk.
- Fixed an issue in which "on reconnect" tasks were not correctly getting throttled according to the task configuration if the task was also configured to prompt the user to proceed when the missing volume was reconnected.
- The Compare window now shows files discovered on the source and destination separately. Especially for really slow destinations like NAS volumes, this will give a clearer indication of ongoing progress.
- The clonefile replacement procedure <https://bombich.com/kb/ccc6/performance-suggestions#clonefile> will no longer be used if snapshots are disabled on the destination. The primary purpose of using that procedure is to use storage more efficiently so that we can retain more snapshots, and that's moot if we're not retaining snapshots.
- When you auto-fill a password in CCC's Email Settings (i.e. from the system's "Passwords..." menu option that appears when the password text field is given focus), that password is now correctly stored in CCC's keychain.
- Task groups can now be deleted via the Task menu (e.g. Command+Delete) and via the "Additional Actions" menu in the sidebar.
- Resolved an issue in which a task would appear stalled when converting a disk image to a read-only format. Fixed an unrelated progress indication issue in the same scenario.
- Automated tasks will now be skipped any time a restore task is running to remove any possible conflict between a restore task and a backup task. Users are welcome to run backup tasks manually while a restore task is running, this change only affects automated tasks.
- Fixed the presentation of a snapshot creation failure in cases where the destination is in the midst of encryption conversion.
- The minimum time threshold for "When files are modified on the source" tasks is now 1 minute, but the default is now 5 minutes. The minimum data threshold is now 0; when set to 0, CCC will start an event when changes have been made to a file on the source (and the time threshold is met).
- The CCC Dashboard will now proactively open CCC if CCC's helper tool lacks Full Disk Access. Likewise, the Dashboard will open CCC if corruption in CCC's task database has been detected.
- CCC now applies a two-week sanity limit on the Quick Update feature. We were finding some cases where macOS managed to have retained multiple weeks of FSEvent records, and it was taking longer to slog through all of those records than it would take to simply re-enumerate the source and destination. So if a Quick Update task hasn't run successfully in the last two weeks, it will now proceed with a full audit of the source and destination.
- Added a new "Settings" column to the task events table in the Task History window that will indicate when the "Quick Update" or "Backup Health Check" settings were applied to a given task event. This column is hidden by default; right-click on the table header row to choose which columns should be visible.
- **Ventura**: Modified the steps for granting Full Disk Access. It's now one step! That's right, just one step! Just start dragging the CCC Privacy Fish and CCC will pull some strings in the background to magically make the full disk access table appear for the drop.

- **Ventura**: Fixed the filesystem identity of ExFAT and FAT32 volumes in the disk chart (i.e. when you click on the Source or Destination selector, or select a volume in CCC's sidebar).
- **Ventura**: Adopted a new macOS procedure for adding the CCC Dashboard login item.
- **Ventura**: Adjusted how connections to a remote Mac are initiated from a Ventura client to accommodate changes to the scp utility that are specific to macOS Ventura.
- **Mostly Ventura**: Fixed a memory access issue that occurs (with more frequency on Ventura) in the SQLite encryption library that CCC has been using to encrypt task audit and task history databases. After applying this update, CCC will temporarily decrypt the task audit and task history databases, then re-encrypt them with a replacement encryption library. In the unlikely event that an exception occurs while decrypting one of these databases, the affected database will simply be recreated. This change has no effect on task configurations, which are stored in a separate, non-encrypted database, and no effect on any of your data on your backup disk.

CCC 6.1.2

May 23, 2022

- Fixed an issue in which CCC's CloneKitService could report an exception when an edge-case error condition was encountered while reading or writing a file.
- Snapshot thinning on the source and snapshot/archive thinning on the destination is now skipped for restore tasks.
- Fixed a cosmetic issue in the snapshot navigator when a subfolder is selected as the source.
- Made a few small adjustments to how task configuration is handled when selecting the current startup disk as the destination (e.g. to a restore task).
- Addressed an issue that could cause CCC to errantly report that multiple volumes were present with the same unique identifier.
- Fixed the window location of the Dashboard window when multiple screens are present. The Dashboard window will now be presented next to the menubar icon that was clicked, rather than retaining its previous window position.
- The minimum data threshold for "When files are modified on the source" tasks is now 1MB (i.e. 0.001GB).
- Addressed an issue specific to macOS Catalina in which a verification of files on the source or destination would errantly report System volume files as missing.
- Resolved a latency issue that a handful of users were noticing when switching between tasks. We tracked the latency down to poor performance of Apple's "nsattributedstringagent" service on macOS Monterey. In some cases the service was crashing repeatedly, and when macOS throttled its relaunch, there would be a noticeable delay when CCC attempted to render the Task Plan. We no longer rely on that macOS service for rendering the Task Plan.
- Fixed a couple cases where the background color of a view was not switching automatically when the system appearance was changed in System Preferences (e.g. Dark to Light).
- Corrected the error handling in cases where unreadable folders are encountered on the source.
- Corrected the presentation of dropped OneDrive placeholder files for pre-Monterey users.
- Addressed a race condition that could occur if two tasks try to simultaneously mount the same NAS volume. One task would "win", the other task would wait indefinitely for the system's NetAuthSysAgent service to reply.

CCC 6.1.1

March 23, 2022

- Fixed an exception that was causing tasks to fail with no clear reason when a task was configured with a remote Mac source or destination, and the specification for that remote

Mac was missing a "volume name" attribute.
- macOS 12.3 introduced a problem that causes Legacy Bootable Copies of the system to fail on Apple Silicon Macs. In earlier beta builds of 12.3, that failure rendered the destination unmountable. In the final release of 12.3, that failure is now innocuous. CCC now ignores the error and completes the task. Please note that we still recommend using this procedure only when making a copy of the system that you intend to use immediately <https://bombich.com/kb/ccc6/cloning-macos-system-volumes-apple-software-restore> (e.g. when migrating to a new disk, or setting up a sandbox test system). A CCC "Standard Backup" provides a more comprehensive strategy for regularly-updated backups.
- Fixed a cosmetic accounting issue that was making it look like more files were re-verified than were copied. Also fixed an errant subtask timeout that was occurring during postflight verification.

CCC 6.1

February 23, 2022

- Fixed an issue in which CCC was unable to create files and folders in some OneDrive-related folders on the destination.
- Added an option to reveal the Advanced Settings persistently in the main window.
- Added a contextual menu to the CCC menubar icon for "quick access" functions (e.g. open CCC, run a task, quit the Dashboard). Right-click on the CCC menubar icon to access this menu.
- Added navigation buttons to the CCC toolbar to make it easier to get back to a task after making volume configuration changes (e.g. when adjusting snapshot settings).
- Added an option for a light background for the sidebar (i.e. in Light Mode).
- Added settings to choose a specific appearance (i.e. light or dark, independent of the system setting).
- The Source and Destination selectors are now enabled while a task is running. You can click on these to see details about the source and destination (e.g. disk usage, free space) as the task progresses.
- Task History events now show information about how many files and how much data was removed from the destination (in addition to how many files and how much data was copied to the destination).
- Every Mac that is supported by macOS Catalina has native USB 3.0 support, so now CCC's Copy Coach proactively warns when a source or destination is connected via USB 2.0 (e.g. due to using an old USB hub or non-USB 3.0 compliant cable).
- The Dashboard now shows both "last run time" and "next scheduled run time" for each task. Previously this was an option, but presenting both at the same time seems to be what most people are looking for.
- Enhanced the search feature in the CCC Documentation window to offer an option to search the current page for matching text, or to execute a search of the entire CCC Kbase.
- Task groups can now be specified via the "Run another task" option in Advanced Settings > Postflight.
- Fixed a minor apparent discrepancy when using the "Verify files copied by this task" feature on a NAS volume. Previously this would show size-based differences due to the absence of extended attributes despite that those were deliberately not copied.
- Audit records can now be exported to a CSV file.
- Added a "Copy Link" option to the Tasks contextual menu. These links will open CCC and select the applicable task. These can be useful alongside other Mac automation.
- Fixed a couple conditions where CCC would report an error and fail to create a symlink becase a folder with the same name already existed on the destination. Fixed a similar issue where CCC was unable to create new folder on the destination because a file (often a symlink) with the same name already existed.
- Fixed a mouse tracking issue in the CCC Dashboard "mini progress" window that could make

it impossible to click on the pause/stop buttons.
- The CCC Dashboard window size and placement is now retained across launches.
- Made a handful of adjustments to how older versions of files are presented in the Snapshot Comparison Browser. Checksums are now calculated on-the-fly for any files smaller than 2MB.
- The System exclusion limit is no longer applied to a subfolder destination when the source OS is Big Sur or later.
- Made some adjustments that should improve performance when using an ExFAT or NTFS volume as a source or destination.
- Made some modest improvements to the "time remaining" estimate. This estimate will now include componesation for time that that will be required for re-verifying files that were copied (if specified for the task).

CCC 6.0.5

November 11, 2021

- We added a new "macOS Downgrade Assistant" feature, accessible via CCC's Utilities menu. The Downgrade Assistant can assess a backup volume's compatibility with Migration Assistant, and will create macOS Installer media using a specified volume and installer application.
- We added another small new feature in the source and destination selectors. If the selected source or destination is a network volume, or a folder on a network volume, you can hold down the Option key to reveal a "Switch to AFP" or "Switch to SMB" menu item in the Source and Destination selectors. We frequently see slow performance and errors from SMB-mounted volumes, and we often recommend that people try "the other" protocol when the current protocol isn't working out. Now we've made it really simple to switch between the two to see if using a different protocol will yield better results.
- Tasks in the sidebar can once again be arranged when the sidebar sorting is configured as "Manual".
- Made some adjustments that should improve performance when a task is writing large files to a rotational destination. Made a separate adjustment that should improve performance when writing to ExFAT-formatted volumes.
- Fixed a display issue in the Legacy Bootable Backup Assistant that would occur when selecting a SoftRAID destination volume.
- Fixed an issue that arose recently in macOS Monterey that was causing failures while trying to configure new Remote Macintosh tasks.
- Fixed an issue affecting tasks configured to run "When the source or destination is remounted" in which the tasks would fail to run on volume appearance if the destination's System volume had been removed.

CCC 6.0.4

October 20, 2021

This version of CCC adds official support for macOS 12 Monterey

This update includes a handful of changes that are applicable to Catalina and Big Sur users too:

- The expansion state of the last task group in the sidebar is now properly retained across launches.
- The order of tasks within a task group as shown in the sidebar now tracks the run order defined in the "Upcoming Group and Task Events" table when the sidebar is configured for manual sort ordering. Likewise, tasks within a group cannot be sorted manually *in the*

sidebar when the sidebar is configured for manual sorting. Order the tasks within the "Upcoming Group and Task Events" table to set that custom order.
- Improved the handling of some failure cases when copying the Catalina System volume, e.g. when the destination volume drops offline, or when the destination Data volume can't be unmounted.
- Fixed an issue in which CCC would fail to mount the destination Data volume in cases where the destination System volume had been removed.
- CCC will no longer remove the System volume from an encrypted destination volume after an OS upgrade. We can't update that System volume, so it becomes essentially useless, but removing it exposes a bug in Disk Utility in which it's unable to unlock the volume. Also fixed an issue in which CCC was failing to unlock those orphaned Data volumes.
- Fixed a couple issues that were causing exceptions.

CCC 6.0.3

September 14, 2021

- Fixed an issue in which CCC was unable to replace a folder on the destination with a symbolic link (i.e. because a folder on the source had been replaced by a symbolic link). This issue primarily affected macOS Catalina users, but could also affect Big Sur users for tasks that used the "Don't delete anything" SafetyNet setting.
- Improved the handling of cases where a source NAS presents a symlink as an ordinary file. Fixed an accounting issue that led to unusually high "data copied" values in those cases.
- Resolved a condition in which the "Maintain a record of transactions" checkbox became practically uncheck-able in CCC 6.0.2.
- Fixed a permissions issue that can cause applications to not work correctly when restored from a volume whose ownership is disabled.
- Relative date references (e.g. "Today", "Yesterday") in the Task Plan and Task History window are now correctly updated when a date change event occurs (i.e. at midnight).
- SafetyNet pruning settings are now consistently visible when the destination is HFS+ formatted.
- Errors that occur due to the OneDrive service's interference with CCC archiving activity on the destination are now suppressed. These typically go away on their own without intervention.
- Fixed a logic issue that caused the "Never show this dialog" setting to be ignored for the "Remove task audit" dialog.
- Fixed the "Bring all to front" menu item in the Window menu.
- Improved the handling of manual sort order changes of the Tasks list.
- The CCC Dashboard window position is now retained when it's closed and later reopened.
- Fixed an issue in which CCC would not remove additional snapshots from the destination when free space was exhausted in the middle of a backup task (specific to cases where SafetyNet was disabled).
- Fixed an issue that could cause slow performance during postflight re-verification of files copied by the current task in cases where the task was also configured to use the "Find and replace corrupted files" setting.
- CCC will no longer create a snapshot on the source when the source and destination are folders on the same APFS volume. Instead CCC will use the APFS clonefile() function to make clones of files in these cases.
- Resolved a case where CCC was stripping the destination volume's custom icon in a folder-to-volume task configuration.
- The search field in the Task History window Audit tab now yields results that match folder names as well as file names.
- Added a new "Last Successful Run" token for the email notification template.
- Added a Start button to the "Upcoming Group and Task Events" view for task groups.
- **Monterey**: Updated how APFS volume disk usage is calculated on macOS Monterey.

- **Monterey**: Fixed a rendering issue for the Task Plan text on macOS Monterey.
- Eliminated some spurious "updated attributes" transactions that were getting created when backing up to a NAS volume.
- Resolved a conflict between the "Remove excluded items" setting and custom protection rules. Custom protection rules now have precedence over the "Remove excluded items" setting.

CCC 6.0.2

June 30, 2021

- By default, CCC will process up to four folders simultaneously and copy up to eight files simultaneously. This update reduces simultaneous folder handling to two if CCC cannot verify that both the source and destination are Solid State devices. We have also exposed a setting that allows the user to adjust this value manually in Advanced Settings > Performance & Analysis, including an option that configures the task to use the CCC v5 legacy file copier instead of the new file copier.
- Addressed a case where CCC would abort the backup task, indicating that a subtask had timed out, in cases where the destination was particularly slow to deliver information about a folder that had an exceptionally high file count (e.g. tens of thousands, or millions).
- Fixed a math issue that was previously causing inflight snapshot or SafetyNet archive removal to not remove enough snapshots or archives in cases where the destination was very full.
- Fixed a scheduling issue that was causing "When files are modified on the source" tasks to not resume monitoring when the task was back within a user-specified time limit.
- "Next run date" in the CCC Dashboard now correctly rolls over from "tomorrow" to "today" when the date changes.
- Addressed a handful of crashers and exceptions.
- When thinning snapshots, CCC now indicates the name of the snapshot using the user's preferred date format.
- The "Files evaluated" statistic is now updated appropriately during a Preview run.
- File and folder name changes that only affect the case of characters in the string are now detected (i.e. when that is the only change to the source file) and applied to the destination.
- CCC will no longer preserve system-immutable file flags when restoring items to the startup disk. This was leading to the creation of a folder (typically "Users") that couldn't be removed by the Finder.
- CCC now properly imposes a High Sierra+ requirement for the Remote Macintosh feature.
- Fixed the tooltip on the Source selector when a Big Sur startup volume is selected. Technically that volume is not mounted, but pointing this out is not really necessary.
- Added color pickers for the lines on the Dynamic Performance Chart.
- Improved the handling of moved folders in the Quick Update feature. Technically these don't cause modifications to files, but nonetheless we should apply these changes when the task runs.
- Fixed an errant case-conflict error that can occur on Case Sensitive APFS destination volumes when a folder name has a non-normalized Unicode character.
- Corrected the behavior of the "Remove excluded files" setting in the Task Filter window. Folders were only getting removed when explicitly excluded via a custom rule (not when unchecked in the main table), and files that were only implicitly excluded (i.e. via the default filter behavior) were getting removed. While that matched CCC v5 behavior, it was not the more conservative result that we were aiming for.
- When creating a read-only disk image, CCC now uses sparsebundle as the default format for the intermediate read-write disk image. Big Sur, in particular, seems reluctant to create sparseimage files, especially on NAS volumes.
- Fixed a timing issue that led to errors when running a "When files are changed on the source" task soon after startup.

- Addressed an edge case in which a source NAS device may lie about the nature of a symlink (i.e. initially the NAS reports that it is a regular file), leading to errors.
- Corrected the presentation of the startup disk's custom Snapshot Retention Policy.

CCC 6.0.1

May 26, 2021

- Fixed a handful of crashers, and some cases where a task would fail, indicating an exception had occurred in the CloneKitService.
- CCC no longer removes the "has a custom icon" bit from the destination volume's root folder, causing the Finder to not show the icon.
- Clicking the "X" widget to dismiss a CCC notification in Notification Center will no longer activate CCC.
- Files that fail postflight verification are now automatically tossed onto CCC's "try it again at the end of the task" queue for a second chance. If the secondary copy and verify fails, then we report the error.
- Fixed an issue in which a task that was configured to create a bootable backup would fail, indicating that the destination volume was read-only.
- Improved the handling of low-space conditions in cases where SafetyNet or snapshots are enabled on the destination.
- Addressed a memory leak that led to task failure while handling sparse files on APFS volumes (e.g. Dropbox online-only placeholder files were a big driver of this one).
- Addressed a handful of cases where a task would errantly report a "subtask timeout" while working through folders with very large numbers of files (e.g. 150K), despite no actual stall occurring.
- When copying content from a volume that has ownership disabled (especially NAS volumes), the ownership of the items on the destination is now set to the user that created the CCC backup task.
- Addressed an edge case in which CCC would miss some folders when copying from an APFS volume to a non-APFS volume (typically when an iTunes Music folder had a non-ASCII character in its name). Note that if you have a Quick Update task that matches this configuration, CCC 6.0.1 will automatically perform a "standard copy" audit of the destination during the next task event.
- Improved the performance of the dynamic performance chart when moving the CCC window from a retina to non-retina display.
- The End User License Agreement, and the preflight and postflight script names now appear correctly in Dark Mode.
- Addressed a performance issue that led to a "subtask timeout" at the end of a task that was using the "Reverify files copied by this task" setting.
- Fixed a loop condition that can occur if a destination NAS volume drops offline in the middle of a task and CCC lacks the credentials to remount that volume.

CCC 6.0

May 18, 2021

- New file copier that offers faster performance and powers several of the new features noted below.
- Compare: Offers a visual comparison of your task's source and destination, and provides details if the differences are the result of a task filter.
- The new Dashboard offers one-click access to starting, stopping and monitoring your CCC tasks, plus details about recent task activity. The Dashboard also gives you a heads up to snapshot disk usage on the startup disk.

- Postflight verification of files that were copied by the current backup task.
- Ad hoc verification of files that were copied by the current task — source or destination.
- The Snapshot Navigator allows you to step through older versions of your backups and get a preview of your files as they were at specific points in time.
- Quick Update decreases the length of the backup by comparing a reduced list of folders provided by the macOS FSEvents service.
- New scheduling option to run a task when a threshold of modifications have been made on the source.
- Backup audit shows what was copied by your backup tasks, and why.
- Dark Mode support.
- Task Preview: See what changes CCC is going to make before actually making them.
- Per-task control over the file copier's CPU usage.
- You can temporarily pause a backup task.
- A new, cleaner user interface. We reorganized the main window to make it smaller while making many of the controls and font sizes larger.
- Refined Simple Mode – quitting and reopening CCC to switch modes is no longer necessary.
- More detailed progress indication while a task is running, including a time remaining estimate.
- File processing and transfer rates are now charted live during backup tasks.
- Items that cause task errors can be excluded directly from the Task History Errors table.
- CCC's Task Filter now offers support for respecting macOS "backupd" exclusions (i.e. exclusions defined for Time Machine).

Carbon Copy Cloner 5.1.22

October 16, 2020 [macOS Big Sur qualification]

Carbon Copy Cloner 5.1.10

August 20, 2019 [macOS Catalina qualification]

Carbon Copy Cloner 5.1.5

September 17, 2018 [macOS Mojave qualification]

Carbon Copy Cloner 5.1

April 24, 2018

Carbon Copy Cloner 5.0

August 24, 2017 [macOS High Sierra qualification]

Carbon Copy Cloner 4.1.10

September 16, 2016 [macOS Sierra qualification]

Carbon Copy Cloner 4.1.4

September 1, 2015 [OS X El Capitan qualification]

Carbon Copy Cloner 4.0

October 1, 2014 [Mac OS X Yosemite qualification]

Carbon Copy Cloner 3.5.3

October 22, 2013

Carbon Copy Cloner 3.5

July 20, 2012

Carbon Copy Cloner 3.4

July 20, 2011

Carbon Copy Cloner 3.3

September 21, 2009

Carbon Copy Cloner 3.2

March 18, 2009

Carbon Copy Cloner 3.1

March 24, 2008

Carbon Copy Cloner 3.0

September 18, 2007

Carbon Copy Cloner 2.3

October 23, 2003

Carbon Copy Cloner 2.0

November 19, 2002

Carbon Copy Cloner 1.0

January 18, 2002

macOS Ventura Known Issues

Apple published macOS Ventura in November 2022. CCC 6.1.3 (and later), published in September 2022, is fully compatible with macOS Ventura. We cite known problems that Apple introduced in the new OS below.

Some backup volumes don't appear in the Finder (sidebar, nor Desktop, nor Computer)

If you created a bootable copy of Catalina, Big Sur, or Monterey in the past, and then proceed with CCC backups to that volume on Ventura without specifically using the Legacy Bootable Copy Assistant <https://bombich.com/kb/ccc6/cloning-macos-system-volumes-apple-software-restore>, CCC will remove the incompatible System volume from the destination. Prior to Ventura, the remaining Data volume would appear just fine on the Finder Desktop, and also in the volume list when you select "Computer" from the Finder's Go menu, but not in the sidebar. In Ventura, this volume no longer appears in any of these locations, regardless of your Finder preferences to show external volumes in the sidebar, and regardless of any attempts to drag the volume explicitly into the sidebar.

We reported this issue to Apple (FB9739492) in November 2021.

Update March 2023: Apple mostly addressed this issue in the 13.3 update. Some backup volumes may still not appear in the Finder sidebar, but they should appear on the Desktop and in the window that appears when you choose Computer from the Finder's Go menu.

Workaround: You can create an alias of the volume on your Desktop:

1. Click **Volumes** in CCC's sidebar
2. Right-click on your backup volume in CCC's sidebar and choose **Reveal in Finder**
3. Choose **as Columns** from the Finder's **View** menu
4. Hold down Command+Option while dragging the revealed volume to your Desktop to create an alias

Solution: Erase the volume in Disk Utility <https://bombich.com/kb/ccc6/preparing-your-backup-disk-backup-os-x> and start the backup from scratch. The underlying cause of this problem is the presence of an irrevocable "Data" role applied to that volume by Apple's ASR replication utility. macOS has documented functionality to remove that role, but that functionality does not work (FB7208067, Sept 2019). Erasing the volume is the only remaining recourse.

ExFAT filesystem corruption

We're tracking a new ExFAT-specific filesystem bug in macOS Ventura. We have seen a handful of cases where a folder's inode number is identical to the inode number of its parent folder. Some filesystem enumeration facilities (e.g. fts) identify this (correctly) as an insane "directory cycle" (i.e. infinite loop) condition and refuse to enumerate the content of the corrupted subfolder. CCC (6.1.4+) identifies this result, reports it as an error, and suspends any deletion/archival activity on the destination when this condition is encountered to avoid errantly removing content from the destination that was copied in a previous backup task.

In the handful of cases we're tracking, the issue appears to be both transient and recurrent, e.g. sometimes the condition is absent when running the task again at a later time, and sometimes it

recurs immediately after remounting the source volume. We have seen other related aberrant behavior on these volumes, e.g. folder inode numbers change when the volume is remounted. These aberrations are harmless as far as a backup/file copying task is concerned, but could cause trouble for other applications that expect folder inode numbers to be constant.

We consider this a serious filesystem bug, however we are not concerned that this will lead to data loss on ExFAT source volumes. This bug is exposed only when performing a complete enumeration of the volume starting from the root folder, it's not something that would necessarily affect the collection of an individual folder's content (e.g. in the Finder). Regardless, this condition is not sane and could lead to unexpected results from applications that are not guarding against this kind of filesystem corruption. Our recommendation right now is to avoid using ExFAT on macOS Ventura if you're not specifically using that filesystem to share files with a non-macOS device. Except when required to share files with a non-Mac system, ExFAT is generally a poor choice on macOS. It's very slow on macOS (usually 2-4x slower than APFS), and uses space much less efficiently.

We have reported this bug to Apple (FB11834215, November 29, 2022).

Update October 2023: Apple reports that this issue is resolved in macOS Sonoma. If you're seeing this corruption, then our primary recommendation is to upgrade to Sonoma, if possible.

Workaround: A "folder swap" on the source should resolve individual occurrences of this problem. For example, if CCC identifies that a folder named "Projects" is affected, then you would:

- Create a new folder adjacent to "Projects" named "Projects-new" [on the source volume]
- Move the content of "Projects" into the "Projects-new" folder
- Move the (now empty) "Projects" folder to the Trash
- Rename "Projects-new" to "Projects"
- Run your CCC backup task again to complete the backup

Solution: After you have resolved any corrupted folder issues (see above), you can do the following to migrate your data away from the ExFAT volume:

- If your destination is also ExFAT formatted, erase that volume in Disk Utility using the APFS format <https://bombich.com/kb/ccc6/preparing-your-backup-disk-backup-os-x>
- Run your CCC backup task again to complete an error-free backup
- Click the Compare button in CCC's toolbar <https://bombich.com/kb/ccc6/comparing-source-and-destination> to verify that the content of the destination matches that of the source
- Erase the affected source volume in Disk Utility using the APFS format <https://bombich.com/kb/ccc6/preparing-your-backup-disk-backup-os-x>
- Click **Restore** in CCC's toolbar to configure a new task to restore your data to the new volume from the backup <https://bombich.com/kb/ccc6/how-restore-from-your-backup#ccc>

If you have any concerns about this procedure, or you would like a review of your case prior to erasing the source, please don't hesitate to ask us for help <https://bombich.com/software/get_help>. We greatly prefer to get involved **before you erase your source** if you have any questions or nagging concerns about the procedure.

Apple's APFS replication utility ('asr') may fail to produce a bootable USB device on Apple Silicon Macs

When using the Legacy Bootable Copy Assistant on an Apple Silicon Mac running macOS Ventura, the resulting volume may not be bootable if it resides on a USB-attached device. ASR can produce bootable copies to the same device on an Intel Mac. This does not appear to be a general shortcoming of USB devices on this platform, rather it appears to be a shortcoming of the Apple asr

utility.

Workaround: Use a Thunderbolt device if you're trying to make a bootable copy of macOS Ventura on an Apple Silicon Mac.

Workaround: If you only have access to a USB device, proceed with a Standard Backup <https://bombich.com/kb/ccc6/cloning-macos-system-volumes-apple-software-restore#standard_backups> (do not use CCC's Legacy Bootable Copy Assistant). When the backup is complete, open the Ventura Installer <https://apps.apple.com/us/app/macos-ventura/id1638787999?mt=12> (or boot into Recovery Mode) and proceed to install Ventura onto the USB device.

Credits

CCC includes, in source or binary form, the following open source projects.

vsdbutil and hfs.util

CCC contains portions of source code available under the Apple Public Source License. That code may be downloaded by clicking the links below.

- vsdbutil_main.c <https://opensource.apple.com/source/diskdev_cmds/diskdev_cmds-332.11.5/vsdbutil.tproj/vsdbutil_main.c.auto.html> (View our modifications: vsdbutil.h <https://bombich.com/software/opensource/vsdbutil.h> and vsdbutil.c <https://bombich.com/software/opensource/vsdbutil.c>)
- hfs_util <https://opensource.apple.com/source/hfs/hfs-226.1.1/hfs_util/> (Our only modification is #define HFS_UUID_SUPPORT 1 in hfsutil_main.c)

View the APSL 2.0 license <https://www.opensource.apple.com/apsl>

rsync

CCC also includes, independently in binary form, rsync version 3.0.6. rsync is made available under the GNU General Public License. Per the license requirements, the source code and our modifications may be downloaded via the links provided below. This modified software is provided at no cost and with no warranty, also per the GNU GPL.

- Download the complete rsync 3.0.6 project <https://rsync.samba.org/ftp/rsync/src/rsync-3.0.6.tar.gz>
- Download the rsync 3.0.6 patches <https://rsync.samba.org/ftp/rsync/src/rsync-patches-3.0.6.tar.gz>
- Download the diff file (diff between 3.0.6 + [crtimes.diff, fileflags.diff, log-checksum.diff, and backup-dir-dels.diff] and my modifications) <https://bombich.com/software/opensource/rsync_3.0.6-bombich_20190114.diff>
- View the GNU GPL <https://bombich.com/software/opensource/COPYING.txt>

CCC is not a derivative work of rsync. Rsync is called in binary form only. You can access the build of rsync that is included with CCC via the application bundle: right-click on the CCC application icon, choose "Show Package Contents", then navigate to Contents/Library/LoginItems/CCC Dashboard.app/Contents/Frameworks/CloneKit.framework/Versions/A/rsync.

Sparkle

CCC's software update mechanism was inspired by Sparkle <http://sparkle-project.org>. We're no longer using the Sparkle code base, but we'd still like to credit Andy Matuschak for his enduring contribution to the macOS third-party software community.

Sparkle is Copyright (c) 2006 Andy Matuschak and licensed under the following terms:

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

View the complete license for Sparkle, including external attributions <https://bombich.com/software/opensource/SparkleLicense.txt>

skpsmtpmessage

The SimpleSMTP framework included with CCC is a derivative work of the skpsmtpmessage <https://code.google.com/p/skpsmtpmessage/> project. skpsmtpmessage is licensed under the MIT license:

The MIT License (MIT)
Copyright (c) 2008 Skorpiostech, Inc. All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

CocoaFob

We leverage CocoaFob <https://pixelespressoapps.com> for license generation and verification in CCC. CocoaFob is distributed under the BSD License <http://www.opensource.org/licenses/bsd-license.php>, Copyright © 2009-2015, PixelEspresso. All rights reserved. The following statement pertains to CocoaFob:

```
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY E
XPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES O
F MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SH
ALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENT
AL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROC
UREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS I
NTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRI
CT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF T
HE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
```

SQLCipher (Community Edition)

CCC leverages SQLCipher <https://www.zetetic.net/sqlcipher> for encrypting Task Audit databases. SQLCipher is distributed under a BSD License <http://www.opensource.org/licenses/bsd-license.php> , Copyright (c) 2008-2020 Zetetic LLC. All rights reserved. The following statement pertains to SQLCipher:

System Requirements for CCC

CCC is an advanced backup and file copying utility for the Mac.

System Requirements

- macOS 10.15 Catalina (10.15.7+)
- macOS 11 Big Sur
- macOS 12 Monterey
- macOS 13 Ventura
- macOS 14 Sonoma
- CCC is a native application on both Intel and Apple Silicon Macs (i.e. a "Universal" application)

Older versions of CCC <https://bombich.com/download> are still available for users running older OSes. Note that these older versions are not actively being developed and support is provided on a case-by-case basis.

Supported configurations

- An APFS formatted volume is required for a backup of the macOS startup disk
- SSDs and hard disk drives in Thunderbolt and USB 3.0+ enclosures — please see our list of recommended backup devices <https://bombich.com/kb/ccc6/choosing-backup-drive#recommendations>
- CCC is supported only on Apple Macintoshes that officially support macOS Catalina (or higher)
- A minimum screen resolution of 1024x768 is required

Configurations that are not supported

- CCC will not back up to or from an unformatted or unmounted device — the source and destination must have a filesystem recognized by macOS and visible in the Finder
- Copying Windows system files is not a supported configuration <https://bombich.com/kb/ccc6/can-ccc-back-up-my-bootcamp-windows-partition>
- CCC will not back up directly to optical media (e.g. CD-ROM or DVD-ROM)
- WebDAV, FTP, NFS and other "cloud" destinations are not supported
- CCC is not a two-way synchronization solution designed to keep two Macs in sync with each other — this is not a supported configuration.
- Performing mass deployments with CCC is not supported. Apple discourages this sort of deployment <https://support.apple.com/en-us/HT208020> and offers additional resources here <https://support.apple.com/guide/deployment/welcome/web>, and there are alternative solutions to consider. <https://twocanoes.com/products/mac/mac-deploy-stick>
- We can only support configurations of macOS that are supported *by Apple* on your hardware. For example, we cannot help you get Catalina running on a 2008 MacPro. Likewise, you cannot restore Mojave onto a 2019 MacBook Pro that shipped with Catalina. Hackintosh bootability issues should be pursued through a Hackintosh community forum. If Apple doesn't support it, we cannot support it.
- CCC can copy virtual machine container files, but copying to or from a virtual machine is not supportable.

Purchasing CCC

Bombich Software Sales Policies and Frequently Asked Questions

How can I purchase CCC?

Bombich Software products are available directly through our online store <https://bombich.com/store>, hosted by FastSpring <http://www.fastspring.com>, our e-commerce partner and Seller of Record.

Redemption codes that can be redeemed for single user licenses are also available from select consultants and resellers. For a list of authorized resellers, please see our license redemption page <https://cccreseller.com/redeem>.

Licenses are valid for prior versions of CCC. (e.g. If you purchase a CCC 6 license, it can be used with CCC 5 and 4.) For more info about purchasing CCC, see How much does CCC cost and how can I purchase it? <https://bombich.com/kb/ccc6/how-much-does-carbon-copy-cloner-cost-and-how-can-i-purchase-it>

What is your return policy?

As we offer a fully functional 30 day trial version of CCC <https://bombich.com/download> which you may use to evaluate its suitability for your needs prior to purchasing, all refund requests are evaluated on a case-by-case basis and may be subject to a minimum 15% processing fee. To request a refund, please contact our sales department <mailto:sales@bombich.com?subject=Refund%20Request> within 30 days of your purchase.

Need help?

If you are experiencing technical issues with CCC, we are happy to work with you to resolve them so that you can keep using CCC. To open up a support ticket, you can select **Ask a question about CCC...** from CCC's **Help** menu.

What are the terms of sale?

All products are offered subject to the terms of the particular license agreement included with each product.

How is CCC delivered?

All of our products are available exclusively via electronic delivery. There will be no actual shipment of a physical product. You can download the software at any time from our download page <https://bombich.com/download> and the registration key will be sent to you by email.

Because your purchase receipt and registration number are only provided in electronic format, you should print or otherwise safely archive a copy of the email invoice that you receive after your order has been processed. This invoice will serve as your proof of purchase and eligibility for technical support, future upgrades, and special offers.

Which payment types do you accept?

We accept the following methods of payment for orders placed through our online store <https://bombich.com/store>, hosted by FastSpring <http://www.fastspring.com>, our e-commerce partner and Seller of Record. Please note that not every form of payment is accepted in every country.

Credit Cards: We accept MasterCard, Visa, Discover, American Express and JCB.

Checks and Money Orders: We accept either company or personal checks. Please note that acceptance of checks and money orders varies by country. If you do not see this option at checkout, we do not accept this form of payment for your country. Checks are not accepted for subscription products, such as Maintenance.

PayPal: We accept payments originating from PayPal accounts.

Amazon Payments: We accept payments originating from Amazon Payments. If you do not see this option at checkout, we do not accept this form of payment for your country.

Alternative Payment Methods: In certain countries, we accept Giropay, iDEAL, Sofort, WebMoney and Alipay. If you do not see this option at checkout, we do not accept this form of payment for your country.

Do you accept purchase orders? Will you accept my PO terms?

We are happy to reference a PO number on an invoice for your internal tracking and record keeping. However, we do not accept purchase orders as form of payment nor the terms and conditions commonly associated with purchase orders. We provide a fully functional 30 day trial for you to use while payment is being arranged.

We are able to keep our prices low by offering a standard End User License Agreement <https://bombich.com/software/CCC_EULA.rtf> to all our customers and do not offer commercial credit. Our payment terms are Net 0-day for all of our customers. Once full payment is received, we issue the license and send it via email. Please contact our Sales Department <mailto:sales@bombich.com> for more information.

Do you charge tax, such as VAT, or other duties?

Applicable taxes are charged at the discretion of the importing country, and are the responsibility of the customer. These costs may be added at the end of the checkout process and are not necessarily displayed on the product selection pages.

What kind of e-commerce security do you use?

E-commerce services for our online store are provided by FastSpring <http://www.fastspring.com>.

Review FastSpring's Privacy Policy <http://www.fastspring.com/privacy.php>

Where can I download your W-9 form?

We do not sell directly to the public. All sales are from our trusted reseller partner, Fastspring.

Fastspring's W-9 Form <http://www.fastspring.com/w9.pdf>

Frequently Asked Questions

- How does the free 30-day trial work? <https://bombich.com/kb/ccc6/how-does-free-30-day-trial-work>
- How much does CCC cost and how can I purchase it? <https://bombich.com/kb/ccc6/how-much-does-carbon-copy-cloner-cost-and-how-can-i-purchase-it>
- If I pay for CCC now, will I have to pay for future updates? <https://bombich.com/kb/ccc6/if-i-pay-ccc-now-will-i-have-pay-future-updates>
- Purchasing an Upgrade for CCC 6 <https://bombich.com/kb/ccc6/purchasing-upgrade-carbon-copy-cloner-5>
- Can I use one license of CCC on multiple Macs in my household? <https://bombich.com/kb/ccc6/can-i-use-one-license-ccc-on-multiple-macs-in-my-household>
- Do you offer an academic discount? <https://bombich.com/kb/ccc6/do-you-offer-academic-discount>
- Can I give CCC as a gift? <https://bombich.com/kb/ccc6/can-i-give-ccc-gift>
- Do you offer a volume licensing program? <https://bombich.com/kb/ccc6/do-you-offer-volume-licensing-program>
- Why isn't CCC on the Mac App Store? <https://bombich.com/kb/ccc6/why-isnt-ccc-on-mac-app-store>
- Do you offer telephone support? <https://bombich.com/kb/ccc6/do-you-offer-telephone-support>

Purchasing an Upgrade for CCC 6

Will my CCC 3.5, 4 or 5 license work with CCC 6?

No, CCC 6 requires a new license. However, **if you purchased a CCC 5 license on or after February 18, 2021, we will grant you a FREE license for CCC 6**. CCC 5 licenses purchased prior to **February 18, 2021** are eligible for upgrade pricing.

I purchased a license for CCC 5 on or after February 18, 2021. How do I get my FREE CCC 6 license?

When you open CCC 6 for the first time, it will attempt to retrieve your new license using the details from your CCC 5 license. If this succeeds, you will receive an email containing your new license and details for applying the new license to CCC 6. If this does not occur (e.g. because your system can't be connected to the Internet), you can retrieve your license via our website <https://bombich.com/forgot>.

What licenses are eligible for online upgrade pricing?

CCC 4 and CCC 5 licenses are eligible for the following upgrade pricing:

If you have used CCC 1, 2, or 3	no discount is offered
If you own a CCC 4 Personal & Household license	your discount is 25%
If you own a CCC 5 Personal & Household license	your discount is 50%
If you own a CCC 4 Corporate & Institutional or Pro license	no discount is offered
If you own a CCC 5 Corporate & Institutional or Pro license	your discount is 25%

Corporate and Institutional Licenses (Volume License Program) are eligible for an upgrade discount of 25% off the current corresponding price tier <https://bombich.com/store/corporate>. Upgrades are free if Maintenance has been purchased and is currently active.

How do I purchase a license for CCC 6 at upgrade pricing?

If you are (or were) using a registered copy of CCC 5, download and open CCC 6. CCC 6 will recognize your CCC 5 license and check it for upgrade eligibility. If our automated system can determine that it is eligible for upgrade pricing, CCC will retrieve a coupon code that will automatically be applied to your in-app purchase.

If you have any trouble upgrading in-app, you can also use our upgrade offer request form <https://bombich.com/store/upgrade>. If you have any problems with or questions about purchasing an upgrade, please don't hesitate to contact us for help <mailto:sales@bombich.com?subject=Upgrade%20Eligibility%20Question>.

My Mac is too old for CCC 6. If I purchase a license for CCC 6, will that work with CCC 4 or 5?

Yes! If you purchase a license for CCC 6, that license will be recognized by CCC 4 or later. If you upgrade your Mac at a later date, you can upgrade to CCC 6 and begin using your CCC 6 license.

What licenses are not eligible for upgrade pricing?

Legacy licenses such as a Department or Site license are not eligible for upgrade pricing.

Can I apply an EDU discount to my upgrade purchase?

No, additional discounts cannot be applied to upgrade pricing.

Additional Resources

- What's New in CCC 6 <https://bombich.com/kb/ccc6/whats-new-in-ccc>
- System Requirements for CCC <https://bombich.com/kb/ccc6/system-requirements-carbon-copy-cloner>
- Contact Sales Support <mailto:sales@bombich.com?subject=Upgrade%20Eligibility%20Question>
- Download CCC <https://bombich.com/download>

How does the free 30-day trial work?

You can try the complete feature set of CCC for 30 days before purchasing it. *No features are disabled during the trial.* We encourage you to use that time to explore CCC's automated, incremental backup functionality and versioned backups.

Download the latest and greatest version of CCC <https://bombich.com/download>

If you have any questions about the behavior or functionality of CCC either during the demo period or after purchase, you can select **Ask a question about CCC...** from Carbon Copy Cloner's **Help** menu.

How much does CCC cost and how can I purchase it?

Pricing

A household license of CCC 6 costs $49.99 USD plus any applicable local taxes. In some countries, we offer a pre-set price in local currency in order to allow a greater number of payment types. In other countries, the price in local currency is calculated at the time of sale and depends upon the current exchange rate with USD.

Purchasing

Businesses and institutions can purchase single workstation licenses, volume licenses and pro (technician) licenses in our **Corporate Store <https://bombich.com/store/corporate>**.

Bombich Software products are available directly through our online store <https://bombich.com/store>, hosted by FastSpring <http://fastspring.com>, our e-commerce partner and Seller of Record. CCC software delivery is electronic only. There is no actual shipment of a physical product. You can download the software at any time from our download page <https://bombich.com/download> and from within CCC you can request that your registration key be emailed if you have misplaced it.

Redemption codes that can be redeemed for single user licenses are also available from select consultants and resellers. For a list of authorized resellers, please see our license redemption page <https://cccreseller.com/redeem>.

Upgrade Pricing

If you own a CCC 4 or 5 household license, you can receive a discount when purchasing CCC 6.

- If you have used CCC 1, 2, or 3: no discount is offered.
- If you own CCC 4: your discount is 25%.
- If you own CCC 5: your discount is 50%.

Please visit our upgrade page to determine your discount offer <https://bombich.com/store/upgrade>.

Note: If you purchased CCC 5 on **February 18, 2021** or later**,** you already have a free CCC 6 license. Retrieve it here <https://bombich.com/forgot>.

Additional Resources

- Purchasing an Upgrade for CCC <https://bombich.com/kb/ccc6/purchasing-upgrade-carbon-copy-cloner-5>
- Contact Sales Support <mailto:sales@bombich.com?subject=Upgrade%20Eligibility%20Question>

If I pay for CCC now, will I have to pay for future updates?

When updates consist of minor improvements and fixes (e.g. bug fixes, going from version 6.0 to 6.1, etc.), they are always free to licensed users.

From time to time, there will be new versions that require significant changes to our application. These upgrades are specified by a new version number (e.g. going from version 5 to 6) and will include new features and functionality and support for newer operating systems. This process requires significant research, design, development and testing time. These releases will be handled like most commercial software: current users will be offered an upgrade price but the previous version will continue to work on older OSes if you decline to purchase the update.

Volume license customers with current software maintenance agreements will receive any paid upgrades at no additional charge.

Please note that we do not support older versions of CCC indefinitely. To find out which versions of CCC are currently supported and anticipated support sunset dates, please see our download page <https://bombich.com/download>.

For more information about our current upgrade pricing options, please see How much does CCC cost and how can I purchase it? <https://bombich.com/kb/ccc6/how-much-does-carbon-copy-cloner-cost-and-how-can-i-purchase-it>

Can I use one license of CCC on multiple Macs in my household?

Yes, the CCC License <https://bombich.com/software/CCC_EULA.rtf> allows you to install and use CCC on any computer that you own or control for personal, noncommercial use. If you're using CCC commercially or institutionally, check out our Corporate <https://bombich.com/store/corporate> or Academic <https://bombich.com/edu> purchasing options.

A CCC 6 license will also be accepted by CCC 4 and CCC 5. If you have multiple Macs in your household and some do not meet the requirements for CCC 6, you can use the same license on all of your Macs with CCC 4, CCC 5 and CCC 6. You can download all available versions of CCC at any time from our download page <https://bombich.com/download>. Misplaced your license? Request the registration key from within CCC or via our website <https://bombich.com/forgot>.

To learn more about how to use the license on multiple Macs, please see How do I use CCC on multiple Macs in my household? <https://bombich.com/kb/ccc6/how-do-i-use-one-license-ccc-on-multiple-macs-in-my-household>

Do you offer an academic discount?

We offer a 25% academic discount.

Who is eligible?

To qualify for Bombich Software education pricing, you MUST be an Eligible Educational End User:

- Faculty, staff or administrator, currently employed at an accredited K-12 school or higher education institution, with a valid academic email address.
- Students who are currently enrolled at an accredited higher education institution, with a valid academic email address.

What is eligible?

New purchases of CCC Household licenses, Workstation licenses, Pro licenses, and Volume licenses qualify for an academic discount. Upgrade purchases are discounted for current license holders and are not eligible for an additional educational discount.

How do I receive a discount for personal use?

1. **Visit our EDU discount verification page <https://bombich.com/edu> to have a coupon code emailed to your academic email address.**
2. **Purchase CCC using the "Personal purchase" link in the email you just received.**

*We maintain a long list of academic email domains that are eligible for our automatic academic discount. If your domain is not on the list, you may still receive a discount but you will need to complete a manual verification process. If manual verification is necessary, we'll email you instructions.

How do I receive a discount for institutional use?

1. **Visit our EDU discount verification page <https://bombich.com/edu> to have a coupon code emailed to your academic email address.**
2. **Purchase CCC using the "Institutional purchase" link in the email you just received.**

*We maintain a long list of academic email domains that are eligible for our automatic academic discount. If your domain is not on the list, you may still receive a discount but you will need to complete a manual verification process. If manual verification is necessary, we'll email you instructions.

*If you have any questions about accepted payment methods, please email sales@bombich.com <mailto:sales@bombich.com>.

Is there anything else I should know?

Terms and Conditions

Personal Use: For personal use, each Eligible Education End User may purchase one CCC license per version and academic email address. Bombich Software reserves the right to request evidence of

employment or student status before Carbon Copy Cloner has been sold with an academic discount. This may include proof of school accreditation, faculty or student ID, and/or email address verification.

Institutional Use: If CCC is purchased for institutional use, the one copy limit does not apply, although Bombich Software reserves the right to limit the number of purchases by a single institution. Bombich Software also reserves the right to request evidence of employment before Carbon Copy Cloner has been sold with an academic discount. This may include proof of school accreditation, faculty or student ID, and/or email address verification.

Prices do not include local taxes or local customs charges. Bombich Software reserves the right to change this offer at any time and to revoke discounts or cancel orders in their sole discretion.

What if I have questions?

Please email sales@bombich.com <mailto:sales@bombich.com> for assistance.

Do you offer a volume licensing program?

Yes, you can save your organization money with volume licensing.

We offer multi-user license pricing for CCC. Volume licensing is open to anyone purchasing 5 or more licenses of CCC. A volume license agreement includes:

- Discounts off standard prices
- A single license key for all of your CCC licenses for easy administration
- Optional Software Maintenance

To learn more about our volume license, please see our Volume License and Maintenance Agreement. <https://bombich.com/software/CCC_Volume_License_and_Maintenance_Agreement_2014.pdf>

Product Delivery and Ordering

We offer CCC volume licenses via download delivery only; we do not ship physical, boxed copies of the software.

To place your order, or obtain a price quote for a new volume license, please shop our Corporate Store <https://bombich.com/store/corporate>. To learn about our education discounts or place a discounted education order, please read about our Education Pricing <https://bombich.com/edu>. If you would like to add additional seats to an existing volume license, please email our Sales department <mailto:sales@bombich.com?subject=Add%20Volume%20License%20Seats%20to%20CCC%20License> for a custom quote.

Software Maintenance

Volume licenses offer the option of including software maintenance, a service which provides all updates to CCC at no additional charge beyond the subscription fee. Maintenance subscriptions can be cancelled at any time via a link found in your CCC volume license delivery email. For additional details, please see the CCC Maintenance Terms <https://bombich.com/software/maintenance_terms_2014.pdf>.

Sales Policies

For information on our sales policies, please refer to our Sales Policies and Frequently Asked Questions <https://bombich.com/sales-terms-and-conditions>.

If CCC is licensed at an education discount, then it may only be used by enrolled students, faculty, teachers and administrators at an accredited K-12 educational institution (or equivalent) or higher education institution organized and operated exclusively for the purpose of teaching its students. In addition, there are no portable or home use rights included with our volume licenses.

If you have any other questions, please send us an email. <mailto:sales@bombich.com>

Can I give CCC as a gift?

Yes, using our Online Gift Store <http://sites.fastspring.com/bombich/product/ccc6?option=gift>.

CCC registration is tied to the name and email address that is entered in the order and our Online Gift Store <http://sites.fastspring.com/bombich/product/ccc?option=gift> allows you to specify a gift recipient. You will receive a receipt via email and the gift recipient will receive license information immediately via email.

Why isn't CCC on the Mac App Store?

We would love to add the Mac App Store as a distribution channel for CCC, but there are certain classes of applications that do not meet the policy requirements imposed by Apple. Unless Apple changes these policies, you will never see a full-featured, advanced file copying and backup utility on the Mac App Store. You can send Apple some feedback <https://www.apple.com/feedback/> about this policy, but judging from the absence of the Mac App Store from Apple's Feedback page (for more than a decade now), and Apple's pertinacious position on this matter, we don't anticipate a change in this policy.

Do you offer telephone support?

Our support team is standing by to field your questions about using CCC, however we do not staff an incoming telephone support desk.

In providing support to our customers since 2002, we have determined that we can provide more efficient and higher quality support when that support interaction is started with an online submission process. When you submit a support request directly through CCC's Help menu, your logs are (with your consent) submitted alongside your request, allowing us to analyze your unique CCC configuration and any error messages you're encountering. Frequently we'll get requests with no more detail than "I'm having trouble getting this to work." That level of detail is OK. After a brief review of CCC's logs we can very quickly follow up with a list of steps to resolve the problem, along with annotated screenshots.

Every support request is answered by a member of the Bombich Software support team and we do our best to respond to every request within one business day. We provide online support, in English, Monday through Friday between 9:00 AM and 5:00 PM, US Eastern Time.

Please note that our support is primarily limited to answering questions about CCC and fielding bug reports. We cannot provide extensive consultative support for setting up extremely complex backup strategies, nor can we offer general troubleshooting for macOS issues that are outside the scope of our product. If you are interested in getting more in-depth, hands-on, phone/screen sharing setup assistance with CCC or macOS, a consultant that is familiar with CCC <https://cccreseller.com/redeem> can offer that level of assistance.

Related Documentation

- Establishing an initial backup <https://bombich.com/kb/ccc6/how-set-up-your-first-backup>
- How do I get help? <https://bombich.com/kb/ccc6/how-do-i-get-help>
- About Us <https://bombich.com/about>

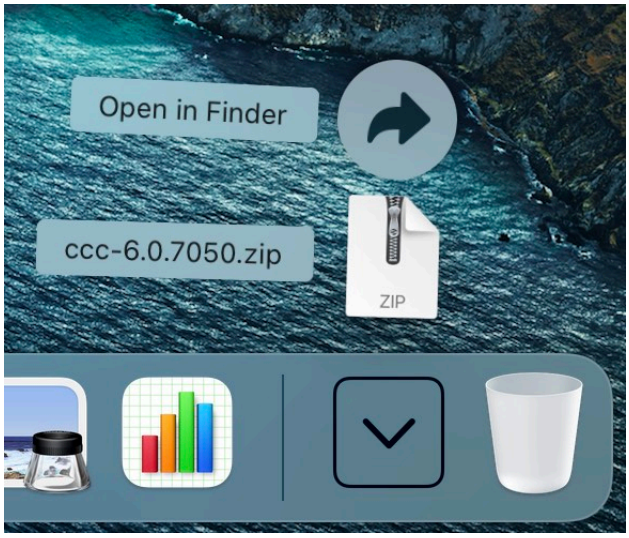
Downloading, Installing and Registering CCC

How do I download and install CCC?

Visit bombich.com

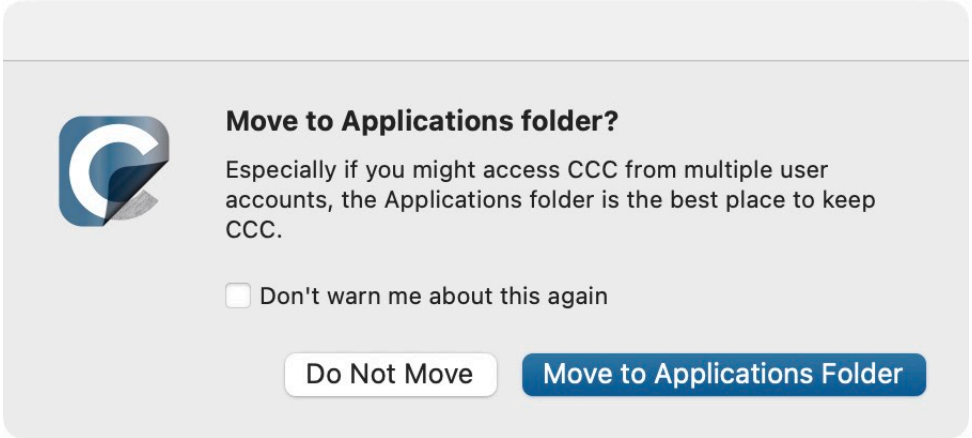
Go to https://bombich.com <https://bombich.com> and click on the **Download** button.

Allow download to complete and open the CCC Zip archive in your Downloads folder



Once the download is complete, open the CCC zip archive in your Downloads folder to unarchive CCC.

Open CCC and allow it to move itself to the Applications folder



Click **Move to Applications Folder**. From now on you'll find CCC in your Applications folder with the rest of your applications.

(Optional) Add CCC to your Dock

To add CCC to your dock, drag and drop it from the Applications folder into your Dock.

Upgrading from CCC 5 to CCC 6

If you download CCC 6 via the upgrade interface in CCC 5, CCC 6 will be downloaded to your Mac and placed adjacent to CCC 5. When CCC 6 opens for the first time, you will begin a full-featured, 30-day trial. Please take all of that time to evaluate CCC 6. When you're ready to purchase CCC 6, click the **Purchase** button in the Trial window that is presented when you open CCC.

I already have a license for an older version of CCC. Do I have to pay for the CCC 6 upgrade?

Yes, CCC 6 is a paid upgrade. However, CCC 4 or 5 license may be eligible for upgrade pricing. Check here for eligibility <https://bombich.com/store/upgrade>.

If I decide to not purchase the CCC 6 upgrade, can I downgrade to CCC 5?

Yes. Downgrading to CCC 5 restores your tasks as they were prior to upgrading. If you still have CCC 5 in your Applications folder, simply open it and choose the option to **Downgrade**. If you downloaded CCC 6 from our website and replaced your copy of CCC 5, you can re-download CCC 5 from our website <https://bombich.com/download#ccc5>.

I'm happy with CCC v6. How do I delete the older version of CCC?

To remove the older version of CCC, simply drag the older application file to the Trash. You don't have to uninstall any other components, all other components are shared with CCC v6.

Will my CCC v5 tasks work with CCC v6? Will I have to erase my backups?

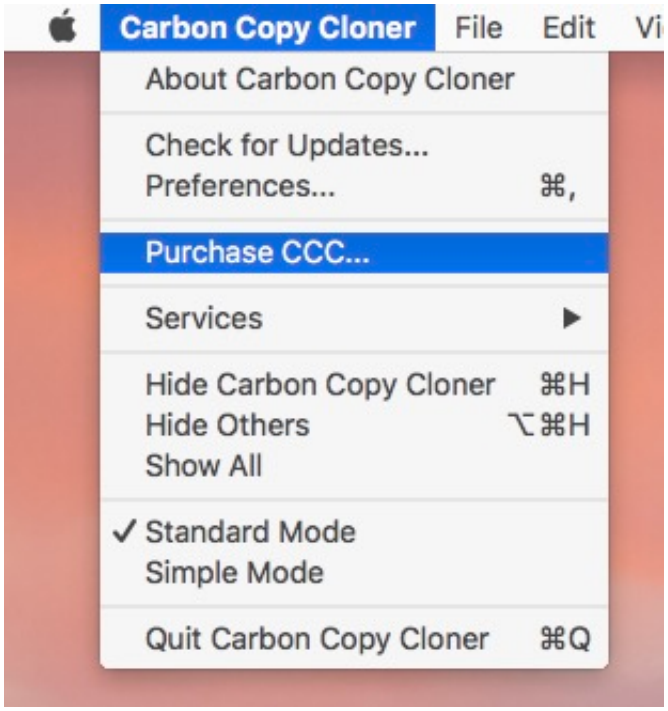
The upgrade from CCC 5 to 6 should be seamless. Your existing tasks will be imported into CCC v6, and your existing backups should continue to run without requiring any changes.

Additional Resources

- Purchasing an Upgrade for CCC 6 <https://bombich.com/kb/ccc6/purchasing-upgrade-carbon-copy-cloner>
- How does the free 30-day trial work? <https://bombich.com/kb/ccc6/how-does-free-30-day-trial-work>
- What's new in CCC 6? <https://bombich.com/kb/ccc6/whats-new-in-ccc>
- System Requirements for CCC 6 <https://bombich.com/kb/ccc6/system-requirements-carbon-copy-cloner>
- CCC 6 Release Notes <https://bombich.com/kb/ccc6/release-notes>
- Report a problem or ask a question about CCC 6 <https://bombich.com/software/get_help>

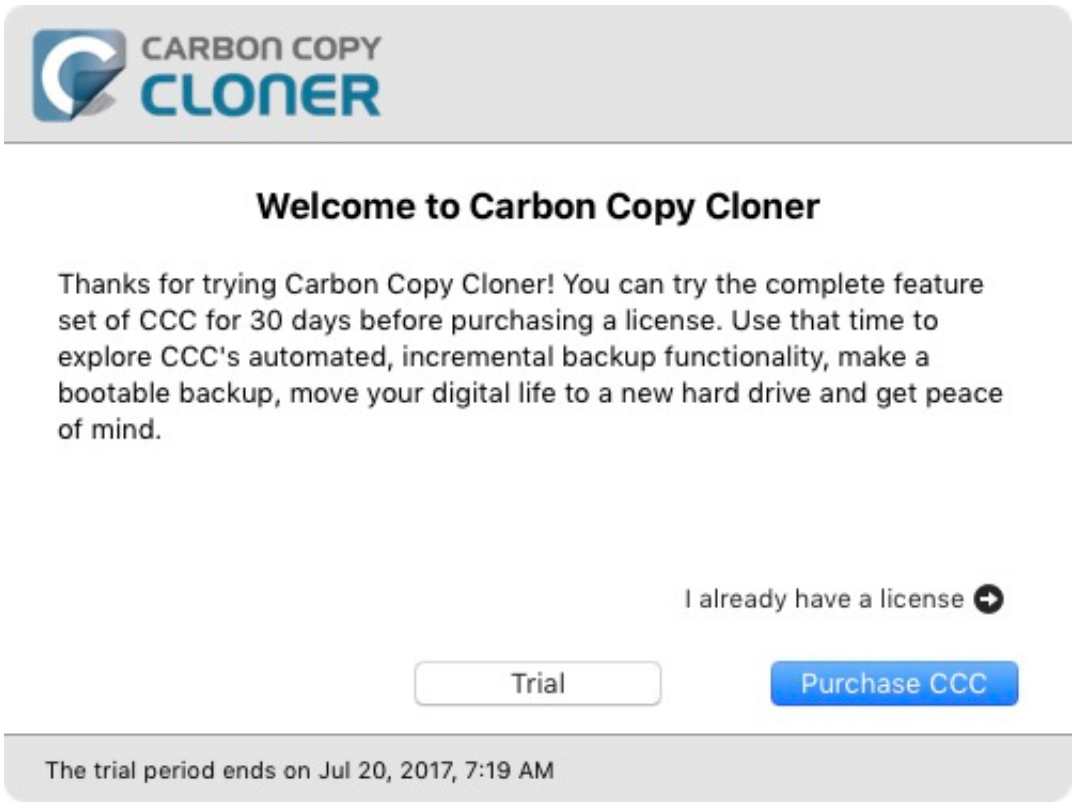
How to Manually Enter a CCC Registration Code

Open CCC and Check Registration Status



Click on the **Carbon Copy Cloner** menu. If you see a **Show Registration...** menu, then CCC is already registered on your Mac. You can select **Show Registration...** to view the registration details. If CCC is not yet registered, you will see a window that opens on launch indicating that CCC is currently running on a trial basis. If you already dismissed that window, you can choose **Purchase CCC...** from the Carbon Copy Cloner menu to reopen the Trial window.

Unregistered CCC

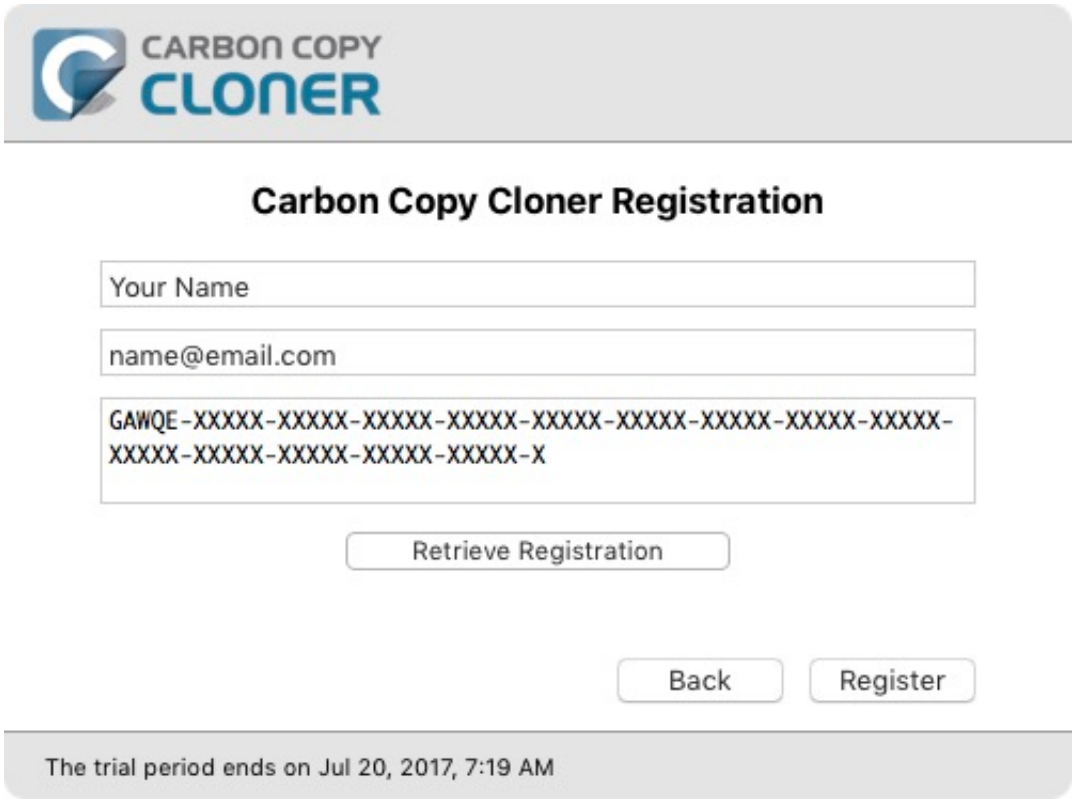


If CCC is unregistered, you will see the **Welcome to CCC** registration screen. If you have previously purchased CCC, click on **I already have a license.**

Copy and Paste in Registration Codes

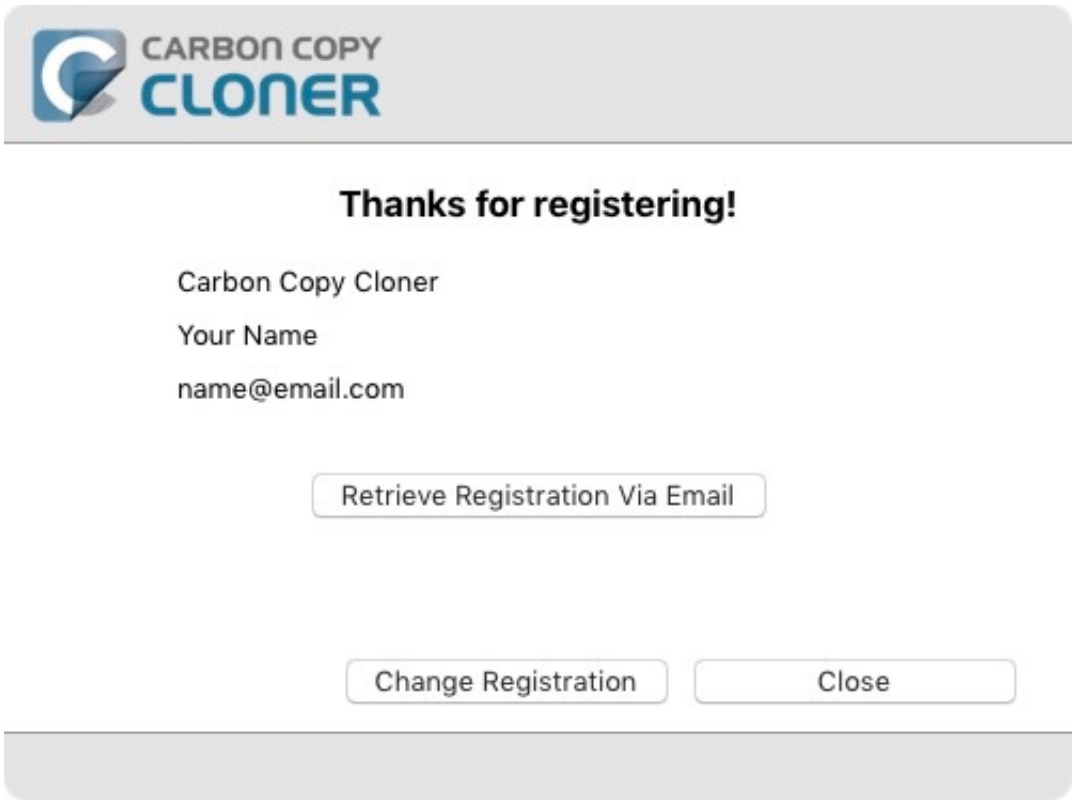
Copy and paste in the name, email address and license key exactly from your registration email. Note: If you try to use a different name or email address, the license key will show as invalid. Click **Register**.

Properly Entered Code



For your reference, here is what a registration code should look like. Note that the registration code automatically breaks between the two lines; do not use the Return key when entering your registration code.

Successfully Registered



Once your copy of CCC is successfully registered, you should see a "Thanks for registering!" screen.

Can I download the old versions of CCC?

Older versions of CCC can be downloaded at https://bombich.com/download <https://bombich.com/download>.

We do not sell CCC 4 or CCC 5 licenses. To use CCC 4 or 5, please purchase a CCC 6 license. **CCC 6 licenses can be used to register CCC 4 and CCC 5.**

Trouble Applying Your Registration Information?

Frequently Asked Questions

How do I retrieve my registration information? I bought CCC, but it says that I'm unregistered.

If you see a prompt to purchase CCC and you have paid for CCC in the past, you can retrieve your registration information at our website <https://bombich.com/forgot>. Simply provide the email address that you used when you paid for CCC, and we'll send your registration information via email. Clicking a button in the email will instantly register CCC (no copying/pasting of registration codes is required) <https://bombich.com/kb/ccc6/how-register-ccc-in-one-click>.

Your registration code is tied to the name and email provided when the license was purchased. **If your email or name are entered incorrectly (capitalization matters!), the license will show as invalid**.

To ensure that the license information is applied correctly, just open your license email and click on the "Click Here to Register CCC" button to automatically apply the settings (if prompted, select CCC as the application to use when opening the link).

What if I can't retrieve my registration information?

There are several reasons that this might happen, e.g. you don't have access to the email account you used when you originally paid for CCC or you don't remember which email you used. If you can't automatically retrieve your registration information, we need to verify your previous purchase. Please submit a request for registration assistance <https://bombich.com/forgot?found=0> and we'll work it out as quickly as possible.

When I click on the button to apply my registration settings, my browser says that it can't open this weird-looking URL.

If you click on the "Click Here to Register CCC" button in the email that you received from us and you get a message similar to "Safari can't open com.bombich.ccc.lic://blah-blah-blah because macOS doesn't recognize Internet addresses starting with com.bombich.ccc.lic", that means that CCC hasn't yet been registered as the application that handles those URLs. Typically CCC is registered as that URL handler when you launch CCC, so be sure that you have downloaded CCC and opened it on the Mac where you're trying to apply the registration settings. If you have already opened CCC and

you're still getting this message, try entering the registration values manually <https://bombich.com/kb/ccc6/how-manually-enter-ccc-registration-code>, or contact us for assistance <https://bombich.com/forgot>.

How do I register CCC in one click?

View step-by-step one-click registration directions, complete with pictures. <https://bombich.com/kb/ccc6/how-register-ccc-in-one-click>

How do I manually enter a CCC registration code?

View step-by-step manual registration directions, complete with pictures. <https://bombich.com/kb/ccc6/how-manually-enter-ccc-registration-code>

I'm still having trouble. How do I get someone to help me with my registration?

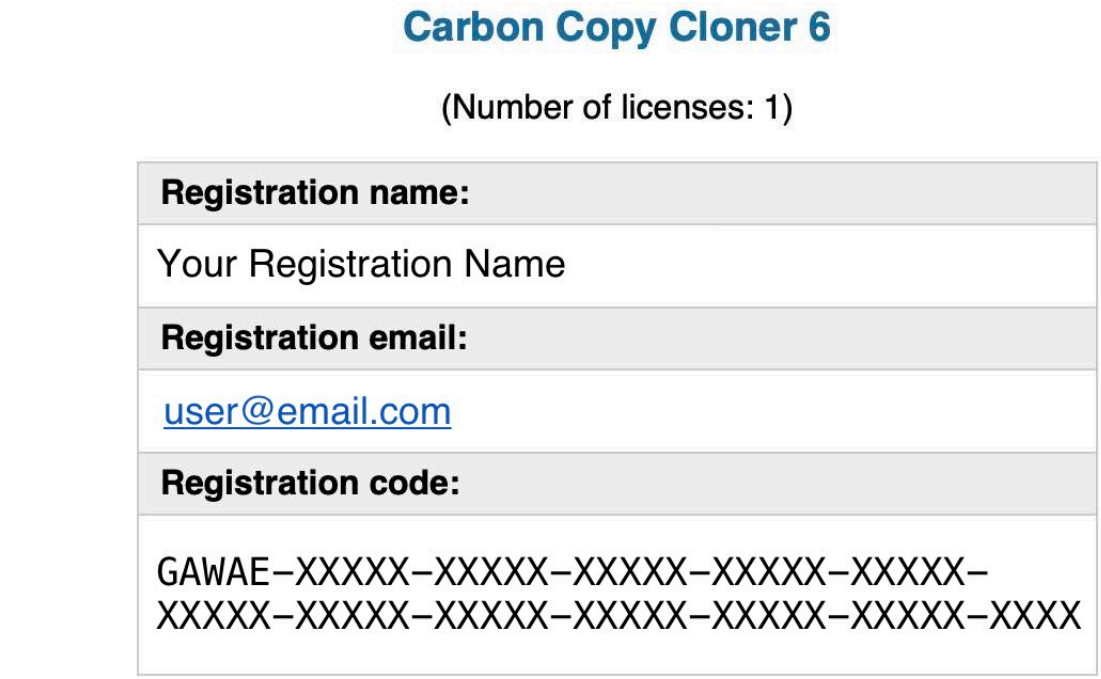
We're here to help. Just contact us via this Registration Assistance form <https://bombich.com/forgot?found=0>, and we will help you sort it out as quickly as possible.

How to Register CCC in One Click

Install and Open CCC

For one-click registration to work, you must first install and open CCC. To download CCC, please visit https://bombich.com <https://bombich.com> and click on the download button.

Open Your Registration Email



Open your registration email and click on the **Click Here to Register CCC** button. That's it! You're all set!

Troubleshooting Note: If you get a message similar to "**Safari can't open com.bombich.ccc.lic://blah-blah-blah because macOS doesn't recognize Internet addresses starting with com.bombich.ccc.lic**", double-check that you have (1) downloaded CCC and (2) opened it on the Mac where you're trying to apply the registration settings. If you have already opened CCC and you're still getting this message, try entering the registration values manually <https://bombich.com/kb/ccc6/how-manually-enter-ccc-registration-code>, or contact us for assistance <https://bombich.com/contact>.

How do I use one license of CCC on multiple Macs in my household?

The CCC license allows you to install and use CCC on any computer that you own or control for personal, non-commercial use. If you're using CCC commercially or institutionally, the instructions in this article are also applicable, but be sure to check out our Corporate and Education Licensing options <https://bombich.com/store/corporate> so that your use is in compliance with the license.

Install and open CCC on the unregistered Mac first

Download CCC <https://bombich.com/software/download_ccc.php?v=latest> on the other Mac before attempting to apply the registration settings. Open CCC and allow CCC to move itself to your Applications folder when prompted. Full installation instructions are available here: How do I download and install CCC? <https://bombich.com/kb/ccc6/how-do-i-download-and-install-carbon-copy-cloner>

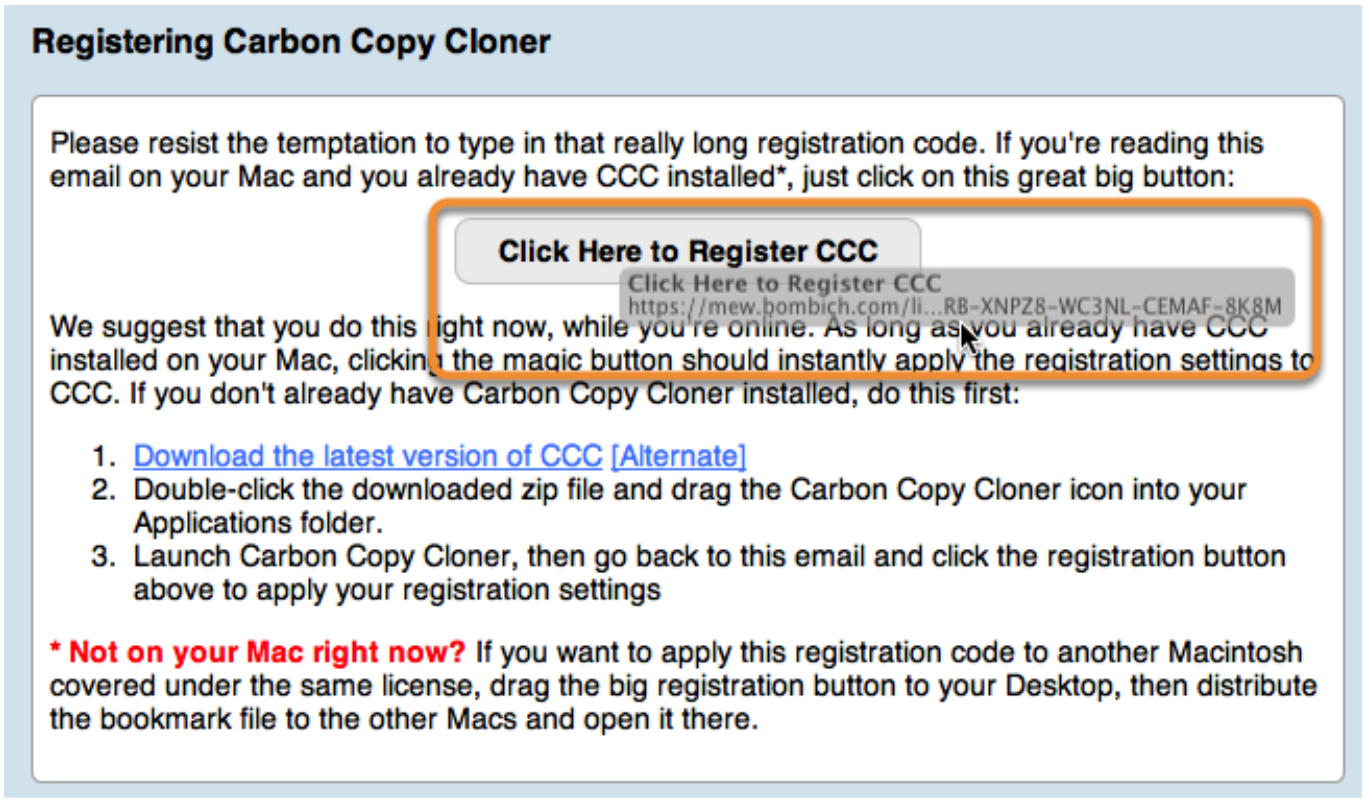
Option 1: I can check my email the unregistered Mac

Open your email and locate your CCC registration email. Click on the "Click Here to Register CCC" link. For more info, see How to Register CCC in One Click <https://bombich.com/kb/ccc6/how-register-ccc-in-one-click>. Misplaced your registration email? Request a new one via our website <https://bombich.com/forgot>.

Option 2: I can't check my email the unregistered Mac

1. Open the registration email on the already registered Mac

To apply the registration settings to another Mac, drag the **Click Here to Register CCC** button or link from your purchase confirmation email to your Desktop.



2. Drag the registration link to your Desktop

When you drag the link to your Desktop, a bookmark file will appear on the Desktop.

3. Transfer and double-click

Transfer this file to your unregistered Macs (via email, flash drive, file sharing, cloud storage, etc.) and double-click it to apply the CCC registration settings there.

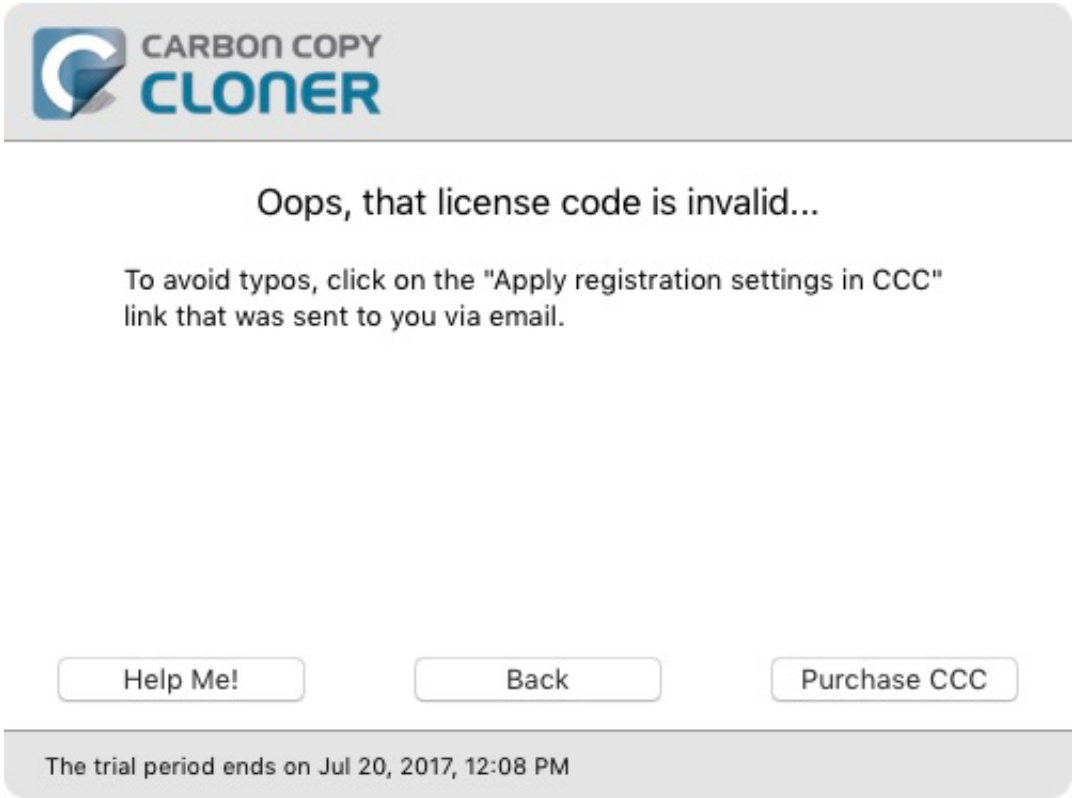
Oops, that license code is invalid...

If you see this window when trying to launch CCC

There are two common issues that cause this.

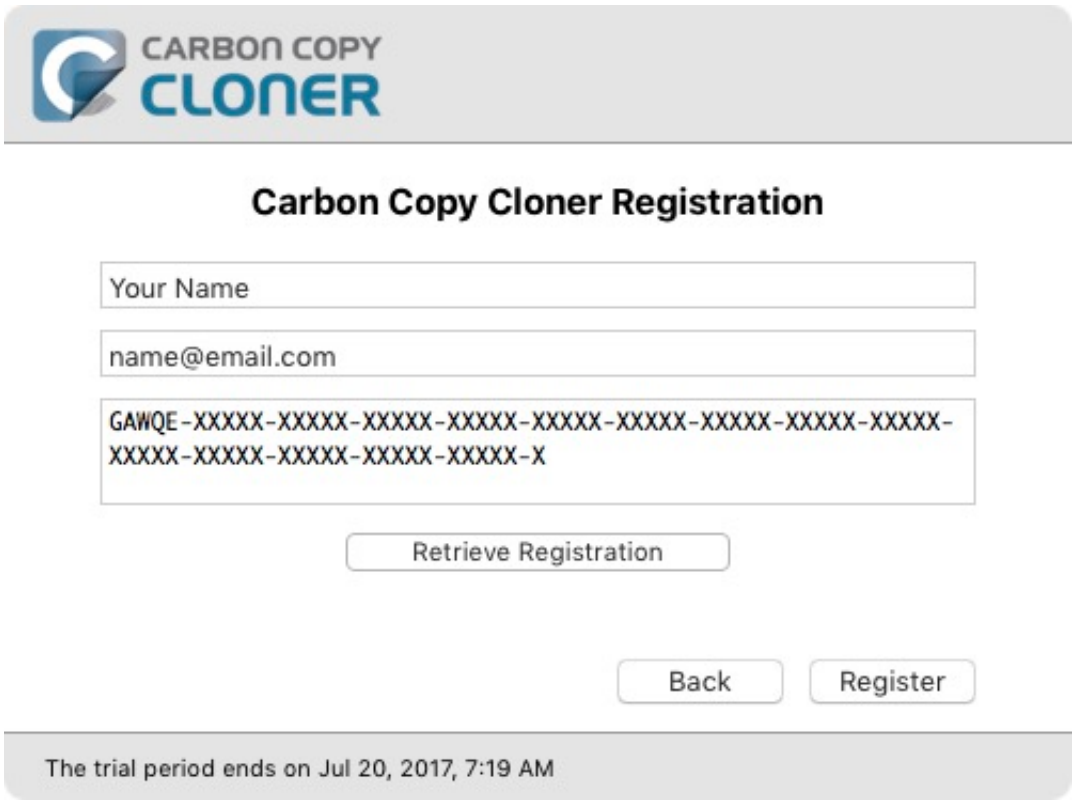
1. Your name, email address or registration code doesn't exactly match the information provided at the time of purchase. Your name and email must **exactly** match your registration email - **capitalization matters!** - or your license will show as invalid.
2. The version of CCC that you are running is damaged and needs to be replaced with a new copy downloaded from https://bombich.com/download <https://bombich.com/download>.

To check on the info entered in CCC, click on **Back**.



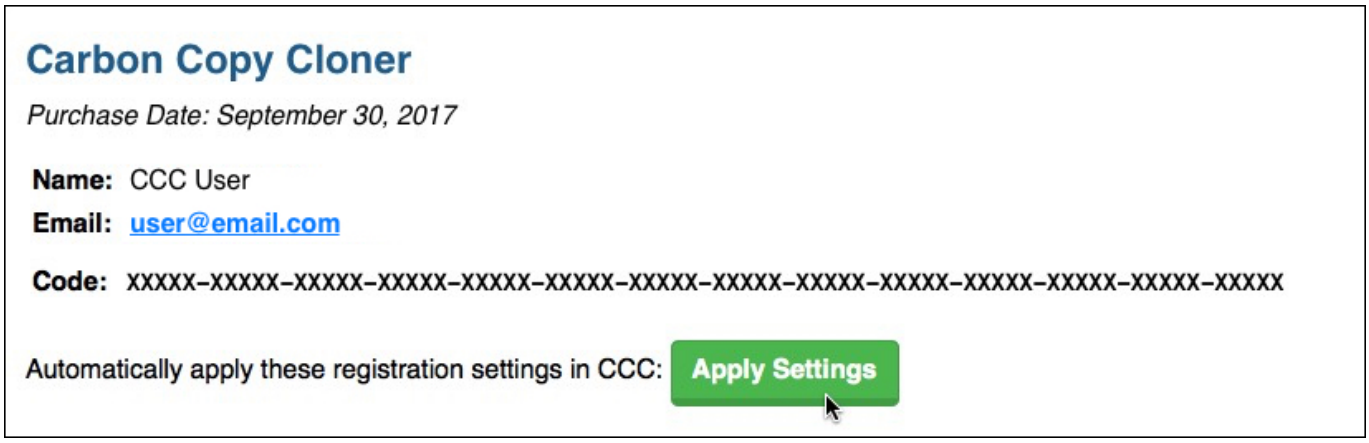
Registration Details

Open your registration email and verify that the information you see **exactly** matches. Click on **Register** when you are done.



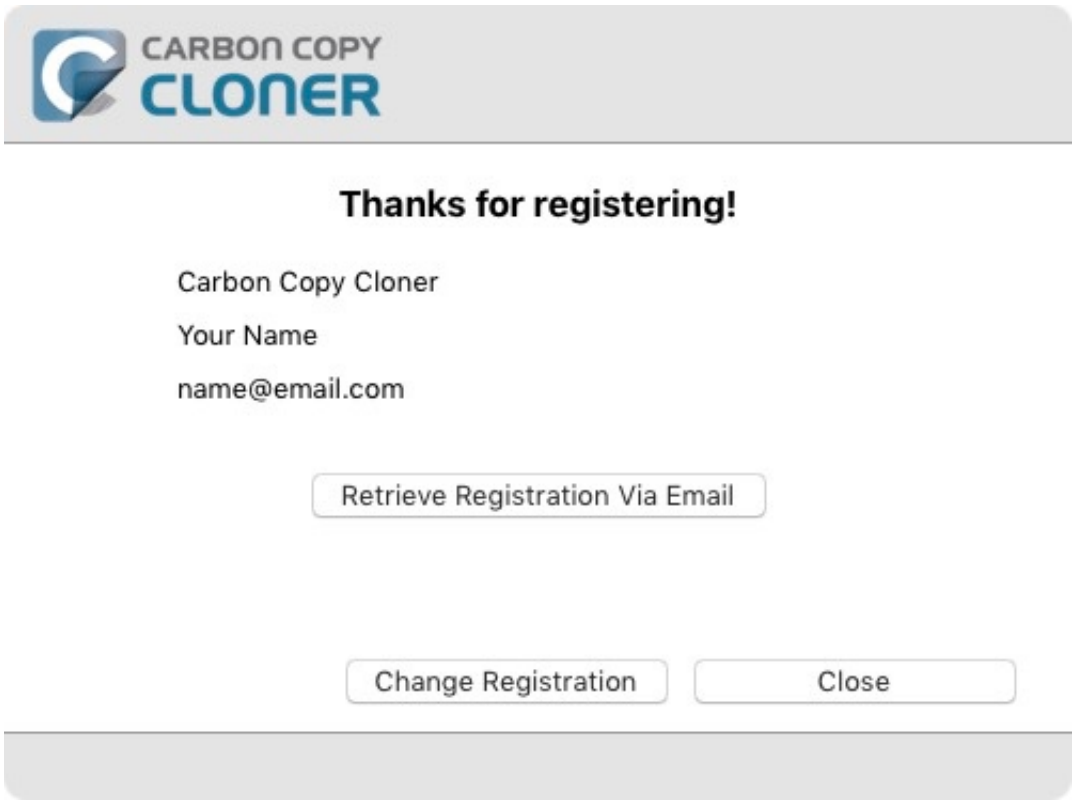
One-Click Registration

Tired of trying to make sure it matches? Just click on **Apply Settings** in your registration email and the information will be automatically entered for you.



Successful registration

Once you are successfully registered, you will see this window. Click **Close** and start backing up.


CARBON COPY CLONER
Thanks for registering!
Carbon Copy Cloner
Your Name
name@email.com
Retrieve Registration Via Email
Change Registration
Close

I already purchased CCC but can't find my registration code. Can you send it to me?

Yes, you can request via our website <https://bombich.com/forgot>. If you're getting a message about a trial and you have already purchased CCC, or if you have any other questions or concerns about your registration, you can retrieve your registration code here <https://bombich.com/forgot>.

How do I use a CCC Pro License?

Pro licenses are issued to a single technician/support person to use CCC temporarily on an unlimited number of computers. CCC may not be permanently installed on client computers or used for scheduled backups on their computers. The Pro License is great for replacing a client hard drive, making an ad hoc backup of a single machine before servicing or replacing that system, or for a consultant setting up new computers for others.

There are two common configurations where a Pro License is applicable, and each has a different method for applying the CCC registration details.

Installing CCC and registering a Pro License on an administrative workstation

An "administrative workstation" is a Mac that is used by a single support technician to service other Macs. For example, the technician could attach other Macs to this workstation via Target Disk Mode, then make an ad hoc backup of the data on that system prior to performing other service on the system. In this scenario, you would apply the CCC Pro License registration details in the same manner as an ordinary license <https://bombich.com/kb/ccc6/how-register-ccc-in-one-click>. Making scheduled backups of this administrative workstation is permissible, however the license does not permit scheduled backups of other Macs.

Using CCC temporarily on a client Mac

The CCC Pro License permits using CCC in an ad hoc manner on an unlimited number of Macs by a **single technician**. For example, a technician that is providing "on site" support could attach a portable storage device to a client Mac, then use CCC from that external storage to make an ad hoc backup of the client's data before performing other service on the system. In this scenario, the CCC Pro License must **not** be applied to the client system. To facilitate this use case scenario, CCC can read a "sidecar" license file adjacent to the CCC application on the external storage. To generate the sidecar file:

1. Open a copy of CCC on an administrative workstation†
2. Apply the CCC Pro License registration details
3. Click on the **Carbon Copy Cloner** menu and select **Create Pro License Sidecar File**
4. A file named "Carbon Copy Cloner.license" will be created on the Desktop
5. Quit CCC
6. Copy the CCC application and the "Carbon Copy Cloner.license" file to an external storage device (the application and license must be in the same folder)

When you attach the external device to another Mac and open CCC, you can click on the **Carbon Copy Cloner** menu to verify that the registration is applied (non-persistently) via the sidecar file.

† If you don't have an administrative work station to use for this, you can apply the Pro License registration details to any Mac, generate the sidecar license file, then uninstall CCC <https://bombich.com/kb/ccc6/uninstalling-ccc> from that Mac when you're finished.

Migrating CCC tasks from one system to another

If you wish to migrate your tasks from CCC on one system to CCC on another system, follow these steps:

1. Choose **Export All Tasks** from CCC's **Task** menu.
2. Specify a name for the exported settings file and a location where to save it.
3. Transfer the exported settings file to another Mac.
4. Install CCC onto the other Mac
5. Double-click the exported settings file.
6. As prompted, review the task settings and reset the source/destination selections as necessary.

Note that CCC uses a unique identifier to positively identify your source and destination volumes. While your other Mac may have a "Macintosh HD" volume and a "Backup" volume, those volumes will appear very different to CCC on the second Mac. Simply reselect those new volumes in CCC's Source and Destination selectors to update the task for your additional Mac.

Also, note that CCC's keychain is not transferrable between Macs. If you migrate CCC tasks to a new Mac, you will have to re-supply CCC with any applicable volume, disk image, or SMTP passwords.

Recovering tasks from a backup

Many people find that "cleaner" applications will aggressively remove CCC's tasks and preferences. If you have lost all of your backup tasks but you have a full backup of your startup disk, you can recover your tasks from the backup with these steps:

1. Open CCC.
2. Click **Settings** in the toolbar to open CCC's Settings window.
3. Click **DB Diagnostics** in the Settings window toolbar.
4. Click the **Restore...** button at the bottom of the window
5. In the Open panel, navigate to **{your backup disk}** > /Library/Application Support
6. Select the folder named **com.bombich.ccc**.
7. Click the **Open** button.
8. Your tasks should now be restored.

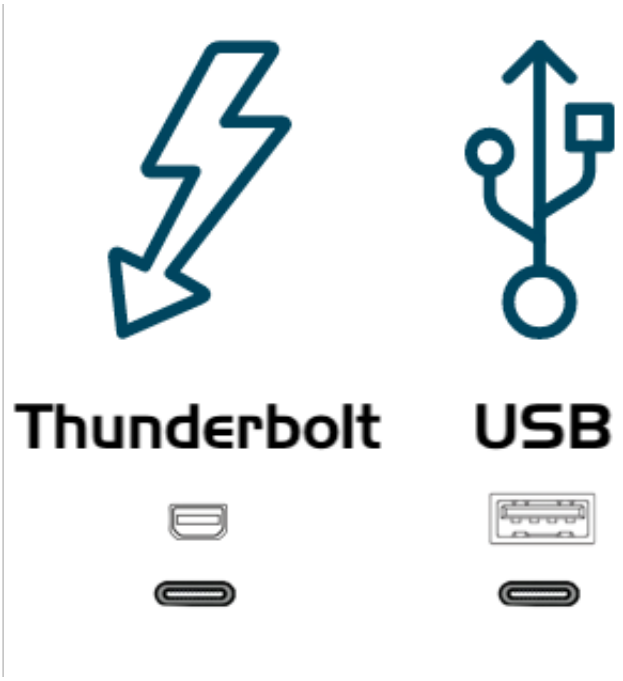
Note that you may have to activate suspended tasks, and/or reselect the source or destination volumes in your tasks.

Please note that you must locate the com.bombich.ccc application support folder that is located in the **root-level** Library folder (e.g. Macintosh HD > Library, NOT Macintosh HD > Users > USER_NAME > Library). **If you're looking in your home folder, you're in the wrong place.**

Getting Ready to Use CCC

Choosing a backup drive

USB, Thunderbolt?



Many hard drive enclosures have USB or Thunderbolt or a combination of interfaces for connecting the hard drive to your computer. Any of these interfaces will work fine for backing up and safeguarding your data. **We generally recommend purchasing an enclosure that offers multiple interface options (e.g. Thunderbolt+USB).**

How big should the backup volume be?

The backup volume should be at least as large as the amount of data that you want to copy to it. If you're planning to make regular backups to this volume, a good rule of thumb is that the backup volume should be at least twice as large as the amount of data that you're initially backing up to it. This allows for a modest amount of data growth and room for backup history (i.e. snapshots).

Specific storage device recommendations

Most external storage devices will work just fine for your backups, however performance and reliability vary. It would be impossible for us to curate an exhaustive list of every device, but we frequently get asked for a recommendation, so here's a list of some storage devices that we have tested with good results. Performance and price go hand-in-hand, we recommend that you avoid the cheapest devices.

USB 3.1/3.2 Portable External SSD

These devices offer a moderate amount of storage and excellent performance. This is our top pick for a backup device:

Oyen Helix NVMe USB-C (250GB-2TB) <https://amzn.to/2MdGemO>

Samsung T5 Portable SSD (1TB & 2 TB) <https://www.amazon.com/Samsung-T5-Portable-SSD-MU-PA1T0B/dp/B073H552FJ/ref=as_li_qf_asin_il_tl?ie=UTF8&tag=bombich>
Samsung T7 Portable SSD (1TB & 2 TB) <https://www.amazon.com/SAMSUNG-Portable-SSD-2TB-MU-PC2T0H/dp/B0874YJP92/ref=as_li_qf_asin_il_tl?ie=UTF8&tag=bombich>†

† We do not recommend the Samsung T7 "Touch" model. The "touch" functionality uses a proprietary locking mechanism that requires Samsung drivers, and comes with a 27-34% price premium. This mechanism is not comparable to FileVault; CCC cannot automatically unlock these devices. The non-touch model provides the same functionality as far as a backup device is concerned, and can be encrypted easily with native macOS Encryption. In general, we do not recommend installing the third-party drivers or software that comes with an external storage device, we frequently see more trouble than benefit from that software.

USB 3.1, Desktop External Hard Drive (mechanical drive)

Oyen Novus External USB-C Rugged Desktop Hard Drive (2TB-16TB) <https://amzn.to/2YroF40>

Thunderbolt, Desktop External Hard Drive Enclosure (without a disk)

Oyen Novus External USB-C Rugged Desktop Hard Drive Enclosure <https://amzn.to/2GPwNE1>

USB 3.1, External Enclosure (without a disk)

Oyen Digital MiniPro 2.5" SATA to USB-C External Hard Drive/SSD Enclosure <https://amzn.to/3tLioEG>

Bare mechanical drive (SATA 3.5") 500GB - 6 TB

These drives are "bare" and will need an enclosure or dock to be used externally:

WD Black Performance Internal Hard Drive - 7200 RPM Class, SATA 6 Gb/s, 256 MB Cache, 3.5" <https://www.amazon.com/Black-4TB-Performance-Hard-Drive/dp/B00FJRS6FU/&tag=bombich-20&creative=9325&linkCode=as2&creativeASIN=B07G3LYX3M&linkId=0561481c219dc81a5c076d88092b4ffa>

Not Recommended

Avoid disks that use Shingled Magnetic Recording

Many years ago Seagate introduced Shingled Magnetic Recording <https://en.wikipedia.org/wiki/Shingled_magnetic_recording> to increase the storage capacity of rotational hard drives, but at the expense of writing performance. We anticipate considerably worse performance for APFS in particular on these devices. Many vendors have not been particularly forthright about the use of SMR in their devices until recently. Some† devices that leverage SMR include:

- These Seagate disks <https://www.seagate.com/internal-hard-drives/cmr-smr-list/>
- These Western Digital disks <https://blog.westerndigital.com/wp-content/uploads/2020/04/2020_04_22_WD_SMR_SKUs_1Slide.pdf>
- These Toshiba disks <https://toshiba.semicon-storage.com/ap-en/company/news/news-topics/2020/04/storage-20200428-1.html>

† This is far from an exhaustive list. None of these manufacturers documents whether the disks in their branded enclosures are using SMR. Due to this lack of transparency and based on experience with these devices, we recommend that you avoid branded external storage *enclosures* from

Seagate, Western Digital and Toshiba. Please bear in mind that this recommendation is specific to the branded **enclosures**. Many Western Digital bare hard drives, for example, have excellent specs and we recommend them above.

Avoid 5400RPM Rotational HDDs, aka "Slim", "Portable" or 2.5" hard drives

These disks are cheap and can be acquired by the pallet at your local consumer warehouse. Unfortunately, these disks are really slow! Here are a few examples of these slower devices:

- Seagate Backup Plus Slim Portable Drive
- Seagate Ultra Portable Drive
- Western Digital My Passport Ultra Portable
- Western Digital easystore
- Western Digital Elements
- LaCie Mobile Drive
- G-Technology G-DRIVE Mobile USB 3.0 Portable External Hard Drive

These devices can be acceptable for use as a backup disk if you already own one, but **you should expect poorer performance from these cheaper devices**. If you're shopping for a new backup disk, we recommend that you avoid these disks altogether.

USB "Thumb" drives and SD cards:

Despite being based on flash storage, which you'd think would be faster than rotational storage, USB thumb drives and SD cards are often quite slow. We don't recommend using these devices for backing up any substantive amount of data, these are usually only useful for ad hoc file sharing between computers. Flash-based memory like that used in SD cards and thumb drives also has limited write/erase cycles that are much lower than that of a traditional SSD or mechanical hard drive making them not appropriate as a primary backup device.

Backing up to Network Attached Storage (NAS)

NAS devices are very trendy these days; many people find the convenience of a wireless backup to be alluring. Based on user feedback, however, we discourage people from relying on NAS devices for their primary backup for several reasons:

- Write performance to a NAS device is typically, at best, comparable to writing to a USB 2.0 HDD
- Performance of a NAS accessed via WiFi can be 10-100 times slower than the average locally-attached hard drive
- Periodically validating the integrity of data on a NAS device may be impractical due to network performance.
- WiFi backups are only as reliable as the network connection and macOS's network filesystem client
- Filesystem transactions on a network filesystem incur a lot more overhead than filesystem transactions on a locally-attached filesystem, leading to very long backup windows when your data set has lots of files (e.g. > 250K files)
- Disk image files can eventually become corrupted if frequent network connectivity loss occurs while they are mounted, or when free space on the underlying NAS volume becomes constrained. If you've seen a recommendation from Time Machine to delete and recreate the backup on a network volume, that's the same underlying issue, and we'd make the same suggestion if the disk image can't be mounted.

For primary backups, we recommend that you procure a USB or Thunderbolt hard drive and create a backup on that locally-attached disk.

NAS devices that we specifically do not recommend

Western Digital MyCloud Home: The "Home" model of this NAS device requires the use of WD-proprietary software to access the storage securely; direct access to the storage via SMB is only available with Guest privileges. Users report <https://community.wd.com/t/use-my-cloud-home-with-finder-without-wds-app/216769/4> that performance of the storage while using WD's software is subpar in comparison to Guest access via SMB, and other users have reported to us that macOS is unable to create or mount disk images on the storage when mounted via Western Digital's software.

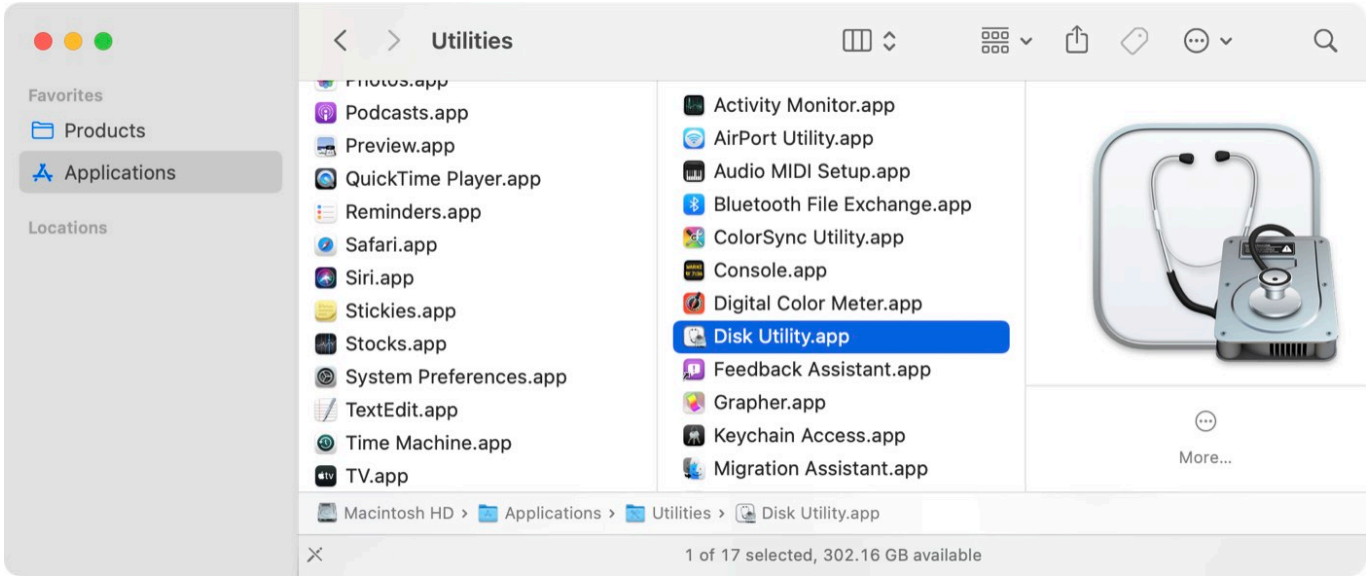
Preparing a disk for a backup or restore

Note: This will erase all data on the specified disk

Watch a video of this tutorial on YouTube <https://youtu.be/5mBO3o570Ak>

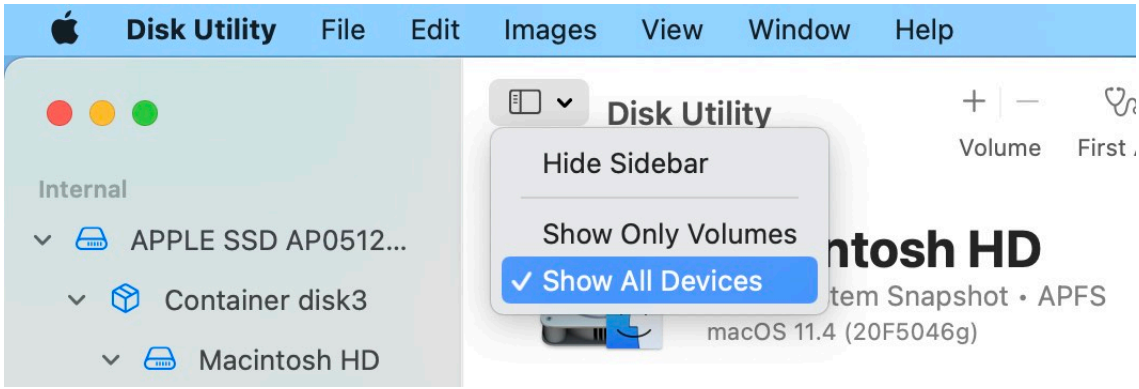
Launch Apple's Disk Utility

Open a Finder window and navigate to **Applications > Utilities** and double click on **Disk Utility.**



Show All Devices

Disk Utility offers a very simplified view of your devices by default. Unfortunately, this hides the devices that you need to select to modify the partitioning of your backup disk. Before doing anything else in Disk Utility, choose **Show All Devices** from the View menu, or from the View popup button in Disk Utility's toolbar.



Select the destination disk

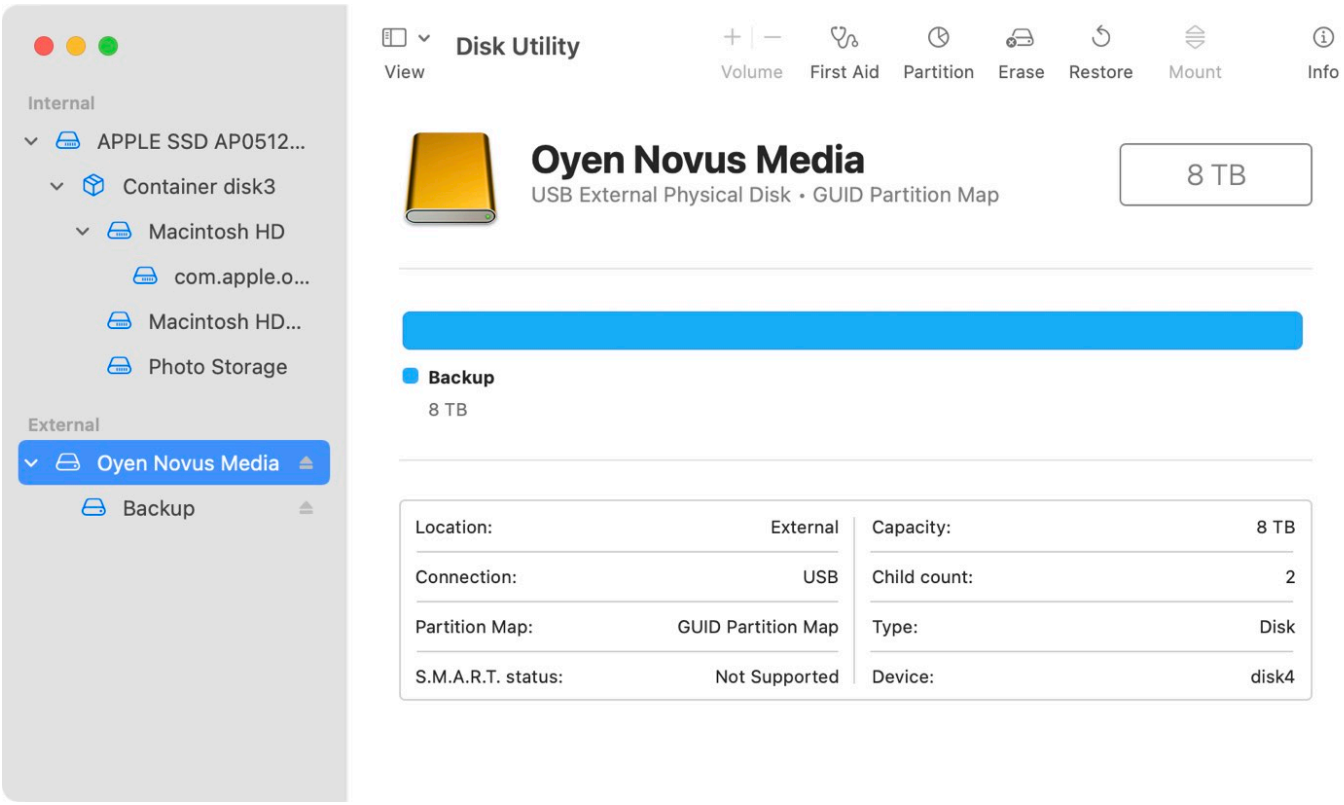
Click to select the disk that you would like to use as the destination for your CCC backup or restore task.

If you're erasing the internal storage on your Mac for a restore procedure

Select the "Macintosh HD" volume. Don't erase the whole internal device, that can make the restore procedure take longer. When you erase this volume, choose the **Erase Volume Group** option when prompted by Disk Utility.

If you're erasing a backup disk

The name of a new disk will often include the manufacturer's name (e.g. WD My Book 111D Media...). Please pay particular attention to selecting the **disk**, not one of the volumes on the disk. You must select the whole disk to correctly initialize the device.



Unmount any volumes on the specified disk

Disk Utility occasionally has problems with unmounting a volume while attempting to erase it (e.g. because Spotlight prevents the unmount request). Click the Eject button next to any volumes on the disk to preemptively unmount them before erasing the disk.

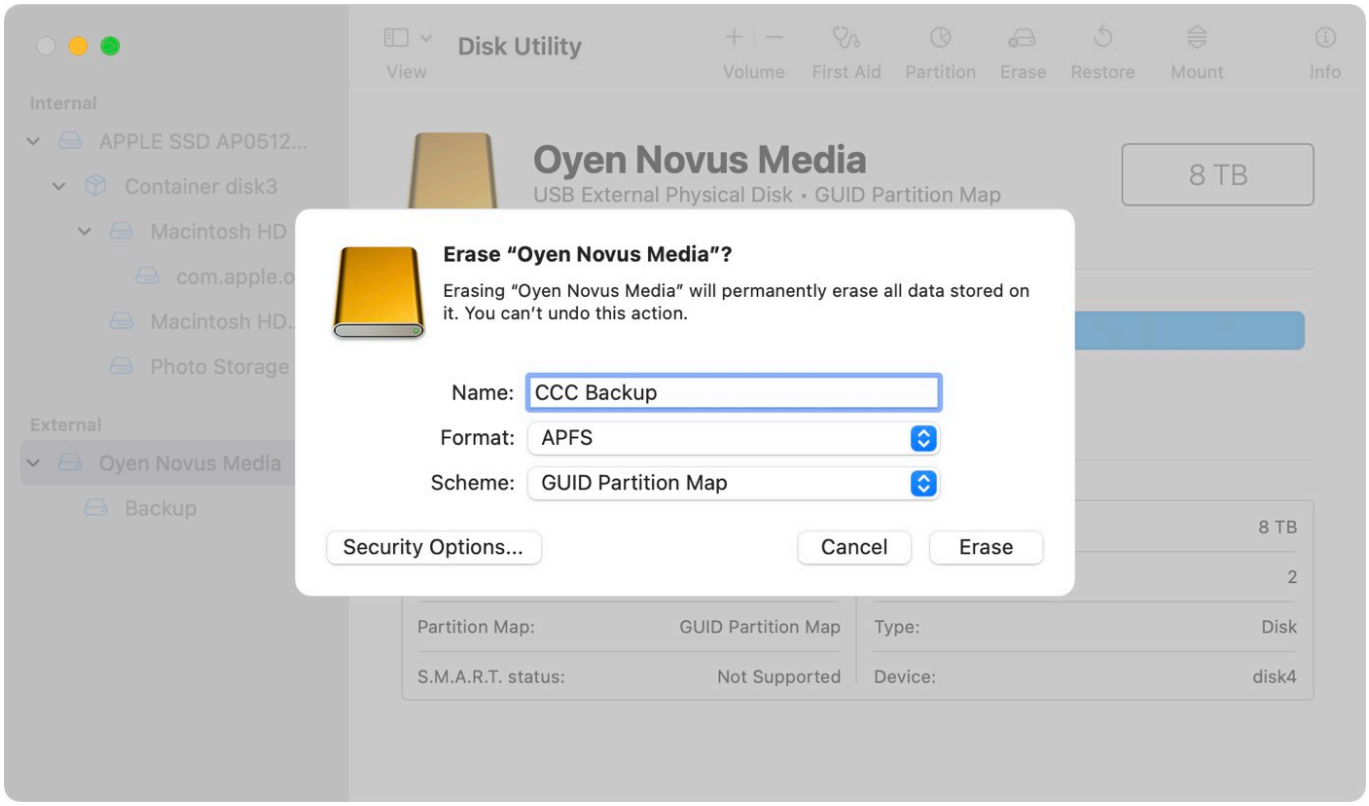
Erase the specified disk

Click the **Erase** button in Disk Utility's toolbar, then configure the name, format, and partitioning scheme of your disk. You can set the name to whatever you like, but when formatting a backup disk, set the Scheme to **GUID Partition Map**. If you do not see the **Scheme** option (and you're erasing an external storage device), go back two steps and select the whole disk device, not one of the volumes on the disk.

Choosing a Format for your destination volume

Choose **APFS** or **APFS Encrypted**. If you intend to create a legacy bootable backup <https://bombich.com/kb/ccc6/cloning-macos-system-volumes-apple-software-restore>, **do not choose APFS Encrypted**; rather you will encrypt your backup by enabling FileVault while booted from the backup volume <https://bombich.com/kb/ccc6/working-filevault-encryption>.

Click the **Erase** button when you are finished configuring the name, format, and partition scheme for your destination. If you are given an **Erase Volume Group** choice, choose that option to erase the whole volume group.



Add a partition (optional)

If you're backing up multiple source volumes to this same backup disk, you can keep things organized by creating partitions. If you formatted your backup volume as APFS, select the volume and choose "Add APFS volume..." from Disk Utility's Edit menu. If you chose another format, select the backup volume, then click the "Partition" button in Disk Utility's toolbar.

Don't Use Time Machine

When you're prompted to use your new volume with Time Machine, click **Don't Use.** You may use the same backup disk for both Time Machine and CCC backups, but if you do so, you must use a dedicated partition for the Time Machine backup (not simply an additional volume in the APFS container). Otherwise Time Machine will consume all available space on the backup volume and make it impossible for CCC to use the backup volume.

Your new hard drive is now ready for CCC!

Related Documentation

- Support for third party filesystems (e.g. NTFS, FAT32) <https://bombich.com/kb/ccc6/backing-up-tofrom-network-volumes-and-other-non-hfs-volumes>

Everything you need to know about CCC and APFS

What's a filesystem?

The file system is perhaps the most important piece of software on your Mac. It’s also one of the most transparent, at least when it’s working correctly. Every user and every application uses the file system. The file system keeps track of and organizes all of the files on the hard drive, and also determines which users and applications have access to those files. The file system also keeps track of how many files you have and how much space they consume. Every time you look for a file, open a file, move a file, save a file or delete a file, it's the filesystem that is fulfilling that action.

Does CCC support encrypted APFS volumes?

Yes, CCC can backup to and from encrypted APFS volumes (aka FileVault encryption). Note that CCC doesn't play any role in the encryption process – encryption is a function of the volume, not of the tool that's writing a file. If you enable FileVault on your startup disk, then the files on your startup disk will be encrypted. Those files are decrypted on-the-fly by the filesystem when they're opened by an application. Likewise, if you enable FileVault on the destination volume (e.g. via the Security Preference Pane while booted from the backup), then the files on the destination will be encrypted. CCC doesn't have to encrypt those files, they're encrypted on-the-fly by the filesystem as the bits are written to disk.

I heard that APFS has a "cloning" feature. Is that the same as what CCC is doing?

No, the cloning functionality within APFS is completely unrelated to the copying that CCC performs, although in some cases CCC does leverage the APFS file cloning functionality.

APFS cloning allows the user to instantly create copies of files **on the same volume** without consuming extra storage space. When cloning a file, the file system doesn’t create copies of the data, rather it creates a second reference to the file that can be modified independently of the first file. The two files will share storage on the disk for portions of the files that remain identical, but changes to either file will be written to different parts of the disk. APFS file cloning only works when you make copies of a file on the same volume (e.g. duplicate a file or folder in the Finder). CCC is typically copying files **between** volumes, so APFS cloning isn't applicable for that kind of task. In some cases CCC may clone a file on the destination prior to updating its contents.

The important take-away is that APFS file cloning can save you space on your startup disk, but CCC backups can save your data if your source disk fails. They serve completely different purposes; APFS file cloning is not at all related to making backups.

Why doesn't the disk usage on my backup disk match the disk usage on the source disk?

CCC's global exclusions <https://bombich.com/kb/ccc6/some-files-and-folders-are-automatically-excluded-from-backup-task> as well as the SafetyNet feature have traditionally led to legitimate differences in disk usage in the past. The aforementioned APFS file cloning feature, however, adds a new dimension to this concern. While APFS file cloning saves space on your source volume, those space savings can't be consistently applied when copying your files to another volume. Making matters worse, Finder does not accurately represent the true disk usage of your files <https://youtu.be/KggyuL8mED0>. Finder doesn't take into consideration whether one file is a clone of another, rather it sums up the total size of each file and folder, presenting a total value that is possibly astronomically higher than the capacity of the disk.

The disk usage on your source and destination may never add up, and therefore may not be a reliable measure for comparing the source and destination.

Related Documentation

- Comparing the source and destination <https://bombich.com/kb/ccc6/comparing-source-and-destination>

Additional Resources

- Preparing your destination disk for a backup or restore <https://bombich.com/kb/ccc6/preparing-your-backup-disk-backup-os-x>
- Video: Setting up your first backup with CCC 6 <https://youtu.be/5mBO3o570Ak>
- How to verify a backup <https://bombich.com/kb/ccc6/how-verify-or-test-your-backup>

We're here to help

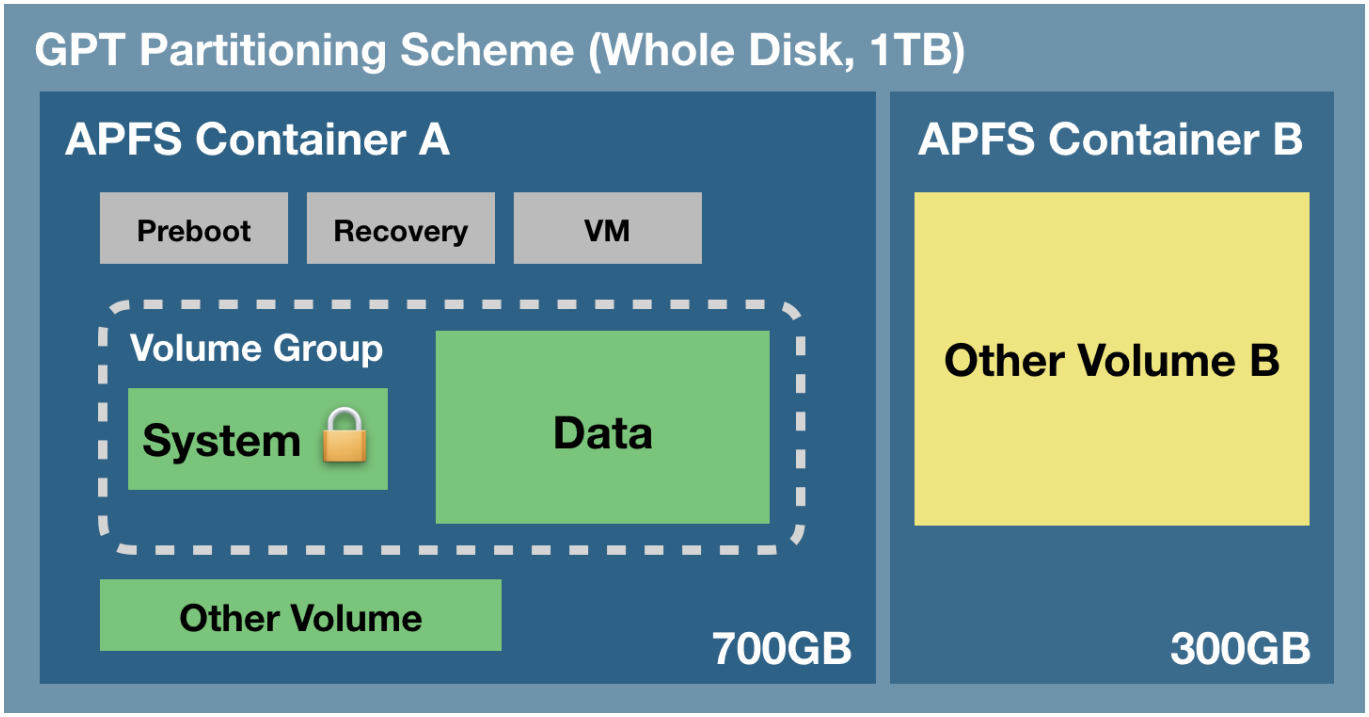
If you get stuck or need some advice, you can get help right from within CCC. Choose "Ask a question" from CCC's Help menu to pose a question to our Help Desk.

Working with APFS Volume Groups

When Apple introduced the APFS filesystem, it came with a new concept: the APFS **container**. All APFS volumes reside within a container, and the container resides within the disk's partitioning scheme. All volumes within a container share the space that is available to the container; separate APFS containers do not share space with each other.

In macOS High Sierra, Apple added the concept of **roles** to volumes. At the time there were only three roles, and these went largely unnoticed by the average user: Preboot, Recovery, and VM (virtual memory). These roles allow the system to identify specific volumes for specific purposes, and then treat the volumes in specific ways (for example, any volume with the above roles would be hidden by default and also not mounted by default).

The following graphic demonstrates a few of these APFS concepts:



The partitioning scheme encompasses the entire physical disk. Within the partitioning scheme you can create one or more APFS containers, and within each container, you can create one or more APFS volumes. Unlike partitioning in the past, all of the volumes within the container share the space that is allocated to the container. In the example above, the three gray helper partitions, the System and Data volumes, and the "Other Volume" all have access to that 700GB chunk of storage. "Other Volume B" is in a separate container, though, and does not share space with the volumes in container "A". Normally a disk would not be partitioned in this manner, but it would be warranted, for example, if you wanted to maintain a backup of your startup disk on that same disk (e.g. for testing purposes by developers).

New concept: APFS Volume Groups

In macOS Catalina, Apple introduced another new concept to the APFS filesystem: **volume groups**. This is more of a conceptual grouping of volumes within an APFS container, not a new sub-structure. Apple also greatly expanded the number of roles available for APFS volumes (now there are 16

unique roles). When you upgrade to Catalina, your current macOS system volume is renamed, e.g. to "Macintosh HD - Data", its role is set to **Data**, and then a new volume is added to your startup disk's APFS container with the **System** role and simultaneously grouped with the Data volume. The two volumes within that group share special bonds and receive special treatment from the Finder and from each volume's filesystem. From the user perspective, these two volumes are treated as a single, unified volume. If you take a look at Disk Utility, however, you'll see the two volumes as distinct, separate items.

The Read-only System volume

Perhaps the single, largest change in macOS Catalina is the manner in which the System volume is mounted on startup – it's **read-only**. By mounting the volume read-only, it becomes impossible for attackers to make changes to the content of the macOS System volume. That doesn't mean that your Mac is 100% free from all possible attack vectors, rather it's just another line of defense against them.

In macOS Big Sur, Apple expanded on the protection of the System volume with the introduction of a cryptographically sealed "Signed System Volume" <https://developer.apple.com/news/?id=3xpv8r2m>. The System volume is no longer mounted **at all** on startup, rather a snapshot of the System volume is mounted and used as the startup disk. The snapshot is read-only and completely immutable.

The Data volume

You can think of the Data volume as a read-write "shadow" of the System volume. The Data volume contains all of your user data (e.g. your home folder, third-party applications), but also contains a handful of system components that can't reside on a read-only volume. For example, Apple has placed Safari on the Data volume, perhaps so it can be updated more frequently. The current startup disk's Data volume is mounted at a special mountpoint on the system. You can find it if you navigate in the Finder to Macintosh HD > System > Volumes > {Data volume name}. What you'll find there is a replica of the System volume's root-level folders. Within these folders are all of the system components that are still writable. Normally you won't see these items in the Finder, though, because the Finder visually mashes the content of the two volumes together to make them appear as a single volume. Also, the Finder won't list your Data volume alongside all of your other volumes – **the Data volume is mounted but hidden**.

Building bonds with firmlinks

To pull off the illusion of a single, unified volume, Apple added support to APFS for **firmlinks**. Like the name implies, a firmlink lies conceptually between a soft link and a hard link. That probably doesn't make them any more clear though (even for people familiar with soft and hard links!). A firmlink is described by Apple as a "bi-directional wormhole" between two filesystems. Let's take a look at the "Users" folder as an example – the Users folder at the root level of the System volume is actually a firmlink that points to the Users folder at the root level of the Data volume. If you attempt to navigate to the /Users folder on the System volume, you're actually going to see the content of the /Users folder on the Data volume. Likewise, suppose you're looking at a folder on your Desktop (so you're looking at the contents of the Data volume) and then you navigate upwards several levels. When you get to the parent of the "Users" folder, you're no longer looking at the Data volume, rather that firmlink has transported you back to the root level of the System volume.

There are about a couple dozen firmlinks on macOS Catalina that link various folders on the System volume to writable counterparts on the Data volume. If you're curious about these, you can find a complete list of firmlinks at /usr/share/firmlinks on your startup disk.

Finder shenanigans with the Applications folder

Firmlinks are mostly transparent, but there is one really noticeable exception: the Applications folder. The Applications folder at the root level of the System volume is a firmlink to the Applications folder at the root level of the Data volume. However, many Applications are not actually stored in the writable Applications folder on the Data volume. The Finder applies some magic here. The read-only System Applications folder actually resides at System > Applications on the System volume, and when you open the Applications folder in the Finder, you'll see the aggregation of that folder and the Data volume's root-level Applications folder (where all of **your** applications reside). To the average user, this is exactly what you expect to see, and that's great. However, you may notice that this same aggregation is not applied to other system volumes that your Mac is not currently booted from (e.g. a Catalina backup, or a legacy bootable copy of Big Sur or Monterey <https://bombich.com/kb/ccc6/cloning-macos-system-volumes-apple-software-restore>). On those volumes, if you open the root-level Applications folder on the visible System volume, you'll only see the content of the firmlink to the root-level Applications folder on the Data volume (i.e. no Apple applications, just your third-party applications and Safari). In those cases, you'll find the Apple System applications at System > Applications.

Related Documentation

- What will CCC do to my backup disk when I run it for the first time? <https://bombich.com/kb/ccc6/frequently-asked-questions-about-ccc-and-macos-catalina#convert>
- Will my encrypted backup volume be automatically converted to an APFS volume group? <https://bombich.com/kb/ccc6/frequently-asked-questions-about-ccc-and-macos-catalina#conversion_encrypted>
- Frequently asked questions about CCC and macOS Catalina <https://bombich.com/kb/ccc6/frequently-asked-questions-about-ccc-and-macos-catalina>
- Working with FileVault Encryption <https://bombich.com/kb/ccc6/working-filevault-encryption>
- Frequently Asked Questions about encrypting the backup volume <https://bombich.com/kb/ccc6/frequently-asked-questions-about-encrypting-backup-volume>
- Everything you need to know about CCC and APFS <https://bombich.com/kb/ccc6/everything-you-need-know-about-carbon-copy-cloner-and-apfs>

Best practices for upgrading your Mac's OS

If you're already running the newest macOS and you're having trouble opening CCC, be sure to download the latest version of CCC <https://bombich.com/software/download_ccc.php?v=latest>.

So Apple has shipped the next major operating system, and you're excited to upgrade! But are you ready? OS upgrades purport to offer new features, better performance and bug fixes, but they can come at a price — your time and potentially your productivity. If you upgrade your OS only to discover that a critical third-party application or peripheral doesn't work right, you could be really lost when you discover that **Apple doesn't support downgrading to a previous OS**. Downgrading is not an impossible task if you made a CCC backup prior to the upgrade, but it is a long procedure that may be too complicated for many users.

Should I upgrade my Mac?

Major system upgrades are often disruptive, so we have always recommended a very conservative approach to applying them. Consider the following:

- Is the upgrade required for my Mac?
- Does the upgrade offer any compelling features?
- Will this upgrade improve the performance of my Mac, or degrade performance?
- Does the upgrade fix a problem that is preventing me from effectively using my Mac?
- What software will no longer work after applying the upgrade?
- Does the application of this upgrade to my aging Mac hasten its obsolescence?

If the upgrade turns out poorly and you have to downgrade, you certainly may downgrade using a CCC backup from an earlier OS <https://bombich.com/kb/ccc6/best-practices-updating-your-macs-os#downgrade>. These sorts of procedures require time and effort, though, so you should weigh that potential hassle against the potential gain of the OS upgrade.

Lastly, we recommend that any users that rely heavily upon the availability of their Mac for work or other productivity consider waiting for several OS updates before making a major upgrade. The early releases are exciting, but that excitement involves risk. Early adopters inevitably find some shortcomings and bugs which are resolved in minor OS updates.

Can I test the new OS before committing to it on my Mac's production startup disk?

Yes! Especially if you have lots of software that could be rendered unusable on the new OS, it's a great idea to test the new OS with your data in a manner that doesn't require a commitment on your production startup disk <https://bombich.com/kb/ccc6/glossary-terms#p>.

Do not use your production CCC backup <https://bombich.com/kb/ccc6/glossary-terms#p> for this procedure. This procedure will erase any backup history (e.g. snapshots) on the volume that you use. We recommend that you acquire an external hard drive, ideally an SSD, that has enough capacity to fit all of the data that is on your current production startup disk. See this CCC Kbase article for some recommendations <https://bombich.com/kb/ccc6/how-set-up-your-first-backup>.

1. Prepare the new device for making a backup <https://bombich.com/kb/ccc6/preparing-your-

backup-disk-backup-os-x>.
2. Click "New Task" in CCC's toolbar to create a new task.
3. Choose your startup disk in the Source selector.
4. Choose your backup volume in the Destination selector.
5. Click the Start button. When the backup procedure is complete, the destination will have a copy of all of your applications, user data and system settings.
6. Open the macOS Installer (e.g. for the newer OS that you want to test).
7. Click "Show all disks", then proceed to install the new OS onto the new external disk.

When the installation is complete, your Mac will boot from the external disk automatically, and all of your user data and applications will be "adopted" by the new OS. Open your apps, kick the tires, etc.

When you're done testing, reset the startup disk to your Mac's internal disk and reboot. You can then erase the new external disk and use it for some other purpose. If you're happy with how the new OS was working on the external test device, you can proceed to install it onto your Mac's production startup volume. If not, simply stick with the OS that you're currently running.

Make a CCC backup before upgrading

If you've read this far and you've decided to proceed with upgrading your Mac's production startup disk, the first thing you should do is make a backup of your Mac with CCC.

1. Get a backup disk. If you would like a recommendation, we offer some here in CCC's documentation <https://bombich.com/kb/ccc6/how-set-up-your-first-backup>.
2. Prepare your backup volume for the backup <https://bombich.com/kb/ccc6/preparing-your-backup-disk-backup-os-x>.
3. Download CCC <https://bombich.com/software/download_ccc> and open it.
4. Choose your startup disk in the Source selector.
5. Choose your backup volume in the Destination selector.
6. Intel Mac running Big Sur+ (optional)†: Click on the Destination selector and choose "Legacy Bootable Copy Assistant", then click the button to allow CCC to erase the destination.
7. Click the Start button.
8. **Detach your backup disk from your Mac and set it aside**. Until you are ready to commit to the newer OS, you don't want the backup disk to be upgraded automatically by a scheduled backup task.

† Should I make a bootable backup?

Downgrading from a bootable backup requires fewer steps, but the reliability of Apple's External Boot solution has waned in the past several years. Having a bootable backup gives you an additional recovery option, but you can downgrade your Mac from a CCC backup whether that backup is bootable or not. The important thing to do is make the backup **before** you upgrade, and understand your downgrade options before proceeding with the upgrade. **Apple Silicon Macs**: You can make a bootable backup on these Macs as well, but the Mac's behavior while attempting to boot from an external device (backup or fresh macOS install) is pretty frustrating after you have erased the internal disk. We recommend the standard recovery procedure to downgrade an Apple Silicon Mac.

Upgrade to the new OS

Download the newest OS from the Mac App Store and apply the upgrade.

Make sure everything is working... then resume your backups

Take some time to run the applications that are most important to you. Keep in mind that when you

open an Apple application (e.g. Mail, Photos, etc.) on the newer OS, those applications will immediately and irreversibly upgrade the user data for those applications. If you decide later that you want to downgrade, you cannot simply reinstall Big Sur (for example), then go about your day with the upgraded user data; the Big Sur versions of those Apple applications can't use the upgraded data from Monterey. **If you need to downgrade to a previous OS, it is imperative that you have a CCC backup of your Mac as it was prior to the upgrade.**

If, after a week or so you decide that everything is copacetic and you are ready to commit to the new operating system, attach your backup disk to your Mac, open CCC and re-run your backup task with the same settings. This is an important step — once the backup task has completed, you will no longer be able to use the backup to downgrade to the previous OS.

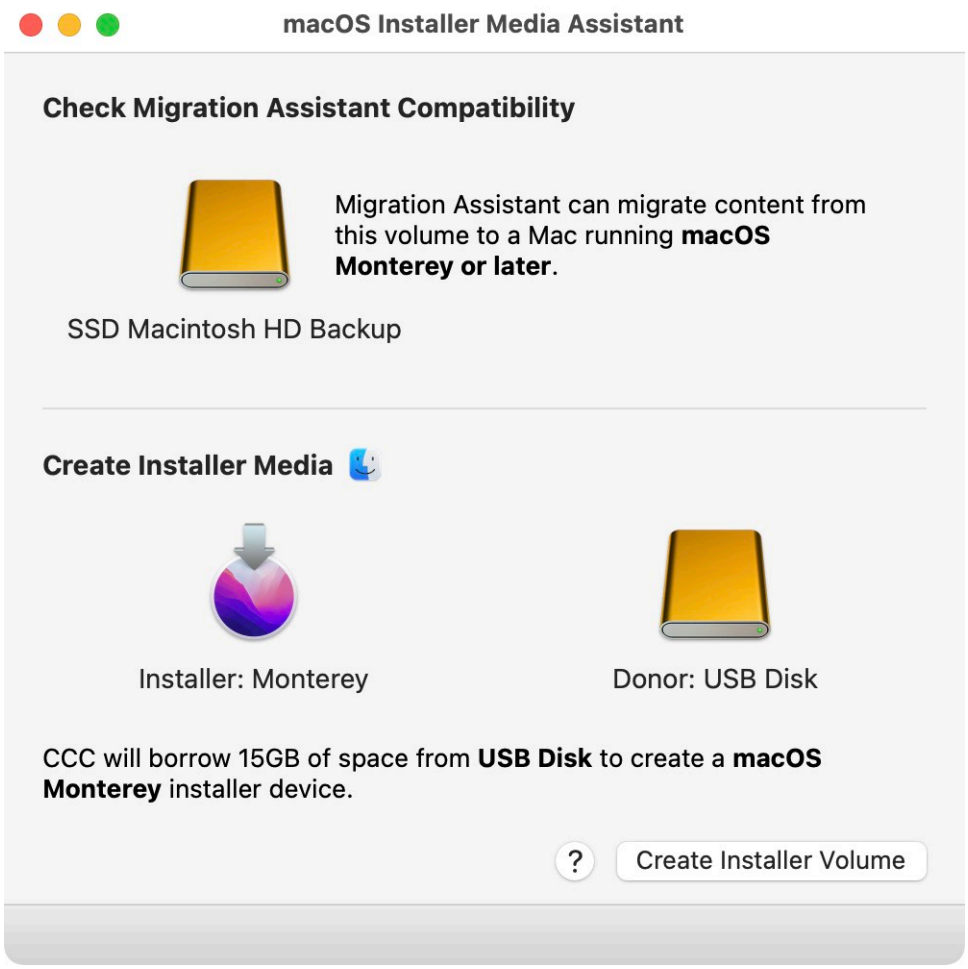
Downgrading your Mac with a CCC backup

Downgrading your Mac's OS with CCC <https://youtu.be/mid5869tdNI>

Note: If you created or modified any documents while the system was running the newer operating system, the older versions of your files will be restored. Unfortunately, your personal data created by **Apple applications (e.g. Mail, Photos, etc.)** while using the newer OS will be incompatible with an older OS <https://bombich.com/images/blog/newer_photos_library_not_backwards_compatible.png>, so it is not possible to restore changes that were made while you were using the newer OS.

Downgrading with a Standard Backup

CCC's macOS Installer Media Assistant will help you navigate the more complicated steps of downgrading your OS. CCC's macOS Installer Media Assistant is available to CCC v6 license holders.



1. Open CCC. If you have any tasks configured to run on a schedule, or automatically when the backup disk is attached, right-click on those tasks in CCC's sidebar and choose the option to disable them.
2. Attach your backup disk to your Mac.
3. Choose "macOS Installer Media Assistant" from the Utilities menu.
4. Drag your backup volume onto the box at the top of the window to verify compatibility with Migration Assistant.
5. Download a macOS Installer. Click on the macOS/Finder icon for convenient download links.
6. Drag the installer application onto the box indicated in the Installer Media Assistant window.
7. Drag an empty volume with more than 15 GB of free space from a USB or Thunderbolt device onto the "donor volume" box.
8. Click the "Create Installer Volume" button.
9. Restart your Mac while holding down the Option key (Intel Macs) or the Power button (Apple Silicon Macs).
10. Select the installer device as the startup disk and proceed with startup.
11. Open Disk Utility.
12. Choose "Show all devices" from the View menu.
13. Select the parent-level device of your Mac's internal storage in the sidebar.
14. Click the Erase button in the toolbar. Erase the internal disk with the APFS format.
15. [Intel Macs]: Quit Disk Utility.
16. [Apple Silicon Macs]: Proceed when prompted to "fully erase the Mac".
17. [Apple Silicon Macs]: The system will automatically reboot into Recovery Mode and prompt you to activate the Mac. Connect to WiFi or ethernet; the Mac will activate itself.

18. [Apple Silicon Macs]: Shutdown, then boot the system while holding down the Power button.
19. [Apple Silicon Macs]: Select the installer device as the startup disk and proceed with startup.
20. Choose the option to reinstall macOS, then proceed to reinstall macOS on the internal disk of your Mac.
21. When prompted during Setup Assistant, choose the option to migrate data from your CCC backup volume. Proceed as directed by Migration Assistant to migrate data from your CCC backup volume.

Downgrading with a bootable backup

If your CCC backup is bootable, then do the following to restore everything back from your last pre-upgrade backup. *We do not recommend using this procedure for Apple Silicon Macs, please use the procedure above instead.*

1. Restart your Mac while holding down the Option key.
2. Attach your CCC backup disk to your Mac (do not attach your backup disk prior to the first step).
3. Select your CCC bootable backup volume in the Startup Manager and proceed with startup.†
4. Open Disk Utility
5. Unmount the original (upgraded) startup disk.
6. Choose "Show all devices" from the View menu.
7. Select the whole disk device that contains your original startup disk — the **parent** of the "Macintosh HD" volume.
8. Click the Erase button in Disk Utility's toolbar. Erase the internal disk with the APFS format.
9. Open CCC and click the Restore button in the toolbar to create a new Restore task.
10. Select your backup volume from the source selector.
11. Select your original (now empty) internal volume from the destination selector.
12. Big Sur (and later): Click on the Destination selector again and choose "Legacy Bootable Copy Assistant", then click the button to allow CCC to erase the destination.
13. Click the Start button.
14. When the restore process has completed, restart your Mac while holding down the Option key.
15. Select the restored volume in the Startup Manager.
16. When the system has rebooted, reset the startup disk selection in the Startup Disk Preference Pane.

† Intel T2 Mac users: If you're downgrading to Catalina and your bootable backup is encrypted, we recommend using the "Downgrading with a Standard Backup" procedure above instead. See macOS Catalina Known Issues <https://bombich.com/kb/ccc6/macos-catalina-known-issues#t2_vg_fail> for additional context.

"I don't have a pre-upgrade backup, and now I want to downgrade. What can I do?"

Downgrading (to macOS Monterey or later) without a pre-upgrade CCC backup is possible (using the procedure described above), but will not be as successful. There are some items that the older system applications can't read, e.g. Apple Mail, Photos – basically all of the Apple applications won't be able to use the upgraded data stores.

Additional Resources

- Everything you need to know about CCC and APFS <https://bombich.com/kb/ccc6/everything-you-need-know-about-carbon-copy-cloner-and-apfs>
- Preparing your backup volume for an installation of macOS

<https://bombich.com/kb/ccc6/preparing-your-backup-disk-backup-os-x>
- Working with Disk Utility to prepare your CCC backup disk <https://youtu.be/5mBO3o570Ak>
- Testing your CCC backup <https://bombich.com/kb/ccc6/how-verify-or-test-your-backup>

We're here to help

If you get stuck or need some advice, you can get help right from within CCC. Choose "Ask a question" from CCC's Help menu to pose a question to our Help Desk.

Using CCC

How to set up your first backup

Watch a video of this tutorial on YouTube <https://youtu.be/5mBO3o570Ak>

Most first-time CCC users are looking to back up the Macintosh HD "startup disk". We walk through the steps for setting up that first backup task here.

Attach the backup disk to your computer

See the Choosing a backup drive <https://bombich.com/kb/ccc6/choosing-backup-drive> section for additional advice on this subject.

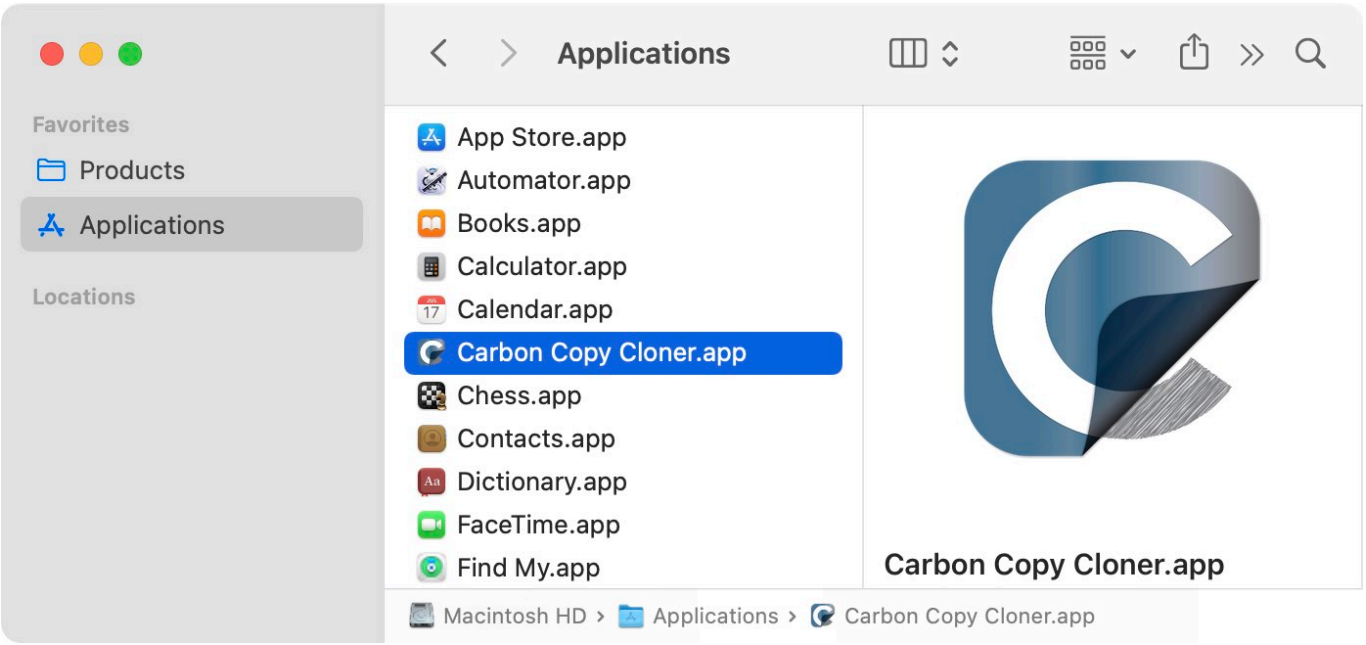
Format the disk

Before you can use a new disk for a backing up your Mac, you must first initialize it with the correct format using Disk Utility.

See the Preparing your destination disk for a backup or restore <https://bombich.com/kb/ccc6/preparing-your-backup-disk-backup-os-x> section of the documentation for step-by-step instructions. You can also watch a video of that tutorial on YouTube <https://youtu.be/5mBO3o570Ak>.

Open CCC

Applications > Carbon Copy Cloner

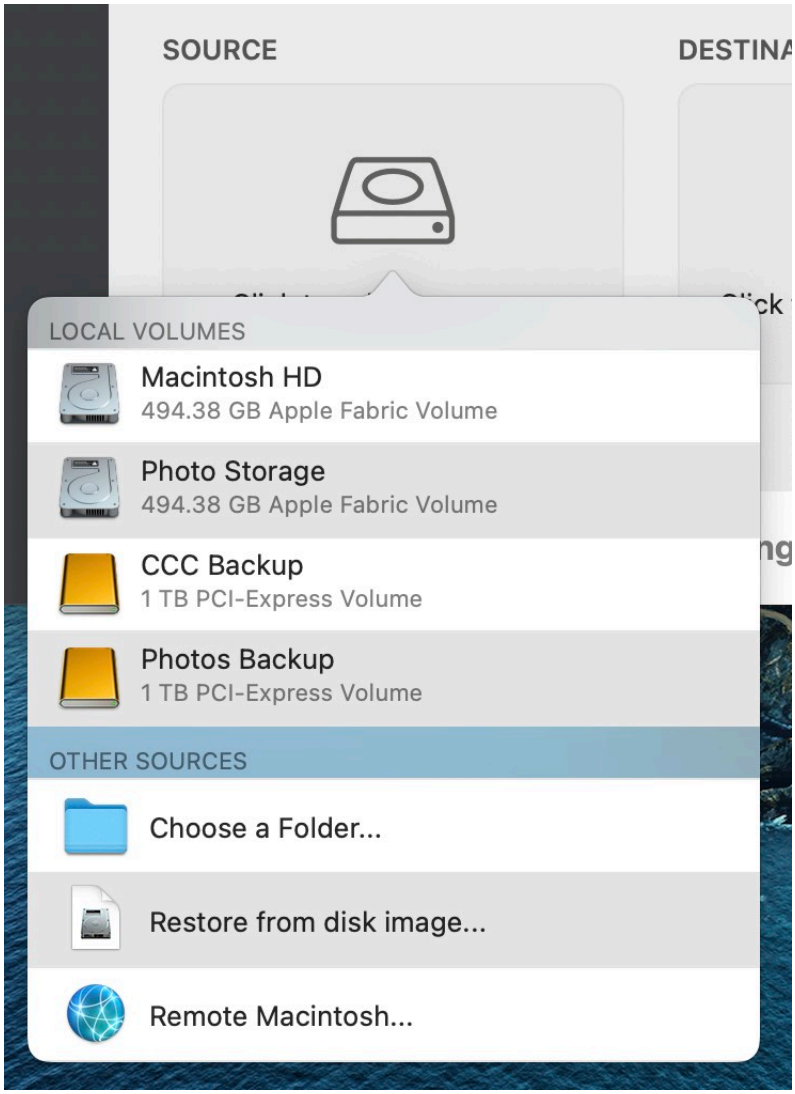


When you open CCC for the first time, you'll be guided through your first task setup. If you prefer to not be guided, click the **Tips** button in CCC's toolbar.

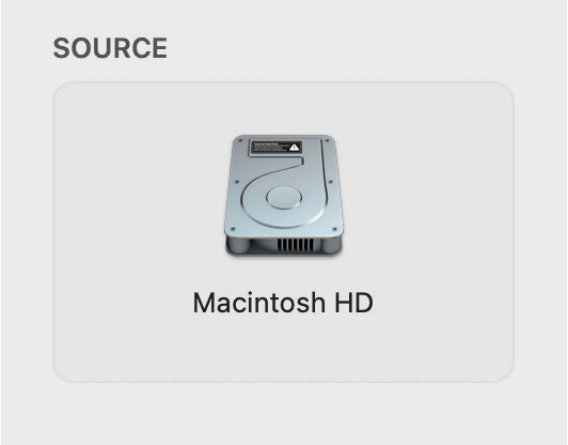
Select the Source

Click in the box under the SOURCE heading to view available sources.

See also: "Do I need to create separate backup tasks for "Macintosh HD" and "Macintosh HD - Data"? <https://bombich.com/kb/ccc6/frequently-asked-questions-about-ccc-and-macos-catalina#separate_tasksCollapse>"

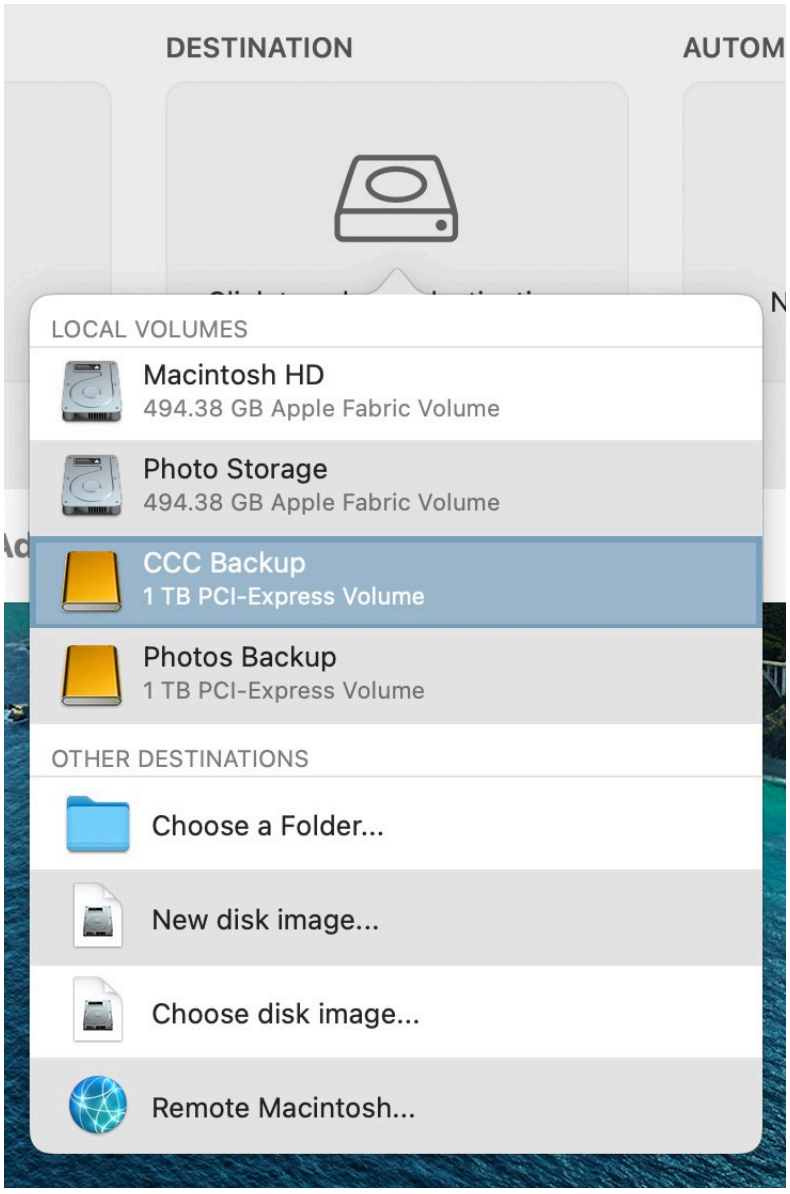


Select your startup disk from the menu of available volumes for the source.



Select the Destination

Click in the box under the DESTINATION heading to view available destinations, then select your new backup drive from the menu of available volumes for the destination.



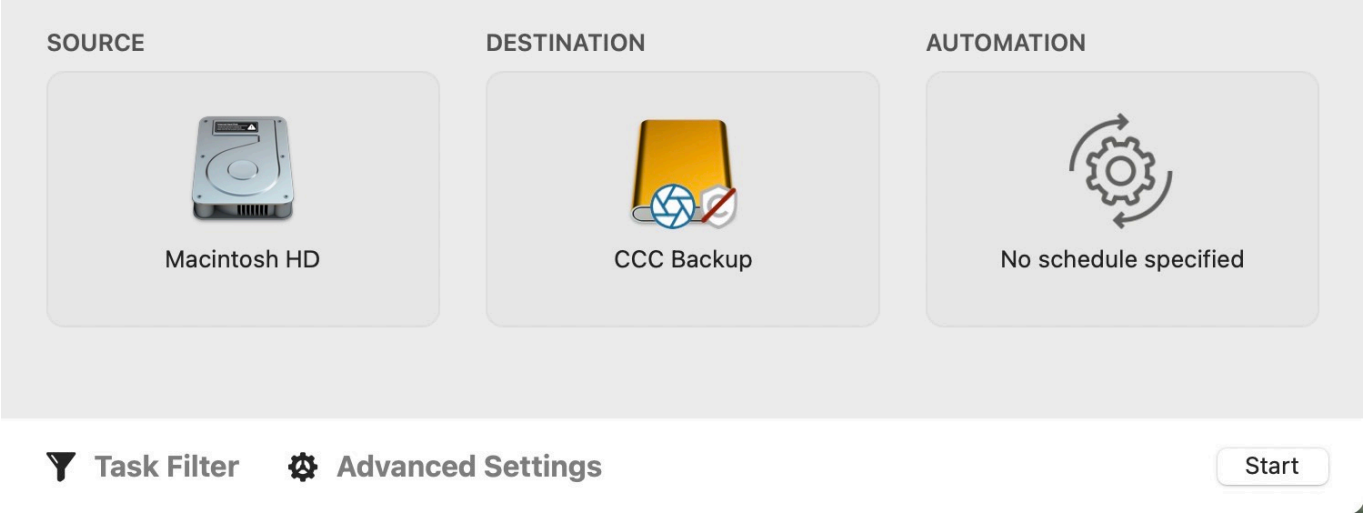
What is the meaning of the badges on the source and destination icons?

You can hover your mouse over those badges for a description of what they indicate. You can also click on these badges to change the associated settings.

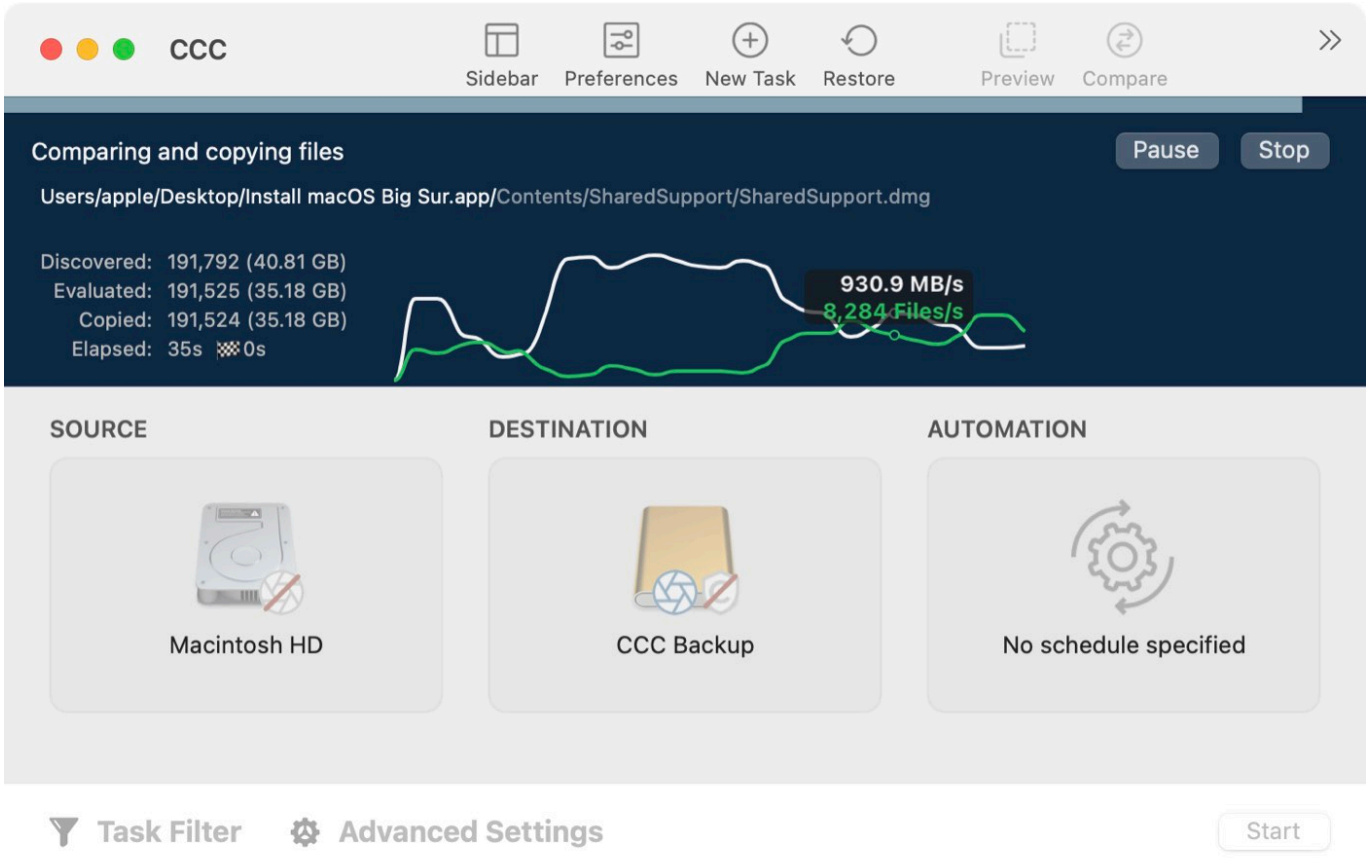
- SafetyNet is enabled [What is SafetyNet? <https://bombich.com/kb/ccc6/protecting-data-already-on-your-destination-volume-carbon-copy-cloner-safetynet>]
- SafetyNet is disabled
- Snapshots are enabled on this volume [What are snapshots? <https://bombich.com/kb/ccc6/leveraging-snapshots-on-apfs-volumes>]
- Snapshots are disabled on this volume

Begin the backup task

Click **Start**. The first time you run a backup task, CCC will prompt you to grant it Full Disk Access, and also to authenticate so it can install its privileged helper tool. This helper tool is required to perform privileged tasks, e.g. to copy system settings and applications.



Congratulations - your first backup is in progress!



Live Performance Chart

As CCC copies your files, you'll see a live performance chart like the one shown in the screenshot above. The white (or blue) line tracks the write rate and the green line tracks the number of files evaluated per second. Hover your mouse over the chart to see the numerical values.

The "Discovered" value indicates how many files CCC has found on the source. "Evaluated" indicates how many of those files have been evaluated to determine if they should be copied. "Copied" is the number of files copied. The estimated amount of time remaining, when available, follows the "Elapsed" value, adjacent to the □□ icon.

Smart Updates

If you run the same backup task again, CCC will copy only the items that have changed. There's no special setting to achieve this behavior, simply click the **Start** button again or configure your backup task to run automatically on a scheduled basis <https://bombich.com/kb/ccc6/how-set-up-scheduled-backup>.

Task icons

CCC uses the following icons to describe tasks in the CCC sidebar:

- This item is a CCC task (task hasn't run, or the last result was dismissed)
- This item is a CCC task group <https://bombich.com/kb/ccc6/task-organization> (group

hasn't run, or the last result was dismissed)

-  **Last event result**: Task completed successfully
-  **Last event result**: The task completed, but errors occurred while transferring some files
-  **Last event result**: An error occurred that prevented the task from completing
-  This task is configured to run "When the source is modified" (blue: monitoring is active, yellow: monitoring is suspended)
-  This task is waiting (e.g. for another task to complete, for the destination to reappear, or for AC power to be restored)

Last event result icons: If you select the task or group, you can click on that icon in the Task Plan to dismiss the status, i.e. to express, "I have acknowledged this result".

Related Documentation

- Granting Full Disk Access to CCC and its helper tool <https://bombich.com/kb/ccc6/granting-full-disk-access-ccc-and-its-helper-tool>
- Creating legacy bootable backups of macOS Big Sur (and later OSes) <https://bombich.com/kb/ccc6/cloning-macos-system-volumes-apple-software-restore>
- How to verify or test your backup <https://bombich.com/kb/ccc6/how-verify-or-test-your-backup>
- How to restore from your backup <https://bombich.com/kb/ccc6/how-restore-from-your-backup>
- Sample Usage Scenarios <https://bombich.com/kb/tags/sample-usage-scenarios>
- How do I get help? <https://bombich.com/kb/ccc6/how-do-i-get-help>

How to verify a backup

CCC offers several different ways to verify data on the source and destination. The procedure that you use will depend on when you want to verify data and why you want to verify the data.

- Backup Health Check: Verify before copying, automatically replace corrupted destination files
- Postflight verification: Verify files that were copied during the current task event [New in CCC 6!]
- Ad hoc verification: Verify the source or the destination against the "last known state" [New in CCC 6!]

Backup Health Check: Verify before copying, automatically replace corrupted destination files

CCC normally uses file size and modification date to determine whether a file should be copied. When you use the **Find and replace corrupted files** setting (Advanced Settings > Performance & Analysis), CCC will calculate a checksum of every file on the source and every corresponding file on the destination. If the checksums differ:

- If the source file is 100% readable, CCC will recopy the file to the destination.
- If the source file is not completely readable, the existing destination file will be left in place. CCC will record an error for the file in Task History and raise it to your attention when the task completes.

This option will increase your backup time (because CCC is tasked with re-reading every file on the source and destination), but it will expose any corrupted files within your backup set on the source and destination.

When and why would I use this feature?

Media failures occur on nearly every hard drive at some point in the hard drive's life. These errors affect your data randomly, and go undetected until an attempt is made to read data from the failed sector of media. If a file has not been modified since a previous (successful) backup, CCC will not ordinarily attempt to read every byte of that file's content. As a result, it is possible for a corrupted file to go unnoticed on your source or destination volume. Obviously this is a concern if the file is important, and one day you actually need to recover the contents of that file. **Use the "Find and replace corrupted files" feature to avoid and to proactively deter bit rot.**

Frequent use of the checksum calculation option is unnecessary and may be a burden upon your productivity, so CCC offers additional options to limit how frequently the checksumming occurs (e.g. weekly, monthly, quarterly, on specific days of the week, etc.).

Note: CCC will never replace a valid file on your destination with an unreadable, corrupt file from the source. If CCC cannot read a file on your source volume, any existing backup of that file will remain intact on your backup volume and CCC will report an error, advising you to replace the source file with the intact backup version. The **Find and replace corrupted files** setting will only automatically replace corrupted files on the destination, and only when the source file is completely readable.

What is a "corrupted" or "unreadable" file?

With regard to files on the source, CCC's **Find and replace corrupted files** option specifically

refers to files that cannot be **physically** read from the disk. It does not refer to files that have been mistakenly or maliciously altered such that they cannot be opened by the application that created them.

Postflight verification: Verify files that were copied during the current task event

As CCC copies files to the destination, it calculates a checksum of the data it's writing. If your task is configured to use the **Re-verify files that were copied** setting (Advanced Settings > Postflight), at the end of the task, CCC will read the destination files that were copied and verify that the data matches the data that was initially read from the source.

When and why would I use this feature?

Generally this kind of verification is unnecessary — if no errors were reported by the destination filesystem while copying a file nor when closing the file on the destination, you should expect the destination device to have permanently retained the data of that file. However, media failures are only discovered when data is read from the destination device, so it is possible for a device to accept writes without failure, but then fail to deliver the data on a subsequent read due to media failure. **Especially if you are migrating data to a new device, or if you are planning to delete items from the source after completing the backup**, this additional verification confirms that the freshly-written files are intact on the destination.

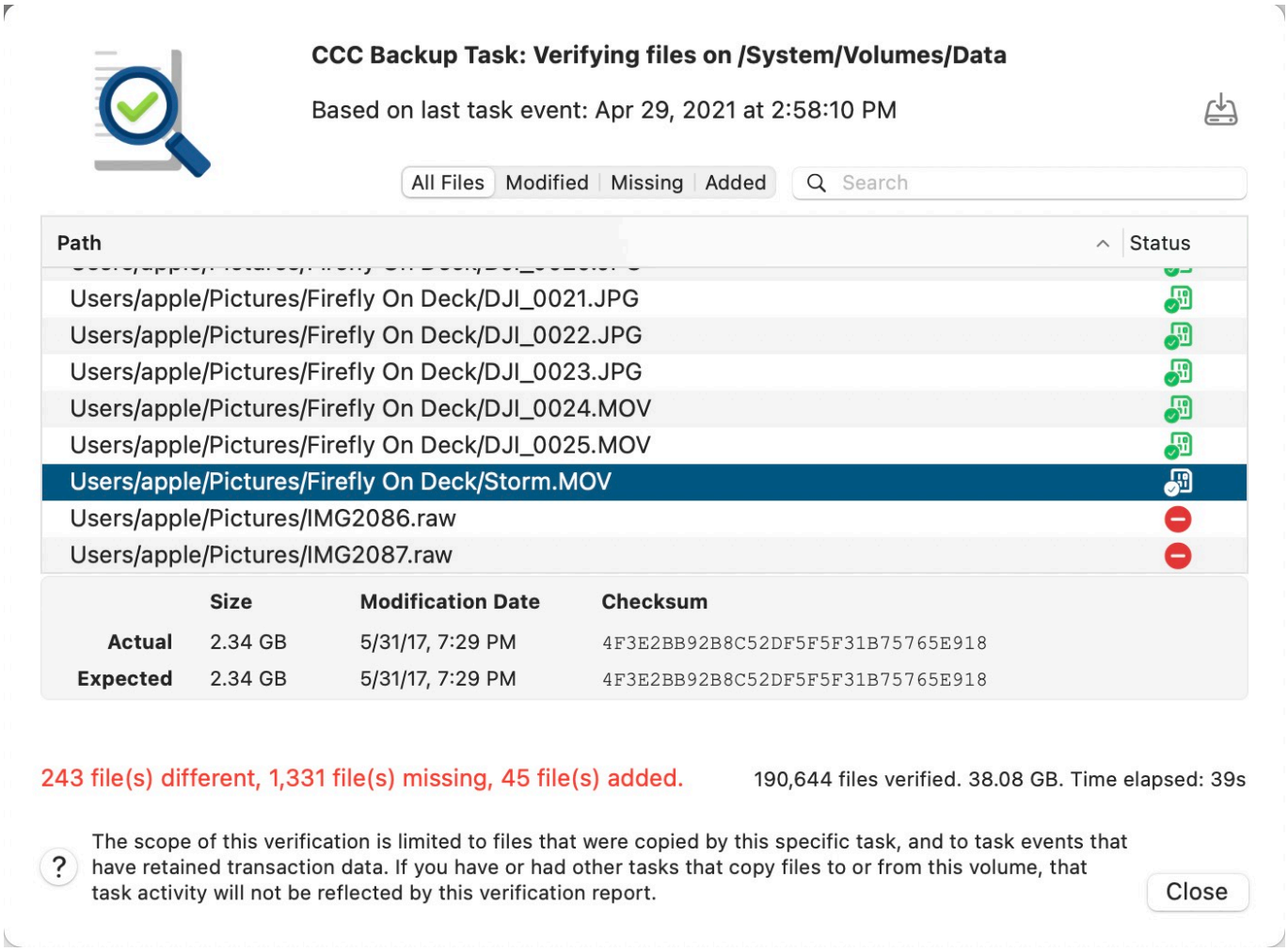
Ad hoc verification: Verify the source or the destination against the "last known state"

When CCC copies files to your destination, it maintains a record of the files that were copied (by default; that setting is available in Advanced Settings > Performance & Analysis > "Maintain a record of transactions"). That record includes the size, modification date, and a checksum of the latest version of each file. On demand, CCC can evaluate either the source or the destination against those records to determine if any files differ since the files were copied. Click on the Source or Destination selector, then choose **Verify files copied by this task** to start that verification.

When and why would I use this feature?

Unlike the previous two features that offer automated verification of files based on a comparison of the source against the destination, this feature is something you would use in an ad hoc manner. Suppose, for example, that you just installed some software, and now you're a bit concerned that something untoward has happened to your source volume. You can open CCC, click on the Source selector, then choose **Verify files copied by this task**. CCC will then read every file on the source and compare its checksum against the checksum of the file when it was last copied by the selected task. If any files have been modified since then, CCC will present those to you, along with context about the change (e.g. modification date, size, and/or checksum differences).

Another example: Suppose you want to restore some files from your backup, but prior to doing so, you want to verify that the files haven't been modified since the last CCC backup task. Open CCC, click on the Destination selector, then choose **Verify files copied by this task**. This time CCC will read the files on the destination and compare them against the same task records that hold the "last known state" information about those files.



The verification report shows some differences. What do these mean?

The verification report shows the status of items found on the selected volume based on the attributes of the file at the last backup event:

- This item matches the transaction record
- This item was added since the task last ran
- This item's content changed without affecting the size or modification date (flagged false positive, see below)
- The modification date of this item differs
- The size of this item differs
- This item's checksum differs
- This file is no longer present
- No transaction record (see below)

Click on the status icon of the selected item to reveal the actual and expected size, modification date, and checksum of the selected item.

False positives

There are a handful of file types whose content can change without affecting the size or modification date. Database memory files are a good example. Based on our past experience, CCC will flag some items as "false positives", meaning that while the content changed without affecting the size or modification date, the modification is unlikely to be malevolent, nor an indication of something wrong with the file or the backup procedure.

No transaction record

Transaction records are created when CCC 6 copies a file from the source to the destination. If you've recently upgraded to CCC 6, your destination may have an existing backup, but CCC won't have any transaction records for those files that were copied with an older version of CCC. If you perform a verification on an existing source or backup volume, only the files that were copied since upgrading to CCC v6 will have transaction records. Likewise, any items that are excluded from the backup task or protected on the destination by a filter or the SafetyNet feature will not have transaction records.

Rather than erasing your destination and re-establishing the backup to create those transactions, you can enable the **Find and replace corrupted files** setting in Advanced Settings (Performance & Analysis) and run your task once to establish the transaction records.

What do I do about differences noted in the verification report?

When the verification report shows differences, that means that the files on the selected volume are different now than they were when the selected task last copied those items. Before you draw any conclusions about differences identified by CCC's verification report, it's essential to keep in mind:

- CCC can only verify files that were copied by the selected task. Files that were (legitimately) modified by another backup task or another application will appear as "different". Likewise, files that are excluded from the backup task cannot be verified, and will appear as differences.
- It's normal for files to be modified on the source; differences identified on the source do not necessarily indicate an error condition, you may simply need to run your backup task again to get those files updated on the destination, and updated in CCC's transaction records.

If you're seeing differences on a destination volume, run the backup task again using CCC's Find and replace corrupted files setting:

1. For reference, you can save a copy of the verification report before closing the window. Click the "Save Verification Report" icon in the top-right corner to save the report.
2. Close the Verification window
3. Click the **Advanced Settings** button at the bottom of CCC's window
4. Click the **Performance & Analysis** tab
5. Check the box next to **Find and replace corrupted files**
6. Choose **Only on the next run** from the popup menu to the right of the "Find and replace corrupted files" setting
7. Click the **Done** button
8. Click the **Start** button (or Save, then Start)
9. When the task has completed, click on the Destination selector and choose **Verify files copied by this task** to repeat the verification.

Differences found on a source volume indicate changes that were made to the source since the backup task last ran, or otherwise outside of the purview of the selected CCC task. If you are seeing differences on the source, then you should consider each difference that is noted and decide if the

transaction records are simply out of date (i.e. if a file has been modified since the last backup, then you may simply need to re-run the backup to update the backup file and the transaction record), or if the files should be restored from a verified backup instead.

Verification cannot be effective when "Strict volume identification" is disabled and multiple destination volumes are used

If you're using a single task with multiple destinations, CCC isn't going to track transactions for each destination volume separately. As a result, attempts to verify a volume will only be effective for the last volume that was updated by your task. If you use the verification feature frequently, then we recommend that you use separate tasks for each of your destination volumes.

Transaction privacy and disabling transaction collection

Transaction records are maintained on a per-task basis in an encrypted database. These databases are only accessible to administrator users, and can only be accessed via CCC, and only on the Mac upon which they are created.

Transaction records for any given task are deleted when:

- The CCC task is deleted
- All task events associated with the task are removed in the Task History window
- After changing the source or destination of the task, if you choose the **Remove Audit** option
- When you specifically delete the Audit records for a task in CCC's Settings > DB Diagnostic > Audit Records
- When transaction collection is disabled for the task (see below)

To disable the collection of transactions in any particular task:

1. Click the **Advanced Settings** button at the bottom of the window
2. Click the **Performance & Analysis** tab
3. Uncheck the box next to **Maintain a record of transactions**

Can I delete, or otherwise reduce the size of the task audit records?

Task audit records are stored in a database on your startup disk, at Macintosh HD > Library > Application Support > com.bombich.ccc > TaskDBsV3. Tasks that record a lot of transactions will eventually create a large database file. CCC does take measures to limit the size and growth of these files, but that activity is balanced against a desire to retain transactions for as many task events as possible. Once transaction records are removed, you can no longer see the changes that were associated with a particular task event. If all transactions are removed for a task, the verification functionality noted above will no longer be available for that task.

You can see a list of these databases, as well as their size and health status, in CCC's Settings > DB Diagnostic > Audit Records.

If you would like to delete all of the records associated with a task:

1. Open CCC Settings
2. Click **DB Diagnostic** in the toolbar
3. Select the **Audit Records** tab
4. Select a task
5. Click the **Delete Records** button

Alternatively, if you would simply prefer to reduce the size of a task's database, you can delete some of the task history events associated with that task:

1. Choose **Task History** from CCC's Window menu
2. Select a task from the filter popup menu at the top of the window
3. Select the some of the oldest events (i.e. click and drag to select multiple items)
4. Right-click on the selection and choose **Remove**

How to restore from your backup

Restoring data to a new or different Mac, or to a clean installation of macOS on the same Mac

If you are trying to restore all of your data to a **new or different** Mac, or to a clean installation of macOS on the same Mac, you should generally use Migration Assistant to migrate that data; do not perform the restore with CCC.

Related Documentation

- Use Setup Assistant or Migration Assistant to migrate data from a CCC backup to a new Mac <https://bombich.com/kb/ccc6/i-want-clone-my-entire-hard-drive-new-hard-drive-or-new-machine#dont_install_older_os_versions>

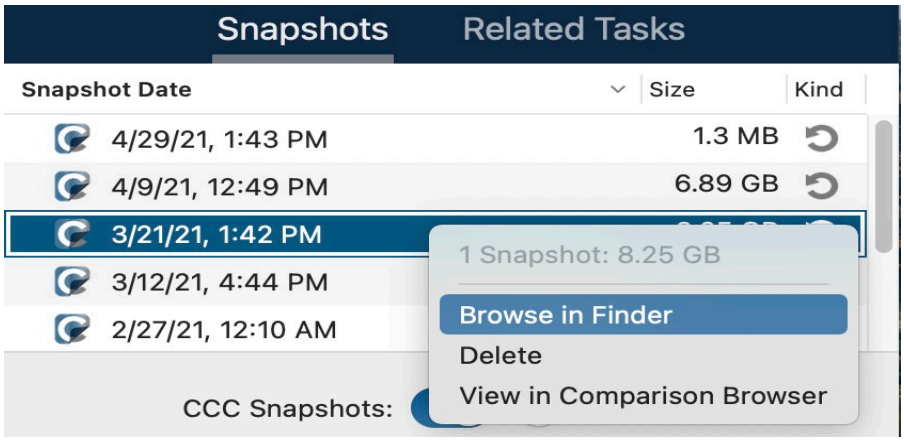
Restoring individual files from a backup

Drag and drop via the Finder

How to find and restore individual files and folders from your CCC backup <https://youtu.be/qzGexY1Q46k>

You can restore individual items from your backup volume in the Finder via drag and drop — simply find that item on the backup disk, then drag it back to your startup disk. If the item you're looking for is hidden, or resides in a hidden folder, you can press Command+Shift+Period to toggle the Finder's display of hidden items.

If you would like to restore an older version of a file, you can restore that from a CCC snapshot (what's a snapshot?). Select your destination volume in CCC's sidebar, then **double-click on a snapshot** to reveal the snapshot in the Finder. The snapshot is mounted read-only, so it is impossible for you to make any harmful modifications to the snapshot. If you would like to restore a single item, you can simply drag the item from the snapshot to wherever you want to restore it to.



If you're trying to restore system files, applications, or perhaps everything from your backup, proceed with one of the other methods indicated below.

Restoring a backup using CCC

Restoring an entire volume from a CCC backup <https://youtu.be/veI4G8XMhSY>

Restoring data to your startup disk from a CCC backup <https://youtu.be/FNi-H0QBjK8>

If you're working with a larger amount of content to restore, CCC can usually do it more efficiently than the Finder:

1. Quit all applications other than CCC
2. Click the **Restore** button in CCC's toolbar.
3. Click on the **Source** selector and choose your backup volume as the source.
4. Click on the **Destination** selector and choose your original source volume as the destination (e.g. "Macintosh HD").
5. If you are not trying to restore the entire backup, click the **Task Filter** button at the bottom of the window. Click the **Include** button in the toolbar, then explicitly select items that you would like CCC to restore.
6. Consider the warning below. If you do not want CCC to remove anything from the destination, click on the Destination selector and choose **Don't delete anything** from the SafetyNet submenu.
7. Click the **Start** button

Warning: When CCC restores content from the backup, files that aren't on the source may be removed from the destination <https://bombich.com/kb/ccc6/files-arent-on-source-may-be-removed-from-destination>. That's deliberate, and usually required to produce the outcome you expect. Please note, however, that if you excluded something from your backup, that content will be removed during the restore procedure. If you do not want that result, click on the Destination selector and choose "Don't delete anything" from the SafetyNet submenu.

Note: Some background services may not "notice" the restored data until they are restarted (e.g. because they store state data in memory). Reboot after restoring if you're restoring data to your home folder.

Restoring a folder from a CCC backup

Restoring a folder from a CCC backup <https://youtu.be/qtFeznrDn8k>

If you're trying to restore a specific folder, you should refine the scope of your restore task to avoid unintentional modifications to other content on the volume you're restoring to:

1. Quit all applications other than CCC
2. Click the **Restore** button in CCC's toolbar.
3. Click on the **Source** selector and choose **Choose a folder**. Select the folder on your backup volume that you would like to restore.
4. Click on the **Destination** selector and choose **Choose a folder**. Select the folder on your original source volume that you would like to restore to. Typically this folder will follow the same path as the source. E.g. if you are restoring (your backup disk) > Users > yourname > Desktop folder, you should select Macintosh HD > Users > yourname > Desktop as the destination.
5. If you do not want CCC to remove anything from the destination, click on the **Destination** selector and choose **Don't delete anything** from the SafetyNet submenu.
6. Click the **Start** button

Restoring an older version of a backup

Restoring an older version of a backup <https://youtu.be/eEkLNIpQAyc>

If you would like to restore an older version of a backup, you can restore from a snapshot on your backup disk.

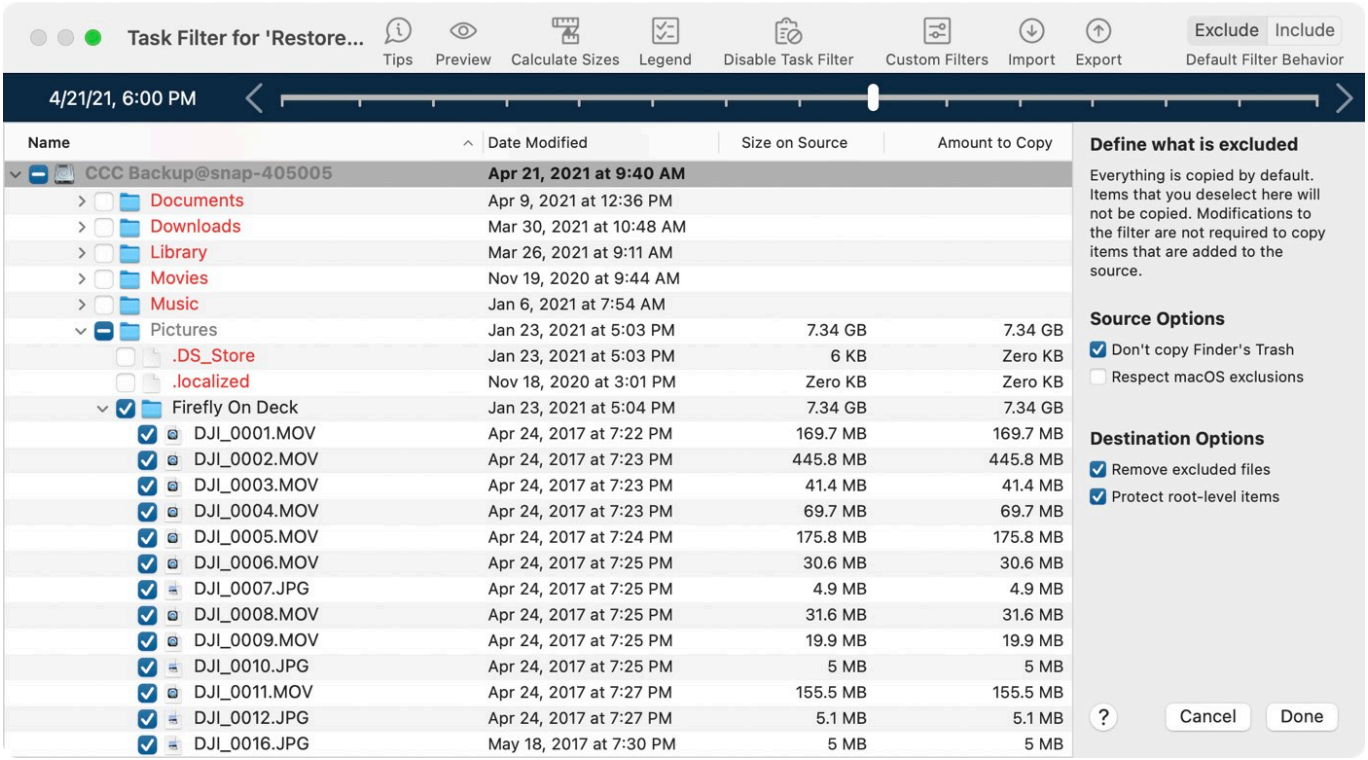
1. Quit all applications other than CCC
2. Click the **Restore** button in CCC's toolbar.
3. Select your backup disk as the source to the task.
4. Click on the source selector and select a specific snapshot from the "available snapshots" menu.
5. Click on the Destination selector to select a destination volume or folder.
6. Click the Start button to run the task.

Restoring older versions of files using CCC's Snapshot

Navigator

Restoring an older version of a specific file from a CCC backup
<https://youtu.be/eEkLNIpQAyc?t=145>

If you're planning to restore specific items, and especially if you would like to compare the contents of snapshots or look for a specific version of a file, you can use CCC's Snapshot Navigator:



1. Quit all applications other than CCC
2. Click the **Restore** button in CCC's toolbar
3. Select a source volume, or a specific folder from your backup disk if you're restoring just a particular folder
4. Click on the Task Filter button at the bottom of the window to open the snapshot navigation interface
5. Click the **Include** button in the toolbar to set the Default Filter Behavior to **Define what is included**
6. Find the version of your files and folders that you would like to restore (see below for additional detail)
7. Check the boxes next to the items that you want to restore
8. Click the Done button
9. Click on the Destination selector to select a destination volume or folder
10. If you're not restoring the entire backup, click on the Destination selector and choose **Don't delete anything** from the SafetyNet submenu
11. Click the Start button to run the task

In the Task Filter window, use the slider to select specific snapshots. Alternatively, select an individual file that you're interested in restoring, then use the arrow buttons at the ends of the slider to navigate to previous and next versions of the file. When you have found the version of the item you would like to restore, you can either right-click on the item to reveal it in the Finder (then drag and drop the file to wherever you'd like to restore it to), or you can configure the task filter to restore specific items to a selected destination.

Note: Some background services may not "notice" the restored data until they are restarted (e.g. because they store state data in memory). Reboot after restoring if you're restoring data to your home folder.

Restoring files to your destination from a SafetyNet Snapshot

Undoing a backup that was made to the wrong disk <https://youtu.be/tj8Hl78QmIg>

SafetyNet is a mechanism that is designed to protect files on your destination volume from accidental deletion. If you errantly selected the wrong volume as a destination, or if you were storing files on your destination that were unrelated to the source data set and you're now missing those files, you can restore those files to your destination from a SafetyNet Snapshot.

1. Open CCC and select the affected destination volume from CCC's sidebar.
2. Select the applicable SafetyNet Snapshot in the snapshots table.
3. Click the **Restore...** button.
4. Verify the settings of the task that CCC creates for you, then click the Start button.

When you proceed with this restore task, CCC will copy the files from the snapshot back to your selected destination. Keep in mind that CCC cannot delete the snapshot that holds the files that you're restoring prior to restoring those files to the destination. As a result, the destination must have enough additional free space to accommodate a copy of all of the files that you're restoring. In some cases, it may not be practical to restore files back to the original destination, you may need to recover them to another disk first.

Related Documentation:

- Excluding files and folders from a backup task <https://bombich.com/kb/ccc6/excluding-files-and-folders-from-backup-task>
- "Why does CCC report that the destination is full when it appears to have enough room for newer files?" <https://bombich.com/kb/ccc6/ccc-reported-destination-full.-what-can-i-do-avoid#destination_is_tight_on_space>

Using Migration Assistant to restore your startup disk from a CCC backup

Recovering your Mac from a CCC backup <https://youtu.be/eFTUmC1DiDs>

You can use Migration Assistant to migrate data from a CCC backup on locally-attached storage to a clean installation of macOS. Follow these steps to reinstall macOS and restore your data:

1. Boot your Mac while holding down Command+R (Intel Macs) or the Power button (Apple Silicon Macs) to boot into Recovery Mode <https://support.apple.com/en-us/HT204904>.
2. Use Disk Utility to erase your Mac's (new) internal disk as APFS (see this Kbase article for additional guidance <https://bombich.com/kb/ccc6/preparing-your-backup-disk-backup-os-x>).
3. Quit Disk Utility.
4. Select the **Reinstall macOS** option and proceed to install macOS onto your new disk.
5. When macOS boots for the first time on your new disk, you will be prompted to migrate data — accept the migration offer.
6. When prompted to select a source for the migration, select your CCC backup volume† and proceed as directed by Migration Assistant.

† **Big Sur (and older OSes):** Migration Assistant won't list volumes that are encrypted and locked

(i.e. not mounted), and won't helpfully offer any UI for unlocking and mounting those volumes. If you would like to migrate data from an encrypted volume, proceed with creating a new user account instead. After logging in, you'll be prompted to unlock the volume, and then you can open Migration Assistant (Applications > Utilities > Migration Assistant.app) and proceed with the migration.

Migration Assistant will not accept a backup on NAS storage as a source for migration. Use the method described below to restore files and folders from a NAS backup.

Related Documentation

- Sample Usage Scenario: I want to migrate data to a new Mac <https://bombich.com/kb/ccc6/i-want-clone-my-entire-hard-drive-new-hard-drive-or-new-machine>

Working around Migration Assistant restrictions

There are a handful of cases where Migration Assistant will not accept a volume as a source for migrating content. For example, if you have a volume that is formatted as case-sensitive, Migration Assistant will not allow you to migrate content from that volume to a case-insensitive-formatted startup disk. Likewise, if any user account resources are missing from the volume (e.g. because they were excluded from the backup, or because they are damaged), Migration Assistant will not accept it as a source. CCC can help with these cases.

1. If you're currently proceeding through the first-boot Setup Assistant, decline the migration offer and instead proceed to create a new user account.
2. Open Disk Utility
3. Choose "Show all devices" from the View menu
4. Select the startup disk (any volume associated with the startup disk, or its parent container)
5. Click the "+" button in the toolbar to add a new volume. Name it "Macintosh", or something like that (something that you can live with long-term).
6. Open CCC and configure a new task to restore your backup to the "Macintosh" volume (You may also restore an older version of your backup)
7. When the task has completed, install macOS onto the "Macintosh" volume <https://bombich.com/kb/ccc6/cloning-macos-system-volumes-apple-software-restore#install_macos>
8. When the macOS installation is complete, go back to Disk Utility and delete the "Macintosh HD" volume group to free up the space that it's using.

Restoring your startup disk from a legacy bootable copy of macOS

These instructions are only applicable to macOS Catalina. We recommend that you use the instructions in this previous section to restore the startup disk on a Mac running Big Sur or later.

1. Boot your Mac from the backup disk

Attach the backup disk to your Mac using a USB or Thunderbolt cable.

Hold down the Option key as you start up your Mac. Your backup disk should appear as a startup disk option in the Startup Manager <https://support.apple.com/en-us/HT204417>.

Note: If you cannot boot your Mac from your backup disk, use the alternate procedure documented above.

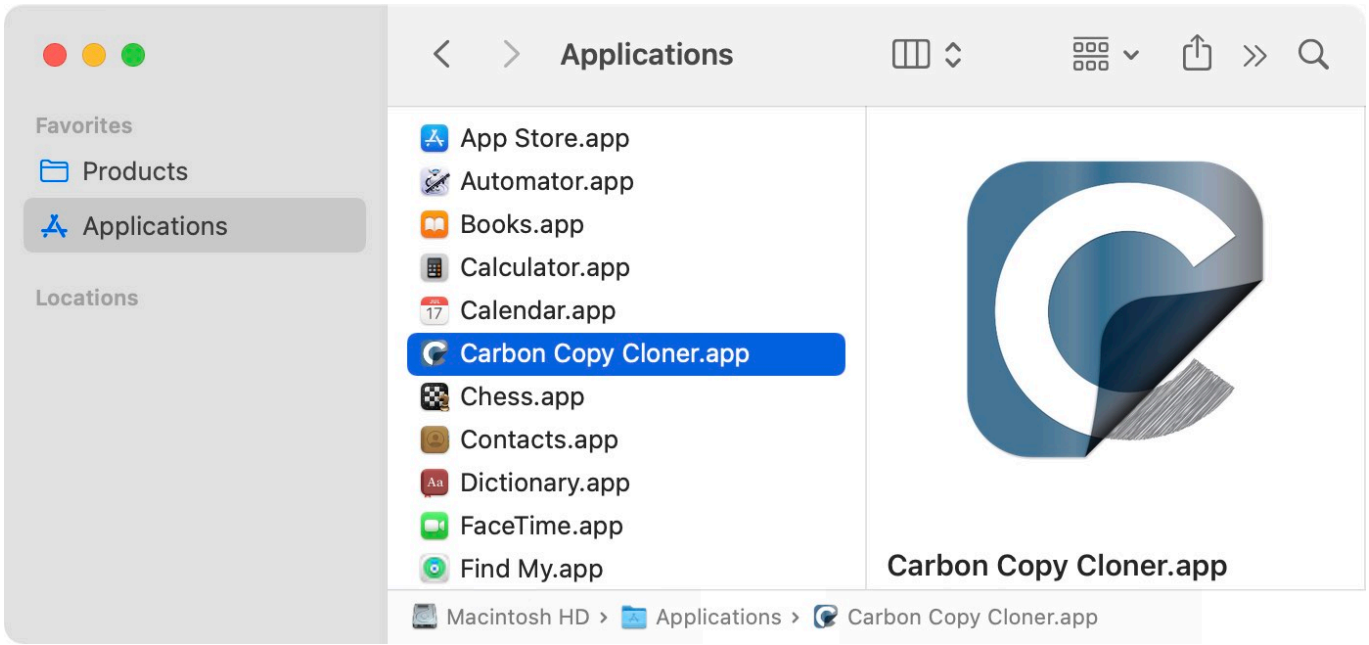
2. Prepare the disk that you're restoring to

Unless you're restoring just a handful of individual files, we recommend that you restore your backup to a freshly-formatted disk. See Preparing your backup disk for a backup of macOS <https://bombich.com/kb/ccc6/preparing-your-backup-disk-backup-os-x> for complete instructions on how to format the destination. Please note that this is especially important when restoring a macOS startup disk.

3. Open CCC

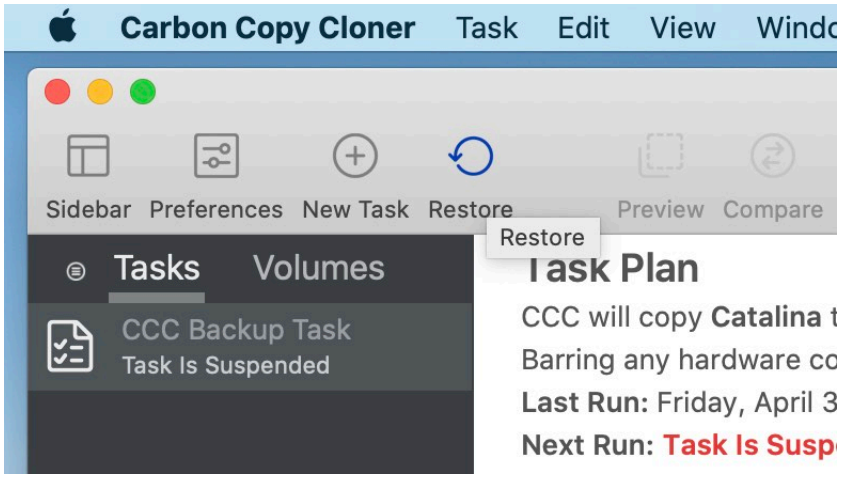
When your Mac has finished restarting, open CCC. **Applications > Carbon Copy Cloner**

Note: When you open CCC on your backup volume, CCC will prompt to guide you in setting up a restore task, in which case the instructions here are redundant. If you decline this offer, CCC will indicate that your regularly-scheduled tasks are suspended. If prompted, choose the option to leave your tasks suspended. Likewise, choose "Revert changes" if prompted to save your tasks.



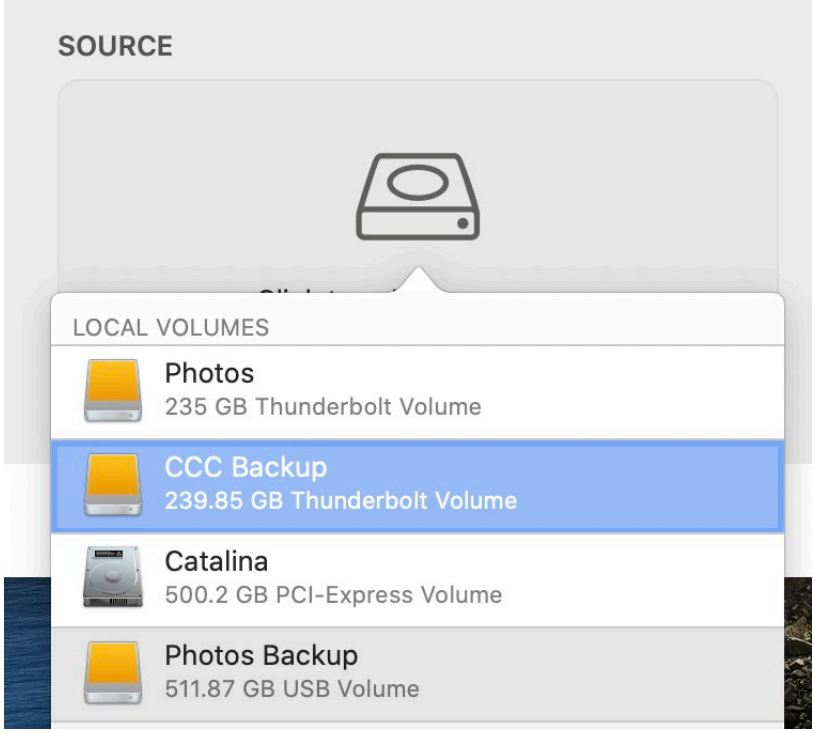
4. Create a New Restore Task

Click the **Restore** button in the toolbar or choose **New Restore Task** from the Tasks menu.



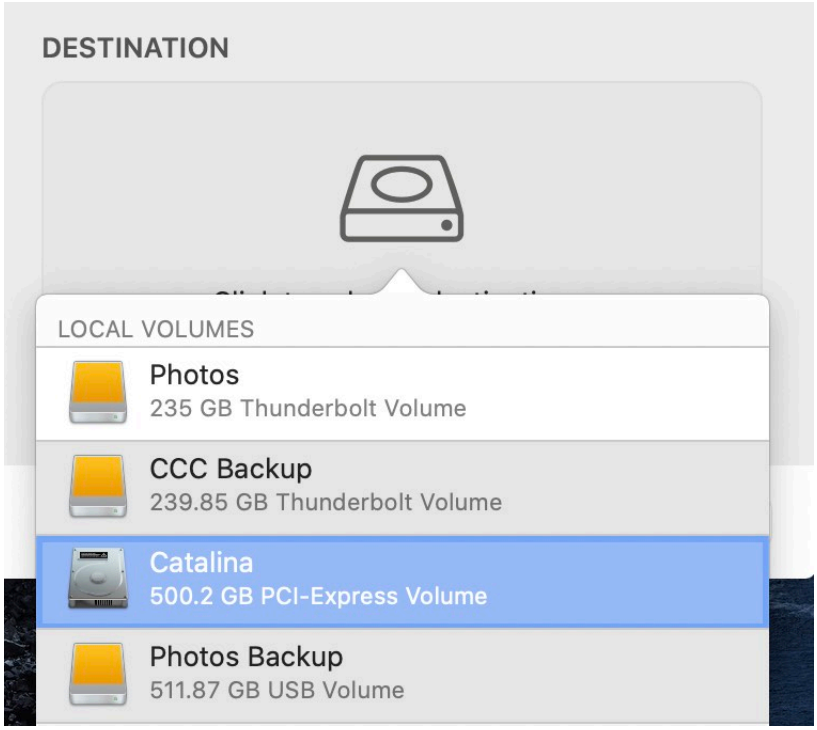
5. Select the Source

Click on the icon in the Source box to view available sources. Click to select your backup **volume** as the Source. You do not need to create a separate restore task to restore the System and Data volumes, CCC will restore both volumes.



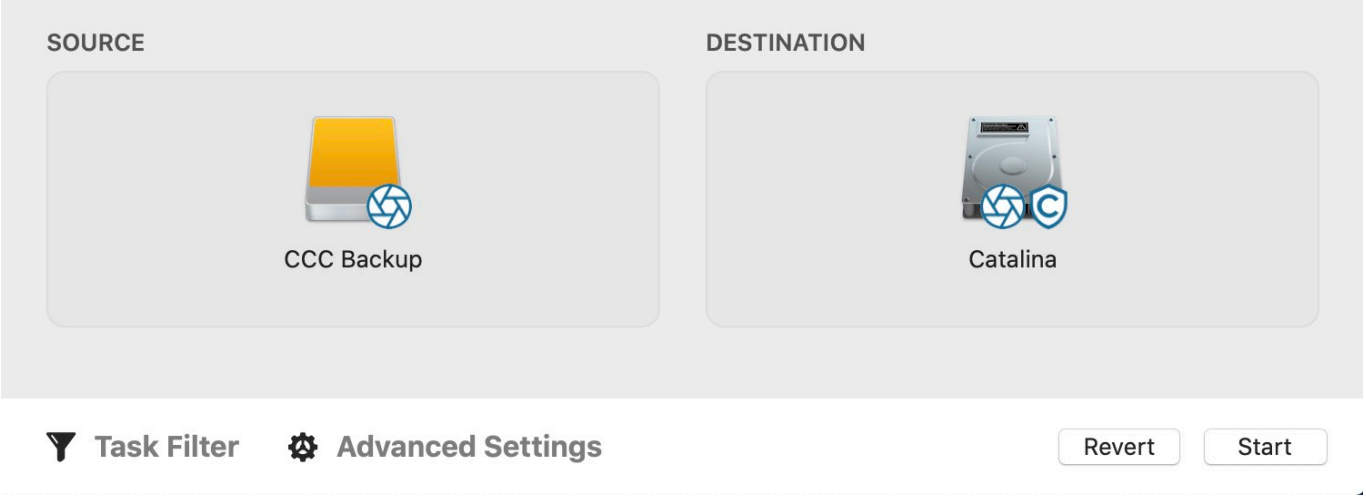
6. Select the Destination

Click on the icon in the Destination box to view available destinations. Click to select the **volume** that you want to restore to.



7. Click Start

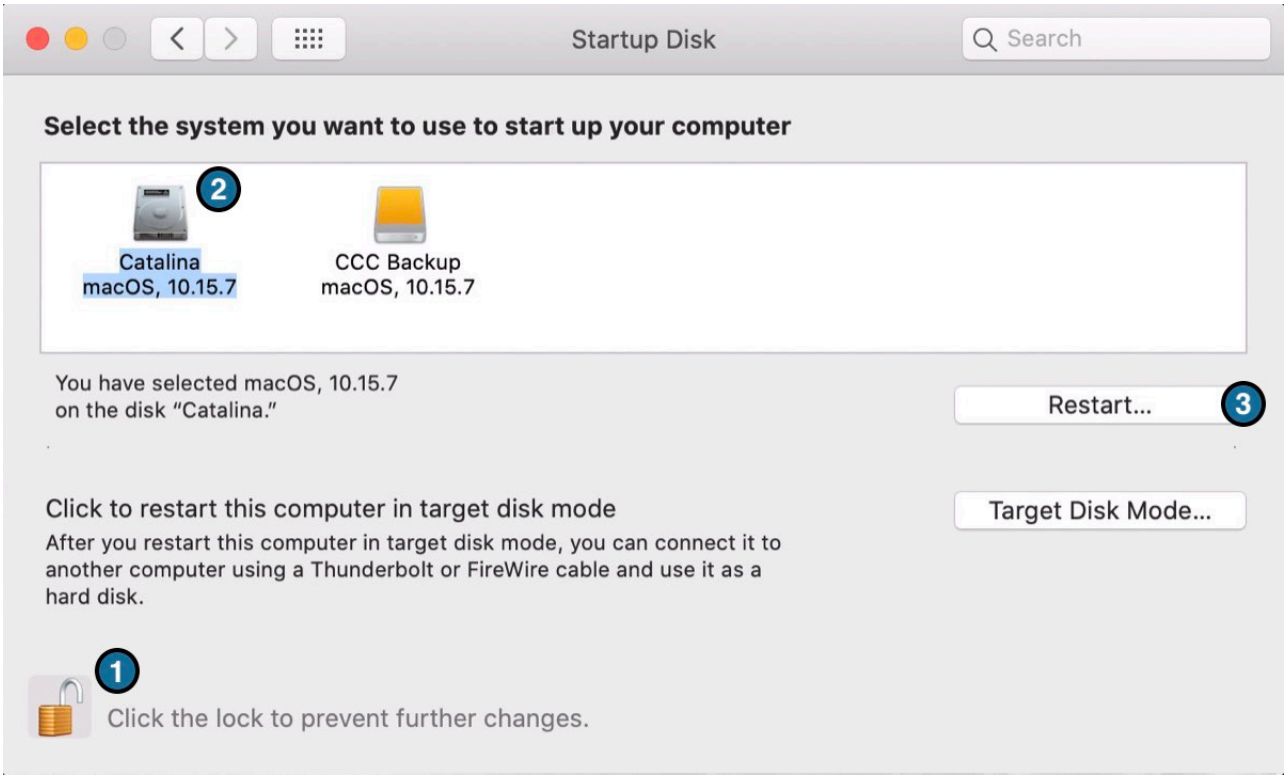
Click the Start button in the lower-right corner to start the restore task.



8. Reset the Startup Disk

Open the Startup Disk Preference Pane

After the restore is finished, choose **Startup Disk** from CCC's **Utilities** menu, click the padlock icon at the bottom of the window to authenticate, then reset the startup disk to your original startup disk and restart your computer.



Related Documentation

- Troubleshooting External Boot <https://bombich.com/kb/ccc6/help-my-clone-wont-boot>

- Restoring from a disk image <https://bombich.com/kb/ccc6/restoring-from-disk-image>
- "I have a full-volume backup in a folder or a disk image. How can I restore everything?" <https://bombich.com/kb/ccc6/i-have-full-volume-backup-in-folder-or-disk-image-i-dont-have-bootable-backup.-how-can-i>

Restoring from a backup on a NAS or network share

To restore data from a folder on a NAS volume:

1. Close all applications and all Finder windows
2. Open CCC and click the **Restore** button in CCC's toolbar to create a new restore task
3. Drag the folder that you would like to restore from the network share onto CCC's Source selector
4. Create a new folder at the location where you would like to restore data
5. Drag that new, empty folder onto CCC's Destination selector
6. Click the Start button

Bear in mind that NAS backups are not compatible with Migration Assistant. <https://bombich.com/kb/ccc6/i-want-back-up-my-whole-mac-time-capsule-nas-or-other-network-volume#nas_annoyances> You can restore specific folders from the NAS backup, but you need a backup on locally-attached storage to restore your complete "Mac experience" (e.g. system settings, user accounts).

Restoring a home folder from a backup on a NAS to a clean install of macOS

As noted above, NAS backups are not compatible with Migration Assistant. If you have a new Mac or an otherwise clean installation of macOS, and your only backup is on a NAS volume, then the following steps are the Best Practices method for restoring the user home folders and creating new user accounts.

1. Proceed through Setup Assistant, creating a new "utility" account. Do not use the same name as an account from the backup, and do not log in to iCloud.
2. Mount your NAS backup volume in the Finder.
3. Navigate to Macintosh HD > Users in the Finder. Create a new folder using the name of the user whose home folder you are restoring.
4. Download and open CCC.
5. Click **Restore** in the toolbar to create a new Restore task.
6. Drag the user home folder from the NAS backup volume in the Finder onto CCC's Source selector.
7. Drag the user home folder from the Macintosh HD volume in the Finder onto CCC's Destination selector.
8. Click the Start button.
9. When the restore procedure has completed, open System Settings > Users & Groups.
10. Click **Add User…**
11. Configure a new user account. Set the "Account Name" to the same name as the home folder that you restored.
12. Log out, then log in to the restored user account. You may delete the "utility" account, if desired.

Migrating data from an Apple Silicon Mac booted in "Share Disk" mode

When Apple introduced Apple Silicon Macs, they replaced "Target Disk Mode" (TDM) with a new

"Share Disk" mode. With TDM, you simply connect two Macs via FireWire or USB, and the storage of the TDM Mac appears and behaves as a locally-attached device. That device would be inherently compatible with Migration Assistant. Share Disk mode is completely different. Instead of behaving like a locally-attached device, the attached Mac shares a specific volume via SMB file sharing. That volume is *not compatible with Migration Assistant*, and due to some limitations of the SMB service on the sharing Mac, applications copied via the Finder do not work correctly.

CCC can work around these limitations and produce a backup of the Shared-Disk Mac that has functional applications and is compatible with Migration Assistant. Ideally you would have an ordinary CCC backup of the Shared-Disk Mac to use instead (i.e. a backup made while that Mac is booted from its own hard drive), but if you are only able to access the Mac via Share Disk mode, then you can use the following steps to migrate data from that Mac.

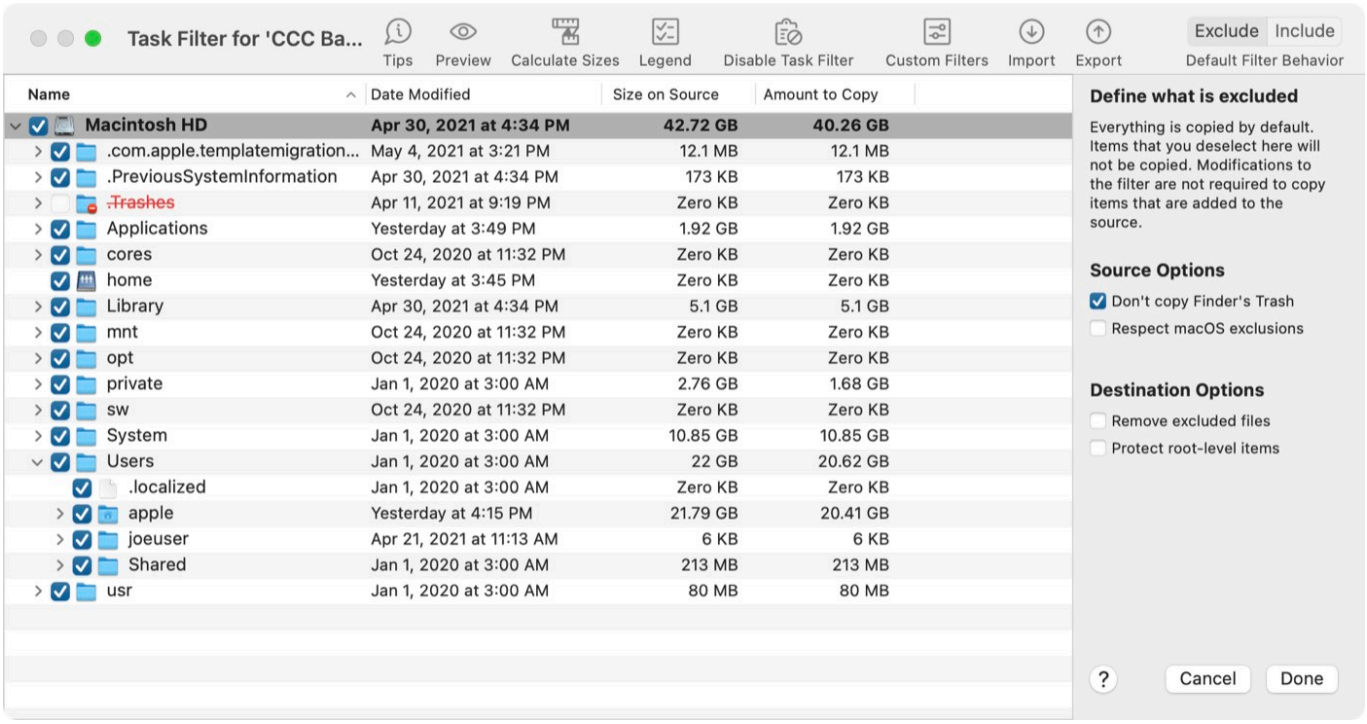
1. Follow Apple's instructions for sharing the startup disk of another Mac <https://support.apple.com/guide/mac-help/transfer-files-a-mac-apple-silicon-mchlb37e8ca7/mac>
2. Erase a new backup disk in Disk Utility <https://bombich.com/kb/ccc6/preparing-your-backup-disk-backup-os-x> to use as a destination for the backup task, or add a volume to an existing backup disk <https://bombich.com/kb/ccc6/i-want-back-up-multiple-macs-or-source-volumes-same-hard-drive#apfs_add_volume> that has enough space for the procedure.
3. Click the **New Task** button in CCC's toolbar.
4. Select the Shared-Disk volume as the source.
5. Select your local backup volume as the destination. Do not select your current startup disk as the destination to this task.
6. Click the **Start** button to run the task.
7. When the task has completed, eject the Shared-Disk volume and detach the second Mac.
8. Open Migration Assistant and migrate data from the CCC backup volume.

CCC won't run automated tasks while a restore task is running

To avoid any potential conflicts, CCC will avoid running any automated tasks while a Restore task is running. This is designed to prevent mishaps, e.g. overwriting the backup while you're restoring the backup to another volume. If you have an unrelated task that you would like to run while a restore task is running, you can start that task manually to override CCC's safety mechanism.

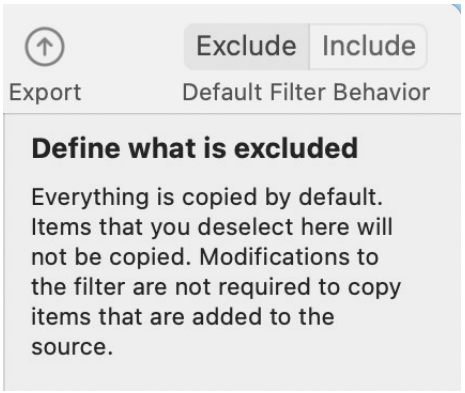
Configure the task filter to exclude files and folders from a task

By default, CCC will copy everything from the volume or folder that you specify as the source. If you do not want to copy every item from the source, you can define a task filter to limit what items will be copied. Click the **Task Filter** at the bottom of the window to open the Task Filter window.



Default Filter Behavior

The CCC task filter offers two paradigms for defining the task filter. The default filter behavior determines whether you will define what should be excluded (i.e. everything is copied by default, except for what you specifically exclude), or whether you will define what should be included (i.e. nothing is copied by default, except for what you specifically include). Which behavior you choose depends on what you want CCC to do with new items that are added to the source. You can change the default filter behavior by clicking the button in the top-right corner of the Task Filter window:



Exclude: Define what is excluded

CCC's default behavior is to copy everything by default. In this mode you define what is excluded from the task by unchecking the box next to an item in the file list. This mode is simplest for users that only want to exclude a handful of items, but generally copy everything because you don't have to revisit the task filter to indicate that new items should be included in the task. If you add a file or folder to the source (e.g. in the future after defining your task filter), and that item is not in a folder that you have excluded from the task, that item will automatically be included in the task.

Include: Define what is included

In this mode, nothing is copied by default, and you define what is **included** in the task by checking the box next to an item in the file list. If you add an item to the source in the future, and that item is not in a folder that is specifically included by the task filter, that item will **not** be copied. This mode is helpful in cases where you only want to copy a handful of items on a volume whose subfolders frequently change.

When the Default Filter Behavior is changed, the task filter is reset

This behavior is intentional, the Include and Exclude Default Filter Behaviors and their rules are mutually exclusive. When you change the Default Filter Behavior, that makes a fundamental change to how each rule is defined by you and interpreted by CCC. As such, all previously-defined rules are inapplicable, so the "conventional" rules are cleared (in contrast to Custom Rules, which are left in place).

Consider this example — suppose the filter is configured to Exclude, and that you have excluded just one folder, "Applications". The task filter has exactly one rule, "Exclude /Applications". If you then change the filter behavior to "Define what is *Included*", that "Exclude /Applications" rule becomes irrelevant and extraneous. With an "Include" filter, *nothing* will be copied until you explicitly include it, therefore the Applications folder is already not going to be copied. Making matters potentially worse, though, suppose you next choose to include just one application. If we didn't clear the "Exclude /Applications" rule, there would be a conflict between "Exclude /Applications" and "Include /Applications/foo.app". To avoid these sorts of negative interactions as you start to define new Include rules, CCC removes the extraneous Exclude rules.

Calculating disk usage and "Amount to copy"

You can right-click on any folder and choose **Refresh size** to have CCC enumerate the contents of that folder and evaluate the task filter against its contents. CCC will report the total size of the folder on the source and the amount of data included to be copied. You can also click on the **Calculate Sizes** button in the toolbar to enumerate the contents of the entire source. This could take a while, especially for network volumes, so consider refreshing the disk usage of individual folders instead. If CCC is in the midst of enumerating a folder, you can right-click on that folder to stop enumeration, or click again on the **Calculate Sizes** button to stop the calculation.

Source and destination options

Finder's Trash is excluded by default

By default, CCC won't copy the contents of the Finder Trash because, well, it's Trash. If you want CCC to copy your Trash, click the **Task Filter** button, then uncheck the **Don't copy Finder's Trash** box in the Task Filter window sidebar to remove the exclusion. See this section of CCC's documentation <https://bombich.com/kb/ccc6/backing-up-and-restoring-finders-trash> to learn more about the idiosyncrasies of the Finder Trash mechanism and how it relates to backing up and restoring the

content of the Trash.

Excluded files are not deleted from the destination

When you exclude an item from the CCC task, this tells CCC, "**Do not copy that item**". That does not, however, indicate that CCC should **delete** that item from the destination, e.g. if it had been copied there by a previous task. In fact, excluding an item from the task implicitly protects that item on the destination. If you have items on the destination that are now excluded from a task that you no longer want to retain on the destination, you can simply remove them from the destination by dragging them to the Trash. If you would like CCC to facilitate that cleanup, check the **Remove excluded files** checkbox in the sidebar.

The **Remove excluded files** option is ignored if your task is configured with the **Don't delete anything** SafetyNet setting. This setting also will not override CCC's explicit protections placed on the _CCC SafetyNet folder, so when this option is used in conjunction with CCC's "SafetyNet On" setting, items will be moved to the SafetyNet folder rather than deleted immediately. Likewise, the **Protect root-level items** setting overrides the **Remove excluded files** setting for root-level items.

When using the **Include** default filter behavior, the **Remove excluded files** option will only remove items that you have explicitly excluded via a custom filter. Items that are implicitly excluded (i.e. because you did not specifically include them using a conventional inclusion rule) will not be deleted from the destination.

We strongly recommend that you enable CCC's SafetyNet feature when using this setting until you are familiar with its behavior. Click on the Destination selector and choose **SafetyNet On** to enable SafetyNet.

The **Protect root level items** setting is described in more detail in the Advanced Settings article <https://bombich.com/kb/ccc6/advanced-settings#protect>.

Respect macOS exclusions

Apple offers a method to third-party applications for flagging specific files to be excluded from Time Machine backups. When backing up to a locally-attached volume, CCC ignores these exclusion flags by default. You can check the **Respect macOS exclusions** checkbox in the sidebar to change that behavior. Note that CCC automatically enables this option when backing up a locally-attached source to a network volume destination to reduce the amount of unnecessary content being evaluated in NAS backup tasks.

CCC will show these excluded items in the Task Filter window when the **Respect macOS exclusions** setting is enabled. If you would like to get a complete list of files flagged in this manner, though, you can paste the following into the Terminal application (replace "/Users/yourname" with any folder you want to search within):

find /Users/yourname -xattrname "com.apple.metadata:com_apple_backup_excludeItem"

Custom Filters

If the files you want to match are scattered across your filesystem, it may be tedious to manually locate each of them and create conventional rules (i.e. check or uncheck the item in the file list). To address this, CCC offers custom filter options in which you define a filter rule using an expression. Click the **Custom Filters** button in the toolbar to reveal the custom filters table.

To add a custom filter rule, click the **+** button in the custom rules table header, or drag a file or

folder from the file list into the custom filters table to add that item as a template. To reorder custom filters, simply drag and drop the items in the custom filters table. Custom filter rules will be evaluated by the task filter before conventional filter rules.

Anchored path filter

An anchored path filter defines a rule using an absolute path relative to the root of the source. /Library/Caches, for example, is an anchored path filter because it starts with a "/". This filter would match /Library/Caches, but would not match /Users/someuser/Library/Caches. You can also include wildcards in the expression, e.g. /Users/*/Library/Caches would match the Library/Caches folder in each user home folder.

Subpath filter

A subpath filter defines a rule using a partial path or filename that does not start with "/". Continuing the example above, Library/Caches would match /Library/Caches and /Users/someuser/Library/Caches. Wildcards are accepted in the expression; to match a particular file type, use an expression like *.mov to match all .mov files.

Wildcard characters

Wildcard characters can be added to an expression to match a wider range of files and folders. * will match one or more characters in any single file or folder name, e.g. *.mov will match all movie files.

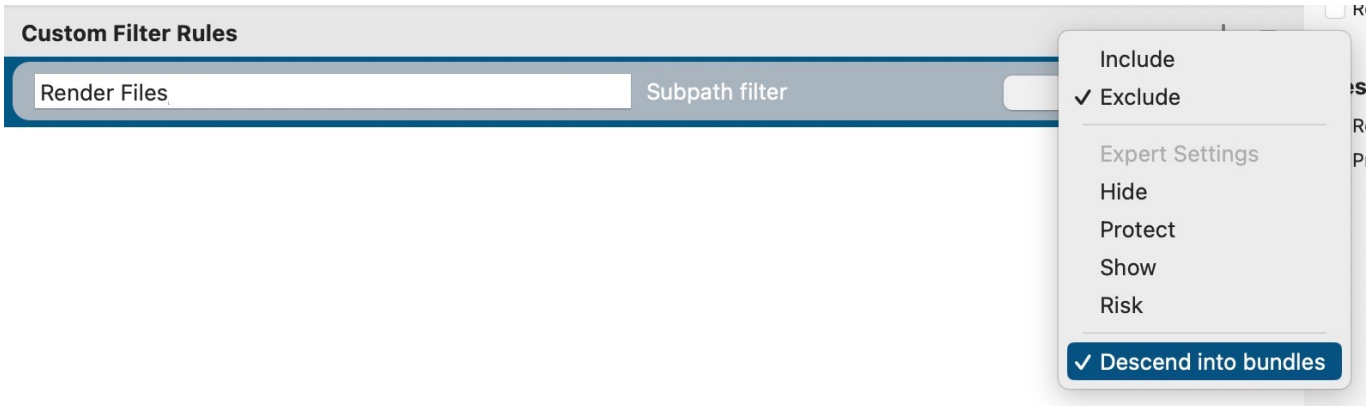
/**/ will match one or more path components, e.g. /Users/**/*.jpg will match any JPEG photos in any user home folders, but won't match JPEG photos elsewhere, e.g. those in /Library/Desktop Pictures. You would also use the ** wildcard when defining an inclusion rule that should copy all items within a particular folder and its subfolders. For example, /Users/yourname/Documents would include only that folder itself, not any of its contents. /Users/yourname/Documents/** would include the Documents folder, all of its contents, and the contents of every subfolder within it.

If you specify additional path components after a ** wildcard, then that wildcard is only applicable up to a match against the path component that follows the wildcard. For example, the exclusion rule /Data/**/Marine/Invertebrates would exclude /Data/2018/Marine/Invertebrates, but it would not exclude /Data/2018/Marine/Benthic/Marine/Invertebrates. In the latter case, **/Marine matches 2018/Marine, but then the the next path component fails to match (and we are deliberately choosing to not allow the ** wildcard to match 2018/Marine/Benthic in this case).

? can be used to match any single character, e.g. *.mp? will match both .mp3 and .mp4 files. Use the ? wildcard sparingly, it will greatly increase the amount of time required to evaluate the task filter.

Excluding items that exist within a bundle file

CCC's Task filter does not expose the contents of bundle files (e.g. application files, Photos libraries) because bundle files should generally be kept whole, otherwise they may not function correctly when restored. If you have a specific reason to exclude some content from a bundle (e.g. cache files in a Final Cut Pro media bundle), you can do so with a custom exclusion rule. To make the rule apply to bundle components, click on the popup menu adjacent to the filter rule expression and toggle the **Descend into bundles** setting.



Expert settings

Custom filter rules are usually applied to include or exclude an item. Exclusions, however, are actually composed of two behaviors: a matching item on the source will not be copied (**Hide** the item from the copier), and a matching item on the destination will be protected (**Protect** the item from the copier). Likewise, Inclusions indicate that a matching item on the source will be copied (**Show** the item to the copier) and a matching item on the destination may be deleted (**Risk** the item). Occasionally it's helpful to define a rule that affects only matching items on the source or only on matching items on the destination. For example, if you have a folder named "Archives" on the destination that does not exist on the source, that item won't appear in the source list so it cannot be excluded (and thus protected) in the conventional manner. You could add an /Archives **Protect** rule to explicitly protect that item on the destination.

Including folders and their content with the 'Include' filter behavior and custom rules

Including a folder or a bundle file and its contents via a custom rule requires a non-intuitive expression, because the filter rule must match multiple path components. To include a folder and all of its contents, add ** to the end of the filter expression. For example, to include the Photos Library from your home directory, the following expression would apply as an inclusion rule:

/Users/johnny/Pictures/Photos Library.photolibrary**

Exporting and Importing filters

A whole task filter can be imported or exported via the gear menu. When importing a filter, the current filter will be replaced with the filter you're importing. CCC will automatically purge conventional rules from the filter if they are not applicable to the currently-selected source. For example, if you had excluded /Applications in the filter, but /Applications does not exist on the current source, that rule will be removed from the filter to avoid unexpected results should an /Applications folder ever be added to the source. This purging is not applicable to custom filter rules.

You can also export individual or groups of custom filter rules. Select the rule(s), then simply drag the items onto your Desktop. To import custom rules from a file exported in this manner, simply drag the file into the custom filter rules table.

Items automatically excluded

CCC excludes some items from the backup task by default. A complete list of exclusions along with an explanation for the exclusion is available in this section of the documentation <https://bombich.com/kb/ccc6/some-files-and-folders-are-automatically-excluded-from-backup-task> . If you would like to visualize the items that are automatically excluded, hold down the Option key

while clicking on the Task Filter button to open the Task Filters window.

The CCC SafetyNet folder, "_CCC SafetyNet" is excluded by a global filter. See the Frequently asked questions about the CCC SafetyNet <https://bombich.com/kb/ccc6/frequently-asked-questions-about-carbon-copy-cloner-safetynet#restore_archives> section of the documentation to learn how to restore items from that folder.

Additionally, CCC will exclude and protect system folders if you select the startup disk or a non-HFS+/APFS formatted volume as the destination. CCC will also exclude system files if you select a destination volume that is in the same APFS container as the current startup disk (because System Integrity Protection errantly prevents CCC from setting special flags on system files when copying files to another volume in the startup disk's container). If you would like to restore a specific item, such as the contents of /Library/Application Support, this protection can be avoided by choosing a specific folder at the source and destination via the **Choose a folder <https://bombich.com/kb/ccc6/folder-folder-backups>** options in the Source and Destination selectors. With great power comes great responsibility — take care to avoid overwriting your system files.

Related documentation

- Restoring your startup disk from a legacy bootable backup <https://bombich.com/kb/ccc6/how-restore-from-your-backup#bootable_restore>
- Folder-to-Folder Backups <https://bombich.com/kb/ccc6/folder-folder-backups>
- Some files and folders are automatically excluded from a backup task <https://bombich.com/kb/ccc6/some-files-and-folders-are-automatically-excluded-from-backup-task>
- Backing up and restoring Finder's Trash <https://bombich.com/kb/ccc6/backing-up-and-restoring-finders-trash>

Disabling the Task Filter

If you would like to disable the task filter without discarding all of your exclusions, click the **Disable Task Filter** button in the toolbar. This will close the Task Filter window (saving any changes that were made to the filter), but then any user-defined inclusion or exclusion rules will be ignored for subsequent tasks. To re-enable the Task Filter, simply click the **Task Filter** button at the bottom of the window, then click the **Done** button. You'll know that your task filter is active if the icon of the Task Filter button at the bottom of the window is red.

Why is the "Task Filter" button sometimes disabled?

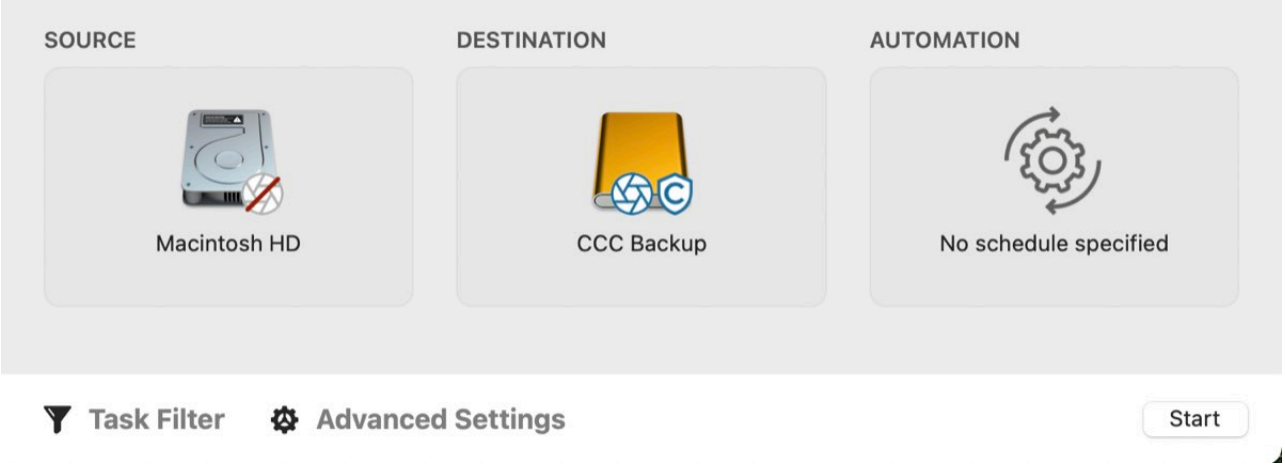
The Task Filter window dynamically evaluates the effect of your task filter, which requires that the source is available while the Task Filter window is open. The Task Filter button will be disabled if the source volume is not mounted, or (if applicable) if the selected source folder is missing. Additionally, the Task Filter button will be disabled if you have configured the task using the Legacy Bootable Copy Assistant <https://bombich.com/kb/ccc6/cloning-macos-system-volumes-apple-software-restore#exclude>; in that case, a filter cannot be applied, so the Task Filter is not applicable.

How to set up a scheduled backup

Watch a video of this tutorial on YouTube
<https://www.youtube.com/watch?v=5mBO3o570Ak&t=173s>

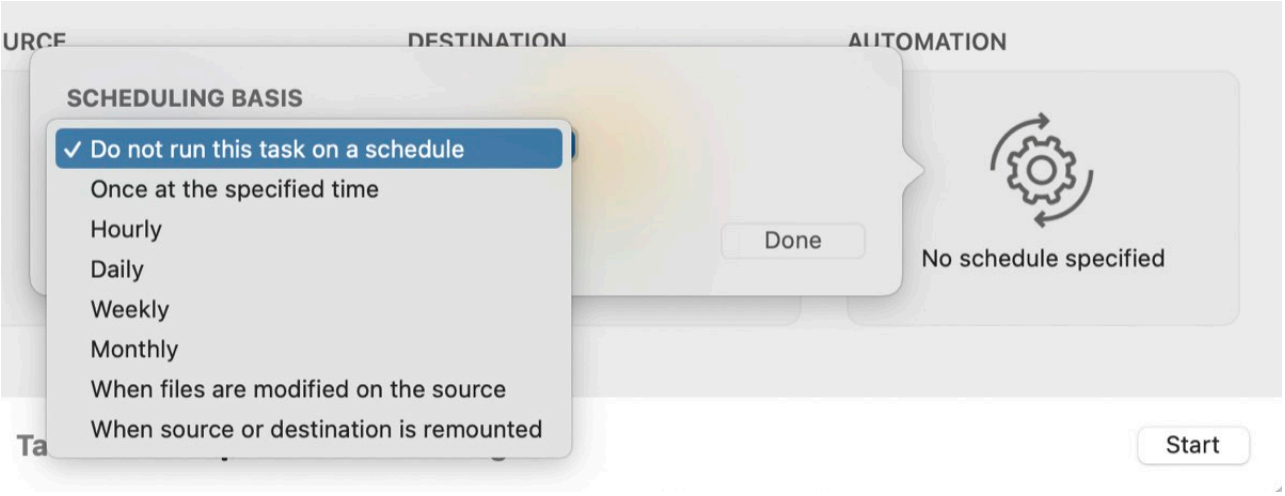
Configure the Task

Configure CCC as if you were going to run a backup task immediately, selecting your **Source** and **Destination**. Click the icon in the **Automation** box to view the scheduling options.

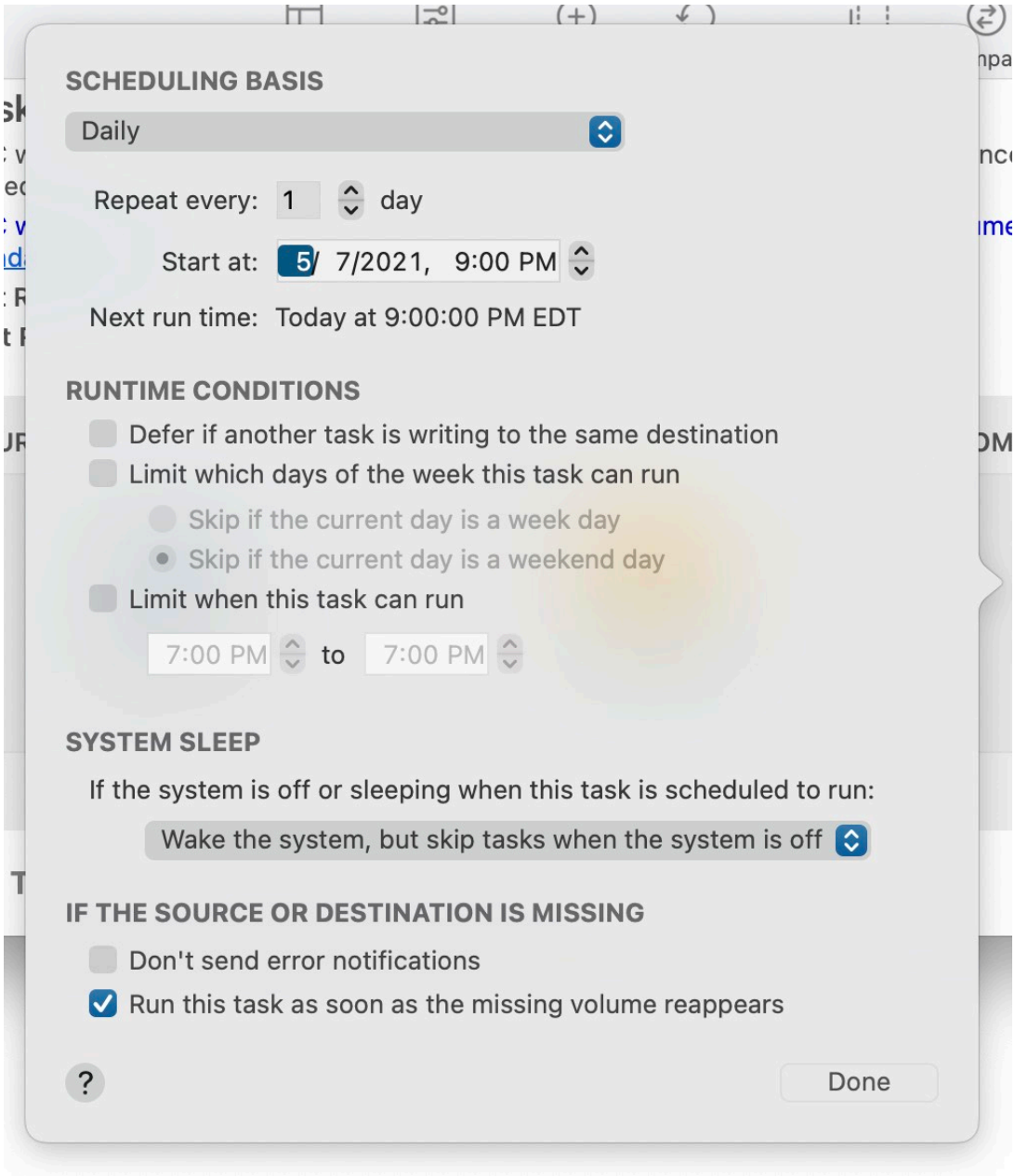


Design a Schedule

Select when you would like the task to run from the drop down menu. If you would like the task to run at a regular interval, choose to have the task run on an hourly, daily, weekly, or monthly basis. If you would like to have the task run when the source or destination volume is reconnected to your Mac, choose the **When source or destination is reconnected** option.

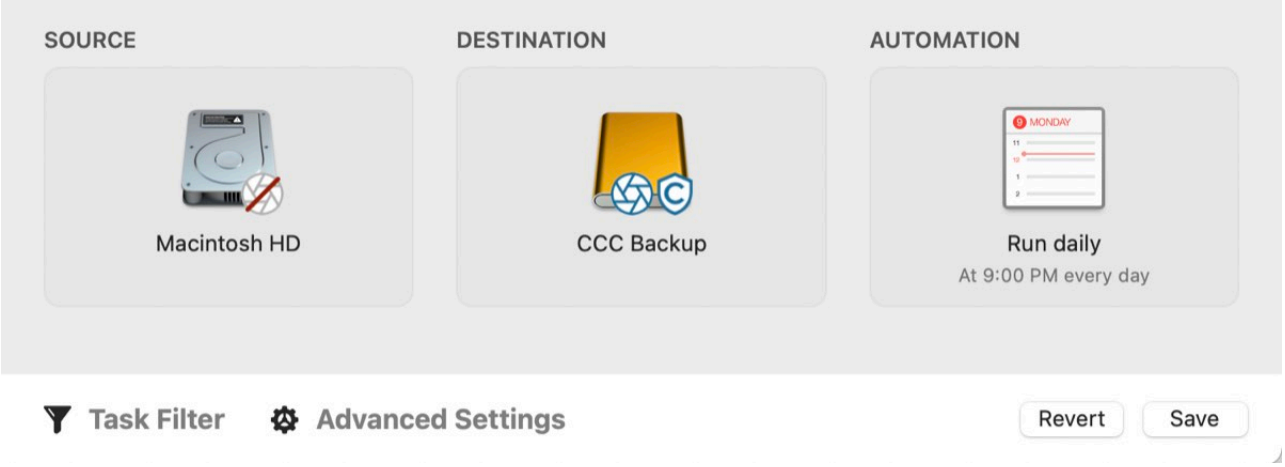


Make any desired changes to the schedule and then click **Done**.



Save the Task

Click **Save**.



Your backup task will run at the times that you have scheduled!

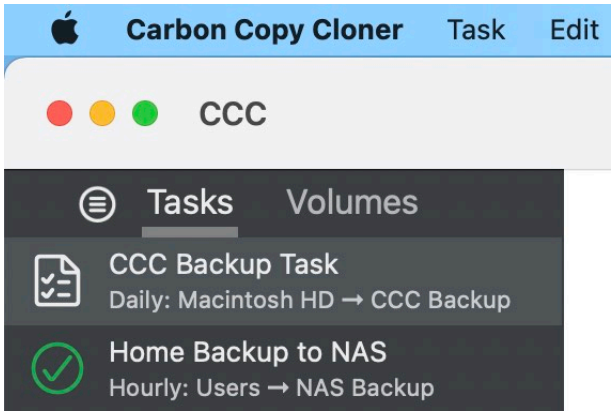
Related Documentation

- How to modify a scheduled backup <https://bombich.com/kb/ccc6/how-modify-scheduled-backup>
- Advanced Scheduling Options <https://bombich.com/kb/ccc6/advanced-scheduling-options>
- Frequently Asked Questions about scheduled tasks <https://bombich.com/kb/ccc6/frequently-asked-questions-about-scheduled-tasks>

How to modify a scheduled backup

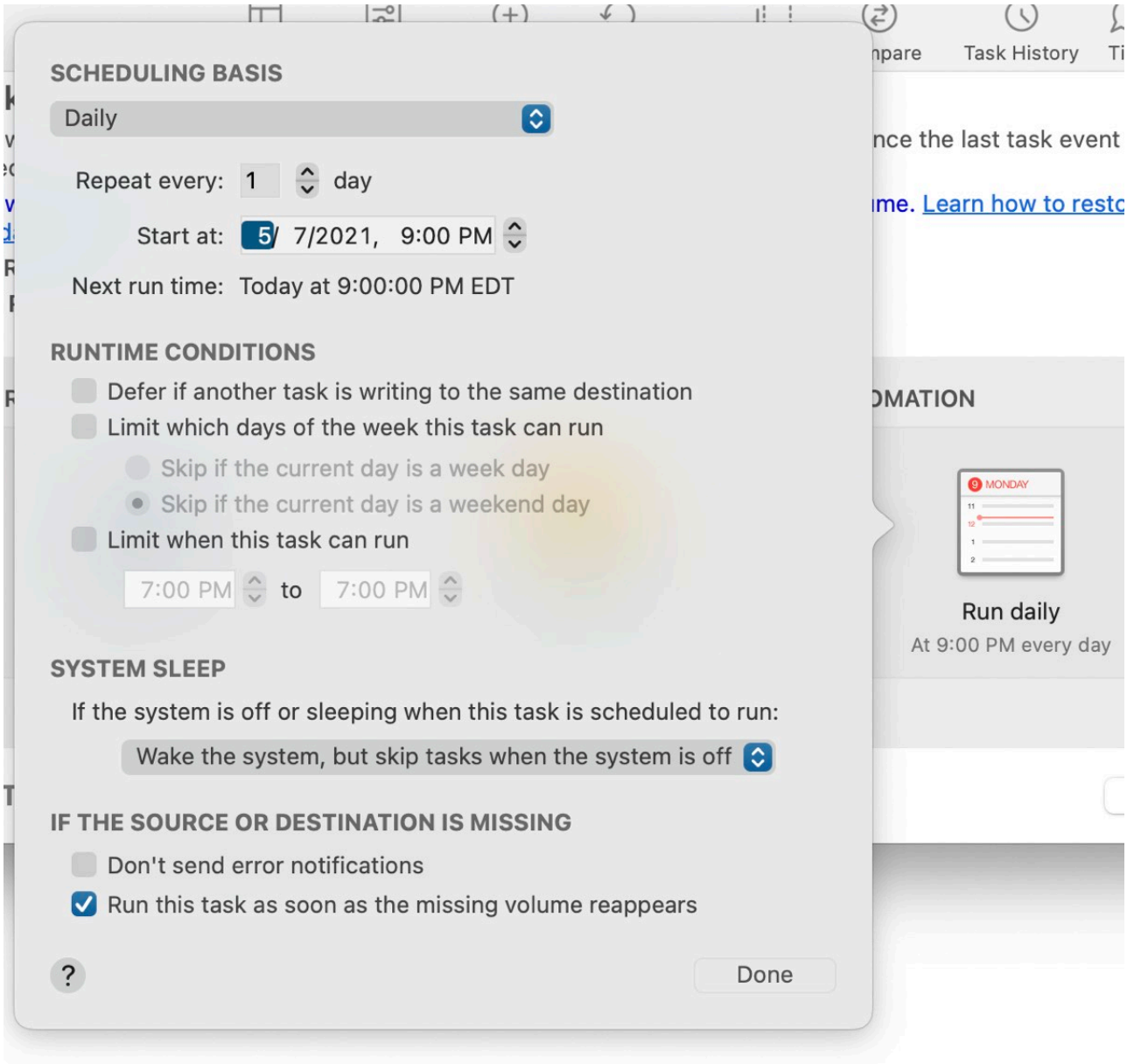
Select the Task

Select the **Task** to be modified. If necessary click **Show Sidebar** in CCC's toolbar to reveal scheduled tasks.

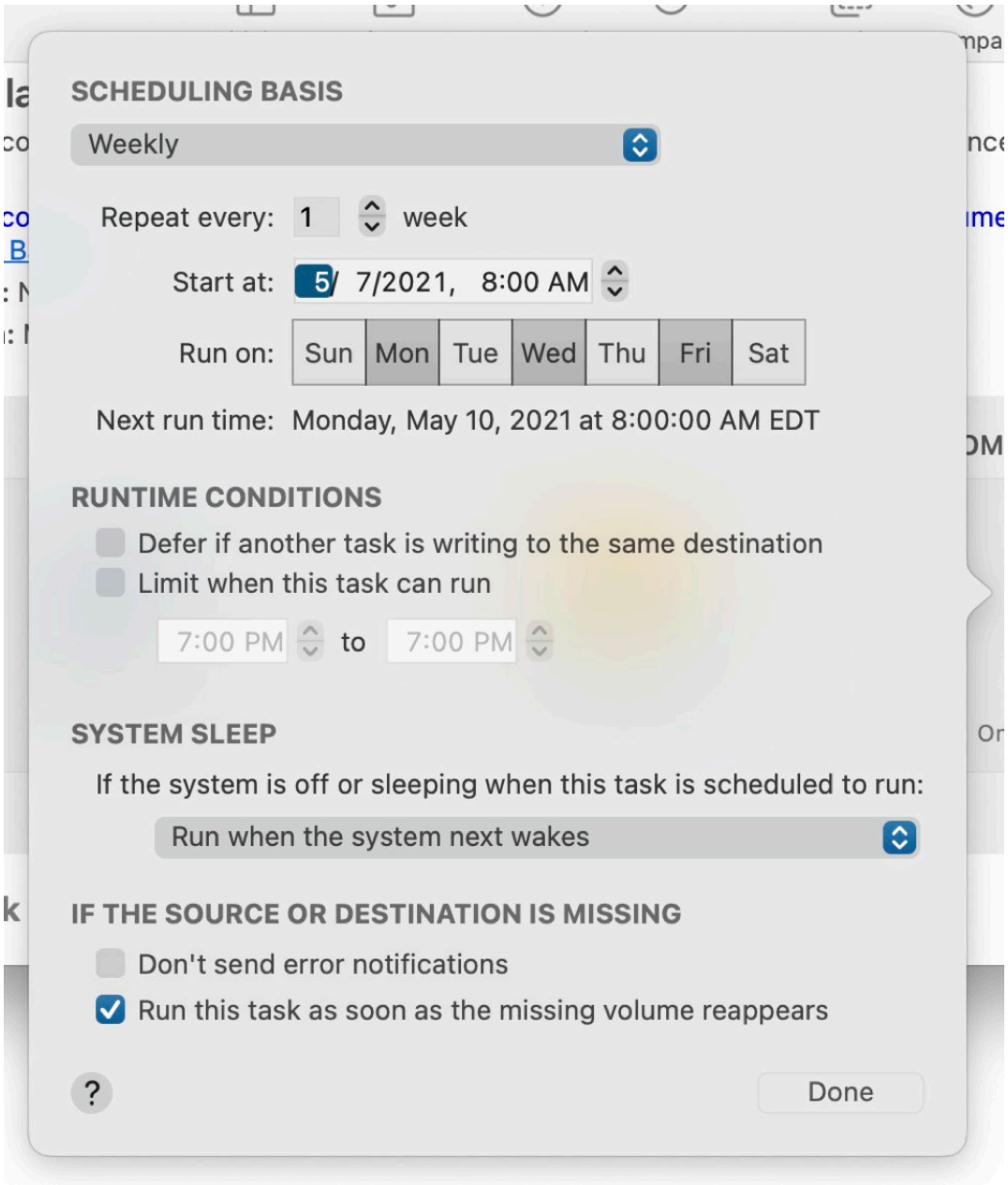


Modify the Schedule

Click the icon in the center of the **Automation** box. If your task is currently scheduled to run "When files are modified on the source", click the  or  buttons to suspend source monitoring, then you can edit the schedule configuration.



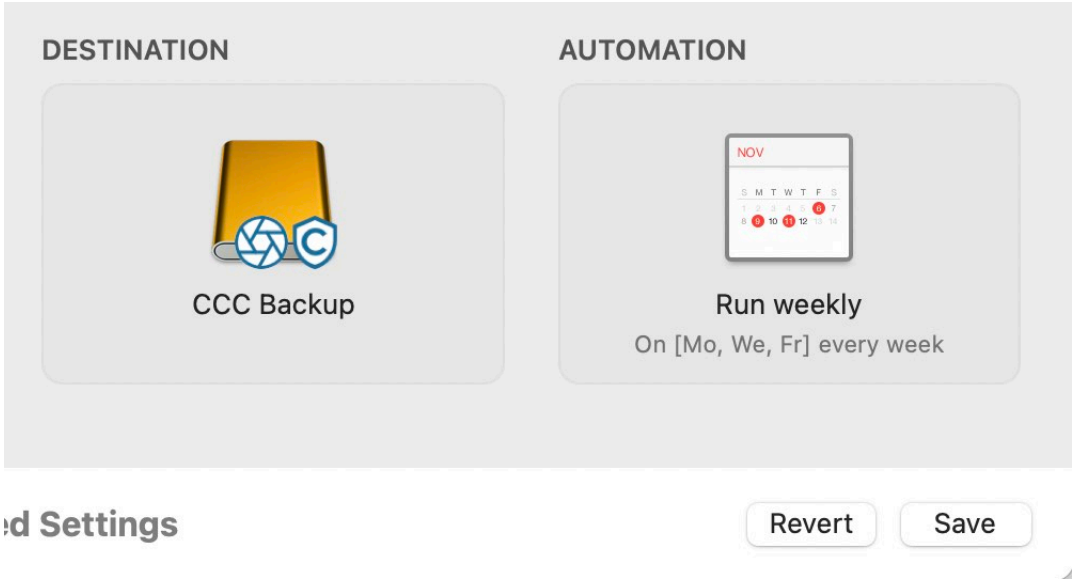
Modify the schedule. Click **Done**.



Save the Schedule

Click **Save**.

Note: If you have changed your mind about any changes you have made to your task settings, you can click the **Revert** button to revert the task to its last-saved settings.



Your backup will now run according to the new schedule!

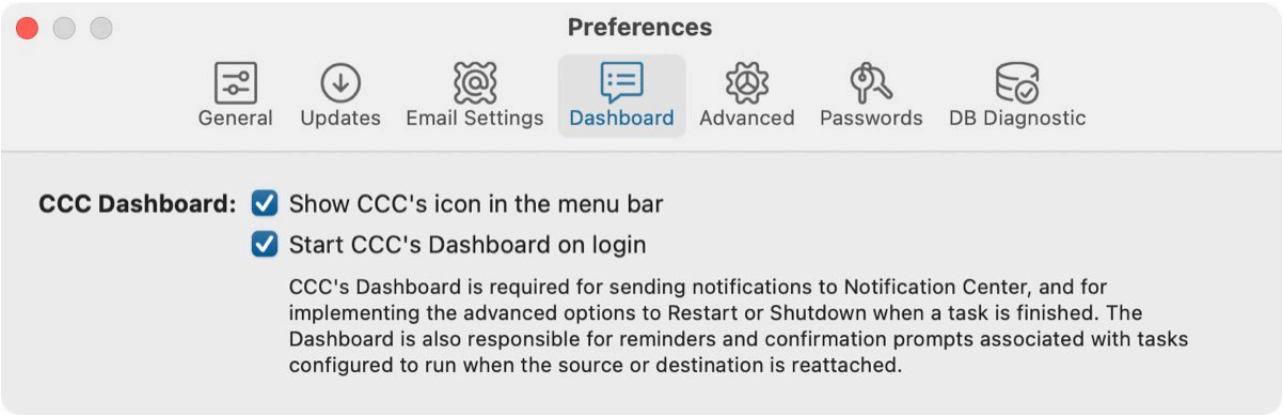
Monitoring backup tasks with the CCC Dashboard

The CCC Dashboard

CCC's Dashboard application gives you quick access to your tasks via a "C" icon in the macOS menubar so that you can quickly determine their status, see which tasks are running, and start, stop, or pause a particular task. The Dashboard also presents a stream of CCC activity, indicates snapshot disk usage on all of the APFS volumes mounted on your Mac, and proactively alerts you to excessive snapshot disk usage on the startup disk. At a glance, the icon that CCC presents in the menubar gives you information about CCC's state:

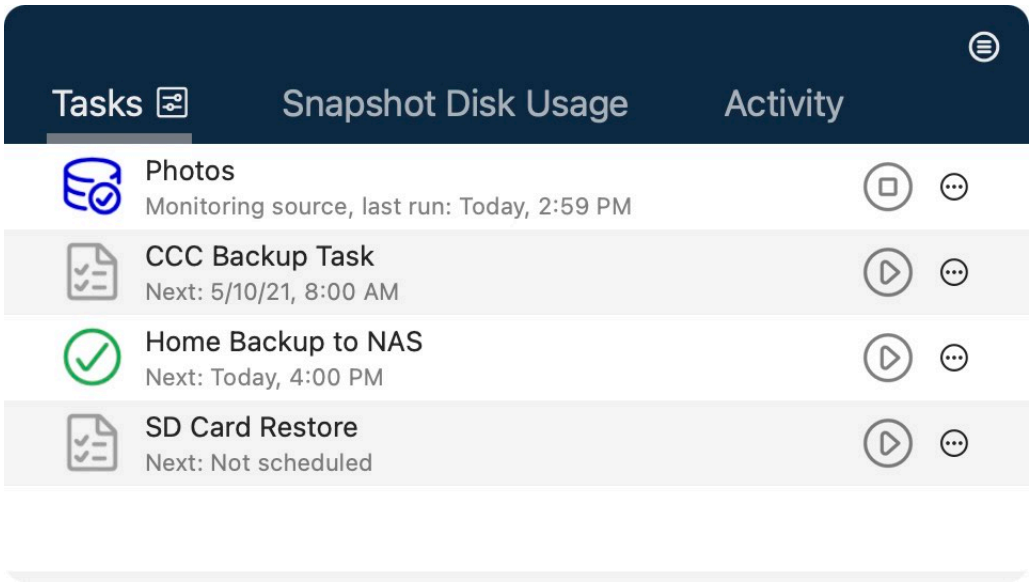
: No tasks are running
: One or more tasks are running
: CCC requires your attention
: CCC tasks are disabled

To choose whether CCC's Dashboard icon appears in your menubar, click **Settings** in the CCC toolbar, then click **Dashboard** in the Settings window toolbar.



Task monitoring

In the Tasks tab of the CCC Dashboard, you can use the controls on each task to start, stop, or (when applicable) pause a task. Click on the "Additional controls" button for options to open the task in CCC and show the task's history.



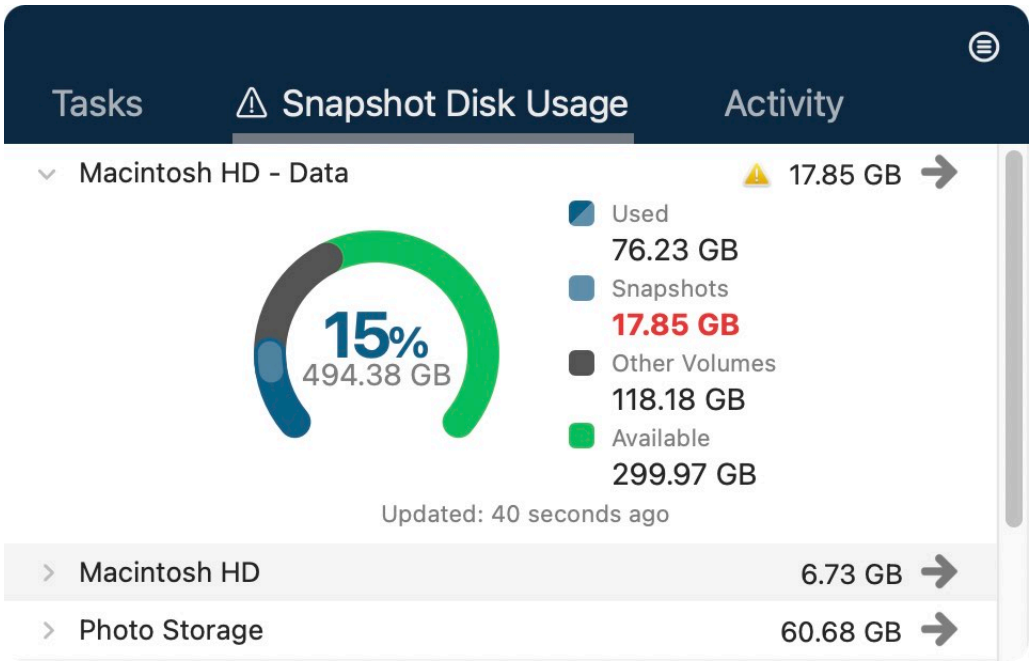
The task icon will indicate the task's most recent state, e.g. a green checkmark to indicate that the task ran successfully, or a red "x" to indicate that the last task encountered an error. Below the task name, CCC will indicate the task's next run time by default. To change the information that is displayed here, click on the Tasks tab header to reveal the settings for this tab.

The mini task progress window

The mini task progress window is still available in CCC v6, but it is disabled by default. If you would like to have this window appear every time a task is running, click on the Tasks tab header, click on the icon to reveal the Tasks tab settings, then check the box to show the mini task progress window when a task is running. Note that the window only appears when a task is currently running.

Snapshot Disk Usage

The CCC Dashboard will periodically calculate snapshot disk usage on every attached APFS volume. For the startup disk in particular, CCC will issue an alert for certain changes to snapshot disk usage. If there is a sudden increase in snapshot disk usage (e.g. a spike of 15GB because you just deleted 15GB of content from the startup disk), the Dashboard icon will change to get your attention, and the Snapshot Disk Usage tab will show an alert icon on the startup disk:



Likewise, if the startup disk's free space has dropped below the free space limit defined in that volume's Snapshot Retention Policy, the Dashboard will raise that to your attention. To see the details of the alert, click the yellow alert button that is adjacent to the volume name.

If you would like to adjust the Snapshot Retention Policy for a volume, or to get to the interface where you can delete snapshots manually, click the arrow button to the right of the volume name.

To adjust the update frequency and the threshold that is used to request your attention, or to turn off this feature, click on the Snapshot Disk Usage tab header, then click on the icon to reveal the settings for this tab.

Activity

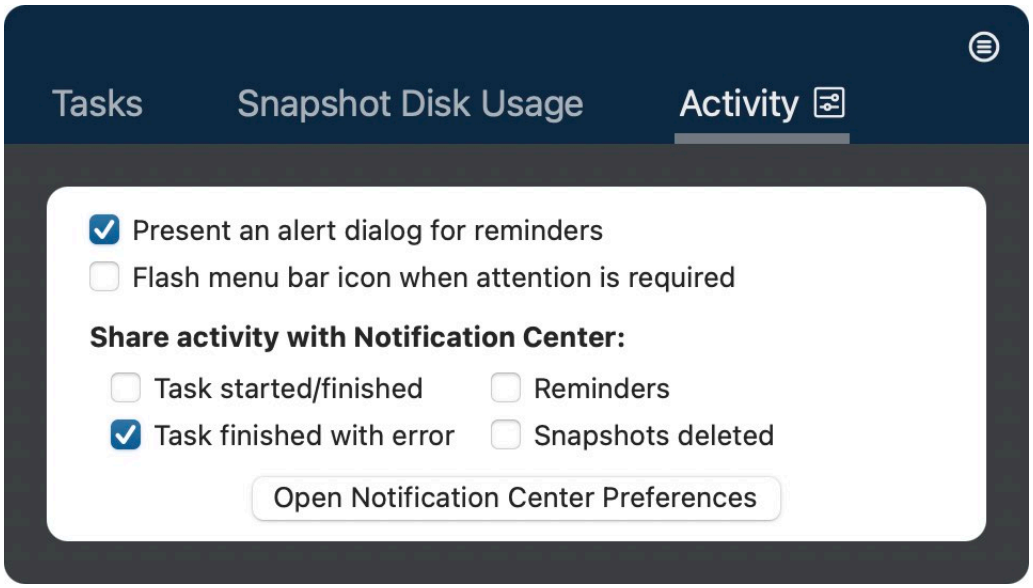
The Dashboard's Activity tab shows a stream of CCC-related activity, e.g. when tasks start and complete, snapshot disk usage-related events, and snapshot removal. When an event occurs that deems your attention (e.g. if a task completes with an error), the CCC Dashboard icon will be adjusted accordingly, and an alert icon will be placed in front of the Activity tab's name. You can click the arrow button to the right of a task-related event to open the affected task in CCC.

Removing activity

Events in the Activity tab are automatically cleared out every time you log in, and whenever CCC is updated – this is not designed to be a permanent record of CCC activity, rather it's a "live stream" of activity. You don't have to remove events from the Activity tab, but if you would like to remove events manually, simply select the event(s) and press the Delete key.

Sending activity notifications to the macOS Notification Center

If you would like CCC activity events to also appear in the macOS Notification Center, click on the Activity tab header, then click on the icon to reveal the Activity tab settings, then check the boxes next to each activity type that you would like to share with Notification Center.



To configure how these notifications are managed and presented by macOS's Notification Center, open the **Notifications** panel in the **System Settings** application.

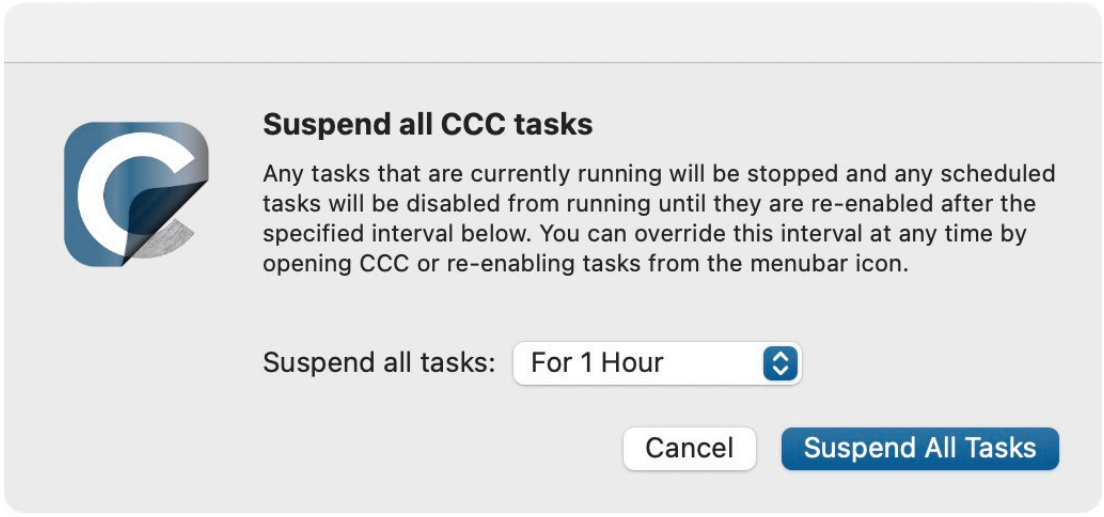
Removing CCC Dashboard from the Notification Center

If you would like to remove CCC Dashboard (or any third-party application for that matter) from the list in the Notification Center, simply select that application in the Notification Center list and press the Delete key.

Suspending tasks

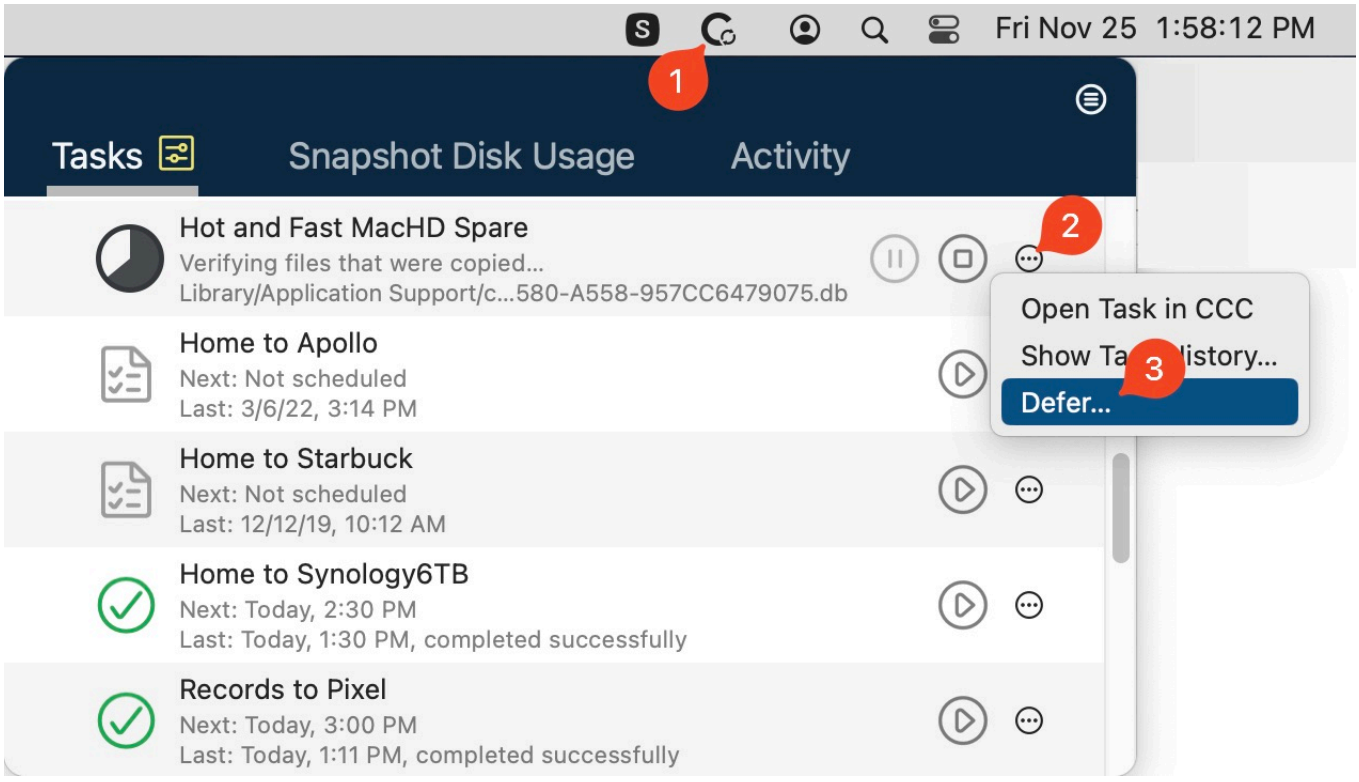
If you would like to suspend all tasks, click the "more actions" button in the Dashboard header, then choose **Suspend all tasks...**. CCC will offer a list of choices ranging from one hour to one week, and also an option to suspend tasks indefinitely. To re-enable tasks, choose **Re-enable all tasks** from the same menu, or simply open CCC and choose to re-enable tasks when prompted.

Note: If you would like to **disable** an individual task, choose **Open task...** from the task's "more actions" button. In CCC, right-click on the task you would like to disable and choose the option to disable the task. Note that task suspension and disabling tasks are separate. If you suspend all tasks, then later lift the suspension, any tasks that you had previously disabled individually will remain disabled.



Deferring a running task

If you find that a task is running at an inopportune time and you want to pause it for longer than a few minutes, you can defer the task to a specific time in the future. Click CCC's menubar icon to reveal the Dashboard, then choose "Defer..." from the "additional actions" menu for the task. A window will appear prompting you to select the date and time that the task should run again.



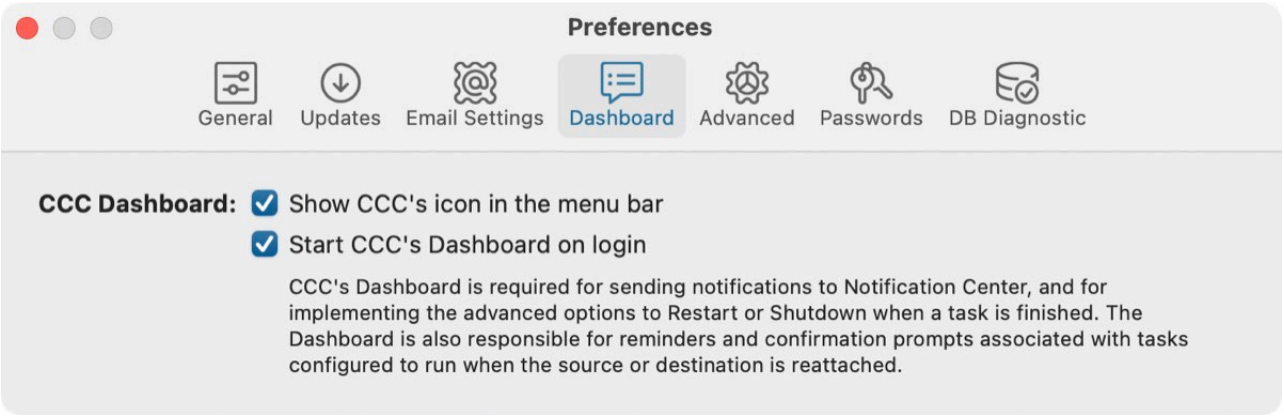
Some features of CCC will be disabled if the CCC Dashboard is not configured to start on login

The CCC menubar application is named "CCC Dashboard", and is bundled inside of the CCC application file. The Dashboard places the CCC icon in the menubar and hosts its associated Dashboard window, but it also provides other proxy-like functionality for CCC's background helper

tool. The following features are provided by the CCC Dashboard:

- **Task started** and **Task finished** Notifications
- The advanced options to **Restart or Shutdown when a task is finished**
- For tasks configured to run when the source or destination is reattached:
    - **Ask for confirmation before proceeding**
    - **Remind me if my task hasn't run in a while**

If you have not configured CCC's user agent to be opened on login, then the features listed above cannot be performed reliably. As a result, those features will be disabled until you configure the Dashboard as a login item. You can change the CCC Dashboard login item setting in the Dashboard section of CCC's Settings window at any time.

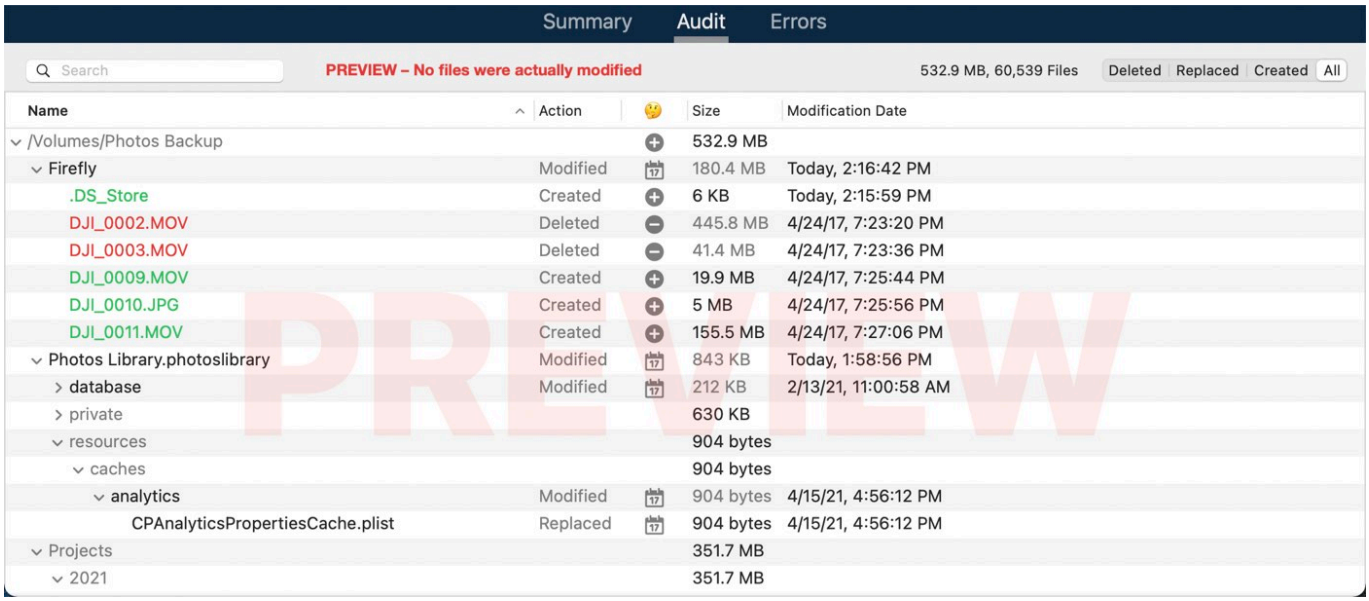


Related Documentation

- Configuring CCC's menubar application preferences
- How to find out when a backup last ran: CCC Task History <https://bombich.com/kb/ccc6/how-find-out-when-backup-last-ran-ccc-task-history>

Preview: See what changes CCC will make to the destination

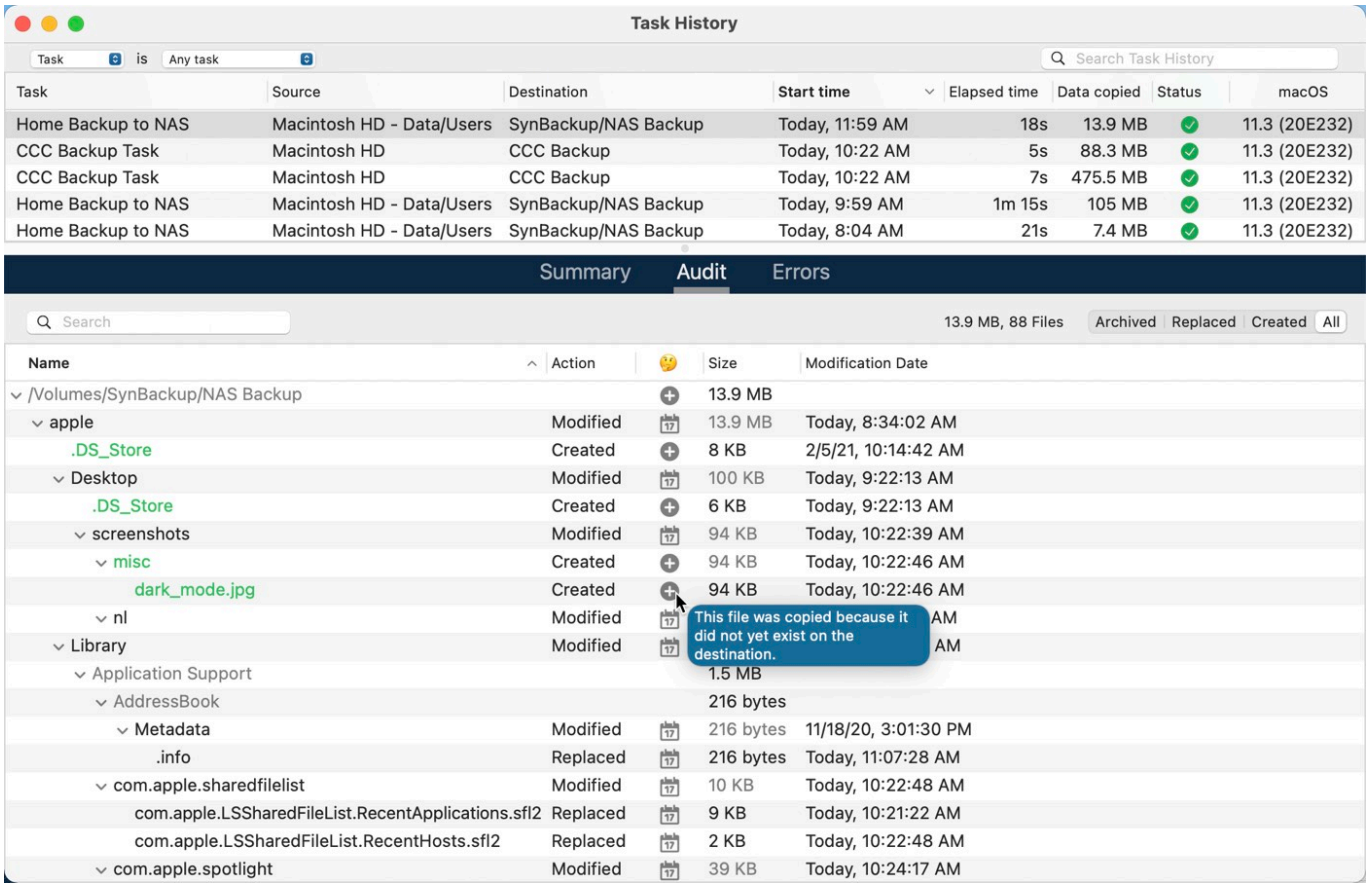
If you're configuring a task and you're a little bit uncertain about what might happen to the current content of the selected destination, **click the Preview button in CCC's toolbar** to perform a "dry run" of the backup task. When the task completes, CCC will present the transaction report in the Task History window:



When you perform a task preview, CCC will go through all of the motions of the task, but won't make any changes to the destination. Note that there are some cases where the Preview will be unavailable, e.g. if the assessment of changes can't be made without actually making changes to the destination. The Preview is also unavailable to tasks that back up to or from a Remote Macintosh.

Task History: See your task event details, statistics, and trends

Each time CCC performs a backup or restore task, the results and statistics of that task are recorded and displayed in CCC's Task History window. To view task history, click on the Task History button in the toolbar, or choose **Task History** from the Window menu.



Task events can be filtered and sorted by task name, source, destination, start time, or status. CCC will show up to 2000 task history events. Each event will indicate when the task started, how long it took, how much data was copied, the overall status of the task, and the CCC and macOS version at the time of the event. There are additional columns available that are hidden by default (e.g. CCC version, Total Size, Settings); right-click on the table header row to choose which columns should be visible.

The color of the status indicator is defined as follows:

- Green: Task completed successfully
- Yellow: The task was completed, but errors occurred while transferring some files
- Red: An error occurred that prevented the task from completing
- Gray: The task was canceled

Audit: Viewing details about the modifications made by the backup task

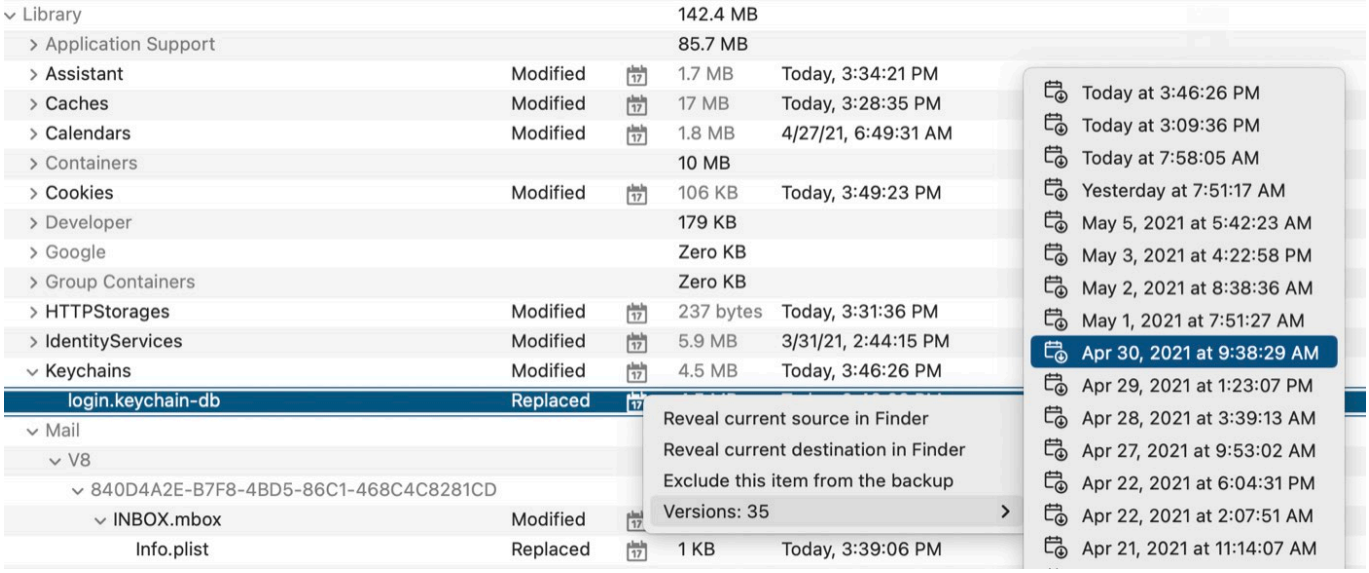
When enabled for a particular task, CCC will record detailed information about the transactions that occurred during the task, e.g. files copied, files updated, folders created or updated, files deleted or archived. Each transaction will indicate the size and modification date of the file at the time of the backup, and the action that was applied to the item. A status icon in the "□□" column indicates why the action was taken, e.g. a file may have been updated because its size or modification date differed on the source and destination. You can hover your mouse over this icon for detailed information about the differences that were noted for that particular item.

Actions applied to files and folders

- Created: (Folders only) This folder was created on the destination because it did not yet exist.
- Modified: (Folders only) The attributes of the folder were modified on the destination (e.g. creation date, permissions, owners).
- Replaced: (Files only) The file was replaced because the size, modification date, or checksum differed.
- Updated: (Files only) The file's content was not changed, but the attributes of the file were updated (e.g. creation date, permissions, owners).
- Cloned: (Files only) The file was not copied, rather it was created via the clonefile feature of the APFS filesystem (only applicable when the source and destination are folders on the same APFS volume).
- Deleted: The file or folder was deleted (note that if snapshot support is enabled on the destination, the item may still be retained by a snapshot).
- Archived: The file or folder was moved into the "_CCC SafetyNet" folder.
- Indexed: The file was not recopied, but CCC read the entire source file and calculated a checksum of this file for future reference.

Viewing the current item on the source or destination, viewing older versions

Right-click on a transaction to view a contextual menu of options specific to that item. If older versions of a file are available in a snapshot, those versions will be listed in the Versions sub menu. Note that these options will be disabled if your source and destination volumes are not mounted.



CCC will prompt to remove a task's audit when you change the source or destination

Transactions stored within a task's audit are specific to the source and destination that were selected when the task ran. When you change the source or destination to a task, CCC will prompt you to either remove the current audit records or to create a new task. Removing the audit records won't affect any of the data on your source or destination, it only removes the record of changes that were made to the destination in the past. When you remove audit records, you'll no longer be able to see the transactions in the Task History window > Audit tab, and you won't be able to verify the integrity of files on the source or destination against the "last known state" <https://bombich.com/kb/ccc6/how-verify-or-test-your-backup#adhoc>.

If you no longer need a record of the changes made to the destination in the past, or if you've erased the destination, then we recommend that you remove the audit records.

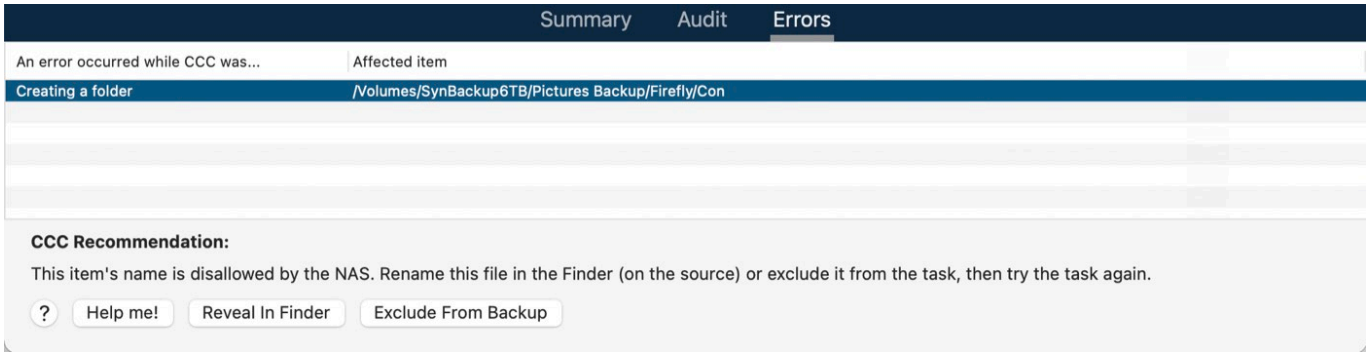
If you're configuring a new source:destination pair, however, we recommend that you create a new task for that purpose. Ideally, you should retain a separate task for each source:destination pair that you have so you can avoid making constant changes to the source and destination configuration.

Related documentation

- Transaction privacy and disabling transaction collection <https://bombich.com/kb/ccc6/how-verify-or-test-your-backup#disable_transactions>

Errors

There are many hardware and filesystem problems that could affect your Mac's hard drives. Filesystem and media corruption are commonplace, and CCC delivers expert advice to you when errors occur. CCC's Task History window shows the results of all of your backup tasks, and details of any errors that occur. CCC enumerates these errors, analyzes them for common conditions, then explains the problem in simple terms with down-to-earth advice for fixing the problem.



Exporting a list of affected files

If you would like to save a list of the affected files in the errors table, select the affected items (or press Command+A to **Select All**), then choose **Copy** from CCC's **Edit** menu (or Command+C) to copy the list of items to the clipboard. Please note that every error may not be the same. When you export a list of files, the per-file contextual information is not retained. Return to CCC's Task History window for the contextual information and advice specific to each file.

Getting help for common errors

When errors occur, CCC will categorize the error and offer troubleshooting advice. For some errors, CCC will offer helpful buttons at the bottom of the task history window that will, for example, take

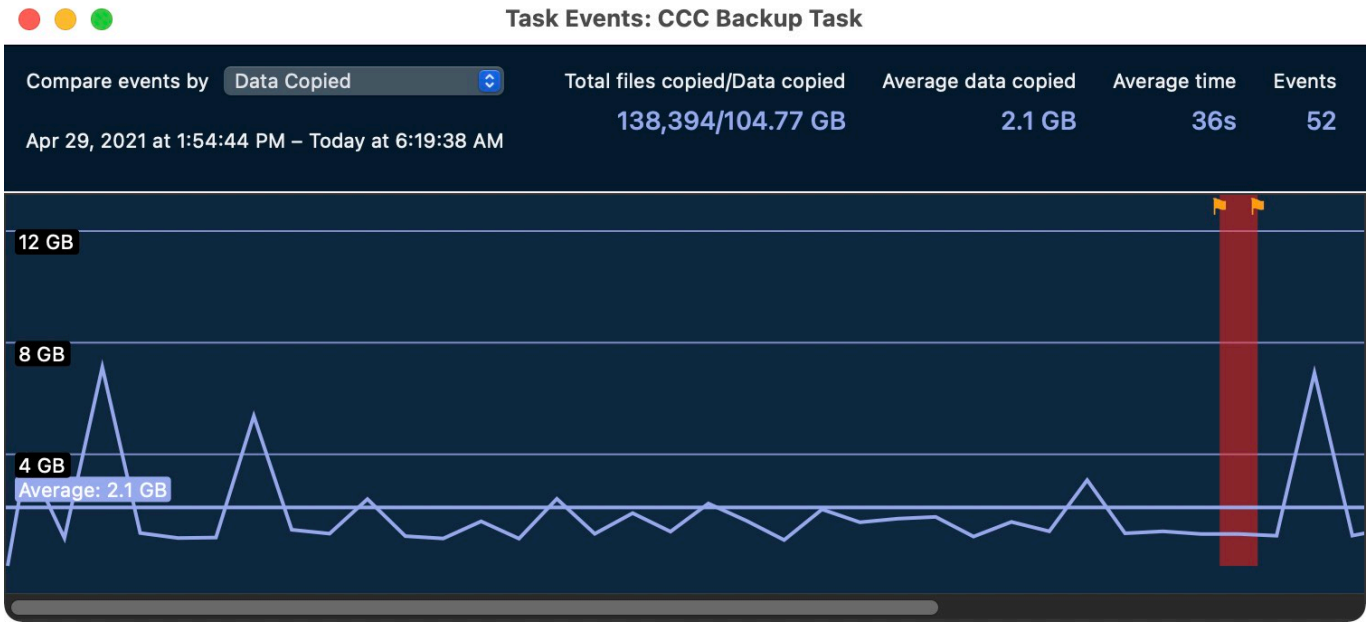
you to Disk Utility or reveal a corrupted file in the Finder. If the affected file is one that doesn't need to backed up, click the button to exclude the item from the backup task to avoid future errors on that file. Click on each error to see what CCC recommends to resolve the error. If you're stuck or overwhelmed, or if CCC's advice alone isn't helping you resolve the problem, click the "Help Me!" button to submit a summary of the problem to the Bombich Software Help Desk.

Related Documentation

- "Where can I find CCC's log file?" <https://bombich.com/kb/ccc6/where-can-i-find-cccs-log-file>

Task Trends Dashboard

To view task-specific statistics over time, right-click on a task event and choose **Show Task Trends Dashboard**. You can view the task trends based on elapsed time, total source data set size, the number of files copied, the amount of data copied, or the size of the largest file. Hover your mouse over the chart to see the details of each event. Click on an event to reveal that event in the Task History window.



Can I remove events from CCC's Task History window?

To remove one or more task events from the history table, select the events, then right-click on the selection and choose **Remove** from the contextual menu. Removing task events from the Task History window has no effect on the backup, it only removes the event from CCC's Task History window, as well as any transactions stored in CCC's task history database. You must be logged in as an administrator user to delete task history events.

If you would like to clear all of CCC's task history, open the Task History window, then choose **Clear Task History...** from CCC's **Task** menu.

Protecting data that is already on your destination volume: The CCC SafetyNet

*SafetyNet is a **safety mechanism** that works to avoid accidental loss of data on the destination. SafetyNet is not designed to offer backup versioning. If you're looking for access to older versions of your files, enable snapshot support on your APFS-formatted backup volume <https://bombich.com/kb/ccc6/leveraging-snapshots-on-apfs-volumes>. If your destination volume is dedicated to a single CCC backup task, you can disable the SafetyNet feature – click on the Destination selector and choose "SafetyNet Off" from the SafetyNet submenu.*

In a typical backup scenario, you have a disk that is dedicated to the task of backing up your startup disk, and you expect the contents of the backup disk to match the contents of the source exactly. In many cases, though, people see lots of extra space on a big 3TB disk and can't resist using it for "overflow" items — large video files, archives of old stuff, maybe your iMovie Library. If you already have that big disk loaded with some overflow items and you're hoping to use it as a backup volume as well, you'll find that CCC's default settings are designed to give you that backup without completely destroying everything else on your backup disk in the blink of an eye.

When CCC copies files to the destination, it has to do something with files that already exist on the destination — files that are within the scope of the backup task, and items that aren't on the source at all. By default, CCC uses a feature called the SafetyNet to protect files and folders that fall into three categories:

- Older versions of files that have been modified since a previous backup task
- Files that have been deleted from the source since a previous backup task
- Files and folders that are unique to the root level of the destination

SafetyNet Snapshots

If you're backing up to an APFS-formatted destination volume that has CCC snapshot support enabled, then CCC's SafetyNet feature is implemented via snapshots. At the beginning of the backup task, CCC creates a **SafetyNet Snapshot** on the destination. This snapshot captures the state of the destination volume before CCC makes any changes to it. When CCC proceeds to update the destination, it deletes and replaces files immediately as applicable. Because the files are retained by the SafetyNet Snapshot, those files are not permanently deleted until the snapshot is deleted. Protection of items that are unique to the root-level of the destination remains the same as described below.

Legacy SafetyNet Behavior: SafetyNet On

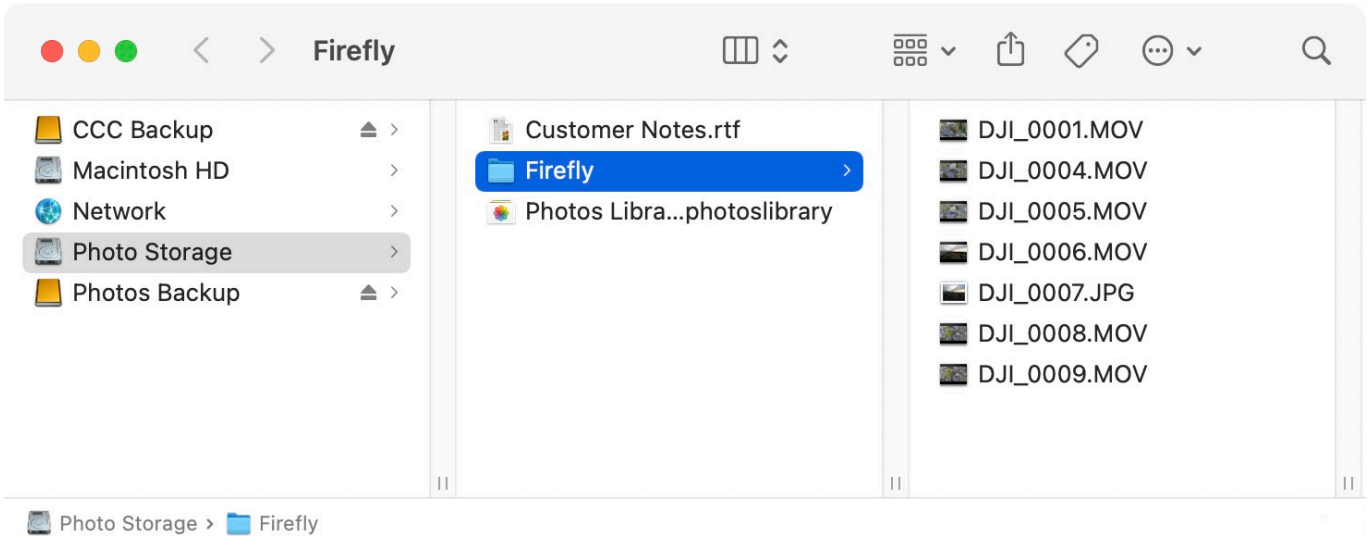
If you're backing up to a non-APFS volume, or if you have snapshot support disabled for an APFS destination, then CCC's SafetyNet is implemented as a folder on the destination.

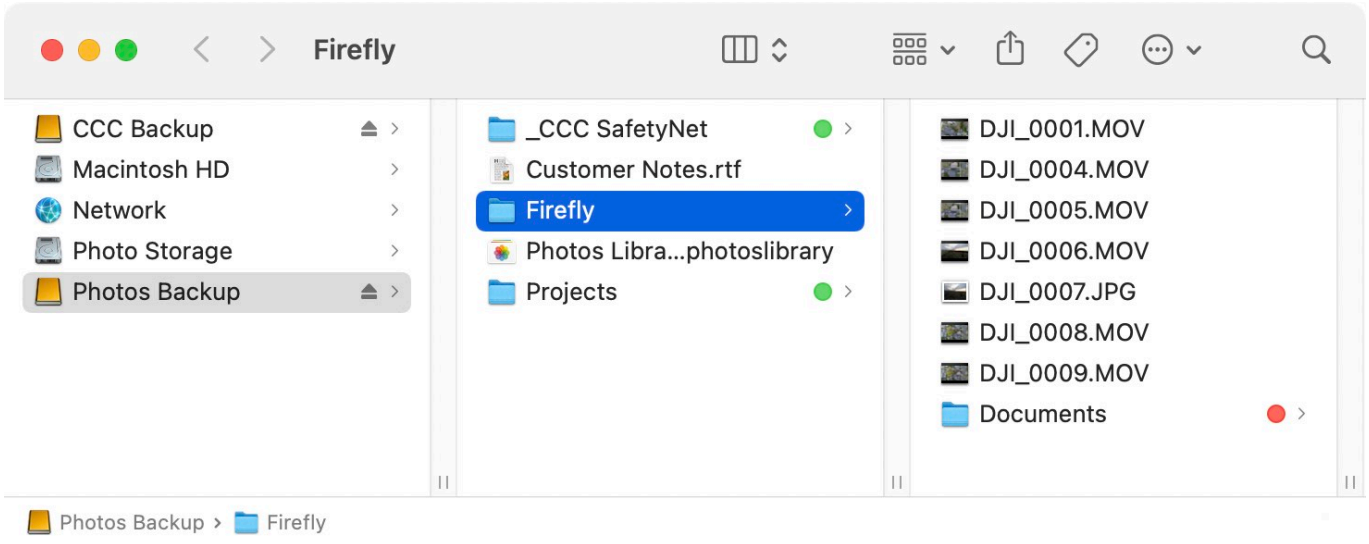
Catalina: Where is the CCC SafetyNet folder on the destination? <https://bombich.com/kb/ccc6/frequently-asked-questions-about-ccc-and-macos-catalina#safetynet>

SafetyNet On

When the SafetyNet is on, CCC places the older versions of modified files, and files that have been deleted from the source since a previous backup, into the _CCC SafetyNet folder at the root of the destination. We call this a "safety net" because the alternative would be to immediately delete those items. The SafetyNet prevents catastrophes — rather than immediately deleting items from the destination, CCC saves these items on the destination as long as space allows.

That third category of files and folders is left alone on the destination when the SafetyNet is enabled. Files and folders that are unique to the root level of the destination will be left completely alone. To get a better of idea of what that means, consider the following two Finder windows:





The first window shows the contents of the source, the second window shows the contents of the destination volume. The "root" of the destination volume is what you see in the second pane. There are two items that are unique to the root level of the destination volume, "**_CCC SafetyNet**" and "**Projects**". If CCC were to update this volume with the SafetyNet on, both of these folders, tagged as green in the screenshot, would be left alone by CCC. The "**Firefly**" folder, however, is not unique to the destination — that folder is present on both the source and destination. As a result, the "**Documents**" folder that is inside the **Firefly** folder would **not** be left in place, rather it would be moved to the **_CCC SafetyNet** folder.

Protecting items at the root level of the destination

The **SafetyNet On** setting includes an option to protect items that exist at the root of the selected destination. This feature was designed to avoid any modifications at all to items that only exist at the root of the destination. Referring again to the example above, suppose you have a folder named **Projects** on a volume named **Photos Backup**. When you choose the **Photos Backup** volume as the destination for your task and leave SafetyNet enabled, CCC will leave that **Projects** folder right where it is — the folder will not be deleted, nor moved into the _CCC SafetyNet folder.

The "root" of the destination refers to the first or top-most folder relative to your **selected** destination. If you selected a volume named **Photos Backup** as the destination, then the root level refers to the root of the volume — what you see when you open that volume in the Finder (again, the middle pane in the screenshot above). If you selected a folder as the destination for your task, then the "items at the root of the destination" refers to the items that you find in that specific folder that you selected as the destination, not the root of the whole volume. When you select a folder as the destination, anything outside of that folder is completely outside of the scope of the backup task, and will be left alone by that particular backup task.

The **Protect root-level items on the destination** setting is not mandatory for the SafetyNet feature. If you would like to keep SafetyNet enabled, but you want CCC to remove items from the root of the destination that were removed from the source, click the Advanced Settings button, then uncheck the **Protect root-level items on the destination** setting.

Limiting the growth of the SafetyNet folder

When the SafetyNet feature is enabled for a CCC backup task, CCC will automatically prune the contents of the SafetyNet folder, by default, when the free space on the destination drops below 25GB. CCC will automatically adjust that pruning limit as necessary, e.g. if you have a backup task that copies more than 25GB, CCC will perform additional pruning and increase the pruning limit.

Generally you won't need to adjust CCC's pruning behavior, but you can customize the pruning settings for each task in Advanced Settings. CCC offers pruning based on size of the SafetyNet folder, age of items within the SafetyNet folder, and amount of free space on the destination.

Auto Adjustment of the SafetyNet Free Space pruning limit

When the **Auto Adjust** option is enabled (and it's enabled by default), CCC will automatically increase the free space pruning limit if your destination runs out of free space during the backup task. For example, if your pruning limit is set to the default of 25GB, and you have 25GB of free space at the beginning of the backup task, no pruning will be done at the beginning of the task. If that task proceeds to copy more than 25GB of data, however, the destination will become full. CCC will then increase the pruning limit by the larger of either the amount of data copied in the current task, or by the amount of data that was required by the last file CCC attempted to copy. For example, if CCC copied 25GB of data, then the pruning limit would be increased by 25GB. If CCC wanted to copy a 40GB file, however, CCC would not fruitlessly copy 25GB of that file, rather it would immediately increase the pruning limit by 40GB, revisit pruning, and then restart the task.

Lastly, note that you may change the pruning limit manually if the automatically-adjusted value is set higher than you prefer. The auto adjustment feature is designed to make SafetyNet pruning more liberal and less fussy, but you may reset the pruning limit to a lower value at any time.

SafetyNet Off

If you always want the destination to match the source, you can disable CCC's SafetyNet – click on the destination selector and choose **SafetyNet Off** from the SafetyNet submenu. When CCC's SafetyNet is disabled, older versions of modified files will be deleted once the updated replacement

file has been successfully copied to the destination, and files that only exist on the destination will be deleted permanently. Files and folders that are unique to the destination will not be given special protection from deletion. **The only exception to this is the _CCC SafetyNet folder — CCC will not delete that folder.** If the _CCC SafetyNet folder was created in a previous task that had the SafetyNet enabled, you can simply drag the SafetyNet folder to the Trash to dispose of it.

Protect root level items on the destination

CCC's SafetyNet includes a key feature that provides protection for items that are unique to the root level of the destination volume (see the explanation in the "SafetyNet On" section above). When you choose **SafetyNet Off** from the SafetyNet popup menu, the **Protect root level items on the destination** setting is disabled if there are no other advanced settings enabled for the task. If you would like to use that setting with the SafetyNet disabled, click the **Advanced Settings** button, then check the box next to that option.

Don't delete anything

With this setting, CCC won't delete anything from the destination. If a file exists on the destination and not on the source, that file will be left in place on the destination. If CCC is updating a file on the destination, the older version of the file will be moved to CCC's SafetyNet folder. This setting is useful for source folders and volumes that leverage excellent organization. For example, if you store photos by project name, and you like to remove those projects from the source as a whole when the project is complete, you can use the **Don't delete anything** SafetyNet setting to avoid removing those archived projects from the destination.

One cautionary note about using this setting: Older files will accumulate on the destination, consuming more space than is consumed on the source. Also, if your files are not well organized, you may find a future restore to be quite tedious because everything you've deleted from the source will still be on the backup.

Other ways to protect the data on your backup volume

If you would rather that CCC did not move or delete files that are unique to your backup volume (e.g. files that are not part of the source data set), there are a couple other ways to protect that data.

Add a new partition to the destination hard drive

You can use Disk Utility to resize existing HFS+ formatted volumes and to add new volumes to APFS containers. These actions can be done non-destructively – without erasing the files and folders on any existing volumes.

Back up to a folder

You can use CCC to back up your data to a subfolder on the destination volume. When backing up to a subfolder on the destination volume, CCC's copying and deleting considerations are made entirely within the scope of that subfolder — content outside of that subfolder is not considered or affected by the backup task. To back up to a folder, select "Choose a folder..." from CCC's Destination selector.

General thoughts on keeping "other" data on your backup volume

We strongly recommend that you find the means to dedicate a volume to the task of

backing up your irreplaceable data. If you have data on your backup volume that exists nowhere else, it is not backed up! Whenever you target a volume for use with CCC, there is a risk that some files will be removed for one legitimate reason or another. CCC offers options and warnings to protect your data from loss, but nothing can protect your data from a misuse of CCC or a misunderstanding of the functionality that it provides.

Related Documentation

- Frequently asked questions about the CCC SafetyNet <https://bombich.com/kb/ccc6/frequently-asked-questions-about-carbon-copy-cloner-safetynet>
- Leveraging Snapshots on APFS Volumes <https://bombich.com/kb/ccc6/leveraging-snapshots-on-apfs-volumes>

Files that aren't on the source may be removed from the destination

CCC makes non-proprietary backups – when you configure a source and a destination to a CCC task, the objective is have the same files on the source and destination, and in the same hierarchical arrangement. To achieve that objective, CCC will make exact copies of your source files on the destination, and CCC will also remove content from the destination that is not on the source. The removal of content from the destination is important to consider when you select a destination volume. If you already have content on the destination that's unrelated to the source, that content may be removed, and possibly even deleted.

Dedicate a volume to the backup task

We recommend that you dedicate a backup volume to each backup task. If you want to store other data on the backup disk (i.e. content that is unrelated to the source that you're backing up), store it on other volumes that are not specified as a CCC destination. This CCC Kbase article explains how to create volumes in Disk Utility:

Adding volumes or partitions to a backup disk <https://bombich.com/kb/ccc6/i-want-back-up-multiple-macs-or-source-volumes-same-hard-drive>

The benevolent CCC SafetyNet

When CCC copies files to the destination, it has to do something with files that are already on the destination. By default, CCC uses a feature called SafetyNet to offer some temporary protection for files and folders on the destination that fall into three categories:

- **Replaced files**: Files that get replaced during the backup task
- **Deleted items**: Files and folders that are not on the source (e.g. because they were deleted from the source, or because they were placed on the destination outside of the scope of the backup)
- **Root-level items**: Files and folders that are unique to the root level of the destination

The SafetyNet setting is indicated by a badge that is applied to the destination icon:

-  SafetyNet is enabled
-  SafetyNet is disabled

To access the SafetyNet settings, click on the Destination selector and make a selection from the SafetyNet submenu. You should expect the following results with the specified SafetyNet settings:

SafetyNet On

- **Replaced files**: Removed, but retained *temporarily* in a SafetyNet snapshot or the "_CCC SafetyNet" folder
- **Deleted items**: Removed, but retained *temporarily* in a SafetyNet snapshot or the "_CCC SafetyNet" folder
- **Root-level items**: Left in place on the destination if "Protect root-level items" is enabled, otherwise removed, but retained *temporarily* in a SafetyNet snapshot or the "_CCC

SafetyNet" folder

SafetyNet Off

- **Replaced files**: Deleted as soon as the replacement file is successfully copied to the destination
- **Deleted items**: Deleted immediately
- **Root-level items**: Left in place on the destination if "Protect root-level items" is enabled, otherwise deleted immediately

Don't delete anything

- **Replaced files**: Removed, but retained *temporarily* in a SafetyNet snapshot or the "_CCC SafetyNet" folder
- **Deleted items**: Left in place on the destination
- **Root-level items**: Left in place on the destination

While the "Don't delete anything" option would seem to be the most conservative and desirable way to avoid losing anything on the destination, please keep in mind that it can make future restore activity very tedious. If CCC is not permitted to remove content from the destination that was removed from the source, that content will build up on the destination, intermingled with all content that is "current". If you want to store archived content on your backup disk, we recommend that you create a separate volume on the backup disk for that purpose.

Recovering content from the SafetyNet

SafetyNet protection is *temporary*. SafetyNet is designed as a temporary reprieve for the **current** backup task event. While that content is not deleted immediately during the current task event, it is still subject to removal in future task events. So, if you want to recover content from the SafetyNet, it's important that you conclude that activity before running additional backup tasks.

If snapshot support is enabled on your destination volume, click on the Destination selector and choose "Manage snapshots on {volume name}" to open the Snapshot settings for that volume. SafetyNet snapshots are indicated by the SafetyNet badge icon indicated above. Double-click a snapshot to reveal that snapshot volume in the Finder. Complete instructions for recovering files from a SafetyNet snapshot are available here: Restoring files to your destination from a SafetyNet Snapshot <https://bombich.com/kb/ccc6/how-restore-from-your-backup#restore_safetynet_snapshot>.

If snapshot support is not enabled on your destination volume, click on the Destination selector and choose "Reveal Data Volume" (if that option is present), or "Reveal in Finder". When SafetyNet content is present, you'll find a folder named "_CCC SafetyNet" at the root level of the destination volume. To restore content from that folder, simply drag and drop the files to wherever you want to keep them.

When the SafetyNet feature is disabled and content is removed from the destination, that content is not recoverable. Likewise, once SafetyNet content is removed in a future backup task event, that content will not be recoverable.

General thoughts on keeping "other" data on your backup volume

We strongly recommend that you find the means to dedicate a volume to the task of backing up your irreplaceable data. If you have data on your backup volume that exists nowhere

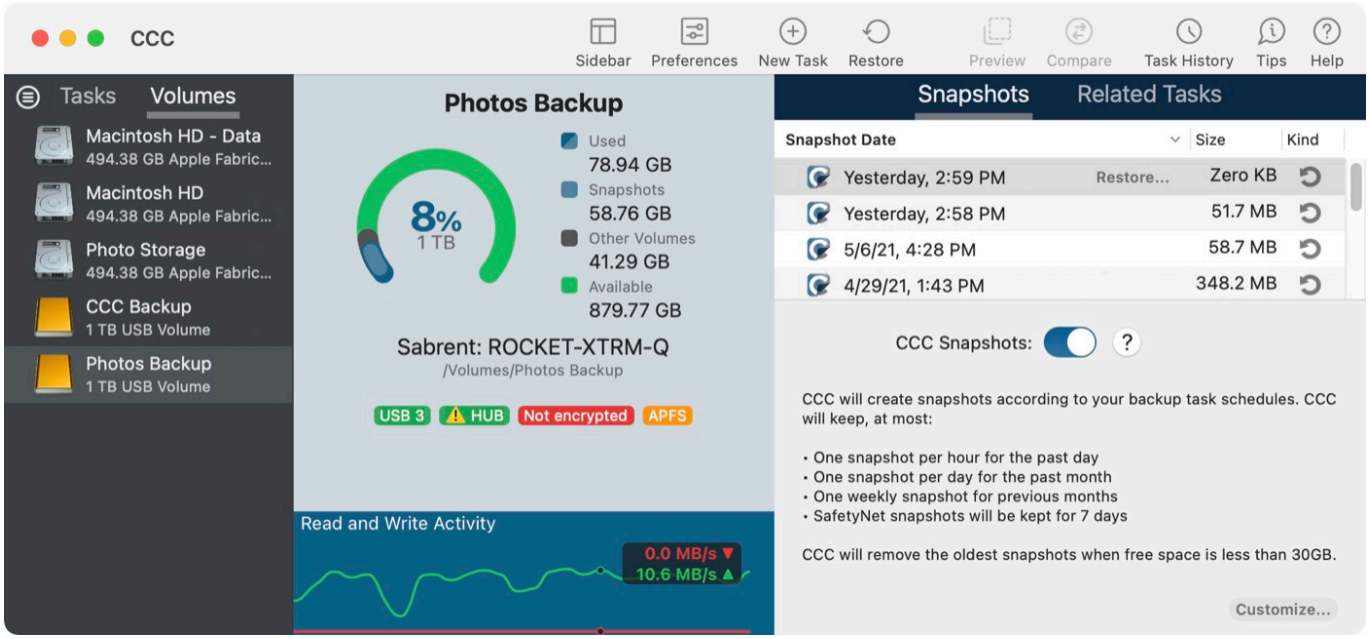
else, it is not backed up! Whenever you target a volume for use with CCC, there is a risk that some files will be removed for one legitimate reason or another. CCC offers options and warnings to protect your data from loss, but nothing can protect your data from a misuse of CCC or a misunderstanding of the functionality that it provides.

Related Documentation

- Protecting data that is already on your destination volume: The CCC SafetyNet <https://bombich.com/kb/ccc6/protecting-data-already-on-your-destination-volume-carbon-copy-cloner-safetynet>
- Frequently asked questions about the CCC SafetyNet <https://bombich.com/kb/ccc6/frequently-asked-questions-about-carbon-copy-cloner-safetynet>
- Leveraging Snapshots on APFS Volumes <https://bombich.com/kb/ccc6/leveraging-snapshots-on-apfs-volumes>

The Disk Center

CCC's Disk Center shows general volume information for each locally-attached volume mounted on your Mac, a list of snapshots and snapshot-related settings for APFS volumes, as well as read and write rate and error statistics for those volumes. Select a volume in CCC's sidebar (click "Show Sidebar" in the toolbar if it is hidden) to view that volume in the Disk Center. CCC also shows any backup tasks that are associated with the selected volume.



Basic volume information

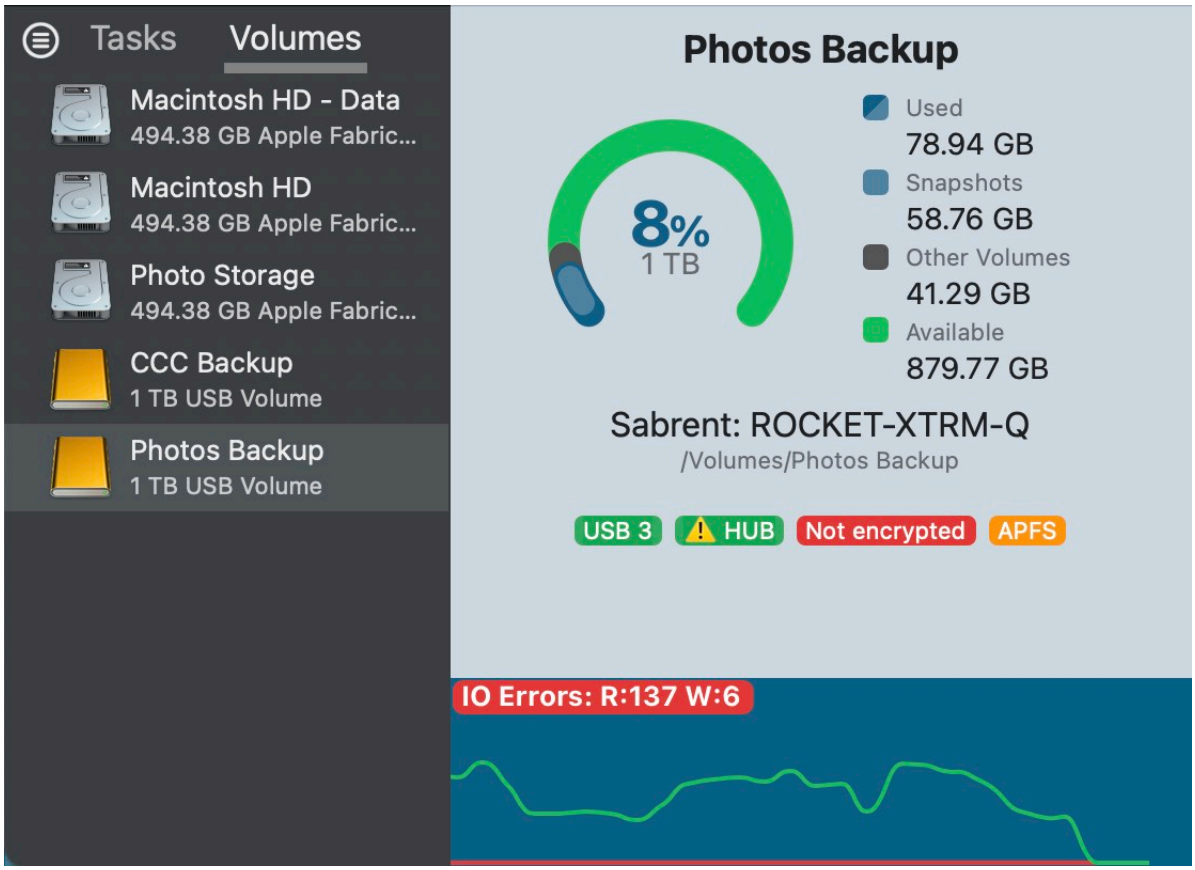
The Disk Center table in the sidebar displays a list of locally-attached, mounted volumes. Click on one of these volumes to display information such as the volume name, filesystem, capacity, disk usage, and a list of snapshots on the volume, as applicable.

Drive Statistics

A chart at the bottom of the window shows current read and write activity for the selected volume. Disk activity is collected by macOS at the hardware interface, so data for multiple volumes residing on the same disk will be identical. The data read and write rate can give you a good indication of how fast macOS is able to read and write data from and to your disk. You will likely notice that these values fluctuate wildly over the course of a backup task. This is quite normal, write performance will generally be lower when copying lots of small files and higher while copying a larger file. When lots of small files are being copied, there is a lot of transactional filesystem activity occurring on your source and destination volumes. This "chattiness" greatly reduces the overall throughput compared to the theoretical throughput of your disks.

Disk error statistics

CCC will report read and write error statistics when they are present:



Read and write errors indicate the number of read or write attempts that have failed since the disk was attached to your Mac (since startup for internal disks). Read errors often occur when files that are residing on damaged sectors cannot be automatically moved by the disk's firmware. Such files would also be unreadable by CCC, and CCC will report the failure to read these files at the end of the backup task. Read errors are not necessarily indicative of a failing hard drive. This number will rise steadily if multiple attempts are made to read the same corrupted file, for example. Read errors are, however, generally associated with physical hardware problems that will reduce the performance of a backup task. In some cases, macOS does not handle read failures well, and attempts to access the disk can lead to system-wide stalls.

Write errors are more serious. If you have a disk that is reporting write failures, there is either a hardware configuration problem with the device (e.g. bad cable, port, or enclosure), or the disk is failing.

Snapshot Management

If you select an APFS-formatted volume, CCC will display a list of volume snapshots and snapshot retention policy settings for that volume. Learn more information about Snapshot Management here <https://bombich.com/kb/ccc5/leveraging-snapshots-on-apfs-volumes>.

Disk Utility and [other third-party utility] doesn't report any problems with this disk, why does CCC?

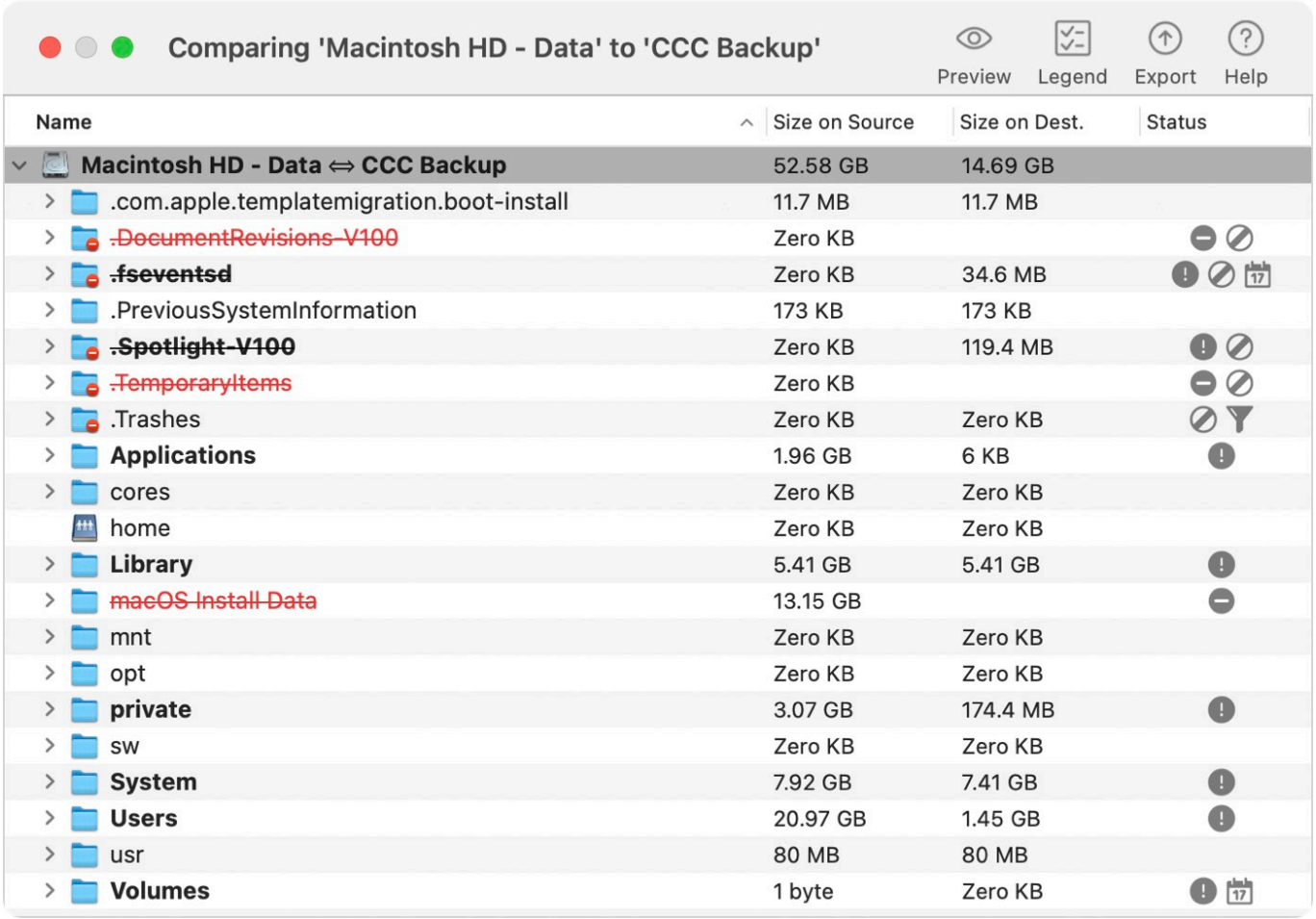
Read and write errors statistics are stored by the lower-level storage drivers, they are not specific to a volume. Usually when a read error occurs, the hard drive firmware attempts to move data on the affected sector to another sector of the disk, then spare out the damaged sector. When that is successful, it's possible for the storage driver statistics to be stale. **These statistics will be reset when the affected disk is physically detached from your Mac, or upon reboot.**

Related Documentation

- Identifying and Troubleshooting Hardware-Related Problems <https://bombich.com/kb/ccc6/identifying-and-troubleshooting-hardware-related-problems>
- Troubleshooting "Media errors" <https://bombich.com/kb/ccc6/identifying-and-troubleshooting-hardware-related-problems#io_errors>
- Working with FileVault Encryption <https://bombich.com/kb/ccc6/working-filevault-encryption>

Comparing the source and destination

CCC's Compare window was designed to highlight any substantive folder size differences between the source and destination. When you click the Compare button in CCC's toolbar, CCC will enumerate the current contents of the source and destination, then present a report of the size differences of each folder.



Name	Size on Source	Size on Dest.	Status
Macintosh HD - Data ⇔ CCC Backup	52.58 GB	14.69 GB	
.com.apple.templatemigration.boot-install	11.7 MB	11.7 MB	
~~.DocumentRevisions-V100~~	Zero KB		
~~**.fseventsd**~~	Zero KB	34.6 MB	
.PreviousSystemInformation	173 KB	173 KB	
~~**.Spotlight-V100**~~	Zero KB	119.4 MB	
~~.TemporaryItems~~	Zero KB		
.Trashes	Zero KB	Zero KB	
Applications	1.96 GB	6 KB	
cores	Zero KB	Zero KB	
home	Zero KB	Zero KB	
Library	5.41 GB	5.41 GB	
~~macOS Install Data~~	13.15 GB		
mnt	Zero KB	Zero KB	
opt	Zero KB	Zero KB	
private	3.07 GB	174.4 MB	
sw	Zero KB	Zero KB	
System	7.92 GB	7.41 GB	
Users	20.97 GB	1.45 GB	
usr	80 MB	80 MB	
Volumes	1 byte	Zero KB	

The comparison is not a byte-by-byte verification of files

The Comparison feature is not designed to perform an in-depth, byte-by-byte comparison of files on the source and destination, rather it's designed to be a simpler and more approachable analysis of size-based differences. We're specifically aiming to address the very common question, "Why is the size of the source and destination different?" If you would like to do a checksum-based verification of the files that were copied by your CCC backup task, click on the Source or Destination selector and choose the option to verify your files.

- Learn more: How to verify a backup <https://bombich.com/kb/ccc6/how-verify-or-test-your-backup>

The comparison is not a preview of changes that CCC will make

Results in the Comparison window should not be used to determine what changes CCC will make to the destination. If you would like to see a preview of the changes CCC will make to the destination, click the **Preview** button in the toolbar instead.

- Learn more: Preview: See what changes CCC will make to the destination <https://bombich.com/kb/ccc6/preview-see-what-changes-ccc-will-make-destination>

The comparison shows some differences. What do these mean?

The comparison window shows the status of items on the source vs. the destination:

-  This item is only present on the source
-  This item is only present on the destination
-  This item is different on the source and destination
-  This item was modified since the task last ran
-  This item is wholly or partially excluded or protected by a CCC task filter
-  This folder could not be enumerated due to access restrictions

You can hover your mouse over the icons in the status menu to produce a tooltip that describes the status.

Common explanations for differences between the source and destination

If you're seeing unexpected differences between the source and destination, be sure to run your backup task to verify that CCC has recently attempted to update the destination.

Your startup disk is constantly being modified

If you're comparing your startup disk to its backup, you should **always** expect to see differences highlighted in the Compare window. This is not an indication that something is wrong, it's normal. macOS is constantly updating various cache and log files, and you'll see those differences even if you immediately compare the source and destination after running the backup task.

CCC doesn't copy virtual memory, Trash and other volume-specific system items

The disk usage on your startup disk does not reflect the amount of data that needs to be backed up; disk usage on the destination should be lower than disk usage on the source after making an initial backup of your startup disk. Special filesystem devices (e.g. filesystem snapshots) and some macOS service data either cannot or should not be copied to another volume. CCC automatically excludes these items to avoid compatibility problems and to avoid unnecessary disk usage. That list of exclusions is documented here: Some files and folders are automatically excluded from a backup task <https://bombich.com/kb/ccc6/some-files-and-folders-are-automatically-excluded-from-backup-task>.

The largest and most notable excluded item is the /private/var/vm/sleepimage file. The sleepimage file contains the live state of your Mac's RAM, so it will be as large as the amount of RAM that you

have installed. This file is potentially very large, changes constantly and it gets recreated on startup, so CCC excludes this file from every backup task.

CCC also excludes the contents of the Trash. If you prefer that CCC copy the contents of the Finder Trash, you can enable that in the Task Filter.

- Learn more: Finder's Trash is excluded by default <https://bombich.com/kb/ccc6/excluding-files-and-folders-from-backup-task#trash>

CCC's SafetyNet feature protects root-level items on the destination by default

By default, CCC's SafetyNet feature protects items that are unique to the root level of the destination. If the Comparison window shows files and folders that only exist at the root of the destination, you can disable the "Protect root-level items on the destination" setting to have CCC remove those items the next time you run the backup task.

- Learn more: Protect root-level items on the destination <https://bombich.com/kb/ccc6/advanced-settings#protect>

Excluding content from the backup task does not cause it to be deleted from the destination

When you exclude an item from the CCC backup task, this tells CCC, "**Do not copy that item**". That does not, however, indicate that CCC should **delete** that item from the destination, e.g. if it had been copied there by a previous backup task. You can change this behavior by checking the box next to **Remove excluded files** in the sidebar of the Task Filter window.

- Learn more: Excluded files are not deleted from the destination <https://bombich.com/kb/ccc6/excluding-files-and-folders-from-backup-task#delete_excluded>

The sum of folder sizes often does not agree with total disk usage

Disk usage is not a simple matter of adding the size of every file on a volume. Special filesystem devices (e.g. hard links) have always complicated this math, but more recently Apple has introduced more special filesystem devices that complicate this even further. The cloning feature in Apple's APFS filesystem can lead to a scenario where it appears that you have more data on the disk than it can possibly contain, and the filesystem snapshots feature can lead to scenarios where disk usage is higher than the total size of the files on that volume. APFS also supports "sparse" files, which consume less space on disk than their file size would suggest. CCC can preserve sparse files between APFS volumes, but HFS+ does not support sparse files, so these files consume more space on an HFS+ formatted backup disk. See these sections of CCC's documentation for additional details on working with these challenges:

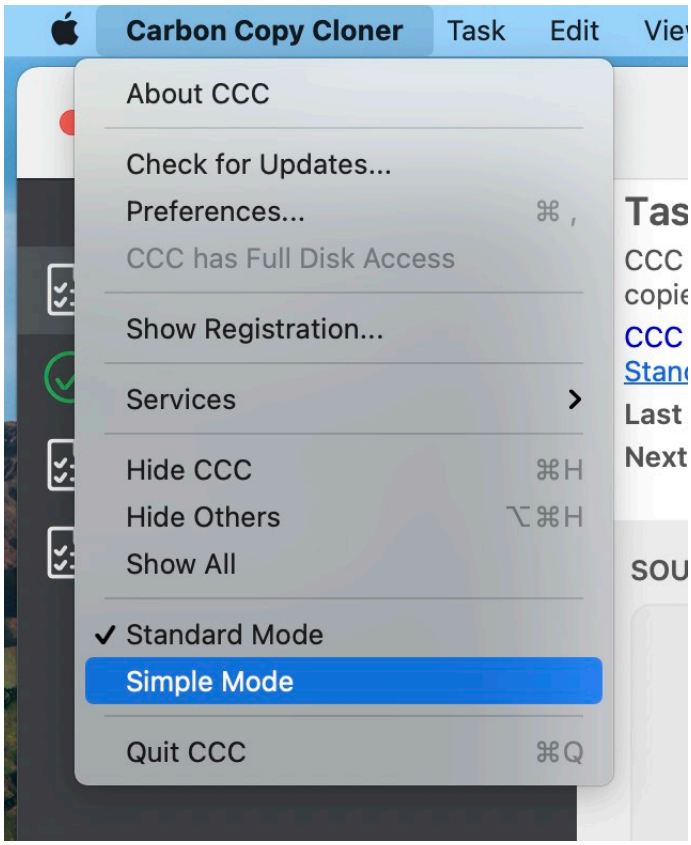
- I heard that APFS has a "cloning" feature. Is that the same as what CCC is doing? <https://bombich.com/kb/ccc6/everything-you-need-know-about-carbon-copy-cloner-and-apfs#math>
- Finder does not accurately represent the true disk usage of your files <https://youtu.be/KggyuL8mED0>
- Understanding disk usage when using snapshots <https://www.youtube.com/watch?v=4wqAC4YXiaY>
- Snapshots and space concerns; Deleting snapshots <https://bombich.com/kb/ccc6/leveraging-snapshots-on-apfs-volumes#space>
- Toggling snapshot support and setting a Snapshot Retention Policy <https://bombich.com/kb/ccc6/leveraging-snapshots-on-apfs-volumes#srp>

Exporting the differences from a comparison report

Click the Export button in the Comparison window toolbar to export a tab-delimited report of the size differences. This report will include only the differences noted in the window.

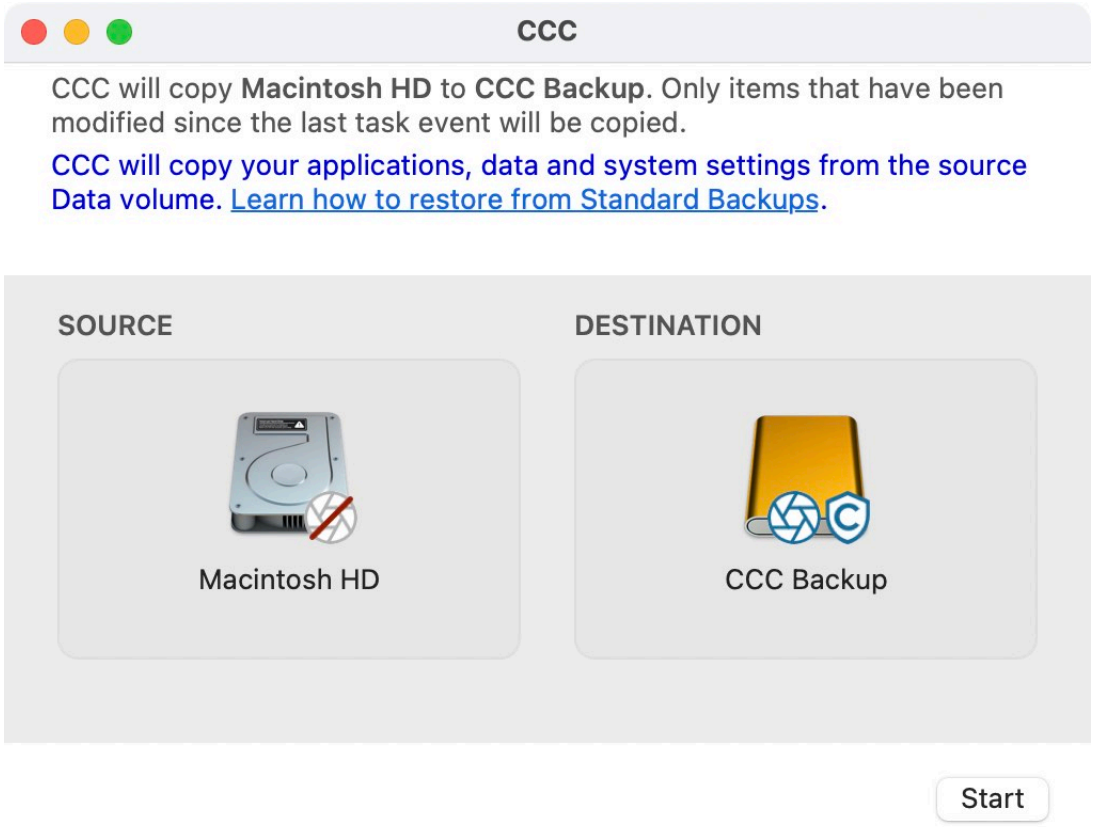
Simple Mode

Simple Mode significantly reduces the number of user interface elements — the sidebar, toolbar, scheduling selector, and advanced settings are all suppressed, leaving the user with only three primary controls: Source, Destination, Start button. For users that desire a basic ad hoc copy from one volume to another and do not want to maintain scheduled tasks, this simplified interface is the perfect solution. To use Simple Mode, choose **Simple Mode** from the Carbon Copy Cloner menu.



Configuring a backup task in Simple Mode

1. Choose a source
2. Choose a destination
3. Click the Start button



Related Documentation

- Preparing your backup disk for a backup of OS X <https://bombich.com/kb/ccc6/preparing-your-backup-disk-backup-os-x>

Can I choose a network volume? How do I schedule this backup? Can I exclude items from the backup task?

Simple mode aims to simplify **basic** backup tasks. For additional options, choose **Standard Mode** from the Carbon Copy Cloner menu to switch back to standard mode.

For the curious, Simple Mode tasks run with the same default settings as tasks created in Standard Mode: SafetyNet is enabled, and the contents of the SafetyNet folder will be pruned when free space on the destination drops below 25GB. CCC will automatically adjust this pruning limit as necessary. When in Simple Mode, your source and destination choices will not be saved between launches of CCC. Every time you open CCC, the source and destination will be empty. Additionally, CCC must remain open while a task is running — if you quit CCC, a running task will be stopped (after a confirmation prompt).

Leveraging Snapshots on APFS Volumes

What is a snapshot?

Snapshots are a feature of Apple's APFS filesystem. A snapshot is a point-in-time representation of a volume on your hard drive. Once the snapshot is taken, each file within that snapshot will be available on the snapshot in its exact state at the moment that the snapshot was taken, even if you delete the file. When you configure CCC to make regular snapshots of your APFS-formatted volumes, you can quickly restore older versions of your files.

Note: Snapshots are only available for APFS-formatted volumes.

The Role of Snapshots in a Comprehensive Data Protection Strategy

There are several aspects of data protection that a backup aims to provide. Protection against:

- Accidental file deletion or modification
- Malicious file modification (e.g. malware/ransomware)
- An OS or software update that causes functionality regressions
- Hard drive failure
- Computer theft
- Catastrophic loss (e.g. tornado, hurricane, flood -- loss of both original and backups)

Support for snapshots at the filesystem level is an important and integral component of a backup strategy, but snapshots are not a complete replacement for a true backup on physically separate hardware. If your startup disk fails, all the snapshots in the world aren't going to help you restore your startup disk and data. Having a backup on an external disk gives you protection against hardware failure.

	Snapshots	External Backup	Backup to Remote Macintosh
Accidental file deletion			
Malware/ransomware	+		
Hard drive failure			
Theft			
Catastrophic loss			

When you develop your backup strategy, consider all of the possible risks to your data and decide whether and how you will mitigate those risks. At minimum, we recommend regularly scheduled backups to a locally-attached hard drive. With a regularly scheduled backup, you will have very good protection against the most common risks to your data.

Using snapshots in CCC

When you select an APFS volume on an external device as a source† or destination to a CCC backup task, CCC will automatically enable snapshot support on that volume and set a default Snapshot Retention Policy for that volume. **For basic snapshot support, you don't need to configure any settings; CCC will automatically manage your snapshots using a sensible set of defaults.**

† CCC will not automatically enable snapshot support on the startup disk. If you would like to use storage on your startup disk for snapshots, you can manually enable snapshot support for that volume.

Snapshots on the source

Maintaining snapshots on the source volume offers protection against accidental file deletion and modification. When snapshots are kept on the source volume, you don't need your backup volume to recover accidentally-deleted files. Retaining snapshots will increase disk usage over time, however, so we recommend limiting retention of snapshots on the source. This recommendation is specifically imposed by CCC upon the startup disk (and again, note that CCC will not automatically enable snapshot support on the startup disk). Additionally, please keep in mind when developing your snapshot retention strategy that Apple's Installer may delete all snapshots from the startup disk when applying updates or major OS upgrades. Snapshots are not a permanent data storage strategy.

When your backup tasks run, CCC will automatically create a snapshot on an eligible source volume and use that snapshot as the source for the backup task. Because the snapshot is mounted read-only, changes that you make to files while the backup task runs won't cause errors during the backup task — you'll get a true point-in-time backup of your data. If you do not have snapshots enabled for the source volume, CCC will automatically remove the temporary source snapshot at the end of the backup task.

CCC won't create snapshots on the source System volume in an APFS volume group <https://bombich.com/kb/ccc6/working-apfs-volume-groups>. These volumes are already read-only so a snapshot is not required. This exception only applies to the special System volume in the source volume group, not to the Data volume. Snapshot creation and retention on the source Data volume follows your Snapshot Retention Policy.

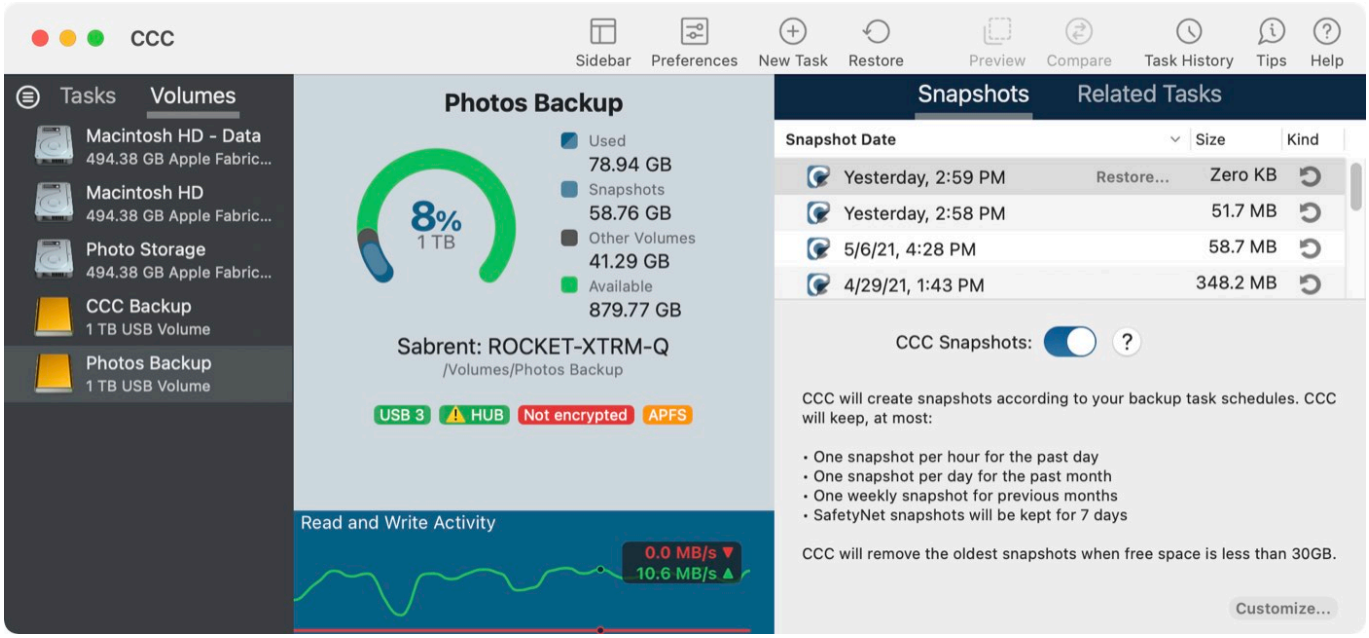
Snapshots on the destination

If you have CCC's SafetyNet feature enabled, CCC will create a SafetyNet Snapshot <https://bombich.com/kb/ccc6/protecting-data-already-on-your-destination-volume-carbon-copy-cloner-safetynet#safetynet_snapshot> of the destination at the beginning of the backup task. CCC will then thin snapshots on the destination according to the Snapshot Retention Policy defined for that volume. At the end of the backup task, CCC will create another "Backup Snapshot" that defines the point-in-time backup for that backup task event.

Toggling snapshot support and setting a Snapshot Retention Policy

CCC considers snapshot support on an individual volume basis. Snapshot support is automatically enabled for a volume on external disks when you select that volume (or a folder on that volume) as a source or destination to a CCC backup task. If you prefer that CCC does not automatically enable snapshot support for source and destination volumes, you can disable that behavior in CCC's Settings window.

To view or change a volume's snapshot support or retention policy, reveal CCC's sidebar, then click on the volume in CCC's sidebar. CCC will list any snapshots currently present on the volume and will display the retention policy for that volume. Remember that snapshot support is limited to APFS volumes. If you select a non-APFS formatted volume in CCC's sidebar, you won't see any snapshot settings.



Default retention policy settings

- SafetyNet snapshots will be retained for 7 days†
- Weekly snapshots will be retained until free space is constrained†
- Daily snapshots will be retained for 30 days†
- Hourly snapshots will be retained for 24 hours
- The oldest snapshots will be deleted when free space is less than 30GB

† CCC applies a more conservative retention policy for the startup disk (when you manually enable snapshot support on that volume) — SafetyNet snapshots are retained for 3 days, weekly snapshots are not retained, and daily snapshots are only retained for 3 days. You can customize those settings if you want a longer retention for snapshots on the startup disk, but be sure to consider the implications this will have on disk usage on your startup disk.

CCC will thin snapshots at the beginning of the backup task, and any time during the backup task if free space becomes constrained (on a destination volume). The retention policy is evaluated in the order listed above. If the free space threshold is still exceeded after thinning snapshots, then the oldest snapshots will be removed to achieve the specified free space limit. The only exception to that is for any snapshots created by other applications, and the snapshot created during the current backup task – CCC will not remove the SafetyNet snapshot that was created at the beginning of the current backup task.

Volume Group Snapshot Retention Policy (Catalina only)

Volume groups <https://bombich.com/kb/ccc6/working-apfs-volume-groups> are handled by a single snapshot retention policy per group. The settings for the policy can be edited when viewing the Data member of the group. CCC will only create snapshots on a destination System volume when changes have been made to the source (i.e. when you apply system updates), and only on macOS Catalina. As such, time-based retention of System volume snapshots is not very applicable. Instead, CCC will retain every snapshot of System volumes and will only remove System snapshots when the free space limit of the retention policy is exceeded.

Snapshots created by other applications

During snapshot thinning, **CCC will never delete snapshots created by other applications**. If

you would like to remove snapshots created by another application, click on the relevant volume in CCC's sidebar, select the snapshots you would like to remove, then press the Delete key.

CCC's snapshot retention policy is only applied when snapshots are enabled for that volume

If you disable CCC snapshot support for a volume that contains previously-created CCC snapshots, CCC will not perform automated snapshot thinning on that volume. When you disable snapshot support, you are welcome to delete the snapshots listed above the snapshot toggle button. Simply select one or more snapshots listed in the table, then press the Delete key.

The snapshot retention policy defines which snapshots will be retained, not when they will be created

CCC creates snapshots when your backup tasks run, and only when your backup tasks run. CCC will never create snapshots outside of a scheduled or manually-run backup task. As such, a retention policy that saves "up to one snapshot per hour for 24 hours" does not imply that you will have 24 snapshots for the last day. If you have a backup task configured to run only on a daily basis, you should expect to see only one snapshot for the source and destination volumes. If you want to have hourly snapshots, be sure to configure your backup task to run on an hourly basis.

CCC will override your free space limit if that's required to complete a backup

The default free space limit of 30GB will generally ensure that CCC can write 30GB of data to your destination volume during each backup task. If CCC finds more than 30GB of data to copy and runs out of room on the destination, it will remove additional snapshots during the backup task to free additional space. When this "emergency" thinning takes place, CCC will add a notification to your backup task event (in the Task History window), suggesting that you review the Snapshot Retention Policy for your destination volume.

To review the Snapshot Retention Policy: Click on the destination volume in CCC's sidebar, then click on the **Customize** button to customize the retention policy settings. The specific setting that you should consider changing is the one labeled "**Delete the oldest snapshots when free space is less than xx GB**". When reviewing the free space limit, consider whether your backup tasks generally copy more than 30GB (you can make that assessment in CCC's Task History window <https://bombich.com/kb/ccc6/how-find-out-when-backup-last-ran-ccc-task-history>). Specify a value that will leave enough space to accommodate the amount of data that usually gets copied to the destination to avoid the emergency thinning and associated notification.

If you notice that your backup task is suddenly copying a lot more data than usual, please take a moment to look for potential problems. For example, if you have more than one backup task backing up different sources to the same destination, those tasks may be conflicting, removing each others' files. You should also determine if disk usage on the destination is unusually high compared to the source (excluding snapshot disk usage). If the disk usage looks suspicious, or if the amount of data that CCC is copying is difficult to explain, please don't hesitate to contact us for an additional review <https://bombich.com/software/get_help> of your setup.

SafetyNet snapshots vs. Backup snapshots

SafetyNet is a feature unique to CCC that aims to protect data on your destination volume. Suppose, for example, that you have three volumes: **Macintosh HD**, **Backup**, and **Photos**. If you created a backup task and accidentally selected the **Photos** volume as your destination, some copying applications would simply erase the destination or delete the files on that volume, with no recourse! With SafetyNet enabled, CCC benevolently retains those items on the destination, but cordons them off to a separate folder so you can recover them later if necessary.

On a snapshot-enabled volume, the SafetyNet is now implemented as a pre-flight snapshot. Before CCC makes any changes to the destination, it will create a "SafetyNet Snapshot" of the destination. Then the task will proceed in the normal manner, copying files from the source to the destination. If you later realize that you had configured the task with the wrong destination, or that you had placed files on the destination volume and they're missing after running your backup task, you can restore those items to the destination from the SafetyNet Snapshot.

At the end of the backup task, CCC will create a second snapshot; a "Backup Snapshot". This second snapshot represents the state of the source for the current backup event. If you ever wanted to restore data back to the original source or to a replacement disk (e.g. because the source disk failed), you would use a Backup Snapshot to restore that data. This is a very important point: you generally will never use a SafetyNet snapshot to restore data back to the original source. SafetyNet Snapshots are used to restore files that were errantly deleted or modified on the destination.

Summarizing, keep these two points in mind:

-  SafetyNet Snapshots allow you to recover files on the destination that were **unrelated to your backup task**
-  Backup Snapshots give you point-in-time restores of the data from your source volume

Do I need SafetyNet? Can I turn it off, or limit the amount of space it uses?

SafetyNet snapshots offer protection from configuration mistakes, e.g. selecting the wrong destination, or using the destination to store files that are not related to the backup task. Because these snapshots have a different purpose, they are managed by a separate retention policy. By default, CCC will remove SafetyNet Snapshots that are more than one week old. If your destination volume is dedicated to your backup task and you never store other files on that volume, then you can reduce the SafetyNet retention value (e.g. to one or two days).

If you're very confident in your tasks' configurations, and your destination is dedicated to the backup task, and your destination does not have a lot of overhead, you can also choose to disable SafetyNet. You can either disable SafetyNet on a per-task basis, or, what we recommend instead, you can set the SafetyNet retention value for your destination volume to zero. With that setting, CCC will still create a SafetyNet snapshot at the beginning of the task, but it will remove all previously-created SafetyNet Snapshots at the beginning of the next task. This configuration gives you a modicum of protection from configuration errors without consuming a lot of extra space on your destination disk.

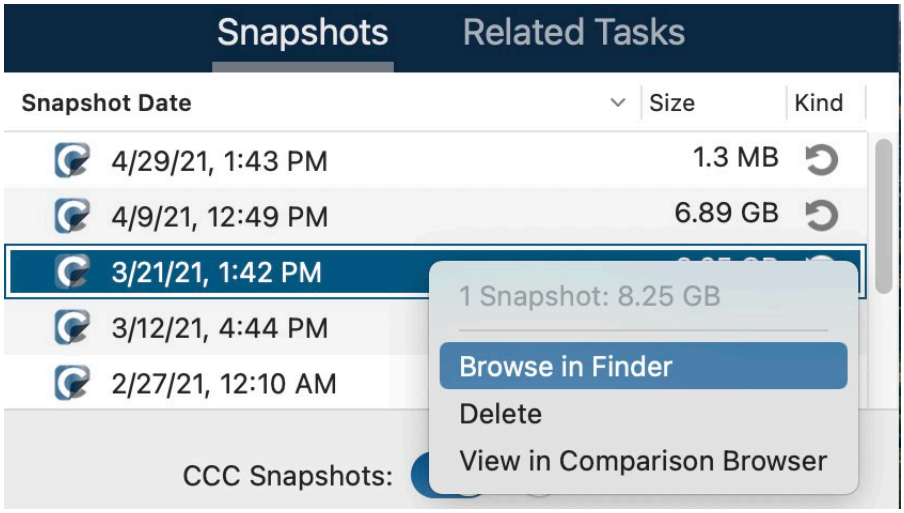
SafetyNet is a safety mechanism, it's not a strategy for retaining other stuff on your backup volume

Wearing a seatbelt doesn't make it OK to drive into a wall every day. **Your backup volume should be dedicated to your backup task.** If you want to take advantage of some extra space on your backup disk, you should add a volume to that disk specifically for storing the other data <https://bombich.com/kb/ccc6/i-want-back-up-multiple-macs-or-source-volumes-same-hard-drive#apfs_add_volume_startup_disk>. That other volume will be outside of CCC's purview, thus protected from any unintentional alterations. Open Disk Utility and select your backup disk, then choose **Add an APFS Volume...** from the Edit menu to add a volume to your backup disk.

Mounting and browsing the contents of a snapshot

If you would like to browse the contents of a snapshot, select that snapshot in the snapshots table, then right-click and choose the **Browse in Finder** option. Or, simply **double-click on the snapshot**. You may then browse the contents of that snapshot in the customary manner in the Finder. The snapshot is mounted read-only, so it is impossible for you to make any harmful

modifications to the snapshot. If you would like to restore a single item, you can simply drag the item from the snapshot to wherever you want to restore it to. When a snapshot is mounted, the creator icon of the snapshot in the Snapshots table will have a green dot to indicate that it is mounted.



Note: Neither the Finder nor Disk Utility shows mounted snapshots by default, so you cannot typically unmount a snapshot in those applications. CCC will indicate when a snapshot is mounted by placing a small green dot on the snapshot creator icon in the snapshots table. You can right-click on a mounted snapshot in CCC and choose the Unmount option to manually unmount a snapshot. For your convenience, however, CCC will automatically unmount any snapshots that it mounted when you quit CCC.

Related Documentation

- How to restore from your backup <https://bombich.com/kb/ccc6/how-restore-from-your-backup>

CCC snapshots vs. Time Machine snapshots

CCC and Time Machine are both capable of creating snapshots on a given APFS volume. The snapshots that are created by each are exactly comparable – there's no technical difference between a snapshot created by CCC vs. a snapshot created by Time Machine. If you enable Time Machine and you do not specifically exclude your CCC source or backup volume from Time Machine's purview, Time Machine will automatically create and delete its own snapshots on those volumes. CCC is ambivalent about the snapshots that it presents for restoring, so it is acceptable to allow Time Machine to create snapshots on your CCC source and destination volumes.

However, you should carefully consider whether you want to allow both CCC and Time Machine to create snapshots on any given volume. Redundant snapshots managed by different retention policies is not harmful, but will probably result in a less effective retention schedule. Time Machine only retains snapshots for 24 hours, though, so the concern is only applicable to one day's worth of snapshots.

Disabling Time Machine snapshots for an individual volume

Many users find that snapshots are still created on a volume even after disabling snapshot support within CCC for that volume. Disabling snapshot support only affects CCC's creation and removal of snapshots from that volume, it does not affect Time Machine. CCC's snapshot list will indicate the

icon of the application that created the snapshot:

-  Snapshot created by CCC
-  Snapshot created by Time Machine

If you would like to prevent Time Machine from creating snapshots on a given volume, you can exclude that volume from Time Machine:

1. Open the System Settings application and click **General** in the sidebar
2. Open the Time Machine panel
3. Click on the **Options...** button
4. Click the **+** button and select the volume you would like to exclude

Snapshots and space concerns; Deleting snapshots

Initially, snapshots do not inherently consume space. When you create a snapshot, the disk usage on the volume containing the snapshot remains unchanged. However, because the snapshot retains references to every file on the volume, space is not freed when you delete a file. Suppose you have a 100GB hard drive with 80GB of content. You create a snapshot, then move 20GB of files to the Trash and empty the Trash. The resulting disk usage is still 80GB. That 20GB of space is not freed until the snapshot is deleted.

This free space behavior is an important factor to consider when you decide whether to enable snapshots for any particular volume, including your startup disk. If you have a hard drive that is particularly full, then maintaining snapshots on that volume may not be a practical solution. In contrast to Time Machine, CCC offers a lot of flexibility in whether snapshots are enabled for a particular volume, and how those snapshots are maintained over time. Additionally, CCC allows you to find and delete specific snapshots with ease. Simply click on a snapshot in the Snapshots table, then press the Delete key to delete that snapshot.

Note: Finder and Get Info windows don't include local snapshots in their calculations of the storage space available on a volume. <https://support.apple.com/en-us/HT204015> If you would like to see the amount of space consumed by snapshots on any particular volume, select that volume in CCC's sidebar. The disk usage indicator will show the percentage of space consumed by snapshots, and the snapshots table will indicate the size of each snapshot on the volume. Calculating the size of snapshots is complex and dynamic – as you delete snapshots, the space consumed by adjacent snapshots may change as those snapshots become the last reference holder for files on the disk. This is normal. Also, note that the size of the snapshot indicates how much space would be freed if that snapshot is deleted, it does not indicate the total amount of data referenced by the snapshot.

To delete a snapshot in CCC:

1. Click 'Volumes' in the sidebar
2. Select a volume (to remove a snapshot from the startup disk, select the volume named "Data" or "Macintosh HD - Data")
3. Select one or more snapshots in the Snapshots table
4. Press the Delete key

Why is the total snapshot disk usage greater than the sum of each individual snapshot's disk usage?

Many people think we don't know how to do math when they see this difference, but the figures are all correct — total snapshot disk usage is not a simple sum of individual snapshot disk usage. The video linked below demonstrates why.

Learn more about snapshots and disk usage concerns in this video on YouTube <https://youtu.be/4wqAC4YXiaY?t=170>

Frequently Asked Questions

The retention policy says it will save one snapshot per hour. Why don't I see more hourly snapshots on my disks?

To give you the most control over the creation of snapshots on your disks, CCC only creates snapshots when your backup tasks run (this is specifically in contrast to Time Machine's non-configurable hourly snapshots). If your backup task is configured to run on a daily or weekly basis, then CCC will not produce hourly snapshots. The retention policy will keep **at most** one snapshot per hour for the specified interval, but that does not imply that you will have **at least** one snapshot per hour for that interval. If you would like to have snapshots created on an hourly basis, then you can schedule your tasks to run on an hourly basis.

Where did the _CCC SafetyNet folder go?

When working with non-APFS volumes, or APFS volumes that have CCC snapshot support disabled, CCC creates a "_CCC SafetyNet" folder at the root of the destination volume when the SafetyNet feature is enabled. As CCC updates the destination, any files that don't exist on the source or that are getting replaced by an updated version will be moved into that SafetyNet folder. When snapshot support is enabled on an APFS destination, however, that folder is no longer used as part of the SafetyNet mechanism. Instead, CCC creates a SafetyNet Snapshot at the beginning of the task, then proceeds to update the destination. Older versions of files and files that don't exist on the source are immediately removed from the destination (but still protected by the SafetyNet Snapshot!), so at the end of the task, the source and destination look identical.

If you enable snapshots on an APFS destination volume that has a legacy SafetyNet folder, CCC will first create a SafetyNet Snapshot. After having successfully created the SafetyNet Snapshot (which will retain your legacy SafetyNet folder), the legacy SafetyNet folder is removed. That SafetyNet Snapshot is then subject to the SafetyNet retention setting defined by the Snapshot Retention Policy for your destination volume. If you would like to access the contents of that SafetyNet folder, double-click the SafetyNet Snapshot to reveal it in the Finder.

If you're familiar with using the SafetyNet for recovering older versions of your files, please keep in mind that Backup Snapshots are designed for that purpose. You should only be looking into a SafetyNet Snapshot if you had kept something on the destination and then lost it after running a backup task.

See also: The legacy SafetyNet folder is not used when snapshots are enabled on the destination <https://bombich.com/kb/ccc6/legacy-safetynet-folder-not-used-when-snapshots-are-enabled-on-destination>

I want hourly snapshots, but my destination isn't available every hour of the day. How can I get hourly snapshots on my source volume?

CCC only creates snapshots during a task event, because snapshots are a **piece** of the backup strategy, not a replacement for it. Snapshots are a convenience, but the true backup requires that your files are safeguarded on a physically different piece of media. Nevertheless, some people would like the convenience of hourly snapshots, but for logistical reasons, can't run a backup task because the destination is not always available (e.g. when you go to work).

To configure CCC to create hourly snapshots on a particular volume, you can configure a new task that copies one folder to another <https://bombich.com/kb/ccc6/folder-folder-backups> on that same source volume. What gets copied in that case isn't important (but the source folder cannot be completely empty), as long as the folders are both on the same disk. CCC will create and retain snapshots on that volume according to the retention policy that you have defined for that volume.

1. Create two new folders somewhere on the source volume, named "source" and "destination". Add at least a blank folder to the source folder (a completely empty source will yield a sanity error).
2. Open CCC and click the **New Task** button in the toolbar
3. Drag the source folder onto CCC's Source selector
4. Drag the destination folder onto CCC's Destination selector
5. Turn off the SafetyNet feature
6. Schedule the task to run hourly
7. Save the task

I just enabled encryption on my APFS-formatted volume. Why am I now getting errors that CCC can't create snapshots?

The APFS filesystem won't create nor remove snapshots while encryption conversion is underway. You can type diskutil apfs list in the Terminal application to see conversion progress.

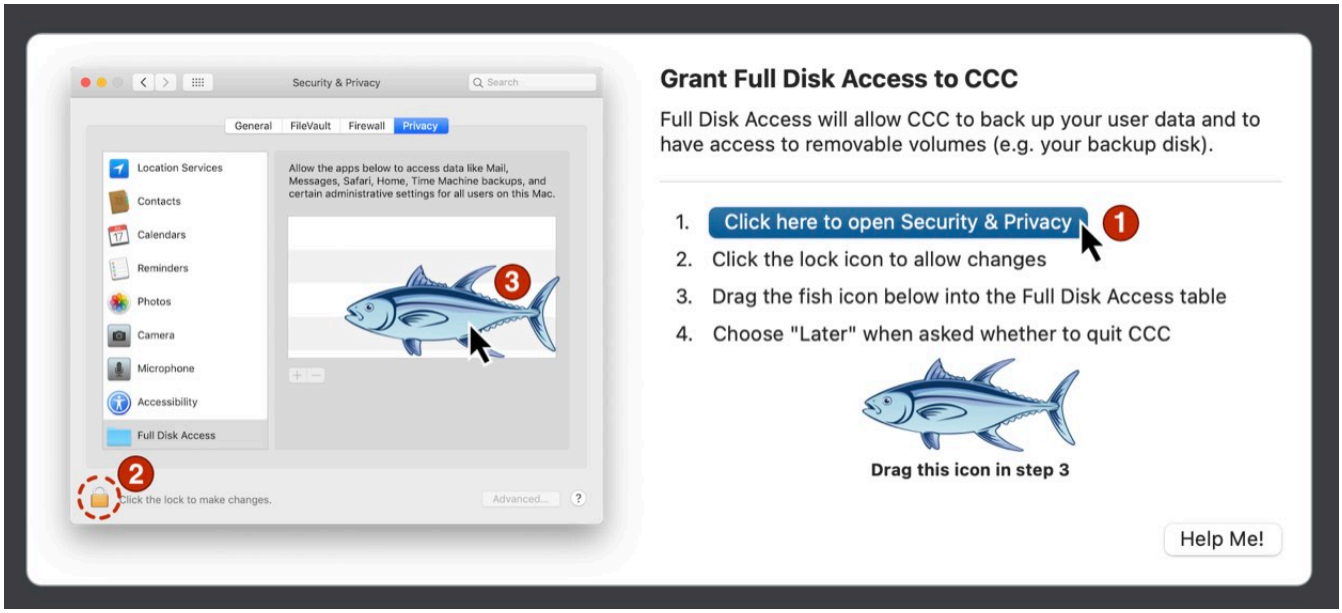
Granting Full Disk Access to CCC and its helper tool

Watch a video of this tutorial on YouTube <https://youtu.be/X1ycBa89eEs>

macOS imposes privacy restrictions that disallow, by default, access to certain application data (e.g. Mail, Messages, Safari, Photos), and all access to any external hard drives and network volumes.

macOS does not conveniently ask you to grant access to an application when that application tries to access that data. Instead, you're required to manually pre-approve the application. As a result, when you download an application specifically to back up your most precious data, that application can't back up that data until you specifically go out of your way to grant it access to that data.

To proactively grant CCC and its helper tool full disk access, choose "Grant CCC Full Disk Access..." from the Carbon Copy Cloner menu.



CCC's Install Assistant, indicated in the screenshot above, will guide you through the pre-approval procedure that grants CCC and its helper tool full disk access.

Catalina, Big Sur, Monterey only: To begin, click the button to open the Privacy & Security panel in the System Settings application. CCC will take you directly to the Full Disk Access category. Click the padlock icon in the lower-left corner of the Privacy window to allow changes.

Ventura, Sonoma: When you start to drag the CCC Privacy Fish, the following happens automatically: the System Settings application will open, the Privacy & Security panel will open, the Full Disk Access panel will be selected. On these newer OSes, simlpy start dragging the fish, then wait for the System Settings application to appear.

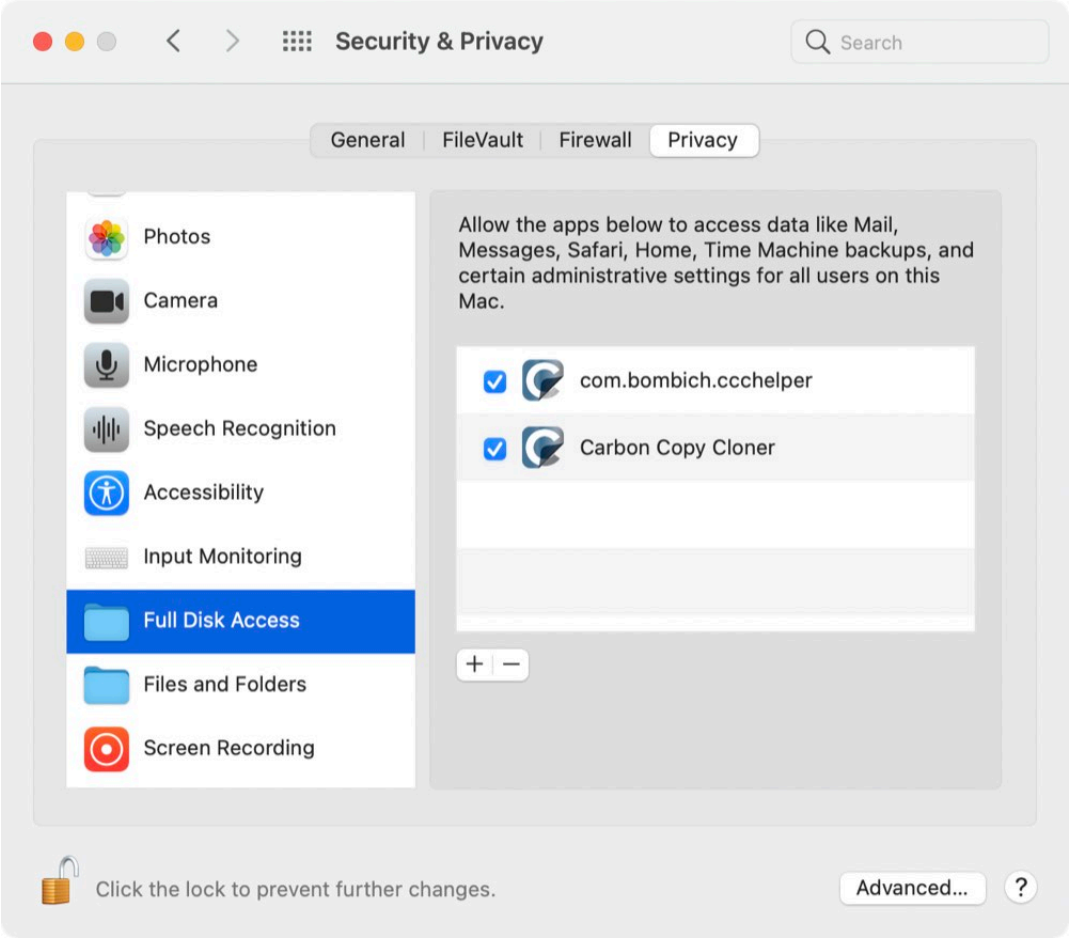
Next, drag the fish icon from CCC's Install Assistant onto the table in the Privacy window. This icon represents two separate files on your Mac — the Carbon Copy Cloner application and its privileged helper tool, so when you drop this onto the Privacy table, you will see both "Carbon Copy Cloner.app" and "com.bombich.ccchelper" appear in that table. Once you have granted CCC's helper tool full disk

access, CCC will dismiss its Install Assistant and resume whatever task led up to the presentation of the Install Assistant. You can close the System Settings window at that point, and if you're prompted to quit CCC now or later, you can choose the "Later" option.

"I added CCC to the Full Disk Access category but I still get errors"

Watch a video of this tutorial on YouTube <https://youtu.be/RUZxezWAJ9U>

It seems intuitive to add the Carbon Copy Cloner application to the Full Disk Access list. Unfortunately, Apple's Privacy measures don't work in an intuitive manner when an application leverages a privileged helper tool. Following Apple's Best Practices for performing tasks with elevated privileges (e.g. backing up your startup disk), CCC leverages a privileged helper tool for managing all aspects of your backup task. Therefore, CCC's privileged helper tool ("com.bombich.ccchelper", or errantly just "com.bombich" on Ventura and Sonoma) also needs Full Disk Access. After granting full disk access to CCC and its helper tool, the Full Disk Access table should look like this:



Related Documentation

- What is CCC's Privileged Helper Tool? <https://bombich.com/kb/ccc6/what-cccs-privileged-helper-tool>

Manually granting full disk access to CCC's privileged helper

tool

If accessibility challenges make the drag and drop procedure too difficult, you can follow the steps below to grant full disk access to CCC's privileged helper tool.

1. Open the Privacy & Security panel in the System Settings application (Pre-Ventura: System Preferences > Security & Privacy)
2. Click on the Privacy tab
3. *Pre-Ventura*: Click the padlock in the lower-left corner to allow changes
4. Click on **Full Disk Access** in the categories table
5. Click the **+** button
6. Navigate to the root-level of your startup disk (e.g. Macintosh HD) > Library > PrivilegedHelperTools
7. Select **com.bombich.ccchelper**
8. Click the **Open** button

Troubleshooting Full Disk Access problems

Apple doesn't offer developers an interface to the macOS Full Disk Access privacy settings, which is why we have to walk you through the odd procedure documented above. We asked Apple to give us an interface similar to that offered for other privacy settings (e.g. access to your camera), "Would you like to grant full disk access to CCC?" Apple indicated that they specifically do not want it to be that easy. Lacking this interface, we don't have any insight into the privacy settings. For example, we can't tell whether you have granted this access to CCC, nor whether you have specifically revoked it. We must stoop to poking at various files on the system to see if we might have access, then proceed as best as possible based on the result. Unfortunately, that method is not very reliable, so there are scenarios where CCC believes that it has full disk access but does not, or cases where it does have full disk access, but concludes that it does not.

Over the last several years we've found a few common problems that lead to this confusion around whether CCC does actually have full disk access, e.g. the macOS service that decides which apps have access is simply making the wrong call or there is corruption within the privacy settings database. In some cases CCC appears to have full disk access for one volume but not another, suggesting that there may be a problem with a particular volume, or its APFS container. We recommend the following steps to troubleshoot these problems:

- Verify that **both** "com.bombich.ccchelper" and "Carbon Copy Cloner" are listed in the Full Disk Access list, and that the boxes next to them are checked, then try the task again
- Restart the Mac, then try the task again
- If the problem appears to be specific to one destination volume, then erase that volume in Disk Utility, reselect the destination in CCC, then try the task again
- Reset the privacy settings database (paste tccutil reset All into the Terminal application, then press the Return key), then re-grant Full Disk Access to CCC and its helper tool, then try the task again. Note: Resetting the privacy settings database will clear out all previously-granted privacy exceptions in the Security & Privacy Preference Pane. Unfortunately Apple does not provide a more granular way to troubleshoot privacy control problems.

Creating legacy bootable copies of macOS (Big Sur and later)

Copying Apple's system is now an Apple-proprietary endeavor; we can only offer "best effort" support for making an external bootable device on macOS Big Sur (and later OSes). We present this functionality in support of making ad hoc bootable copies of the system that you will use immediately (e.g. when migrating to a different disk, or for testing purposes), but we do not support nor recommend making bootable copies of the system as part of a backup strategy.

Please bear in mind that you can restore all of your documents, applications, and system settings from a standard CCC backup without the extra effort involved in establishing and maintaining a bootable device.

In the past, a "bootable backup" was an indispensable troubleshooting device that even novice users could rely upon in case their production startup disk failed. The reliability of Apple's External Boot solution has waned in the past several years, however, and the situation has grown starkly worse on the new Apple Silicon platform. Apple Silicon Macs will not start up (at all) if the internal storage is damaged or otherwise incapacitated, so there is very little value, if any, to maintaining a *bootable* rescue device for those Macs.

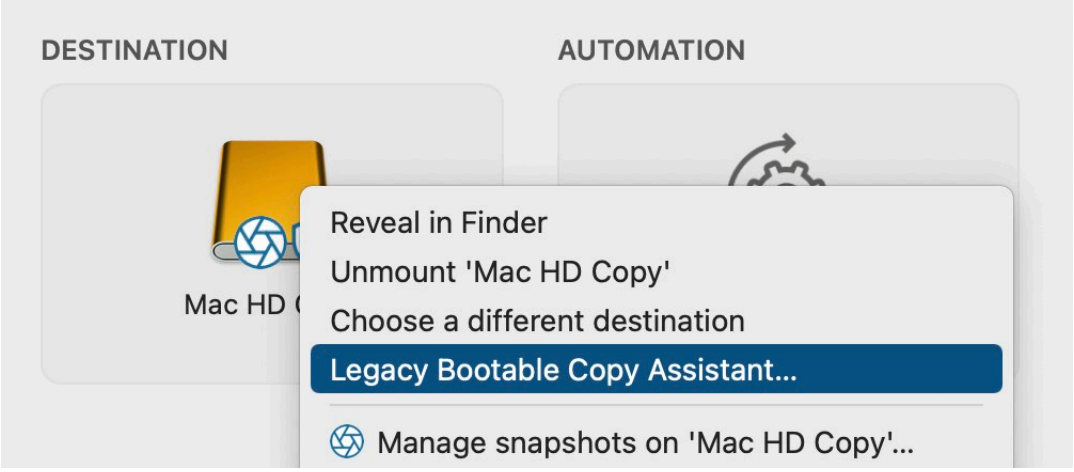
It has also grown increasingly difficult to make a copy of the operating system. Starting in macOS Big Sur (11.0), the system resides on a cryptographically sealed "Signed System Volume" <https://developer.apple.com/news/?id=3xpv8r2m> that can only be copied by an Apple-proprietary utility. That utility is very one-dimensional; choosing to copy the system requires that we sacrifice other **backup** features, e.g. we cannot copy the system and retain versioned backups of your data. Due to these changes and the limitations of Apple's new "Apple Silicon" platform, creating an external bootable device is not only less approachable for novice users, it's also less likely to serve as a reliable troubleshooting device.

CCC 'Standard Backups' do not include the operating system

By default, CCC does not attempt to make backups of the startup disk (Big Sur+) bootable. When you configure a backup of your startup disk, CCC will back up the contents of the Data volume. *That's all of your data, all of your applications, and all of your system settings – everything about your Mac that is customized.* You don't have to be able to boot your Mac from the CCC backup to restore data from it. You can restore individual files and folders using Finder or CCC while booted from your production volume <https://bombich.com/kb/ccc6/how-restore-from-your-backup>. If you ever need to restore everything from a non-bootable backup, you can install macOS via Recovery mode (e.g. onto a replacement disk), then migrate data from the backup via Migration Assistant <https://bombich.com/kb/ccc6/creating-and-restoring-data-only-backups#migrate>. CCC backups are compatible with Migration Assistant, and we support that configuration.

Making a copy of the startup disk with the Legacy Bootable Copy Assistant

If you would like to configure CCC to create a bootable copy of your Mac's startup disk, you can use the Legacy Bootable Copy Assistant. After selecting your source and destination volumes, click on the Destination selector and choose **Legacy Bootable Copy Assistant..**.



Catalina users: The Legacy Bootable Copy Assistant is not applicable. On Catalina, CCC will use its own file copier to make a backup of both the System and Data volumes <https://bombich.com/kb/ccc6/frequently-asked-questions-about-ccc-and-macos-catalina>.

On Big Sur (and later OSes), CCC will use Apple's APFS replicator (named "ASR") to create a copy of the system. The Legacy Bootable Copy Assistant will offer some choices for how to proceed with the task depending on how the selected destination is configured. We recommend that you dedicate a volume to this procedure, because the volume will be erased when making the copy of your startup disk.

Erase the destination

When you select this option, CCC will configure the task to use Apple's APFS replicator to copy the selected source to the selected destination. When you start the task, the destination will be immediately erased. SafetyNet is not applicable in this configuration, so be sure that you have selected an empty volume, or a volume that has data that may be deleted (e.g. an old backup).

Standard Backup

This option is the default behavior when not using the Legacy Bootable Copy Assistant. CCC presents this only as a reminder that non-bootable options are available, and sometimes more palatable, e.g. if you do not want to erase your current backup volume.

Things you should know before relying on an external macOS boot device

This procedure relies on Apple's proprietary APFS replication utility, which is outside of our developmental control. We welcome feedback <https://bombich.com/software/get_help> on this functionality, but we cannot offer in-depth troubleshooting assistance for problems that Apple's replication utility encounters.

- Whether the destination is bootable depends on the compatibility of your Mac, macOS, and the destination device. We cannot offer any troubleshooting assistance for the bootability of the destination device beyond the suggestions offered in our External Boot Troubleshooting <https://bombich.com/kb/ccc6/help-my-clone-wont-boot> kbase article.
- The destination may not remain bootable if you proceed to perform regular backups to the destination. This procedure is not intended to be used for regular backups.
- **Big Sur**: Apple's replication utility may cause a kernel panic while cloning to the internal storage on Apple Silicon Macs <https://bombich.com/kb/ccc6/macos-big-sur-known-

issues#asr_broken_arm>, which could prevent you from restoring your Mac's system from the backup. (Note: Apple has resolved this problem for macOS Monterey, but the problem persists on Big Sur)
- **Apple Silicon Macs running macOS Ventura (or later)**: Apple's replication utility may fail to produce a bootable USB device <https://bombich.com/kb/ccc6/macos-ventura-known-issues#asr_broken_usb>. Results with Thunderbolt devices are more consistent. If you only have a USB device, we recommend making a Standard Backup to that device, then install macOS onto the backup (in that order specifically).
- Apple Silicon Macs will not boot at all if the internal storage fails <https://bombich.com/blog/2021/05/19/beyond-bootable-backups-adapting-recovery-strategies-evolving-platform>. An external bootable device will not serve as a rescue disk for that scenario.

For the reasons noted above, we do not recommend that you attempt to make your backups bootable; we recommend that you proceed with a "Standard Backup" instead. You can restore all of your documents, compatible applications, and settings from a standard CCC backup <https://bombich.com/kb/ccc6/how-restore-from-your-backup#install_then_migrate> without the extra effort involved in establishing and maintaining a bootable device.

Frequently Asked Questions

When the task started running, the destination was renamed to the same as the source. And what's this "ASRDataVolume" volume?

Highly perceptive people may notice that the name of the destination volume changes as Apple's volume replicator goes to work. An additional volume may appear in CCC's sidebar as well. This is normal. These volumes will be aggregated into a "volume group" and presented as a single volume, and CCC will rename the destination to its original name when the replication is complete.

If Apple's APFS replication utility fails and you see an ASRDataVolume or ASRNewVolume persisting, then you may delete those vestigial volumes in Disk Utility. Simply select the volume, then click the "-" button in the toolbar.

Do I have to erase the destination to make a bootable copy of the system?

If your Mac is running Big Sur or later, yes. As of macOS Big Sur, we're required to use Apple's APFS replicator to *establish* a bootable copy of an APFS volume group. We're unable to leverage the SafetyNet feature, and it's no longer appropriate to store other data on the destination volume. You must dedicate a volume to your bootable copy of the system.

Can I use the destination device for storing other data as well?

On a separate, dedicated volume, yes. We recommend that you add an APFS volume to the destination APFS container and use that new volume for your other content. As long as the system copy and the other content are stored on separate volumes, these can coexist peacefully on the same physical device. Likewise, you may add a partition to your destination disk if the destination is not APFS formatted. For example, if you have an external hard drive that already has content on an HFS+ formatted volume, you can add a partition to the disk and use the new partition for the copy of the system.

Related documentation

- Adding a volume or partition to the destination <https://bombich.com/kb/ccc6/frequently-asked-questions-about-ccc-and-macos-catalina#dedicated_volume>

If I continue to make regular backups to the destination, will it remain bootable?

You should not expect the destination to remain bootable after running additional backup tasks to the destination (i.e. via manual or scheduled backups). The Legacy Bootable Copy Assistant is intended only for creating ad hoc, bootable copies of the system *that you intend to use immediately*.

Can I exclude some content when making a bootable copy of the system?

If your Mac is running Big Sur or later, then it is not possible to exclude content and produce a bootable copy of the system. If you must exclude content from the initial copy, then we recommend that you proceed with a Standard Backup.

I already have other volumes on my backup disk. Will those be erased?

No, only the selected destination *volume* will be erased when you proceed with the "Erase {destination}" option. Other volumes on the same physical device will be unaffected. Regardless, we never recommend that you target a disk that has data on it that is not backed up elsewhere. If those other volumes are not yet backed up, then back up that data before proceeding.

I added a volume, but I don't want the extra volume after all. Can I delete it?

Yes. Choose **Disk Utility** from CCC's Utilities menu, select the volume you would like to delete, then press the "–" button in the toolbar to delete that volume.

Can I make the system copy on an encrypted volume?

You may select an encrypted volume as the destination, but the volume will be erased, and will not be encrypted when the task completes. Apple's APFS replication utility will not preemptively enable FileVault on the destination volume. To enable FileVault on the destination, you can boot from the destination volume and enable FileVault in the Security & Privacy Preference Pane.

Related documentation

- Troubleshooting APFS Replication <https://bombich.com/kb/ccc6/troubleshooting-apfs-replication>
- Working with FileVault Encryption <https://bombich.com/kb/ccc6/working-filevault-encryption>
- External Boot Troubleshooting <https://bombich.com/kb/ccc6/help-my-clone-wont-boot>

You can install macOS onto a "Standard Backup" to make it bootable

We recommend using the Legacy Bootable Copy Assistant any time you have an **immediate** need to create a bootable copy of your startup disk. However, if some time in the future you find a need to boot from an external device, and you have an existing Standard Backup *on a non-encrypted APFS volume* that you would like to make bootable, you can install macOS onto that volume:

1. Download and open the macOS Installer: [Catalina <https://itunes.apple.com/us/app/macos-catalina/id1466841314?ls=1&mt=12>] [Big Sur <https://itunes.apple.com/us/app/macos-big-sur/id1526878132>] [Monterey <https://apps.apple.com/us/app/macos-monterey/id1576738294?mt=12>] [Ventura <https://apps.apple.com/us/app/macos-ventura/id1638787999?mt=12>] [Sonoma <https://apps.apple.com/us/app/macos-

sonoma/id6450717509?mt=12>]
2. When prompted to select a disk, click the **Show All Disks...** button and select your backup disk
3. Proceed to install macOS onto your backup disk

Note that the macOS Installer will remove any snapshots on the backup volume, thus revoking any opportunities to restore older versions of your files.

Troubleshooting tip: Some users have discovered that macOS will stall when starting up from the backup disk. If you encounter this problem, try booting in Safe Boot mode (Intel Macs: hold down the Shift key on startup, Apple Silicon Macs: hold down the Power button on startup, then press the Shift key while selecting the startup volume) to disable the loading of third-party storage drivers. If applicable, see this Kbase article to see how to uninstall incompatible third-party storage drivers <https://bombich.com/kb/ccc6/some-third-party-storage-drivers-may-cause-hardware-misbehavior>.

Please note, however, that our recommended and supported procedure for restoring your startup disk from a CCC backup is to install macOS onto a freshly-erased volume, then use Migration Assistant to migrate data from the CCC backup. A bootable volume is not required for this procedure.

Using Migration Assistant to restore your startup disk from a CCC backup <https://bombich.com/kb/ccc6/how-restore-from-your-backup#install_then_migrate>

Sample Usage Scenarios

I want to migrate data to a new Mac

Use Setup Assistant or Migration Assistant to migrate data from a CCC backup to a new Mac

When you get a new computer from Apple, it has a specific version of macOS installed on it, and further, a hardware-specific "build". Your new Macintosh cannot boot from the older version and build of macOS that is installed on your older Mac, so simply restoring your old Mac's backup onto your new Mac won't work. We recommend that you use the Setup Assistant application (runs on your Mac's very first boot) or the Migration Assistant application to migrate content from your old Mac to a new Macintosh. You can migrate directly from a CCC backup of your old Mac.

- Boot your new Mac
- Accept the prompt to migrate data
- Choose the first option to migrate data from a backup
- Select your CCC backup as the source for the migration, then proceed as directed by Migration Assistant

Once you have migrated your user accounts and applications using Setup Assistant or Migration Assistant, you can continue to use CCC to back up your Mac to the same backup volume that you were using for the old Mac.

Migration Assistant and the CCC SafetyNet

If your backup volume has a legacy "_CCC SafetyNet" folder, you can move that folder to the Trash before using Migration Assistant to avoid copying that folder during a migration. This is particularly important if that folder has a lot of data in it and you're migrating to a disk that is smaller than the backup volume. After you have completed the migration, you can resume backups to the same destination volume, however we recommend that you enable CCC Snapshot support on the destination <https://bombich.com/kb/ccc6/leveraging-snapshots-on-apfs-volumes#srp> to avoid using the legacy SafetyNet folder.

Related Documentation

- Can I restore my Mac's backup to another computer? <https://bombich.com/kb/ccc6/can-i-back-up-one-computer-and-use-clone-restore-another-computer>
- How to set up your first backup [that is compatible with Migration Assistant] <https://bombich.com/kb/ccc6/how-set-up-your-first-backup>
- Apple Kbase #HT204350: Move your content to a new Mac <https://support.apple.com/kb/HT204350>

How should I run my last backup on my old Mac?

A standard backup created with CCC's default settings <https://bombich.com/kb/ccc6/how-set-up-your-first-backup> will work just fine with Migration Assistant. But, this is also a great time to verify the integrity of your backup, especially if you're planning on getting rid of your old Mac. So before you proceed to migrate data from your backup, we recommend that you run one last backup on your old Mac with the following steps:

1. Open CCC and select the backup task that backs up your Mac's startup disk
2. Hover your mouse over the Destination selector – if you see **CCC Snapshots: Disabled**,

click on the Destination selector and choose **Manage snapshots on '{volume name}'**. Toggle the **CCC Snapshots** setting to the **On** position, then click the **Back** button in the toolbar to return to your backup task.

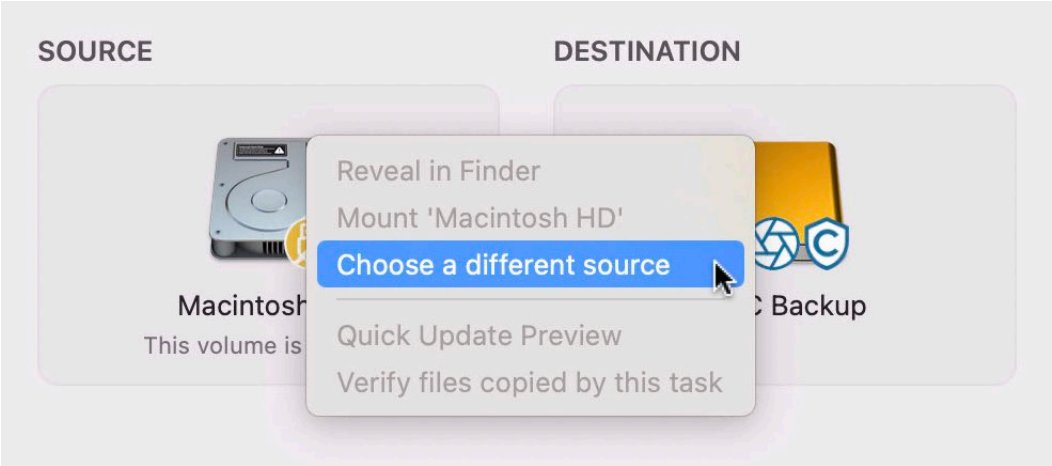
3. Click **Advanced Settings** at the bottom of the window
4. Select the **Postflight** tab
5. Check the box next to **Re-verify files that were copied**
6. Select the **Performance & Analysis** tab
7. Check the box next to **Find and replace corrupted files on the destination**
8. Select **Only on the next run** from the popup menu adjacent to that setting
9. Click the **Done** button
10. Click the **Start** button

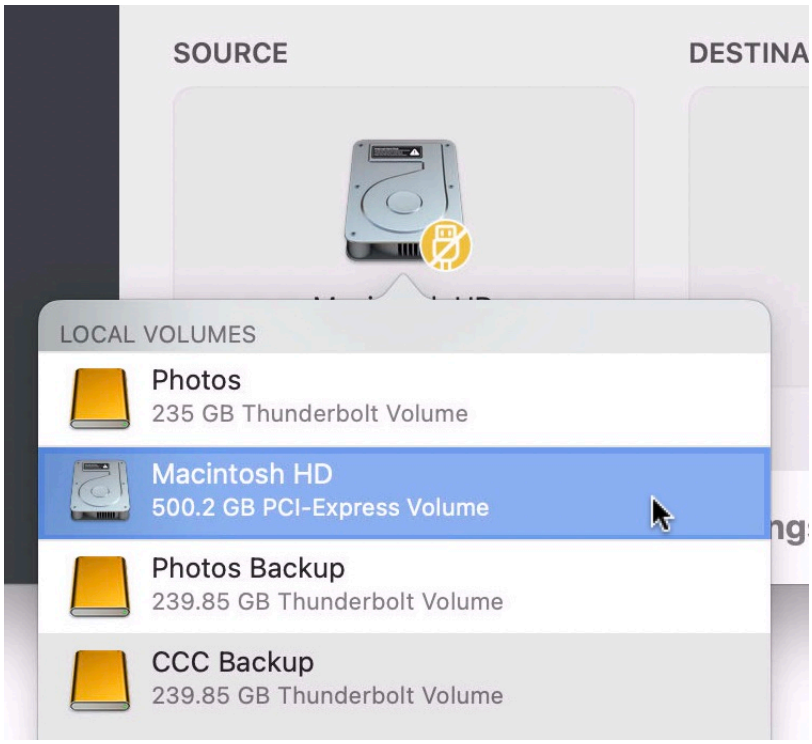
This task will take a while longer than a usual incremental update to the backup, because CCC is going to re-read every file on the source and destination. By doing this, we'll proactively detect any files that have become corrupt due to media failure on either the source or destination, and then you can take a moment to either correct the problem, or simply make a note of what might not be available when you proceed to migrate data to your new Mac.

After you've migrated data to your new Mac...

Once you have migrated data with Apple's Migration Assistant, there will be some housekeeping to perform. Many software companies tie the registration to the disk or Mac it's installed on to reduce piracy, so some applications may need to be re-registered. Some applications may also need to have the location of their data storage re-selected. We cover some common application-specific issues that we've seen here: Why do some applications behave differently or ask for the serial number after restoring from the backup? <https://bombich.com/kb/ccc6/some-applications-behave-differently-or-ask-serial-number-on-cloned-volume.-did-ccc-miss>

CCC will also require some attention to get your backup tasks working on the new Mac. When you migrate tasks to a new Mac, CCC suspends the backup tasks to prevent them from running in error. Open CCC and select each task, choosing to activate the task when prompted. Any tasks that reference a volume from the old Mac will need to be updated to reference the new volume, even if the volume name is the same. For example, if your source was "Macintosh HD" on the old computer and is still "Macintosh HD" on the new Mac, you will have to reset the source to reference the new Macintosh HD volume. Click on the Source selector and choose the option to select a different source, then select the correct source volume.





Once you're certain that you have migrated all of your data to the new Mac, you can clean up the old Mac before you hand it off to someone else. Apple offers some advice on that topic here: Apple Kbase #HT201065: What to do before you sell, give away, or trade-in your Mac <https://support.apple.com/en-us/HT201065>

I want to back up my data to network attached storage (NAS)

Network storage appliances are very popular for providing shared "personal cloud" storage. Naturally, this storage looks very appealing as a backup destination. The thought of backing up all of your stuff without having to plug in a cable is very alluring. "Convenient" and "fast" often go hand-in-hand, but that often is not the case when backing up to a network volume. There are several factors that can greatly reduce the performance of your backup, and this backup strategy encounters several of them.

Backing up your data to a network volume

Before you proceed, your NAS volume should be mounted and accessible in the Finder. Instructions for gaining access to network volumes is available in the macOS Help Center. If your network volume does not appear in CCC's Source or Destination menu, consult the documentation that came with the storage device you are trying to access, or choose "macOS Help" from the Finder's Help menu and search for "connecting to servers".

To back up a folder to a NAS volume with CCC:

1. Choose **Choose a folder** from the Source selector.
2. Select the folder that you would like to back up as the source
3. Choose **Choose a folder** from the Destination selector
4. Navigate to your NAS volume, then click the **New folder** button to create a new folder on this volume, e.g. named "CCC Backup". Click the OK button.
5. To improve the performance of future backup tasks, click **Advanced Settings** at the bottom of the window, select the **Performance & Analysis** tab, then check the box next to Use Quick Update when it's possible to collect a list of modified folders from macOS <https://bombich.com/kb/ccc6/advanced-settings#quickupdate>. Click **Done**.
6. Click the **Start** button to run the task immediately, or schedule the task to run later.

Note: If you select your whole startup disk as the source to a task that backs up to a NAS volume, CCC will automatically exclude all system-related content. Generally when backing up to a NAS, you should drag a *specific* folder onto CCC's Source selector to reduce the scope of the task.

Caveats to backing up to NAS storage

Not compatible with Migration Assistant, no backup versioning

First and foremost, backups to a NAS will not be compatible with Migration Assistant, and they do not support backup versioning. If you want those benefits in your backup strategy, you should use NAS storage only as a secondary backup. To create a backup that is compatible with Migration Assistant and supports backup versioning, configure a task to back up to locally-attached storage (e.g. a USB hard drive attached to your Mac).

NAS backups are slow

Backups to NAS volumes are inherently slow because NAS filesystem enumeration is inherently slow. Filesystem transactions to NAS volumes have a high amount of overhead, so even a simple task of comparing folders that have no changes can take longer than it seems it should. CCC's Quick Update <https://bombich.com/kb/ccc6/advanced-settings#quickupdate> feature can go a very long way

towards mitigating that slower performance on subsequent backups, but the performance of the initial transfer is mostly dependent on the performance of your NAS and network. We recommend connecting your Mac to your network via ethernet for the initial backup.

Not all data can be backed up to a NAS

Many NAS devices impose archaic Windows naming conventions that prevent you from copying some files to the NAS volume. GarageBand is a classic example – there is a folder named "Aux" in the GarageBand bundle that many NAS devices will refuse to accept.

Because NAS backups have several inherent limitations, we recommend using a NAS for a secondary backup. For primary backups, we recommend that you procure a USB or Thunderbolt hard drive and create a backup on that locally-attached disk. Local backups are much simpler, more reliable, offer the added security of "backup history", are compatible with Migration Assistant, and in general they're a lot easier to restore from.

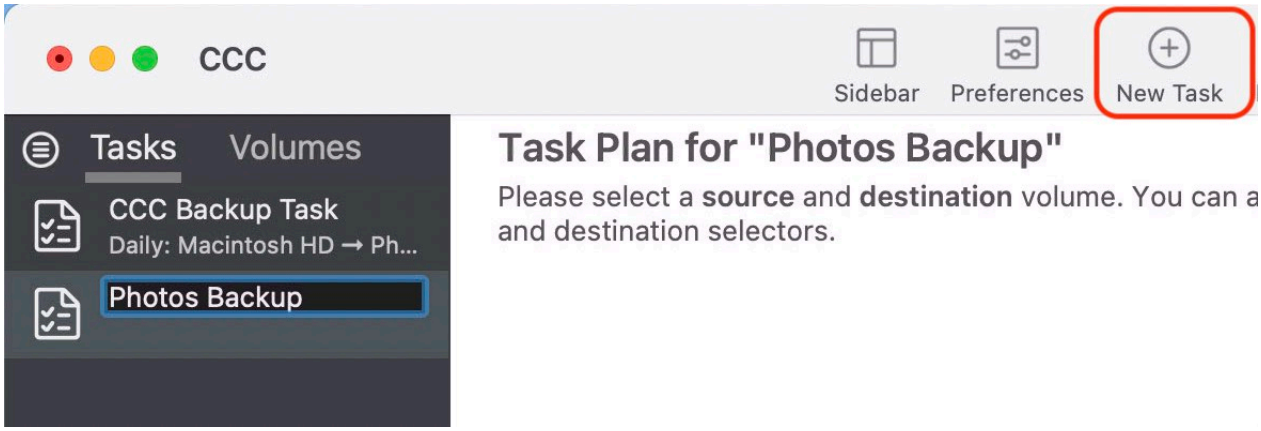
Related Documentation

- Troubleshooting slow performance when copying files to or from a network volume <https://bombich.com/kb/ccc6/troubleshooting-slow-performance-when-copying-files-or-from-network-volume>
- Restoring from a data backup on a NAS or network share <https://bombich.com/kb/ccc6/how-restore-from-your-backup#nas_restore>
- Choosing a backup drive <https://bombich.com/kb/ccc6/choosing-backup-drive>
- Some NAS services have obtuse file name restrictions <https://bombich.com/kb/ccc6/backing-up-tofrom-network-volumes-and-other-non-hfs-volumes#smb_special_characters>
- Character composition conflicts on NAS volumes <https://bombich.com/kb/ccc6/character-composition-conflicts-on-nas-volumes>

Copying one external hard drive to another external hard drive

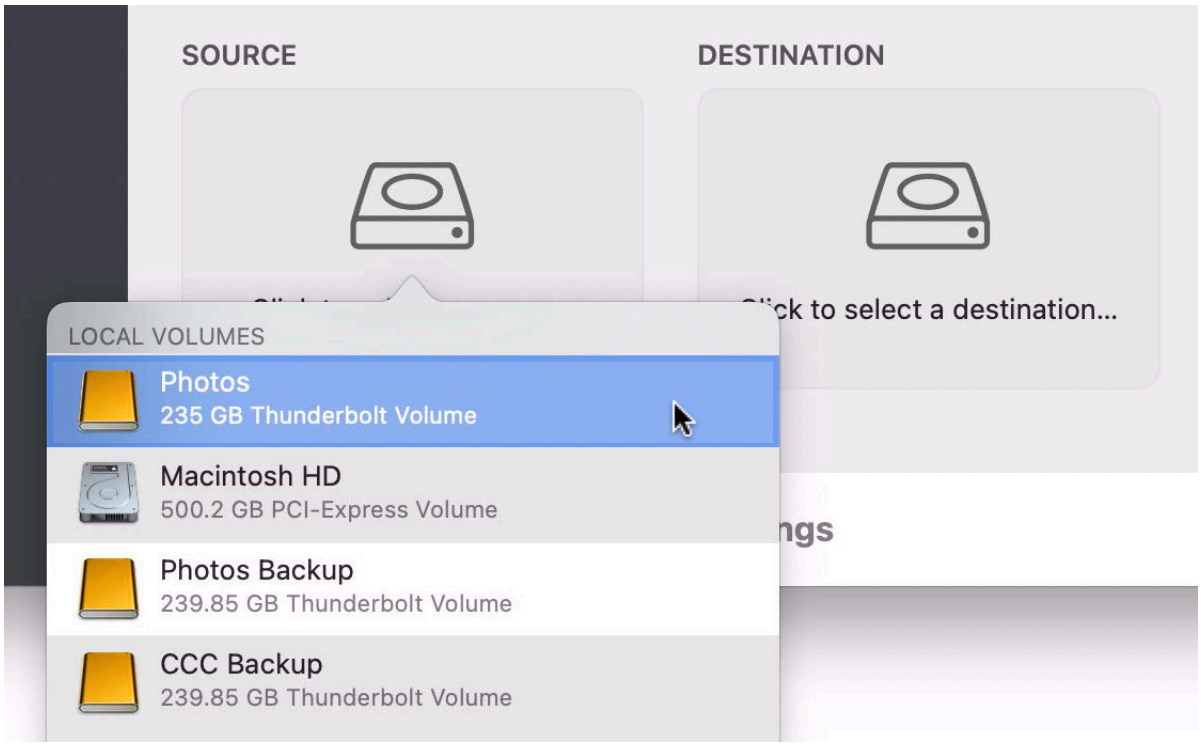
Create a new task

Click the **New Task** button in the toolbar to create a new task, then type in a name for the new task.



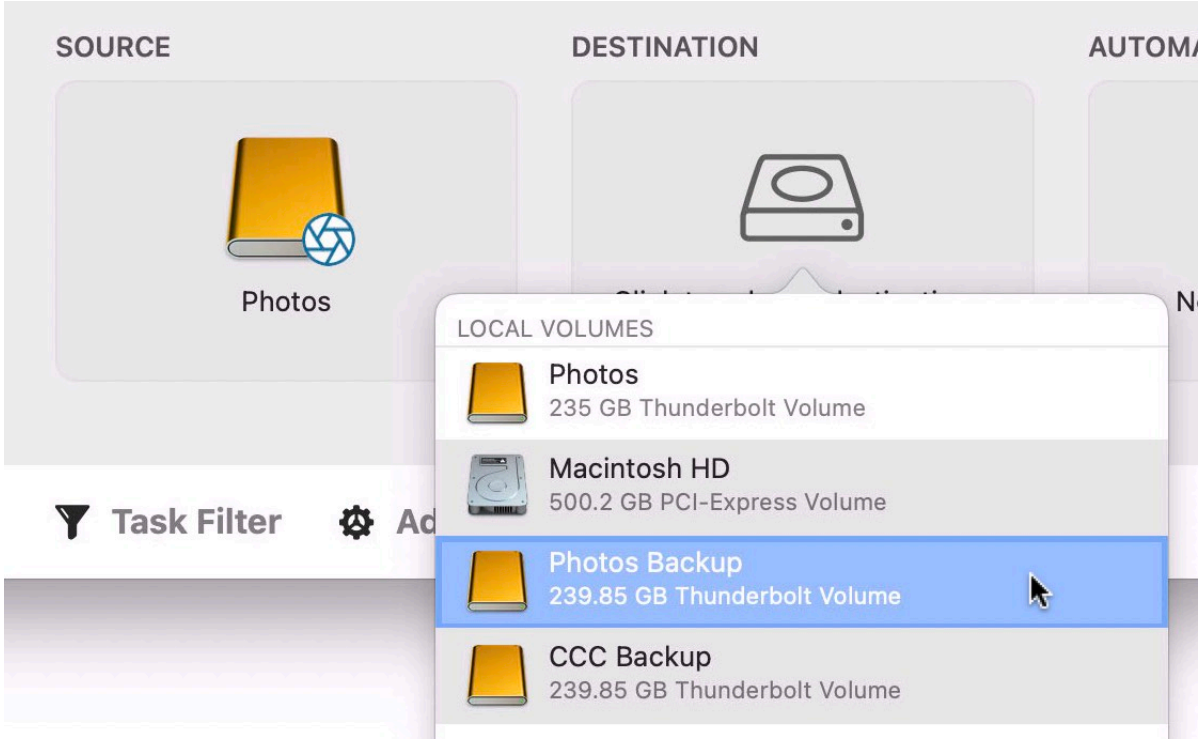
Select a source volume

Click on the Source selector, then choose the volume that you want to copy files from.



Select a destination volume

Click on the Destination selector, then choose the volume that you want to copy files to.



Click the Start button

Click the Start button to copy files right away, or click the Scheduler selector to configure the task to run on a regular basis.

Related Documentation

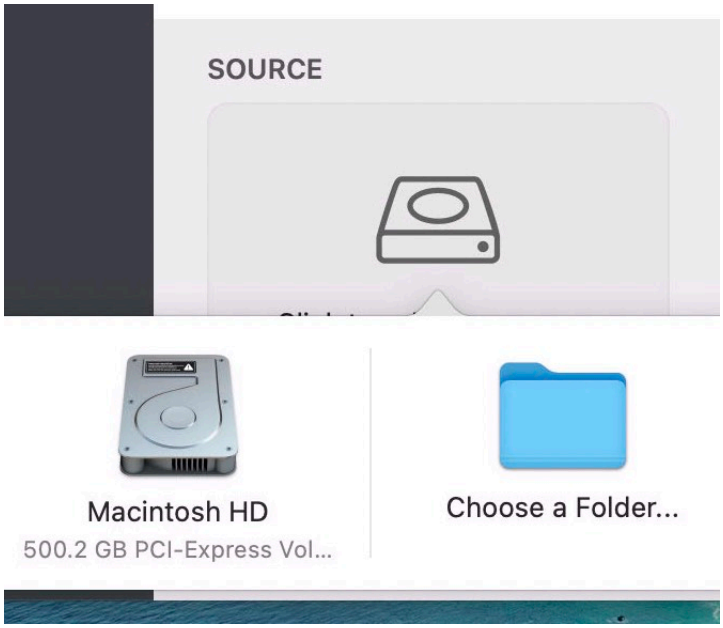
- How to set up a scheduled backup <https://bombich.com/kb/ccc6/how-set-up-scheduled-backup>

Folder-to-Folder Backups

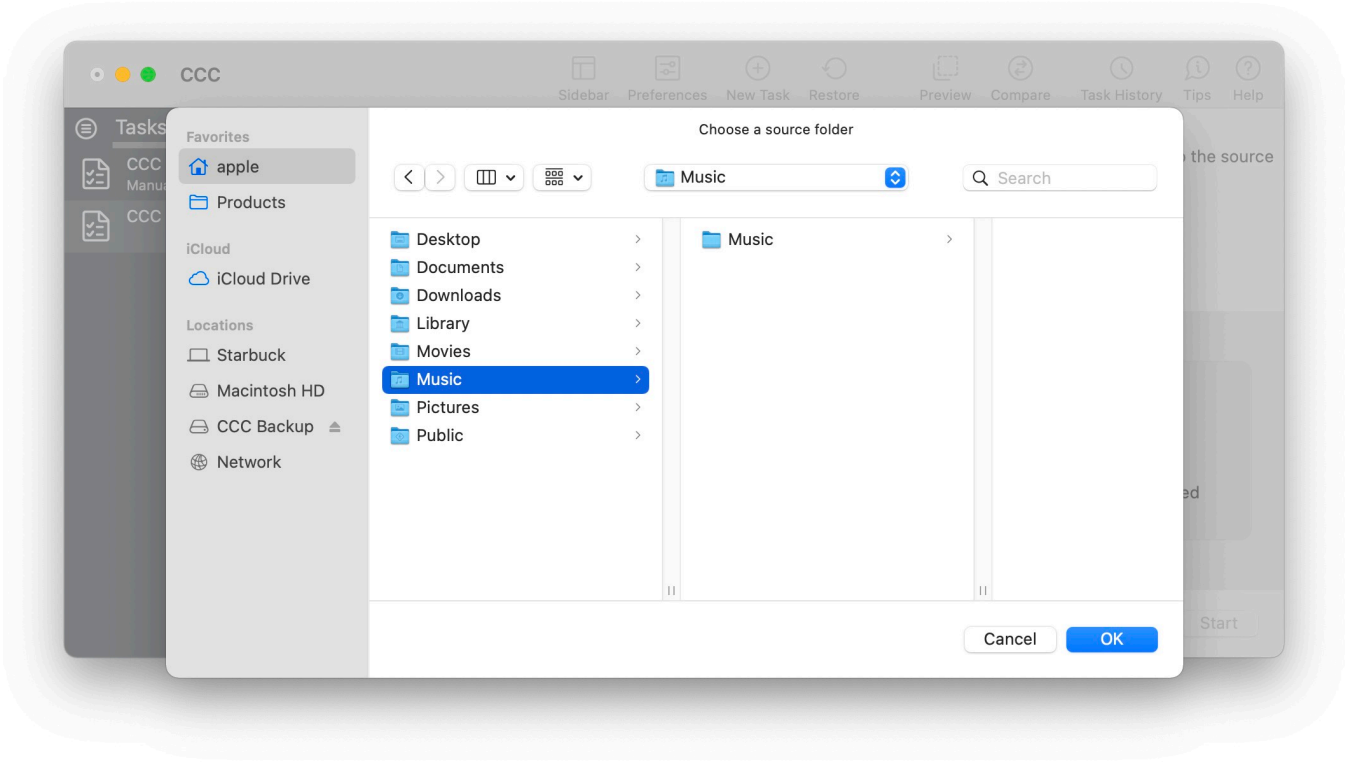
When you select a volume as the source and destination, CCC copies the entire contents of that volume (minus anything you exclude) to the destination volume, preserving the full hierarchy of folders on the source. If you don't want to preserve that hierarchy, you can back up a specific folder from the source to a specific folder on the destination. In this configuration, CCC will copy the contents of the selected folder to the selected destination folder, without the hierarchy up to that source folder.

Choose your source

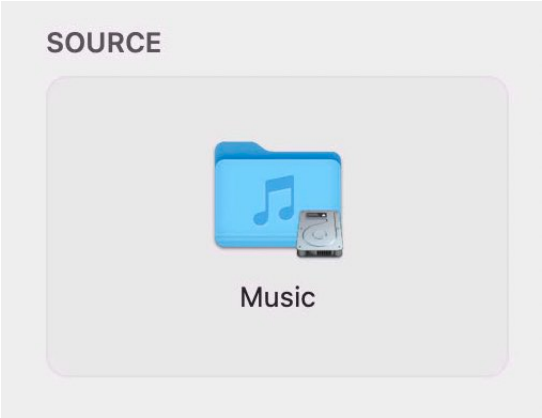
Click the Source selector and select **Choose a Folder...**



Select your source folder and click **OK**.

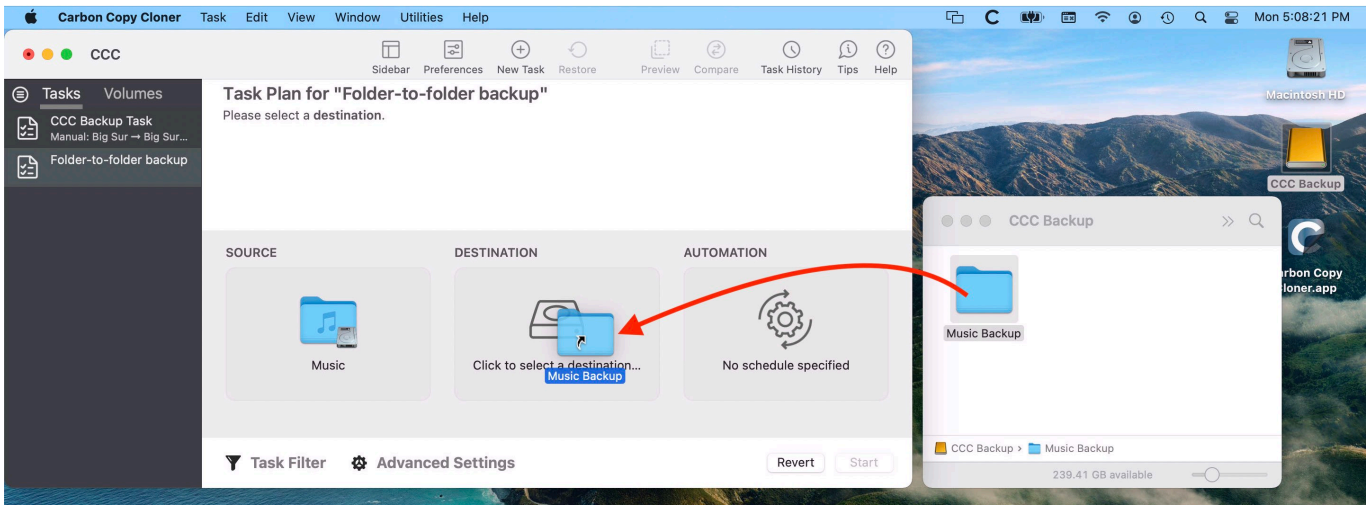


The Source box should display the icon of your selected folder and its name. You can click on the Source selector again for additional details about that selection. Click the **Task Filter** button at the bottom of the window if you would like to exclude some of the content of that folder from the backup task.

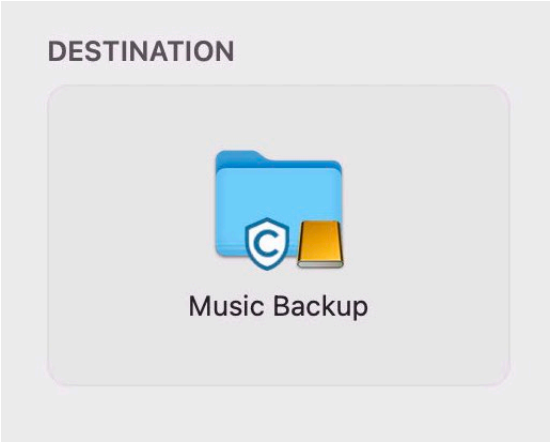


Choose your destination

You can repeat the steps above to select a destination. CCC also supports drag and drop selection, so we'll demonstrate that here. Find your destination folder in the Finder, then drag it onto CCC's Destination selector.

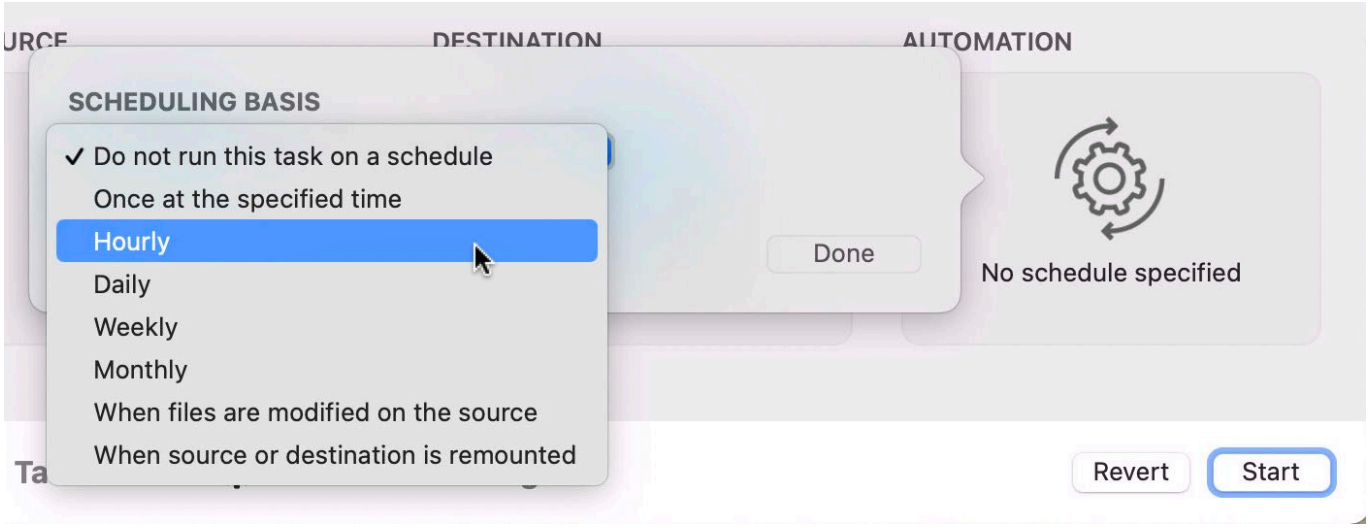


The Destination box should display the icon of your selected folder and its name. You can click on the Destination selector again for additional details and settings specific to that selection (e.g. CCC's SafetyNet feature). To learn more about SafetyNet, please see **Protecting data that is already on your destination volume: The CCC SafetyNet <https://bombich.com/kb/ccc6/protecting-data-already-on-your-destination-volume-carbon-copy-cloner-safetynet>**.



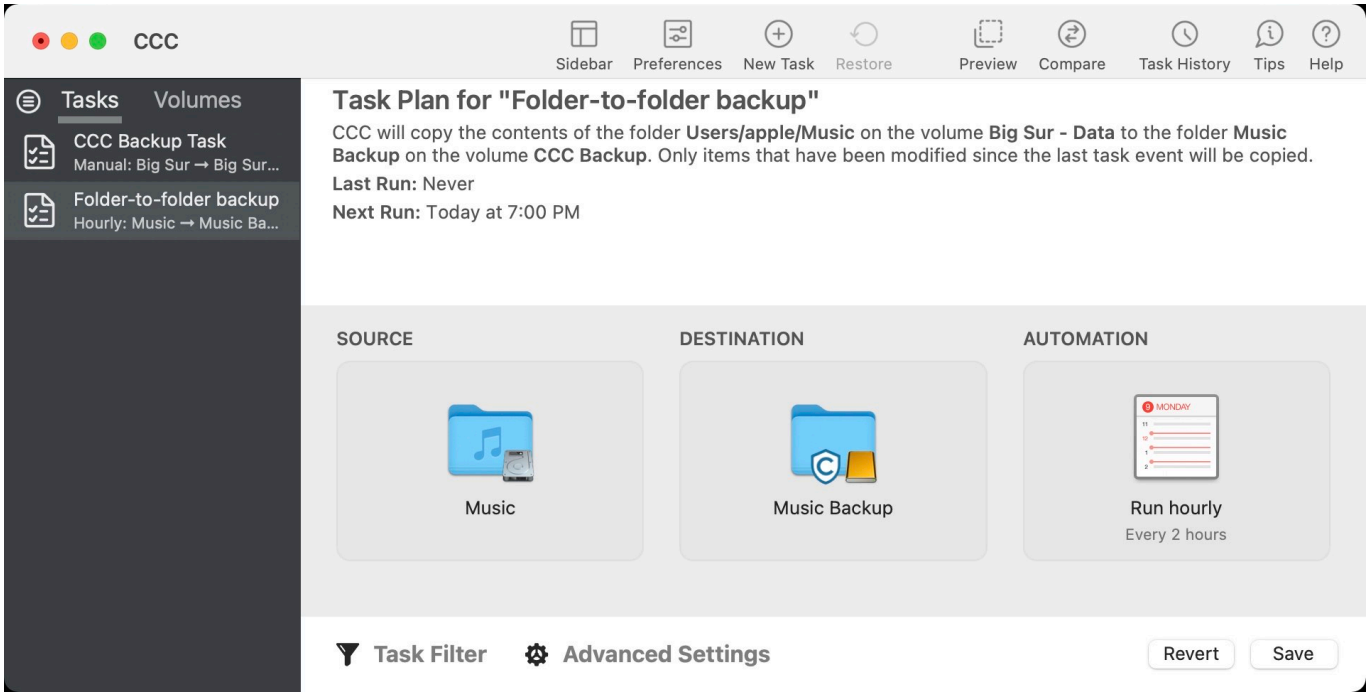
Schedule the backup

Click in the Automation box and design a backup schedule that meets your needs. Click **Done** when you have finished.



Save and optionally run the task

Once you have your source, destination and schedule complete, click on Save in the bottom, right corner of the window. You may click the **Start** button to run the backup manually, or let it run on a schedule.



Using a CCC backup with a loaner Mac

Sometimes when you send your Mac off for a repair, you just can't go without "your computer" for the duration of the repair. In this article we'll offer some best practices on how to quickly get your data backed up and transferred to a loaner Mac, how to get the data back to your Mac when it returns from the shop, and how to quickly and securely remove your data from the loaner Mac.

Before you send your original Mac out for repair

CCC's default settings are designed to create a backup of your Mac that can be easily migrated to another Mac. Configure a CCC backup task to back up your startup disk to a locally-attached, APFS-formatted device. This Kbase article offers step-by-step guidance: Establishing an initial backup <https://bombich.com/kb/ccc6/how-set-up-your-first-backup>. Ideally, you already have a CCC backup. If you wait for your Mac to break before creating a backup, you might not have an opportunity to create one, or it may be logistically difficult (e.g. damaged display).

Before you accept the loaner Mac

Upgrading your data to a newer OS is usually uneventful. Downgrading your data, however, is virtually impossible, and is completely unsupported by Migration Assistant. If your current Mac is not on the latest OS, and if you specifically do not want to upgrade to a newer OS (e.g. when your Mac is returned), then you need to be very careful about what OS you migrate your data to. Before you accept a loaner Mac, verify that the OS installed on that Mac is the same as the OS that you're currently using (or newer, if you're willing to upgrade your Mac upon its return).

If you can't acquire a Mac that has the same OS as your current Mac, you should avoid migrating your data to that Mac. Instead, attach the backup disk to the loaner Mac and access your files directly from the backup. This is a less-ideal configuration because you lose some hardware redundancy when you work directly from the backup, but it's often less risk than dealing with the hassle of trying to downgrade your data from a newer OS.

When you get the loaner Mac

Prior to transferring data to the loaner Mac, we recommend that you enable FileVault on that Mac's startup disk. By enabling FileVault, your data is never placed onto the loaner Mac in an unencrypted form, and securely removing it from that Mac can be done in a matter of seconds.

Transfer data to the loaner Mac using the following steps:

1. Boot the loaner Mac (from its own internal disk).
2. If prompted in Setup Assistant, skip the option to migrate data.
3. Proceed to create a new user account. Name it something temporary, like "utility".
4. Once logged in, open System Settings > Privacy & Security and turn on FileVault.
5. Attach your CCC backup disk to the loaner Mac.
6. Go to System Settings > General > Transfer or Reset and click "Open Migration Assistant..."
7. Proceed to migrate data from "a backup" – choose the CCC backup volume as the source.

While you're using the loaner Mac

Especially if you plan to use the loaner Mac for more than a day or so, we recommend that you establish a backup task that will back up any changes you make to your data while using the loaner Mac. This will also get you prepared for taking your data back to your original Mac when it gets back from the shop.

1. Open CCC.
2. When prompted, leave your other backup tasks suspended.
3. Configure a new backup task to back up the current startup disk to your backup disk.
4. Schedule the task to run at your preferred frequency.

Because all of your data is already on this backup, the task should go pretty quickly to update the changes that you're making on the loaner Mac.

When you get your original Mac back from the service center

1. On the loaner Mac, quit all applications except for CCC.
2. Run the CCC backup task one last time to get everything on the backup up to date.
3. Detach the backup disk from the loaner Mac; now just leave the loaner Mac as it is – don't delete anything from it yet.
4. Boot your original Mac (from its own internal disk).
5. When prompted by Setup Assistant, accept the offer to migrate data from a backup. †
6. Attach the CCC backup disk to your original Mac and select it as the source in Migration Assistant, the proceed as directed to migrate all of your data back to the original Mac.

† If your Mac was not returned from the service center with a clean installation of macOS, open System Settings > General > Transfer or Reset and click **Erase All Content and Settings...** prior to attaching your backup disk to the original Mac.

When the migration has completed

After migration is complete and you've logged in to your account on the original Mac, the very last step is to securely remove your data from the loaner Mac and return it in "clean install" condition.

1. On the loaner Mac, open System Settings > General > Transfer or Reset.
2. Click **Erase All Content and Settings...**
3. Authenticate in the Erase Assistant, then click Continue to remove your data from the loaner Mac.

When that process has completed, the system should reboot to Setup Assistant. Because you had enabled FileVault on the startup disk before transferring data, all of your data was 100% securely removed from that system, pretty much instantly. You can now turn off that system and return it.

Backing up and restoring Finder's Trash

Backing up Trash content

CCC will not back up the contents of Finder's Trash by default, but CCC offers an option to back up the Finder's Trash <https://bombich.com/kb/ccc6/excluding-files-and-folders-from-backup-task#trash> in the Task Filter window. Click the **Task Filter** button at the bottom of CCC's window to reveal the task filter.

The Trash is not a simple folder, it's a complex mechanism that aggregates Trash folders from multiple volumes and user home folders on the startup disk; it behaves quite unlike other folders. When you back up the contents of the Trash, those items are copied to the Trash folder on the destination, and may reside in "the Trash" as viewed in the Finder. If you subsequently empty the Trash, that will delete the Trash on the backup disk if it is mounted when you empty the Trash. If you choose the option to back up the Finder Trash, we recommend that you unmount and detach your backup disk before emptying the Trash if you wish to retain the Trash on the backup disk.

Restoring Trash content

If you eject your backup disk and detach it from your Mac, and then you empty the Trash, you can simply reattach the backup disk to your Mac and the Trash will again appear to be filled. You can simply drag items out of the Trash to recover those items.

The Trash is a little bit more complicated than that

For external data-only volumes, the Trash behaves in the fairly straightforward manner previously described. For your startup disk, though, it's not quite that simple. There is more than one Trash folder on the startup disk, e.g. there is a Trash folder in each user's home folder. When you move an item (that you are the owner of) on your startup disk to the Trash, that item is placed in your home folder's Trash, not in the volume's trash folder. It still appears in "the Trash", but its location is important with regard to the backup. Suppose you do the following (with CCC configured to copy the Finder Trash):

1. Move an item from your Desktop to the Trash
2. Run a backup
3. Detach your backup disk
4. Empty the Trash
5. Reattach your backup disk

Result: That item is not in the Trash! The file is actually in a Trash folder on the backup disk, but the Finder doesn't show you items in the home folder trash folders on external volumes. In this scenario, you can press Command+Shift+Period to toggle the Finder's display of hidden items, and then you will be able to navigate to the Trash folder on your home folder on the backup disk.

Refining the scope of a backup task

Watch a video of this tutorial on YouTube <https://youtu.be/mctdmbKLgNY>

We often see backup tasks configured with the whole startup disk selected as the source, and then everything excluded from the backup except for a single folder. This kind of configuration is suboptimal for several reasons:

- The entire folder hierarchy up to the non-excluded folder is preserved, so it takes longer to navigate to your files on the destination.
- With the startup disk selected, CCC may perform unnecessary subtasks related to making a legacy bootable backup on the destination.
- The task involves more overhead (e.g. evaluating lots of exclusion rules), so it will take longer.
- The scope of the task is very broad; CCC's effects are applicable to the whole destination rather than to a single folder.
- If the destination is a folder on the startup disk or on a non-Apple formatted volume, then the task will likely produce errors related to preserving special file flags of folders on the startup disk.

A better configuration is to create a folder-to-folder backup. With a specific folder selected as the source and a specific folder selected as the destination, you greatly reduce the scope of the task, thus reducing the amount of work that the task has to do and also reducing any risks to other content on the destination.

Converting a whole-disk, single folder task to a folder-to-folder backup

For the sake of an example, let's suppose you selected **Macintosh HD** as the source for a backup task, then configured a task filter that excluded everything except for Users > yourname > Documents > Work In Progress. Let's also suppose that you selected a volume named **CCC Backup** as the destination for this task. If you navigate to the **CCC Backup** volume in the Finder, you will find a folder hierarchy of Users > yourname > Documents > Work In Progress. To convert this backup configuration to a folder-to-folder backup, you would do the following:

1. Navigate to the **CCC Backup** volume in the Finder
2. Navigate to Users > yourname > Documents > Work In Progress
3. Move the Work In Progress folder to the root level of the **CCC Backup** volume
4. Move the (now containing empty folders) Users folder to the Trash
5. Open CCC and select the relevant backup task
6. Drag the Work In Progress folder from the **CCC Backup** volume onto CCC's Destination selector
7. Drag the Work In Progress folder from your home folder on the **Macintosh HD** volume onto CCC's Source selector
8. Save the task

Related Documentation

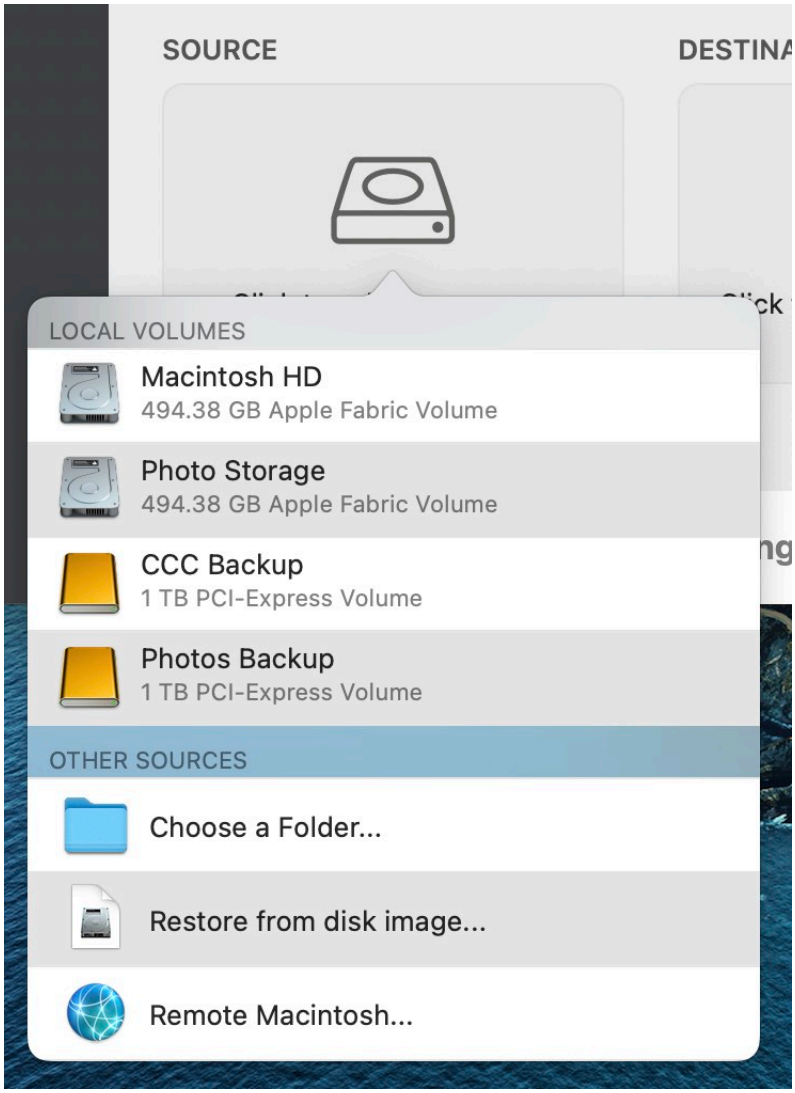
- Folder-to-Folder Backups <https://bombich.com/kb/ccc6/folder-folder-backups>

Upgrading your backup strategy from Time Machine to CCC

Time Machine offers a very basic backup with very few customization options, so setting up CCC to mimic "a Time Machine backup" is simple.

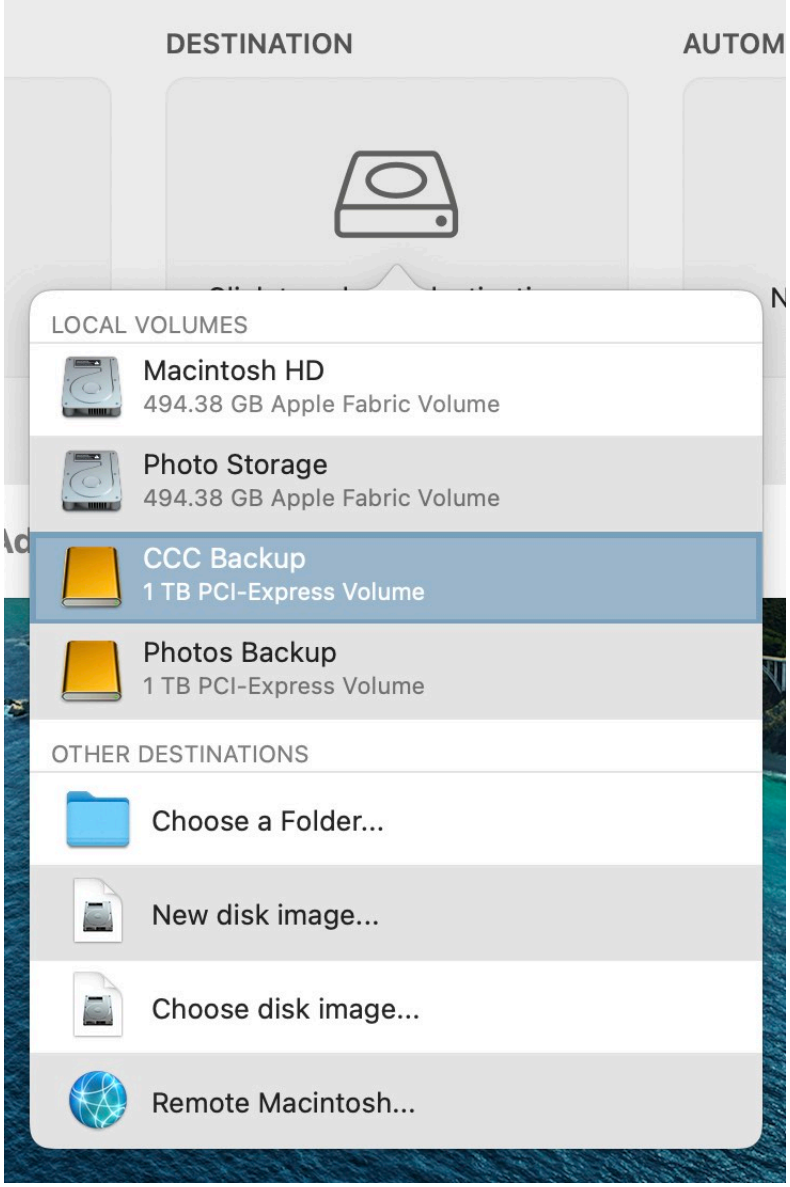
Choose "Macintosh HD" as the source

By default, Time Machine backs up your "Macintosh HD" disk. Click on CCC's Source selector and choose **Macintosh HD** as the source to your backup task.



Choose your backup disk as the destination

The most common Time Machine setup is to back up to an external disk that is connected to your Mac. In CCC, simply select that drive as your destination.

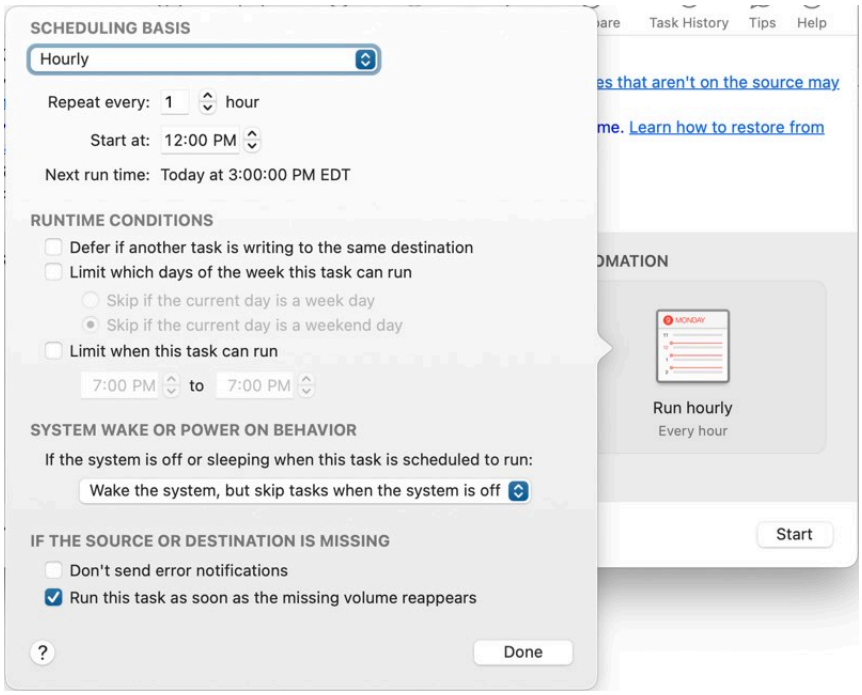


Can I use my Time Machine backup disk for my CCC backups?

CCC and Time Machine cannot share a backup volume, but the backups can reside on the same disk. If you select a Time Machine backup volume as the destination to your task, CCC will automatically create a new volume on that disk. If you want to replace Time Machine entirely with CCC, you can select the Time Machine backup volume in Disk Utility, then click the "-" button in the toolbar to remove that volume. For additional configuration options for your backup disk, see this section of CCC's documentation: I want to back up multiple Macs or source volumes to the same hard drive <https://bombich.com/kb/ccc6/i-want-back-up-multiple-macs-or-source-volumes-same-hard-drive>

Set "Automation" to run hourly

Time Machine requires that your backup runs every hour, or manually – that's it. In CCC, click on the Automation box, then choose **Hourly** from the **Scheduling Basis** popup menu (or any other timing that suits your preference).



That's it! You have now matched Time Machine feature-for-feature. But why stop there, there is a bunch of other functionality in CCC that will greatly enhance your backup strategy. Check out these other features of CCC:

- Integrity checking of files on the source and destination — proactively detect and deter "bit rot" <https://bombich.com/kb/ccc6/how-verify-or-test-your-backup>
- Make incremental updates to your backup even faster with Quick Update <https://bombich.com/kb/ccc6/advanced-settings#quickupdate>
- See detailed backup history, granular error reporting, and a list of changes made in each task event <https://bombich.com/kb/ccc6/how-find-out-when-backup-last-ran-ccc-task-history>
- Compare the source and destination to see what the current differences are <https://bombich.com/kb/ccc6/comparing-source-and-destination>
- Apply granular control over what should and should not be included in your backups <https://bombich.com/kb/ccc6/excluding-files-and-folders-from-backup-task>
- Apply granular control over when your backup tasks run <https://bombich.com/kb/ccc6/advanced-scheduling-options>

Encrypting backups

If you're setting up a new backup volume, erase it as "APFS Encrypted" in Disk Utility.

If you simply want to encrypt your current backup, right-click on it in the Finder and choose the option to **Encrypt** it.

Related documentation

- Preparing your destination disk for a backup or restore <https://bombich.com/kb/ccc6/preparing-your-backup-disk-backup-os-x>
- Working with FileVault Encryption <https://bombich.com/kb/ccc6/working-filevault-encryption>

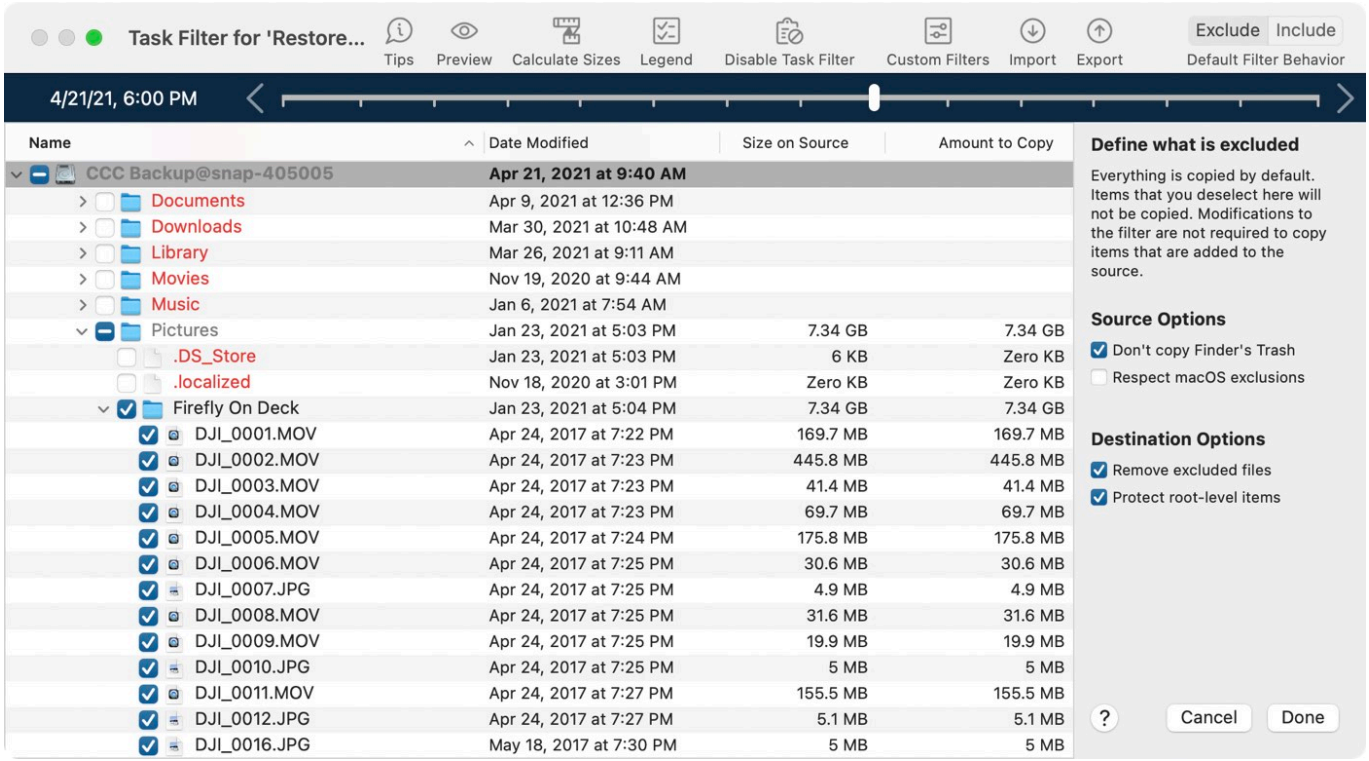
Menu bar icon

Time Machine offers a menu bar icon that tells you the current status of Time Machine, and gives you an option to manually run the backup or "Enter Time Machine" (view older snapshots of files). CCC also has a menu bar icon <https://bombich.com/kb/ccc6/monitoring-backup-tasks-ccc-menubar-application> with status information for all your backup tasks and notification preferences.

Browsing your file history

You can use CCC's Snapshot Navigator to browse older versions of your files:

1. Click **Restore** in CCC's toolbar
2. Click on the **Source** selector and choose your backup disk as the source
3. Click **Task Filter** at the bottom of the window
4. Select a file, then use the navigation controls to navigate backwards and forwards through your backup history



For additional details about restoring from a backup, including tutorial videos, see this section of CCC's documentation: Restoring an older version of a backup <https://bombich.com/kb/ccc6/how-restore-from-your-backup#restore_whole_snapshot>

Backing up to a network volume

When making a backup to a network volume, Time Machine backs up to a disk image. You could certainly configure CCC to back up to a disk image on a NAS volume too — choose "New Disk Image..." in CCC's Destination selector to set that up.

But we don't recommend that, in fact we explicitly discourage it <https://bombich.com/kb/ccc6/backing-up-disk-image>. NAS-hosted disk images are very sensitive to network connectivity loss, and that fragility eventually leads to corruption of the disk image. You

see that with Time Machine too — there are countless reports of "The (Time Machine) backup is corrupt, it needs to be recreated" on the Internet, and most of those would trace back to corruption of the disk image.

You can select a NAS volume, or a folder on a NAS volume as the destination to a CCC backup task. We specifically present this direct-to-NAS functionality in contrast to the inflexibility that Time Machine offers. But we also recommend using NAS backups only as a secondary option for a subset of your most important data. For the **most** reliable primary backup, and also for more functionality from your backup, we recommend that you procure a USB or Thunderbolt hard drive <https://bombich.com/kb/ccc6/choosing-backup-drive> and create a backup on that locally-attached disk. Local backups are much simpler, faster, compatible with Migration Assistant, and offer file versioning via snapshots.

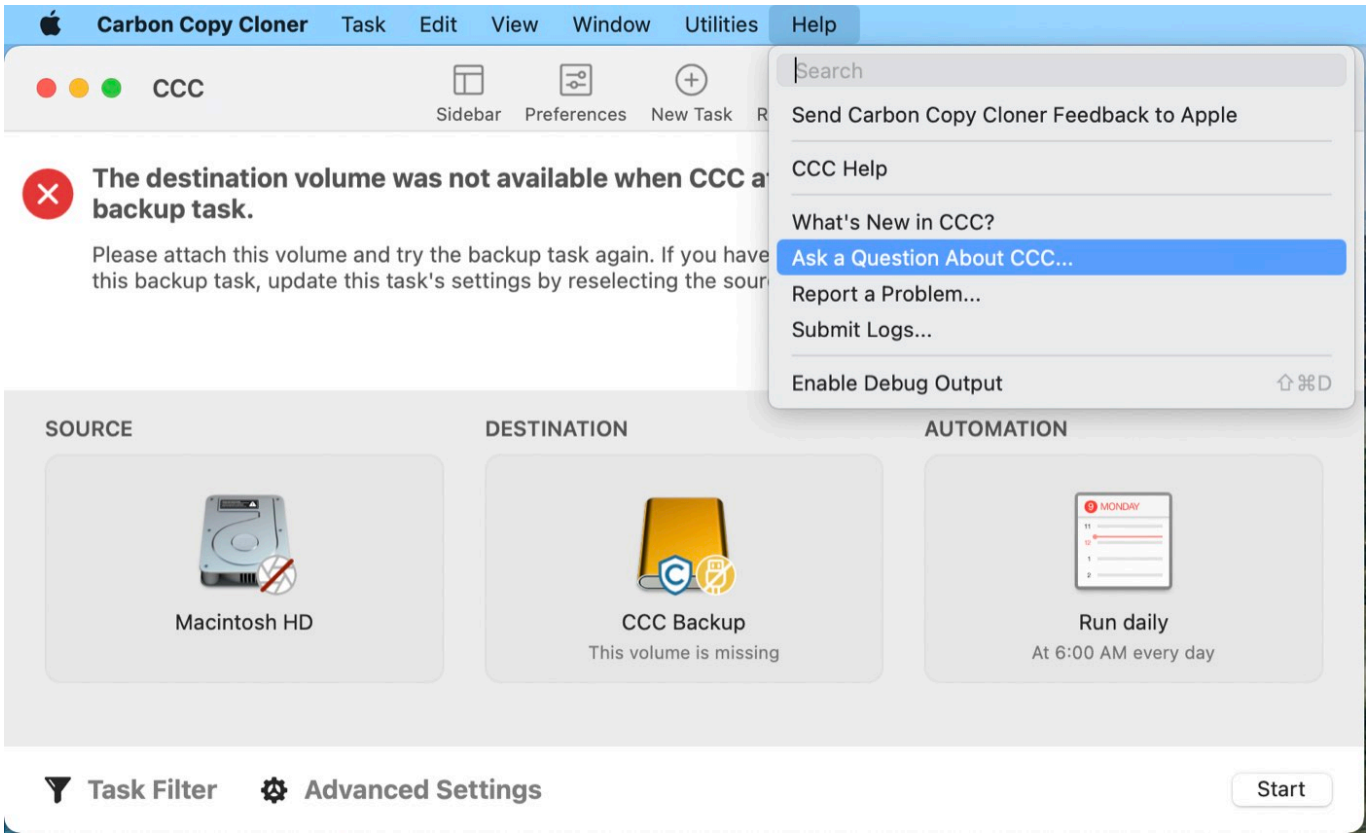
Troubleshooting

How do I get help?

The best way to receive help is by requesting it from within the CCC application. Please note that we provide support in English only and we try to respond within one business day.

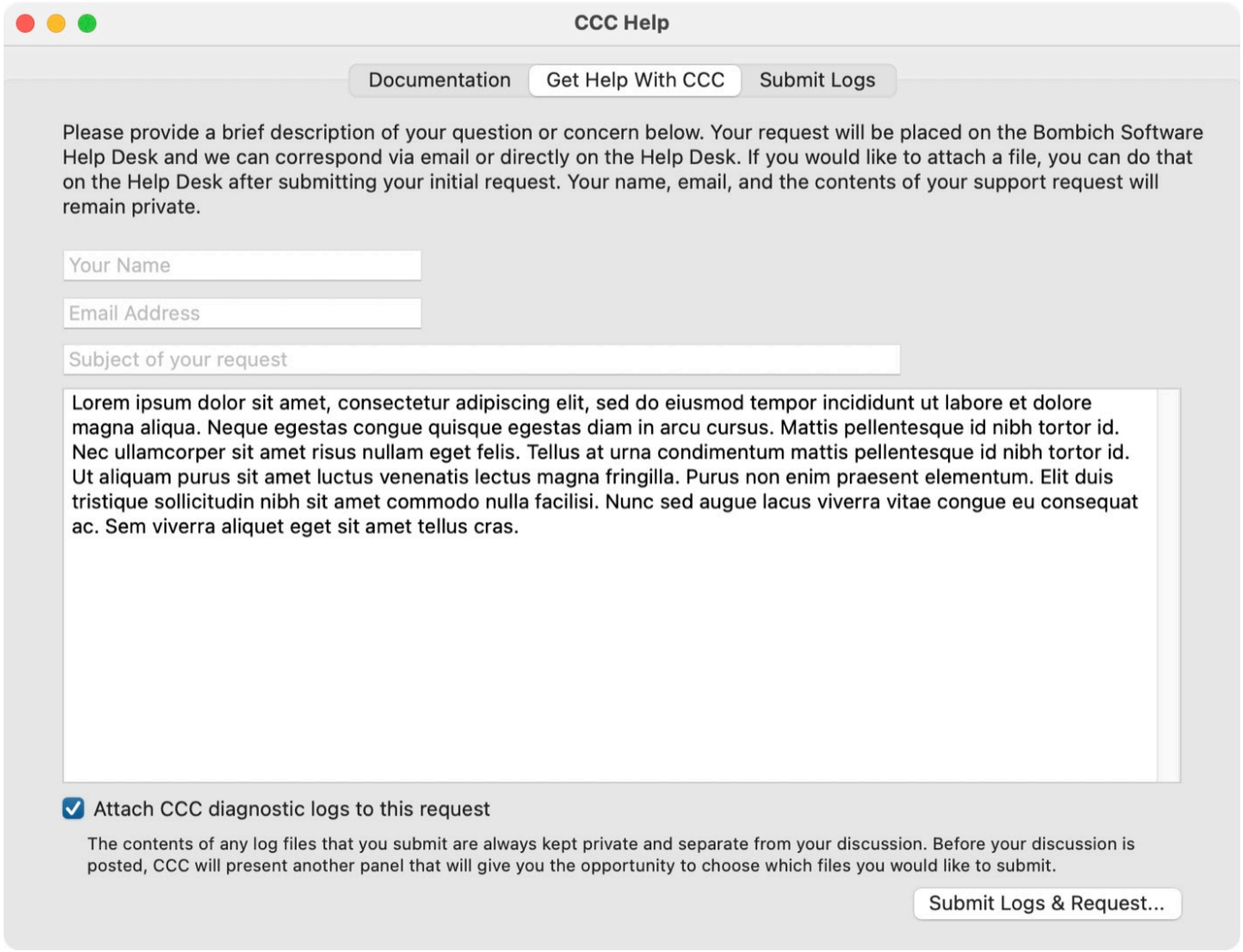
Open Help

If you have a question about CCC or you need help solving a problem, we're here to help you. Choose Ask a **Question About CCC...** from CCC's **Help** menu.



Describe your question

Provide your name, email address, a brief subject, and let us know how we can help you. For the fastest assistance, please include your logs with your help request. We usually get back to folks within one business day from their support request - and often much faster than that.


CCC Help
Documentation
Get Help With CCC
Submit Logs
Please provide a brief description of your question or concern below. Your request will be placed on the Bombich Software Help Desk and we can correspond via email or directly on the Help Desk. If you would like to attach a file, you can do that on the Help Desk after submitting your initial request. Your name, email, and the contents of your support request will remain private.
Your Name
Email Address
Subject of your request
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Neque egestas congue quisque egestas diam in arcu cursus. Mattis pellentesque id nibh tortor id. Nec ullamcorper sit amet risus nullam eget felis. Tellus at urna condimentum mattis pellentesque id nibh tortor id. Ut aliquam purus sit amet luctus venenatis lectus magna fringilla. Purus non enim praesent elementum. Elit duis tristique sollicitudin nibh sit amet commodo nulla facilisi. Nunc sed augue lacus viverra vitae congue eu consequat ac. Sem viverra aliquet eget sit amet tellus cras.
Attach CCC diagnostic logs to this request
The contents of any log files that you submit are always kept private and separate from your discussion. Before your discussion is posted, CCC will present another panel that will give you the opportunity to choose which files you would like to submit.
Submit Logs & Request...

External Boot Troubleshooting

We're happy to help you troubleshoot <https://bombich.com/software/get_help> bootability problems affecting macOS Catalina. Only Apple can make an external device bootable with macOS Big Sur, however, so our support for external boot on Big Sur and later OSes is limited to the suggestions offered below.

No Mac will ever boot from an OS that is older than what it shipped with

Apple has never supported booting a new Mac from an OS that is older than what it shipped with. If you're trying to migrate content to a new Mac, use Migration Assistant for that purpose <https://bombich.com/kb/ccc6/i-want-clone-my-entire-hard-drive-new-hard-drive-or-new-machine> — **do not attempt to restore an older Mac's backup onto a new Mac**.

Related Documentation

- Can I restore my Mac's backup to another computer? <https://bombich.com/kb/ccc6/can-i-back-up-one-computer-and-use-clone-restore-another-computer>
- Apple Kbase #HT204350: Move your content to a new Mac <https://support.apple.com/en-us/HT204350>

External Boot troubleshooting on macOS 11, "Big Sur" and later OSes

Starting in macOS Big Sur, the system now resides on a "Signed System Volume" <https://developer.apple.com/news/?id=3xpv8r2m>. This volume is cryptographically sealed, and that seal can only be applied by Apple; ordinary copies of the System volume are non-bootable without Apple's seal. When you configure a CCC backup task using the Legacy Bootable Copy Assistant, CCC will automatically use Apple's proprietary APFS replication utility (ASR) to make a block-for-block exact copy of the source. If that does not produce a bootable volume, and if you have exhausted the Firmware Discoverability Troubleshooting steps below, then we recommend that you install macOS onto the backup <https://bombich.com/kb/ccc6/cloning-macos-system-volumes-apple-software-restore>. If that does not produce a bootable device, then the device is not suitable for functioning as a bootable device on your Mac.

Our support for system copying and bootability on Big Sur and later OSes is limited to the suggestions noted above.

Related Documentation

- Troubleshooting APFS Replication <https://bombich.com/kb/ccc6/troubleshooting-apfs-replication>
- Some Big Sur startup volumes don’t appear in the Startup Disk Preference Pane <https://bombich.com/kb/ccc6/help-my-clone-wont-boot#ssv>
- Creating legacy bootable copies of macOS Big Sur <https://bombich.com/kb/ccc6/cloning-macos-system-volumes-apple-software-restore>
- Installing macOS onto a CCC backup <https://bombich.com/kb/ccc6/cloning-macos-system-volumes-apple-software-restore#install_macos>

Sometimes the Mac's firmware cannot detect your backup device

When you boot your Mac while holding down the Option key (Intel Macs) or the Power button (Apple Silicon Macs), the Mac Startup Manager <https://support.apple.com/en-gb/HT202796#startupmanager> will display a list of available startup devices. Using only device drivers that are stored on your Mac's firmware chip, the firmware will scan all of your SATA, PCI, USB, and Thunderbolt busses for hard drive devices, then read those hard drive volume headers to determine if a macOS system is available on each volume. Ordinarily, a CCC bootable backup volume will appear in this list, but occasionally your Mac's firmware may have difficulty discovering the hardware that hosts your backup.

If CCC's Task Plan didn't report any configuration concerns for your backup volume and you are having trouble booting from it, try the Firmware Discoverability Troubleshooting steps below.

Some Macs may not boot from USB devices larger than 2TB

Some Macs, especially those produced prior to 2014, cannot "see" the content of a volume that lies past the 2TB mark on the disk at boot. If you have an older Mac and you're having trouble booting it from a USB device that is larger than 2TB, try creating a 2TB partition at the beginning of the disk and make your backup to that partition. Note that when partitioning a disk in Disk Utility, the top of the pie chart is the beginning of the disk; in other words, the first partition starts at "noon".

Possible workaround: If your external device has a Firewire interface, and your Mac is running an OS that is older than Catalina, then you can attach the device to your Mac via Firewire and boot from any size of volume. If your Mac does not have a Firewire port, but has Thunderbolt ports, you can use the Apple Thunderbolt to Firewire adapter.

2012-vintage Macs can't boot macOS Catalina from an encrypted USB device

We have received several reports that the 2012 Mac mini and the 2012 MacBook Pro can initially boot from a non-encrypted external USB device, but then will fail to boot from that device when FileVault is enabled on the external device. This issue is not specific to CCC, we have confirmation that this occurs when installing Catalina directly onto an external device as well. This problem does not appear to be specific to any particular enclosure, rather it appears to be specific to the 2012 models of Mac mini and MacBook Pro. If you require an encrypted backup, we recommend that you erase your destination as APFS or HFS+ encrypted, then create a data-only backup to that volume <https://bombich.com/kb/ccc6/frequently-asked-questions-about-ccc-and-macos-catalina#encrypted_non_bootable>.

We reported this issue to Apple (FB7433465) in November 2019 and we are currently awaiting a response.

Apple no longer supports booting Macs from RAID devices

Starting in macOS Mojave, Apple no longer supports installing macOS onto a RAID device <https://support.apple.com/en-us/HT201316>. Some people have found that backing up Mojave to a RAID array can work, however this is not a supported configuration, and does not appear to be a viable option for macOS Catalina.

Enable "External Boot" on T2 Macs (this is not required on M1 Macs)

If you are attempting to boot a Mac with an Apple T2 controller chip <https://support.apple.com/en-us/HT208862> (e.g. a 2018 MacBook Pro or an iMac Pro) from your CCC bootable backup, be sure to change your Mac's **External Boot** policy to allow booting from an external hard drive. Apple describes the procedure in this Apple Kbase article <https://support.apple.com/en-us/HT208198>, but the steps are:

1. Restart your Mac while holding down Command(⌘) and the "R" keys.
2. Choose **Startup Security Utility** from the Utilities menu in the menu bar (see this screenshot for clarification <https://bombich.com/images/help-clone-wont-boot/startup_security_utility.jpg>)
3. Click the **Enter macOS Password** button, then choose an administrator account and enter its password.
4. Change the **External Boot** (or "Allowed Boot Media") setting to **Allow booting from external media**
5. Restart

Please do not, however, change the **Secure Boot** setting for the purpose of booting from a backup. "Full Security" is the default setting, and that setting is compatible with booting a T2 from its own backup. Do note the exception to this when attempting to boot one of these Macs from a different Mac's backup <https://bombich.com/kb/ccc6/can-i-back-up-one-computer-and-use-clone-restore-another-computer#secure_boot>.

Note for users with non-QWERTY keyboards: When you initially boot into Recovery mode, you'll be prompted to select a language. Be sure to select a language that matches your keyboard, otherwise the Startup Security Utility may not accept your password.

Can I leave this setting unchanged and change it only in the future when I actually need to boot from my backup?

Generally no. Changing settings in the Startup Security Utility requires a functional user account on the internal disk of your Mac. If your Mac's startup disk were to fail, it would be impossible to change the startup security settings. Because the primary purpose of a bootable backup is to function as a rescue disk in the event that your Mac's startup disk fails or otherwise becomes non-functional, we recommend leaving your Mac configured to allow booting from external devices.

For additional startup security, you can apply a firmware password. When a firmware password is applied, your Mac will require a password to load the Startup Manager on startup.

Apple Kbase HT204455: How to set a firmware password on your Mac <https://support.apple.com/en-us/HT204455>

Make the Startup Manager load additional drivers

Some third-party external devices use Option ROM firmware <https://en.wikipedia.org/wiki/Option_ROM>. Macs with "up-to-date software" <https://support.apple.com/en-us/HT202796#optionROM> don’t automatically load Option ROM firmware, so your Mac won't see devices that have Option ROM firmware until you load that firmware. **Press Option-Shift-Command-Period at the Startup Manager window to load Option ROM firmware from any currently-attached hard drive enclosures**. Here's a partial list of devices we've received reports of that use Option ROM firmware:

- LaCie 5Big Thunderbolt <http://www.lacie.com/professional/big/5big-thunderbolt-2/>

Rule out generally incompatible configurations and filesystem anomalies

If you are using an external hard drive enclosure or adapter, see whether your enclosure is listed at the bottom of this page as an enclosure that we've seen problems with in the past. Also, for good measure, use Disk Utility's "First Aid" utility to verify and repair any filesystem problems that may be present on the destination volume.

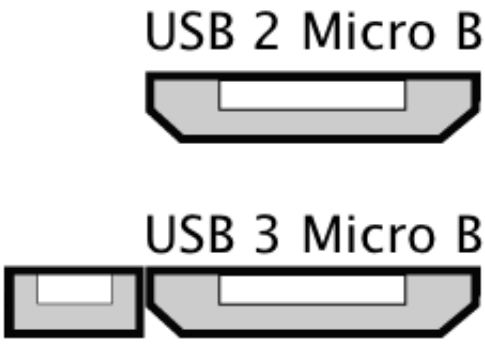
Troubleshoot discoverability issues in the Mac's Startup Manager

1. Turn off your Mac
2. Detach all peripherals from your Mac except for the keyboard and mouse (including any secondary displays)
3. Attach the backup disk directly to a USB or Thunderbolt port on your Mac (no hubs, no adapters, no monitor ports, no daisy chaining, no third-party USB cards)
4. Start up your Mac while holding down the Option key (Intel Macs) or the Power button (Apple Silicon Macs). [Note: A wired keyboard may be required for this step]
5. Wait about 30 seconds to see if the backup volume appears. **If your backup volume appears at this step and the boot process proceeds past the Apple logo,** skip to the section below**.**
6. Press Option-Shift-Command-Period at the Startup Manager window to load any Option ROM firmware that is present and required for an external hard drive enclosure.
7. Detach, then reattach the backup volume's USB or Thunderbolt cable from/to your Mac and wait up to another 30 seconds. If your backup volume appears, select it and proceed with the startup process.
8. If the backup volume still does not appear as an option, shut down your Mac completely. Then start it up holding down the Option key (Intel Macs) or the Power button (Apple Silicon Macs), waiting another 30 seconds for the volume to appear.
9. Repeat the steps above, but using another interface (e.g. USB if you tried Thunderbolt, Thunderbolt if you already tried USB) and see if the volume appears.
10. If the hard drive enclosure is bus powered, try plugging in its DC power supply before starting up your Mac. Bus powered enclosures often take a bit longer to spin up or simply don't make themselves available that early in the boot process.

Additional USB device troubleshooting

Here are a couple additional steps you can perform to try to get your Mac to "see" your USB device early in the startup process.

1. Reboot your Mac while holding down the Option key (Intel Macs) or the Power button (Apple Silicon Macs).
2. If your Mac has multiple USB ports, try attaching your destination disk to each port (and be sure to use the ports on your Mac directly — not a hub, keyboard, or display)
3. If you are using a USB 3.0 enclosure, try using a USB 2.0 cable (yes, it **will** work!). USB 3.0 devices are backwards compatible to USB 2.0, but they don't always play well with the older USB device drivers that are embedded within your Mac's firmware. Using a USB 2.0 cable elicits different behavior from the enclosure that often works around compatibility problems that are only exposed when using the Mac's firmware USB drivers. Here are some pictures that show what the ends of USB 2.0 and USB 3.0 cables look like:



Reset the Mac's Parameter RAM

Lastly, try resetting your Mac's parameter RAM. PRAM maintains settings related to starting up your Mac, and it's possible that invalid settings are interfering with your Mac's discovery of the external enclosure. To reset your PRAM on an Intel Mac:

1. Hold down Command+Option+P+R on startup
2. Hold down those keys until you hear the second startup chime.
3. Release all but the Option key after you hear the second startup chime.

Definitively rule out an incompatible enclosure

If the volume still won't boot, it may be impossible for your firmware to detect your enclosure (despite that macOS, once booted and having access to far more device drivers, can see the enclosure just fine). The Golden Litmus Test for bootability would be to install macOS directly onto the volume <https://bombich.com/kb/ccc6/cloning-macos-system-volumes-apple-software-restore>. **If the macOS Installer fails to make the disk bootable, then your external device will not function as a startup device.**

The backup volume starts to boot the Mac, but fails to get to the Finder, or the Mac reboots and boots from the internal disk

If your backup volume showed up in the Startup Manager, and you selected it and proceeded with the startup process, but...

Your Mac doesn't display the Apple logo (e.g. you get a blank, black or gray screen after selecting the backup volume): your Mac is having trouble finding the "booter" file on this volume. This can occur due to hard drive enclosure interference, due to filesystem corruption on the backup volume, or due to the volume being improperly "blessed" (blessing a volume stores certain information about the startup files in the volume's header, and your Mac uses that information to start the boot process).

1. Erase the backup disk <https://bombich.com/kb/ccc6/preparing-your-backup-disk-backup-os-x>, then back up your startup disk to the destination again.
2. Try booting from the backup volume again.

If your Mac still fails to boot from the selected volume, try installing macOS onto the volume to verify its suitability as a startup device.

The Apple logo and a progress indicator appears, but the startup process never completes (and perhaps the Mac reboots from the internal disk): There may be an extension conflict at play, or a compatibility issue specific to the enclosure.

1. Choose "About This Mac" from the Apple menu to verify that your Mac really did not boot from the volume that you selected
2. Detach all unnecessary peripherals, including secondary displays.
3. Reboot the Mac and hold down Option (Intel Macs) or the Power button (Apple Silicon Macs) to load the Startup Manager
4. Select the backup disk
5. As you click the button to proceed with the startup process, hold down the Shift key to boot in Safe Boot mode

If your Mac successfully boots from the selected volume, open the Terminal application and paste in the following command:

sudo kextcache --clear-staging
sudo kextcache -system-prelinked-kernel
sudo kextcache -system-caches

Press the Return key after pasting in each line and authenticate when prompted. Then try again to boot from the same volume without Safe Boot mode. If your Mac still fails to boot from the selected volume, try installing macOS onto the volume to verify its suitability as a startup device.

Related documentation:

- Some third-party storage drivers may cause hardware misbehavior <https://bombich.com/kb/ccc6/some-third-party-storage-drivers-may-cause-hardware-misbehavior>

Performance expectations while the Mac is booted from the backup

The performance of your Mac while booted from the backup depends almost entirely on the performance of the hardware, and more specifically, the performance of the *filesystem* on that hardware. If your backup disk is an SSD, you can expect very good performance — comparable to the performance that you get when you boot your Mac from its internal SSD. If your backup disk is a rotational HDD, then performance will vary from adequate to very poor, depending on the format of the backup volume, the operating system version, and specific performance characteristics of your backup disk. In particular, Apple's APFS filesystem performs relatively poorly on rotational HDD devices <https://bombich.com/blog/2019/09/12/analysis-apfs-enumeration-performance-on-rotational-hard-drives>, and that performance is considerably worse for 5400RPM disks and disks that use Shingled Magnetic Recording <https://bombich.com/kb/ccc6/choosing-backup-drive#smr>. You may find the performance of one of these slower HDDs to be unusable for the purpose of booting your Mac from the backup.

Related documentation

- Choosing a backup drive: Devices that we recommend <https://bombich.com/kb/ccc6/choosing-backup-drive#recommendations>
- Using Migration Assistant to restore your startup disk from a CCC backup <https://bombich.com/kb/ccc6/how-restore-from-your-backup#install_then_migrate>

If you see the universal "No access" symbol after selecting your startup disk

This indicates that the macOS cannot load the the startup files, or that it cannot mount the startup disk:

The most frequent cause for this is an attempt to boot your Mac from an incompatible (i.e. too old) operating system. Occasionally this also occurs due to a device driver conflict with the enclosure you are trying to boot from, or due to a firmware compatibility problem between the Mac and the enclosure. We occasionally see this when trying to boot pre-2013 Macs from a USB 3.0 enclosure. We also see this more frequently on Yosemite when a critical kernel extension's code signature is invalid. This can happen, for example, when using something like TRIM Enabler <https://cindori.com/trimenabler> to modify macOS Storage drivers.

- **Apple does not support booting a Mac via a FireWire-attached device**. If your device is attached via FireWire and has a USB port as well, try attaching the device to your Mac via USB.
- Try booting into Safe Boot mode (hold down the Option key (Intel Macs) or the Power button (Apple Silicon Macs) on startup, then hold down the Shift key as you select the backup volume as the startup disk).
- Try installing macOS directly onto the backup volume while your Mac is booted in Recovery mode <https://support.apple.com/en-us/HT204904>. If the installation also fails, there is a compatibility issue between the enclosure and your Mac that makes it unsuitable as a startup device.
- If you used a third-party utility to modify macOS software (e.g. TRIM Enabler), undo that modification, then run the backup task again.

If your Mac never progresses past the progress indicator (below the Apple logo) or stalls at the Apple logo+progress bar while booting from the backup volume, there is probably a problem with some of the system files that are called early in the startup process, or macOS is unable to load the correct drivers for your external enclosure at that stage of the startup process. **Again, try installing macOS directly onto the backup volume while booted in Recovery mode <https://support.apple.com/en-us/HT204904> to rule out a compatibility problem with the enclosure.**

"unapproved caller. security agent may only be invoked by Apple software" message appears on startup

This message generally appears when the volume you are trying to boot from is full or nearly full. You can remove items from the _CCC SafetyNet folder (or the entire folder itself), then empty the Trash, or remove snapshots from that volume to free up some space before trying to boot from that volume again. macOS should be given at least 2GB, preferably 5-10GB of free space to accommodate the creation of cache and virtual memory files on startup.

Related documentation:

- Automated maintenance of the CCC SafetyNet folder <https://bombich.com/kb/ccc6/automated-maintenance-ccc-safetynet-folder>
- Snapshots and space concerns; Deleting snapshots <https://bombich.com/kb/ccc6/leveraging-snapshots-on-apfs-volumes#space>

The Mac boots from the backup, but login fails

We have received a handful of reports that login is denied despite providing the correct password, and despite that the user accounts database and password storage is copied correctly to the backup volume. You can correct the problem while booted from your production startup volume:

1. Open the Users & Groups Preference Pane in the System Preferences application
2. Click the "Change Password" button
3. Re-enter your current password (in all three fields – reusing the current password is fine) and add a hint as well. The hint doesn't have to be anything meaningful, just something you can verify later, like "meatball".
4. Run the backup task again
5. Try again to boot from the backup disk and log in

"You can't change the startup disk to the selected disk. The bless tool was unable to set the current boot disk."

Occasionally the Startup Disk Preference Pane will issue this error without any useful context. More often than not, the inability of the Startup Disk Preference Pane to change the startup disk is not actually an indication that the volume will not be bootable, rather it simply means that the Startup Disk Preference Pane cannot **change** the startup disk selection to that particular volume. Use the Startup Manager (boot your Mac while holding down the Option key [Intel Macs] or the Power key [Apple Silicon Macs]) to select an alternate boot disk instead.

System Integrity Protection prohibits modifications to the current startup disk's Preboot helper partition

If you add an APFS volume to your current startup disk's APFS container, the macOS bless facility will be unable to update the container's Preboot volume to include support files for the second partition. System Integrity Protection will also prevent the preservation of system files on **any** other volume that resides in the same APFS container as the current startup disk. As such, CCC will exclude system files when you configure a task with a destination that is in the APFS container of the current startup disk.

Alternatively, you can create a separate partition on your startup disk (rather than adding a second volume to the same parent APFS container) and make your backup to that separate partition.

1. Open Disk Utility
2. Choose "Show all devices" from the View menu
3. Click on the top-most parent device for your Macintosh HD volume
4. Click the "Partition" button in the toolbar
5. When Disk Utility tries to discourage you from doing this, by preselecting "Add Volume" click the "Partition" button
6. Click the "+" button to add a second APFS-formatted partition on the startup disk

Configurations with which we have seen some problems

- USB thumb drives are inherently slow devices, we don't recommend using these for making a bootable backup.
- We have received many reports of inconsistent bootability with SanDisk flash drives (Cruzer, Ultra) and SD cards on macOS High Sierra. These devices are often slow anyway, so we don't recommend using these specifically for a bootable backup. **Catalina+:** The same issue that causes bootability problems with these devices on pre-Catalina OSes now causes errors that

prevent even a basic backup of the System and Data volumes. We recommend using these devices only for creating a non-bootable backup of your Catalina Data volume <https://bombich.com/kb/ccc6/frequently-asked-questions-about-ccc-and-macos-catalina#encrypted_non_bootable>.

- Flash-based memory like that used in SD cards and thumb drives also has limited write/erase cycles that are much lower than that of a traditional SSD or mechanical hard drive making them not appropriate as a primary backup device.
- Western Digital enclosures have an unreliable track record at serving as startup devices. Incompatibilities include:
    - A user reported that the **WD My Passport Studio** 2TB cannot boot a T2 MacBook Pro (this report was confirmed by an unsuccessful attempt to install macOS Mojave onto the device).
    - We have received many reports that **Western Digital My Passport** hard drive enclosures fail to function as a startup disk with macOS Catalina (again, confirmed by a failure to install macOS onto the device or to boot from that device after installing macOS via the Installer).
    - We have received a report that the **Western Digital EasyStore** fails to function as a startup disk with macOS Catalina (same confirmation as above).
    - Exception: The only Western Digital device that we have seen reliable results with is the WD MyPassport SSD.
- Some Macs have trouble booting from USB 3.0 enclosures
- We have received a report that the Nexstar 6G <http://www.vantecusa.com/products_detail.php?p_id=25&p_name=NexStar+6G&pc_id=2&pc_name=3.5%22+Enclosure&pt_id=1&pt_name=Hard+Drive+Enclosures> USB 3.0 hard drive enclosure is not bootable due to a discoverability issue. The Nexstar TX from Vantec was bootable (using the same internal hard drive). We have received another report, however, that the Nexstar 6G **was** bootable, so there may be Mac-specific firmware issues at play regarding this enclosure.
- We have received several reports that multiple-bay hard drive enclosures provide inconsistent boot results. In each case, the Mac can boot from the bootable backup as long as the hard drive is placed in the first bay of the enclosure. When placed in other bays, the bootable volume is not discoverable by the Mac's firmware. If you have trouble booting from a disk in a multi-bay enclosure, try swapping the drive positions within the enclosure. Here is a list of the affected enclosures that we have had reports on so far:
    - Mediasonic HF2-SU3S2
    - CineRAID Home CR-H212 USB 3.0 Bus-Powered Dual Drive RAID/JBOD Portable Enclosure <http://www.cineraid.com/products/home_h212.htm>
    - StarTech S3520WU33ER USB 3.0 Bus-Powered Dual Drive RAID/JBOD Portable Enclosure <https://www.startech.com/HDD/Enclosures/~S252BU33R>
    - MyDigitalSSD BOOST <http://mydigitalssd.com/mobile-ssd.php#boost-usb-3.1>
    - OWC Mercury Elite Pro Dual <https://eshop.macsales.com/shop/Thunderbolt/External-Drive/OWC/Elite-Dual-RAID>
- We have received a report that the Orico 3588US3 USB3 enclosure is not bootable due to a discoverability issue.
- We have received a report that agreeing to Webroot SecureAnywhere's request to "remove threats" during a backup task can produce a non-bootable backup.
- Some users report problems booting pre-2013 Macs from USB 3.0 devices that use the "ASMedia 1051E" chipset (e.g. this OWC Mercury On-The-Go <https://eshop.macsales.com/item/Other%20World%20Computing/MOTGS3U3/> enclosure). A firmware compatibility issue was introduced by a 2015 firmware update to these Macs that prevents them from booting from a USB 3 device with that older chipset.
- Some users have reported discoverability issues with ASM1352R enclosures from ASMedia.
- One user reported that the MyDigitalSSD Boost enclosure is not bootable.
- We have received a report that devices attached to the AmazonBasics 10 Port USB 3.0 Hub are not available in the Option-key Startup Manager. Attach your USB devices directly to a USB port on your Mac if/when you need to boot from your CCC bootable backup.

- Sonnet Customer Support has confirmed that any device attached to the Sonnet Allegro Pro USB 3 PCI card cannot function as a startup disk.
- Some users have reported bootability issues with the Inateck USB 3.0 2.5" hard drive enclosure with a model number of "FEU3NS-1".
- We have received a report that the **Sabrent Rocket Pro 2TB NVMe USB 3.1 External Aluminum SSD** is not bootable.
- We have received a report that the 6-bay ThunderBay 6 from Other World Computing is not bootable on macOS Catalina. macOS proceeds ~75% of the way through the startup process, then stalls. The exact same disk placed into a different enclosure boots fine. In contrast, we have received a report that a non-RAID volume in a ThunderBay 8 enclosure from OWC **was** bootable on macOS Monterey. These are complex devices, so "your mileage may vary".
- We have received at least two reports that the **LaCie d2** is not bootable.
- We have received a report that the **VisionTek 1 GB Thunderbolt3 SSD** is not bootable on macOS Big Sur (test case was a 2019 MacBook Pro, confirmed after the Big Sur Installer completed and the device failed to boot). In this particular case the device had been bootable on Catalina.
- We have received a report that the **GMM M.2 NVMe enclosure** is not bootable (test case was a MacPro running Monterey, confirmed by booting the same storage in another enclosure).
- We have received a report that the the Samsung SSD drivers (i.e. those provided by Samsung) cause macOS to either stall or kernel panic when attempting to boot from a Samsung T7 SSD. We recommend that you avoid installing the Samsung storage drivers, they are redundant to the built-in macOS storage drivers.
- We have received several reports that various external devices fail to boot macOS. The common thread in these reports is that the macOS Installer hangs with "one minute remaining", and never completes the installation procedure (and users are trying the installer as a last resort). As noted above, if the macOS Installer can't produce a bootable installation of macOS on your external device, then that device is simply not going to be capable of booting your Mac. We recommend using that storage for a Standard Backup <https://bombich.com/kb/ccc6/cloning-macos-system-volumes-apple-software-restore#standard_backups> instead.

The 2019 iMac errantly boots from USB-C devices

We've been tracking an emerging issue specific to the 2019 iMac and external disks attached via USB-C (same port as Thunderbolt) in which the iMac will boot from the external device instead of the internal hard drive despite a preference to boot from the internal disk. We believe this is a problem in the firmware of this particular iMac — it's the firmware that decides which device to use as the startup disk, and it appears to be ignoring the user's preference (e.g. the internal startup disk). In one case a user performed a simple and definitive test — he installed macOS Catalina onto a freshly-erased, external device, and as long as that device was attached via USB-C, the Mac would only boot from that device, and regardless of the selected startup disk preference. This behavior is not specific to CCC nor to any particular enclosure, rather it seems to be a firmware bug.

Workaround: If your external hard drive enclosure came with a USB-C to USB Type A cable <https://static.bhphoto.com/images/images2000x2000/1510315603_1335192.jpg>, then you could use that to connect the disk to a USB type A port on your iMac to avoid this issue. Or you could just detach the disk from your Mac prior to rebooting.

Related Documentation

- Can I restore my Mac's backup to another computer? <https://bombich.com/kb/ccc6/can-i-back-up-one-computer-and-use-clone-restore-another-computer>
- Apple Kbase: About the screens you see when your Mac starts up

<https://support.apple.com/en-us/HT204156>

macOS Monterey Known Issues

Apple published macOS Monterey in October 2021. CCC 6.0.4 (and later), published contemporaneously with Monterey, is fully compatible with macOS Monterey. We cite known problems that Apple introduced in the new OS below.

Some backup volumes don't appear in the Finder sidebar

If you created a bootable copy of Catalina or Big Sur in the past, and then proceed with CCC backups to that volume on Monterey without specifically using the Legacy Bootable Copy Assistant <https://bombich.com/kb/ccc6/cloning-macos-system-volumes-apple-software-restore>, CCC will remove the incompatible System volume from the destination. The remaining Data volume appears just fine on the Finder Desktop, and also in the volume list when you select "Computer" from the Finder's Go menu. The Finder sidebar, however, will not show these volumes, regardless of your Finder preferences to show external volumes in the sidebar, and regardless of any attempts to drag the volume explicitly into the sidebar.

We have reported this issue to Apple (FB9739492) and we are currently awaiting a response.

Workaround: Choose "Computer" from the Finder's Go menu to see your destination volume in the Finder.

Apple's SMB filesystem client causes system stalls, random application crashes, and may lead to kernel panics

Update (macOS 12.3): This issue appears to be effectively resolved in macOS 12.3.

We have received several reports from Apple Silicon Mac users of unruly macOS behavior that occurs while copying files to an SMB-mounted NAS volume. The behavior includes the following:

- Random application crashes
- Prompts to grant various macOS system services access to the login keychain (i.e. because the service that retains the unlocked keychain reference crashed, thus locking the keychain)
- Laggy mouse behavior
- System stalls that eventually end with a reboot and kernel panic report

We were able to reproduce this behavior using a simple shell script that creates files and folders on SMB-mounted NAS volumes (and also with Finder copies). The underlying problem appears to be a memory leak in the macOS kernel or one of the kernel extensions. Specifically, the "kext.kalloc.32768" memory zone is expanded until it can no longer be expanded ("zone_map_exhaustion" occurs), at which point the memoryd system process starts to terminate idle processes. This problem is limited to Apple Silicon Macs and SMB volumes.

We reported this issue to Apple in January 2022 (FB9857268). Apple indicated that they had made significant progress on this issue in the 12.3 update. We're still able to reproduce high memory pressure, however we're no longer seeing the complete memory zone exhaustion that was leading to kernel panics. Likewise, we haven't received any additional reports of this issue from any 12.3 users.

Workaround: We have confirmed that using AFP rather than SMB consistently avoids these behaviors (in cases where using AFP is an option):

1. Eject the NAS volume if it's currently mounted
2. Open CCC and select the applicable backup task
3. Click on the Source or Destination selector (whichever is applicable for your particular task)
4. Hold down the Option key and choose "Switch to AFP" (provide the credentials for the NAS volume again if prompted)
5. Save and run the task

While we recommend using AFP whenever it is an available option, it's important to note that AFP is a deprecated protocol and that some NAS vendors have started to drop support for it (e.g. Western Digital MyCloud <https://support-en.wd.com/app/answers/detail/a_id/24148>). If you are not happy with the performance and reliability of Apple's SMB filesystem client on the latest version of maCOS, please share that feedback with Apple <https://www.apple.com/feedback/macos.html>, and please feel free to include our FB9857268 bug report number in that feedback.

CCC will not update the System volume on a Legacy bootable copy of the startup disk (Big Sur and later)

Starting in macOS Big Sur, the system now resides on a cryptographically sealed "Signed System Volume" <https://developer.apple.com/news/?id=3xpv8r2m>. That volume can only be copied using Apple's proprietary APFS replication utility ("ASR"). Right now, ASR will only copy whole volume groups (System and Data); we can't choose to copy just the System volume. As a result, every time an OS update is applied to the source, you would have to erase the whole destination volume (including any existing snapshots on that volume) just to update the system on the destination. We made a feature request to Apple in September 2019 (FB7328230) to allow ASR to clone just the System volume. We do not anticipate that Apple will implement our requested functionality.

To avoid deleting your snapshots and the rest of your backup, CCC will not update the System volume on the destination when System updates are applied to the source.

Our recommendation: We recommend erasing the destination only when you have an *immediate* need for a bootable copy of the system (e.g. if you're migrating to a different disk, or creating a copy of the system for testing purposes). A Standard Backup is simpler and more appropriate for establishing a robust, long-term backup strategy.

Workaround: Any time you want to make the OS on the destination identical to the source, simply click on the Destination selector and choose **Legacy Bootable Backup Assistant**... to configure CCC to re-erase and reclone the entire volume.

Finder will not show, nor allow you to set custom icons on other Catalina, Big Sur or Monterey startup volumes

Finder will show and allow you to customize the volume icon for your current startup disk, but not for other Catalina+ startup volumes that your Mac is not currently booted from. This problem is not specific to CCC backups, but we see this frequently because CCC can create copies of macOS System volumes. This problem is the result of a design flaw in the implementation of custom icons in an APFS volume group. Up to macOS Catalina, the custom volume icon is stored in a file at the root of the startup disk named ".VolumeIcon.icns". To keep the System volume read-only, yet allow the apparent modification of this icon file, Apple chose to create a symbolic link at the root of the startup disk that points to System/Volumes/Data/.VolumeIcon.icns. For the current startup disk, this path resolves correctly because the Data member of the volume group is mounted at /System/Volumes/Data. That's not the case for external volumes, those Data volumes are mounted at /Volumes/CCC Backup - Data (for example). As a result, the symbolic link to .VolumeIcon.icns is unresolvable for any volume that is not the current startup disk.

We reported this issue to Apple in May 2020 (FB7697349) and we are still awaiting a response.

Alternative: We recommend creating "Standard" backups instead of creating a legacy bootable backup. Finder will issue no challenges to customizing the icon of a volume with a Standard Backup.

Other Catalina+ startup disks can't be renamed in the Finder

Finder will let you rename the current startup disk, but you won't be able to rename any other startup disks that have an installation of Catalina, Big Sur or Monterey because the System volume is mounted read-only.

We reported this issue to Apple in November 2020 (FB8912480) and we are still awaiting a response.

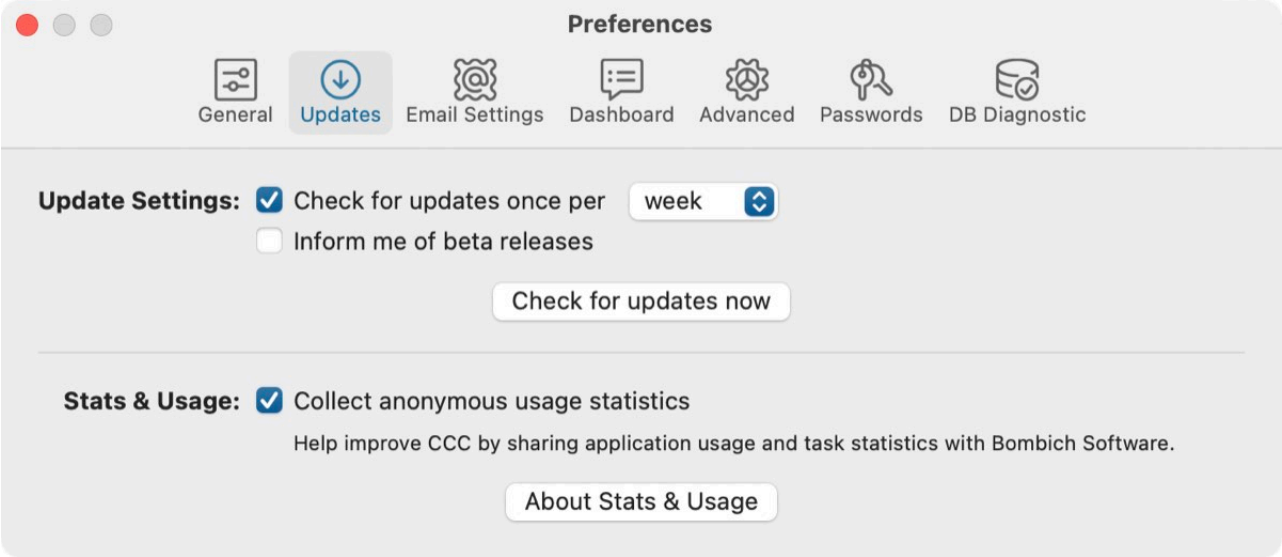
Solution: Unmount and remount the volume in Disk Utility, then right-click on the volume in Disk Utility's sidebar and choose the option to rename the volume.

Keeping CCC up to date

Open Settings

Click the **Settings** button in CCC's toolbar, or select **Settings** from the **Carbon Copy Cloner** menu

Select Updates



You can immediately check for updates by clicking on **Check for updates now**.

By default, CCC will automatically check for updates once per **week**. You can change this preference to **day** or **month**. To disable automatic update checking, uncheck the box next to **Check for updates once per...**.

By default, CCC will not inform you of beta releases. Occasionally, beta updates are provided to confirm that software changes have resolved a particular problem. In general, beta updates are only issued when a user has discovered a problem that the software developer can reproduce. Therefore, you should only apply beta updates when instructed to do so by Bombich Software.

Do not use third-party update mechanisms

We have received numerous reports of poor update experiences when users use third-party update services, such as MacUpdate Desktop or CNET's Installer. In some cases, the third-party update services install **other promotional software** alongside the update, or completely mangle the update such that CCC is unusable. Please do not use these services to apply updates to CCC; use CCC's built-in software update mechanism.

macOS Big Sur Known Issues

Apple published macOS Big Sur in November 2020. CCC 5.1.22 (and all versions of CCC 6), published in October 2020, is fully compatible with macOS Big Sur. We cite known problems that Apple introduced in the new OS below.

Some Big Sur startup volumes don't appear in the Startup Disk Preference Pane

In the past, the Startup Disk Preference Pane would list all available startup volumes, including CCC backup volumes. When Apple's APFS replication utility is used to copy a Big Sur System volume (something that is now required on macOS Big Sur), however, the cloned volume will not appear in the Startup Disk Preference Pane, despite being perfectly bootable.

We reported this issue to Apple in Nov 2020 (FB8889774). Apple resolved the issue in macOS Monterey.

Workaround: To boot from the backup volume, restart your Mac while holding down the Option key, then select the backup volume in the Startup Manager. When your Mac has completed booting, you can optionally choose to set the startup disk to the current startup volume (i.e. if you want the Mac to always boot from the backup volume).

CCC will not update the System volume on a Big Sur bootable backup

Starting in macOS Big Sur, the system now resides on a cryptographically sealed "Signed System Volume" <https://developer.apple.com/news/?id=3xpv8r2m>. That volume can only be copied using Apple's proprietary APFS replication utility ("ASR"). Right now, ASR will only copy whole volume groups (System and Data); we can't choose to copy just the System volume. As a result, every time an OS update is applied to the source, you would have to erase the whole destination volume (including any existing snapshots on that volume) just to update the system on the destination. We made a feature request to Apple in September 2019 (FB7328230) to allow ASR to clone just the System volume. We do not anticipate that Apple will implement our requested functionality.

To avoid deleting your snapshots and the rest of your backup, CCC will not update the System volume on the destination when System updates are applied to the source.

Our recommendation: We recommend erasing the destination only for the purpose of establishing the *initial* bootable backup. CCC can then use its own file copier to maintain the backup of your user data, applications, and system settings.

Workaround: Any time you want to make the OS on the destination identical to the source, simply click on the Destination selector and choose **Legacy Bootable Backup Assistant**... to configure CCC to re-erase and reclone the entire volume.

Apple Software Restore causes a kernel panic when cloning to the storage in Apple Silicon Macs

In the current shipping version of macOS Big Sur (11.3), Apple's ASR utility can copy **from** the Apple Fabric storage in an Apple Silicon Mac, but it causes a kernel panic when cloning **to** Apple Fabric

storage.

We reported this issue to Apple in March 2021 (FB9055615). Apple resolved the issue in macOS Monterey.

Workaround: If you need to recover your Apple Silicon Mac from a backup, we recommend that you reinstall macOS and then migrate data from your CCC backup using Migration Assistant <https://bombich.com/kb/ccc6/how-restore-from-your-backup#install_then_migrate>.

Finder will not show, nor allow you to set custom icons on other Catalina and Big Sur startup disks

Finder will show and allow you to customize the volume icon for your current startup disk, but not for other Catalina- or Big Sur-bearing startup disks that your Mac is not currently booted from. This problem is not specific to CCC backups, but we see this frequently because CCC can create copies of macOS System volumes. This problem is the result of a design flaw in the implementation of custom icons in an APFS volume group. Up to macOS Catalina, the custom volume icon is stored in a file at the root of the startup disk named ".VolumeIcon.icns". To keep the System volume read-only, yet allow the apparent modification of this icon file, Apple chose to create a symbolic link at the root of the startup disk that points to System/Volumes/Data/.VolumeIcon.icns. For the current startup disk, this path resolves correctly because the Data member of the volume group is mounted at /System/Volumes/Data. That's not the case for external volumes, those Data volumes are mounted at /Volumes/CCC Backup - Data (for example). As a result, the symbolic link to .VolumeIcon.icns is unresolvable for any volume that is not the current startup disk.

We have reported this issue to Apple (FB7697349) and we are currently awaiting a response.

Other Catalina and Big Sur startup disks can't be renamed in the Finder

Finder will let you rename the current startup disk, but you won't be able to rename any other startup disks that have an installation of Catalina or Big Sur because the System volume is mounted read-only.

Solution: Unmount and remount the volume in Disk Utility, then right-click on the volume in Disk Utility's sidebar and choose the option to rename the volume.

We have reported this issue to Apple (FB8912480) and we are currently awaiting a response.

The System volume is not encrypted when FileVault is enabled on a Big Sur startup disk

This is not a bug, this appears to be a deliberate change on macOS Big Sur. When you enable FileVault on a Big Sur startup disk, the System volume member of the APFS volume group is *not encrypted*. Considering that this volume is identical on all Macs, encrypting its contents is not going to prevent someone from knowing what's on it, so the encryption does appear to be unnecessary. There is one undesirable effect of this change, however, regarding an encrypted, bootable backup disk. When you attach the device to your Mac, the System volume is mounted automatically, regardless of whether you unlock the associated Data volume. If you specifically choose to not unlock the Data volume, there are three results that range from confusing to annoying to alarming:

- The volume appears to be mounted in the Finder, despite not wanting to mount it
- None of the data on the volume is accessible because the Data volume isn't mounted, so you

might be led to believe that your data has been lost
- There is no apparent way in the Finder to get the Data volume unlocked and mounted

You can unlock and mount the Data volume in Disk Utility to access the data. If you provided the volume's password to CCC, then you can simply run your CCC backup task and CCC will automatically unlock and mount the Data volume.

We have reported this issue to Apple (FB8918177) and we are currently awaiting a response.

Apple's SMB filesystem client causes system stalls, random application crashes, and may lead to kernel panics

We have received several reports from Apple Silicon Mac users of unruly macOS behavior that occurs while copying files to an SMB-mounted NAS volume. The behavior includes the following:

- Random application crashes
- Prompts to grant various macOS system services access to the login keychain (i.e. because the service that retains the unlocked keychain reference crashed, thus locking the keychain)
- Laggy mouse behavior
- System stalls that eventually end with a reboot and kernel panic report

We were able to reproduce this behavior using a simple shell script that creates files and folders on SMB-mounted NAS volumes (and also with Finder copies). The underlying problem appears to be a memory leak in the macOS kernel or one of the kernel extensions. Specifically, the "kext.kalloc.32768" memory zone is expanded until it can no longer be expanded ("zone_map_exhaustion" occurs), at which point the memoryd system process starts to terminate idle processes. This problem is limited to Apple Silicon Macs and SMB volumes.

We reported this issue to Apple (FB9857268) and we are still awaiting a response.

Workaround: We have confirmed that using AFP rather than SMB consistently avoids these behaviors (in cases where using AFP is an option):

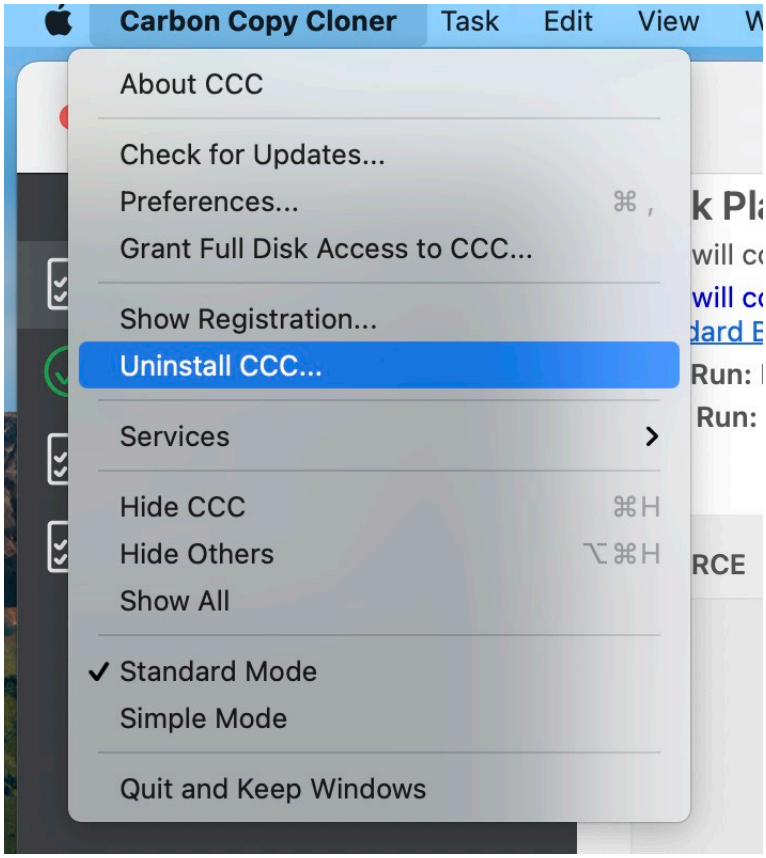
1. Eject the NAS volume if it's currently mounted
2. Open CCC and select the applicable backup task
3. Click on the Source or Destination selector (whichever is applicable for your particular task)
4. Hold down the Option key and choose "Switch to AFP" (provide the credentials for the NAS volume again if prompted)
5. Save and run the task

While we recommend using AFP whenever it is an available option, it's important to note that AFP is a deprecated protocol and that some NAS vendors have started to drop support for it (e.g. Western Digital MyCloud <https://support-en.wd.com/app/answers/detail/a_id/24148>). If you are not happy with the performance and reliability of Apple's SMB filesystem client on the latest version of maCOS, please share that feedback with Apple <https://www.apple.com/feedback/macos.html>, and please feel free to include our FB9857268 bug report number in that feedback.

Uninstalling CCC

Uninstalling from within CCC

To Uninstall CCC, press and hold down the Option key and choose **Uninstall CCC...** from the Carbon Copy Cloner menu. When you uninstall CCC, CCC's privileged helper tool and all saved tasks will be immediately deleted. The CCC application file and CCC's preferences will then be moved to the Trash.



Remove snapshots before uninstalling CCC

If you're permanently removing CCC from your Mac, you should remove any CCC-created snapshots first. Select each volume in CCC's sidebar to see if there are any snapshots present on that volume. If you see any snapshots listed in the Snapshots table, select all of them, then press the Delete key to remove them.

Snapshots and space concerns; Deleting snapshots <https://bombich.com/kb/ccc6/leveraging-snapshots-on-apfs-volumes#space>

Manually removing files associated with CCC

If you deleted the CCC application before leveraging the Uninstall feature, you can manually remove the following files and folders associated with CCC:

- /Library/Application Support/com.bombich.ccc

- /Library/LaunchDaemons/com.bombich.ccchelper.plist
- /Library/PrivilegedHelperTools/com.bombich.ccchelper
- /Users/yourname/Library/Application Support/com.bombich.ccc
- /Users/yourname/Library/Application Support/CCC Stats Service
- /Users/yourname/Library/Caches/com.bombich.ccc
- /Users/yourname/Library/Caches/com.bombich.ccc.stats
- /Users/yourname/Library/Caches/com.bombich.ccc.dashboard
- /Users/yourname/Library/Cookies/com.bombich.ccc.binarycookies
- /Users/yourname/Library/Preferences/com.bombich.ccc.plist

To get to the Library folder in your home directory, hold down the Option key and choose **Library** from the Finder's **Go** menu. When finished moving items to the Trash, restart your computer, then empty the Trash.

Manually disabling the CCC Dashboard and the com.bombich.ccchelper privileged helper tool

When you install and use CCC, two background utilities are installed to support CCC tasks. The helper application runs and coordinates tasks, it is required for all task-related activity. The helper tool will automatically exit if you do not have any scheduled tasks configured, and if you do not have CCC configured to display CCC's icon in the menubar. The helper tool will launch automatically when you open CCC, and whenever the CCC Dashboard is running.

The CCC Dashboard relays notifications from the helper tool to Notification Center, and also presents prompts and reminders to the user, and delivers a subset of error conditions to the user. The CCC Dashboard will automatically exit if you do not have CCC configured to display CCC's icon in the menubar, you do not have any scheduled tasks configured, no tasks are currently running, and if CCC is not running.

If you have a specific reason to disable these applications, for example, if you use CCC infrequently, you can do the following when you are done using CCC:

1. Configure CCC to not show its icon in the menubar (CCC toolbar > Settings > Dashboard)
2. While holding down Command+Option (⌘ ⌥), click on the Carbon Copy Cloner menu
3. Choose **Disable All Tasks & Quit** (the keyboard shortcut is Command+Option+Q)

Please note that any scheduled tasks will not run as long as CCC's privileged helper tool is disabled.

Related Documentation

- What is CCC's Privileged Helper Tool? <https://bombich.com/kb/ccc6/what-cccs-privileged-helper-tool>
- Monitoring backup tasks with the CCC Dashboard <https://bombich.com/kb/ccc6/monitoring-backup-tasks-ccc-menubar-application>

macOS Catalina Known Issues

Apple published macOS Catalina in September 2019. CCC 5.1.10 (and all versions of CCC 6), published in August 2019, is fully compatible with macOS Catalina. We cite known problems that Apple introduced in the new OS below.

Some SMB volumes can't support macOS sparse disk images

We have received several reports that macOS is unable to create disk images on SMB volumes hosted by various NAS devices. If you attempt to create the disk image in Disk Utility (for example), Disk Utility reports an "RPC Error". After months of investigation, we have concluded that macOS Catalina has more stringent requirements for sparse disk images than previous OSes.

Solution: Several users have reported that adjusting the SMB configuration on the NAS to support Time Machine <https://kirb.me/2018/03/24/using-samba-as-a-time-machine-network-server.html> can resolve the problem. Time Machine also uses sparse disk images on NAS volumes, so its requirements for the NAS file sharing service would be the same as those required for generic sparse disk image support.

Workaround A: Several users are reporting that connecting to the network volume via AFP rather than SMB resolved the problem:

1. Eject the NAS volume if it's currently mounted
2. Choose "Connect to Server" from the Finder's Go menu
3. Type in "afp://{server address}" to connect to the NAS volume via AFP
4. Choose "New disk image..." from CCC's Destination selector and specify a new disk image on the AFP-mounted NAS volume

Workaround B: If connecting to your NAS volume via AFP is not an option, then you can back up user data (e.g. your home folder) directly to the NAS volume (i.e. don't use a disk image). We also recommend disabling support for extended attributes (via the Advanced Settings).

2012-vintage Macs can't boot macOS Catalina from an encrypted USB device

We have received several reports that the 2012 Mac mini and the 2012 MacBook Pro can initially boot from a non-encrypted external USB device, but then will fail to boot from that device when FileVault is enabled on the external device. This issue is not specific to CCC, we have confirmation that this occurs when installing Catalina directly onto an external device as well. This problem does not appear to be specific to any particular enclosure, rather it appears to be specific to the 2012 models of Mac mini and MacBook Pro.

We have reported this issue to Apple (FB7433465) and we are currently awaiting a response.

macOS Catalina will not boot from a FireWire device

Apple has dropped support for booting from FireWire devices. The macOS Catalina Installer will explicitly disallow installation onto a FireWire-attached device, and if you attempt to boot macOS Catalina from a FireWire-attached device, the startup process will fail with the universal "no entry" symbol.

Solution: If your external device also has a USB interface, attach the device to your Mac using a USB cable instead.

Workaround: If your external device does not have a USB interface, you can continue to make backups to that device, but they will not be bootable while that device is attached via Firewire. If you need to restore data from this backup, you can either place the external hard drive into a different hard drive enclosure, or you can migrate the data to a fresh installation of macOS Catalina via the Migration Assistant application. If you prefer to maintain bootable backups, you should purchase an enclosure that will be bootable with macOS Catalina. We offer specific hard drive recommendations here <https://bombich.com/kb/ccc6/choosing-backup-drive#recommendations>.

Emerging issue: Higher incident rate of macOS Catalina failure to boot from Western Digital My Passport enclosures

We have received several reports now of Western Digital My Passport hard drive enclosures failing to function as a startup disk with macOS Catalina. In all cases the end user was able to confirm that the macOS Installer was also unable to make the device bootable <https://bombich.com/kb/ccc6/help-my-clone-wont-boot#install_macos>. The results are inconsistent — in some cases the system proceeds approximately 75% into the startup process, then shuts down. In other cases the system transparently boots to the internal disk, and in other cases (probably most) the enclosure boots fine. Due to the number of cases of **confirmed** failed bootability, however, we discourage users from purchasing new WD My Passport HDD enclosures if your intent is to create a bootable macOS Catalina backup. Please note that the WD My Passport **SSD** is NOT included among these reports. WD My Passport enclosures with a rotational HDD should be avoided.

Specific hard drive recommendations <https://bombich.com/kb/ccc6/choosing-backup-drive#recommendations>

Mount issues render USB thumb drives unsuitable for bootable backups

We have discouraged the use of thumb drives in the past <https://bombich.com/kb/ccc5/help-my-clone-wont-boot#known_issues> due to performance and reliability issues related to making these devices bootable. In the past the macOS loginwindow service has prevented CCC from mounting the APFS helper partitions on these devices. Now that the Catalina System and Data volumes are also special APFS volumes, we're seeing the same sort of interference from the loginwindow service, although now it leads to failures in backing up the Data volume. We are no longer offering support for these devices as bootable backups. You're welcome to create a backup of your Catalina Data volume instead:

1. Open CCC and click the Show Sidebar button in CCC's toolbar if it is not already visible
2. Select your backup task in the sidebar
3. Drag the **Macintosh HD - Data** volume from CCC's sidebar into the Source selector
4. Save the task

Startup Disk Preference Pane doesn't show OS versions for external volumes

The System Preferences application lacks full disk access by default, so it cannot read the System Version file on external volumes for the purpose of presenting the system version string underneath the volume icons. Ironically, System Preferences has the privilege to **change the startup disk**, but it can't make a read-only access to the system version file on external volumes.

Solution: Open System Preferences > Security & Privacy > Privacy, click the padlock icon and authenticate when prompted, then add the System Preferences application to the Full Disk Access category.

We have reported this issue to Apple (FB6723060) and Apple addressed the issue in macOS Big Sur.

Spotlight's "mds" helper aggressively prevents volume unmount requests

During our Catalina testing we repeatedly had trouble unmounting volumes in Disk Utility, particularly when erasing a backup volume. Upon closer inspection we found that an mds process is nearly always the process that is preventing the unmount. We've seen this occasionally in the past <https://bombich.com/kb/ccc6/why-cant-i-eject-destination-volume-after-backup-task-has-completed>, and for a long time CCC's option to unmount the destination volume at the end of a backup task has worked around the occasional Spotlight dissent with a followup forced-unmount. In Catalina, however, the problem seems to be far worse, affecting nearly every casual unmount attempt (except in the Finder, oddly).

Workaround for general unmount annoyances: You can disable Spotlight on your CCC backup volume to avoid its interference (and for better performance in general). To disable Spotlight, open the Spotlight preference pane in the System Preferences application, click on the Privacy tab, then drag the backup volume into the Privacy table. This only affects the destination volume, and it's reversible, you can remove it from that list should you decide that you want to re-enable indexing.

Workaround when attempting to erase a volume: If you're trying to erase a volume in Disk Utility and Disk Utility is reporting that it cannot unmount the volume to erase it — brace yourself for this one — unmount the volume before erasing it. That's right, Disk Utility can't walk and chew gum at the same time. If you unmount the volume before erasing it, though, the unmount request typically succeeds and you are then able to erase the volume.

We have reported this issue to Apple (FB6905679) and we are currently awaiting a response. This issue is **still** not resolved on macOS Big Sur.

Apple's volume group manipulation tool doesn't work with encrypted volumes

To create a bootable backup of a macOS Catalina volume, CCC must create a volume group at the destination. If your existing destination is a FileVault-protected volume (e.g. container a backup of Mojave), that destination can't be converted into a volume group — Apple's diskutil utility will fail, e.g.:

apple@Apollo ~ % diskutil ap addVolume disk8 APFS "CCC Backup" -passphrase apple -groupWith disk8s1 -role S
Will export new encrypted APFS Volume "CCC Backup" from APFS Container Reference disk8
Started APFS operation on disk8
Preparing to add APFS Volume to APFS Container disk8
Error: -69475: You cannot request initial encryption while creating a new APFS Volume to be added to an APFS Volume Group

Considering the error message, this appears to be intentional behavior. However, we have submitted an enhancement request Apple (FB7418398) and we are currently awaiting a response.

Workaround: You can temporarily decrypt your destination volume or erase it as APFS <https://bom

bich.com/kb/ccc6/frequently-asked-questions-about-ccc-and-macos-catalina#conversion_encrypted>
, then re-enable FileVault after establishing the initial backup of macOS Catalina.

Related documentation

- Will my encrypted backup volume be automatically converted to an APFS volume group? <https://bombich.com/kb/ccc6/frequently-asked-questions-about-ccc-and-macos-catalina#conversion_encrypted>
- Working with FileVault Encryption <https://bombich.com/kb/ccc6/working-filevault-encryption>
- Frequently Asked Questions about encrypting the backup volume <https://bombich.com/kb/ccc6/frequently-asked-questions-about-encrypting-backup-volume>
- What if I don't want my personal data to ever be on the destination in unencrypted form? <https://bombich.com/kb/ccc6/working-filevault-encryption#highest_security>

Disk Utility fails to create a volume group on T2 Macs when the startup disk is encrypted

Similar to the issue described above, we have discovered an edge case in which Disk Utility fails to create an APFS volume group on the internal SSD of a T2 Mac when the current startup disk is encrypted. The typical scenario in which we see this is when the Mac is booted from an encrypted backup volume, and the user is attempting to restore the backup to the freshly-erased internal SSD. Unlike the issue described above, this failure occurs when the destination is **not** encrypted — it appears to be specific to the *current startup disk* being encrypted, which seemingly should not play a role at all in the creation of a volume group on an unrelated device.

We have reported this issue to Apple (FB7477894) and we are currently awaiting a response.

Workaround A: Decrypt the backup volume

We don't want to even suggest this solution given the hassle that most users have had to endure to get their backups re-encrypted after the Catalina upgrade, but this will effectively work around the bug in Disk Utility:

1. Boot your Mac from the backup volume
2. Disable FileVault in the Security & Privacy Preference Pane
3. Wait for decryption to complete
4. Reboot — this step is important
5. Perform the restore and reset the startup disk
6. Re-enable FileVault on the backup volume, then reboot from the restored internal disk

Workaround B: Boot your Mac from another macOS Catalina volume that is not encrypted

The problem is not specific to the backup volume that you would like to restore from, rather Disk Utility only fails when the current startup disk is encrypted. If you can boot your Mac from another non-encrypted startup disk, you can restore your encrypted backup volume to the internal disk of your T2 Mac.

Workaround C: Reinstall macOS onto your destination, then migrate content from the backup

See: Using Migration Assistant to restore your startup disk from a CCC backup <https://bombich.com/kb/ccc6/how-restore-from-your-backup#install_then_migrate>

When you eject the destination in the Finder, Finder prompts to unmount other volumes that you can't see

When you make a bootable backup of a macOS Catalina system volume, the destination will consist of two volumes arranged in a volume group. Finder shows only one of these volumes, but both volumes are mounted as a pair. When you ask the Finder to eject your destination volume, Finder will indicate that other volumes on that device are mounted, and will ask if you want to unmount all volumes:

> "CCC Backup" is a volume on a disk that has 2 volumes. Do you want to eject "CCC Backup" only, or both volumes?

Finder doesn't tell you the identity of the other volume, which makes the decision a bit difficult to make. Rest assured, though, that the other volume is the hidden Data volume associated with your backup. You should unmount both volumes to avoid any Finder admonitions when you physically detach the backup disk from your Mac.

Solution: Click the **Eject All** button when prompted to unmount both the System and Data volumes.

We have reported this issue to Apple (FB7422542) and we are currently awaiting a response.

Finder will not show, nor allow you to set custom icons on other Catalina startup disks

Finder will show and allow you to customize the volume icon for your current startup disk, but not for other Catalina-bearing startup disks that your Mac is not currently booted from. This problem is not specific to CCC backups, but we see this frequently because CCC is designed to create bootable backups. This problem is the result of a design flaw in the implementation of custom icons in an APFS volume group. Up to macOS Catalina, the custom volume icon is stored in a file at the root of the startup disk named ".VolumeIcon.icns". To keep the System volume read-only, yet allow the apparent modification of this icon file, Apple chose to create a symbolic link at the root of the startup disk that points System/Volumes/Data/.VolumeIcon.icns. For the current startup disk, this path resolves correctly because the Data member of the volume group is mounted at /System/Volumes/Data. That's not the case for external volumes, those Data volumes are mounted at /Volumes/CCC Backup - Data (for example). As a result, the symbolic link to .VolumeIcon.icns is unresolvable for any volume that is not the current startup disk.

We have reported this issue to Apple (FB7697349) and we are currently awaiting a response.

Antivirus software may interfere with a backup

Some antivirus applications may prevent CCC from reading certain files, mounting or unmounting disk image files, or, in general, degrade the performance of your backup. In some cases, antivirus applications can even affect the modification date of files that CCC has copied, which will cause CCC to recopy those files every time as if they have substantively changed. In another case, we have seen such software create massive cache files on the startup disk during a backup, so much so that the startup disk became full. We recommend that you temporarily disable security software installed on your Mac (e.g. for the duration of your backup task) if problems such as these arise.

If CCC reports that antivirus software may be interfering with your backup task, here are some troubleshooting steps that you can take to resolve the problem:

1. Determine whether the files in question are being quarantined by your antivirus software. Perform a system scan with your antivirus software and address any issues that are reported. Please refer to the Help documentation associated with your antivirus product for more information.
2. If the problem persists, try running your backup task with the antivirus software temporarily disabled.

If the antivirus software's behavior cannot be resolved, you may be able to workaround the problem with an advanced setting. Select your task in CCC's main application window, then:

1. Click the **Advanced Settings** button
2. Select the **File Copying Settings** tab
3. Check the box next to **Don't update newer files on the destination**
4. Click the **Done** button
5. Save and run your task

If these steps do not address the issue, or if you do not have antivirus software installed, please open a support request <https://bombich.com/software/get_help> and we'll do our best to help you resolve the problem.

"Real time" protection scanning and Digital Loss Prevention applications have significant performance ramifications

We regularly receive reports that the backup task is running too slow, only to find that some "real time" protection application is directly causing the problem by taking too long to either scan content that CCC is writing, or by taking too long to permit the filesystem requests that CCC makes to the source or destination. While these applications do provide a valuable service to protect your Mac from malware, they're doing a disservice if they're interfering with backups.

The following applications are frequently implicated in these scenarios:

- Symantec DLP (com.symantec.dlp.fsd)
- Avira (avguard-scanner)
- Sophos File Protection (OnAccessKext)

Problem reports related to antivirus software

- BitDefender may generate excessive read activity on the destination volume during a backup task, and may cause the destination device to spontaneously eject. Add the destination volume to BitDefender's exclusion list to avoid the problem.
- We have received a report that agreeing to Webroot SecureAnywhere's request to "remove threats" during a backup task can produce a non-bootable backup.
- Little Flocker (now Xfence) can interfere with some of the subtasks required (e.g. creating a kernel extension cache, blessing the destination) to create a legacy bootable backup.
- We have received and confirmed a report in which Sophos CryptoGuard can have a debilitating effect on system performance while running a backup task.
- We have received several reports that McAfee's FileCore and Symantec's Data Loss Prevention software can cause the backup task to hang or to take a very, very long time. The applicable daemon processes may also consume an exceptional amount of CPU during a backup task leading to debilitating system performance for the duration of the task.
- We have received a report that ESET Endpoint Security can cause the backup task to hang or to take a very, very long time.
- We have received a report that Bit9 Carbon Black can cause the backup task to hang or to take a very, very long time.
- We have received a report that TrendMicro's "filehook" service can cause the backup task to hang or to take a very, very long time.
- We have received a report that Cylance's "CyProtectDrvOSX" kernel extension can cause the backup task to hang or to take a very, very long time.
- We have multiple reports in which CoSys Endpoint Protector <https://www.endpointprotector.com/> prevents CCC from backing up a pair of video-related system files (e.g. /Library/CoreMediaIO/Plug-Ins/DAL/AppleCamera.plugin).
- We have received reports that Avira antivirus may terminate CCC's file copier resulting in an incomplete backup. Avira "Real time protection" will also cause the backup task to take a very long time and consume an exceptional amount of CPU resources.

What criteria does CCC use to determine if a file should be recopied?

CCC will copy only items that are different between your source and destination. So if you complete a backup task, then run it again the next day, CCC will copy only the items that were created or modified since that last backup task. CCC determines that a file is different using its size and modification date. If a file's size or modification date is at all different on the source and destination, CCC will copy that file to the destination.

You can select your most recent completed task in CCC's Task History window and review the task audit <https://bombich.com/kb/ccc6/how-find-out-when-backup-last-ran-ccc-task-history#audit> to see precisely what was copied, and why. It is not uncommon for as much as 2-5GB of files to be updated between daily backups, for example, even when it seems that you have made no changes to the source volume. macOS is constantly updating various cache and log files, and these can really add up over the course of a day.

Organizational changes will lead to large amounts of data being recopied

If you have made large organizational changes on your source volume, e.g. renamed or moved a folder that had a lot of data in it, that will result in many items being recopied to the destination because the path to those items has changed. You can avoid this recopying behavior by applying the same organizational changes to the destination prior to running your backup task.

Some antivirus applications may actually change file modification dates

After CCC has copied a file to the destination, the very last thing that it does is to set the file's modification date to match the modification date of the source file. This filesystem activity prompts the AV software to scan the file, which is generally OK (albeit with a performance hit to the backup task). Reading a file is not sufficient to change the file's modification date, so well-written AV applications should cause no harm by scanning the files that CCC copies. When an AV application "touches" the file, however, or otherwise makes changes to the file, the modification date will be updated to the current date.

If the modification date of the files on your destination are getting set to the date and time of the backup tasks, there's a good chance that AV software or some other background service is making changes to the files after CCC has copied them. If you cannot resolve the modification date tampering of your AV software (or other software), you can configure CCC to avoid updating files that are newer on the destination. To apply this setting, select your backup task in CCC's main application window, then:

1. Click the **Advanced Settings** button.
2. Check the **Don't update newer files on the destination** setting in the **File Copying Settings** tab.
3. Save and run your task.

Related Documentation

- Antivirus software may interfere with a backup <https://bombich.com/kb/ccc6/antivirus-software-may-interfere-backup>
- Advanced Settings <https://bombich.com/kb/ccc6/advanced-settings>

A time zone shift can affect modification dates on some filesystems

HFS+, APFS, NTFS, and other modern filesystems store the modification date of files based on the Coordinated Universal Time (UTC — comparable to GMT). FAT filesystems, on the other hand, store file modification dates based on the local time zone setting of your computer. Generally this difference isn't a problem, but there is a drawback if you copy files between FAT volumes and NTFS or Mac-formatted volumes (or between Mac-formatted filesystems and a NAS device that uses local time for time stamps). During time zone shifts and the Daylight Saving Time/Summer Time shift, the modification dates of files on FAT32 volumes will appear to have shifted. As a result, CCC will see these files as out of date and will recopy each file. Unfortunately CCC cannot remediate this shortcoming of the FAT filesystem, so if you have to copy files to or from a FAT volume, we recommend that the corresponding source or destination volume is also FAT formatted.

Microsoft MSDN Library: File Times <https://msdn.microsoft.com/en-us/library/ms724290(VS.85).aspx>

Coping with the Daylight Saving Time shift with backups to and from the aforementioned filesystems

If you encounter this problem, the suggestion above to use the **Don't update newer files on the destination** advanced setting will resolve the problem for one of the DST changes, but not the other. Another approach is to configure CCC to use a more lenient resolution on timestamp differences. This can be achieved by setting CCC's global "NASTimestampLeniency" attribute. This is an advanced global configuration option that can be set using CCC's command-line utility, e.g. in the Terminal application:

"/Applications/Carbon Copy Cloner.app/Contents/MacOS/ccc" -g NASTimestampLeniency int 3601

With that setting, CCC won't recopy a file if its modification date is less than an hour (and one second) within the modification date of the same file on the destination. Note that a difference in the file's size will have precedence. Also, while this is a global setting, it only applies to tasks that have a non-HFS and non-APFS source or destination (despite the setting's name, it is not limited to NAS filesystems). If you have a bootable backup task, this setting would not be applied.

Mail's "Log Connection Activity" setting creates enormous files

If you enable "Log Connection Activity" in the Connection Doctor window in Mail and you forget to disable that setting, Mail will create enormous log files that will eventually fill up your startup disk. If you find that CCC is copying an unusually large amount of data during every backup, even backups run back-to-back, try the following to verify that this large amount of data is not related to Mail activity logs:

1. Open Mail
2. Choose "Connection Doctor" from the Window menu
3. Uncheck the box next to "Log Connection Activity"
4. In the Finder, hold down the Option key and choose "Library" from the Finder's Go menu

5. Navigate to Library > Containers > com.apple.mail > Data > Library > Logs > Mail
6. Delete the large log files

"CCC found multiple volumes with the same Universally Unique Identifier"

Occasionally a circumstance arises in which CCC presents the following error message before creating or running a backup task:

> **CCC found multiple volumes with the same Universally Unique Identifier that was associated with the volume you designated as the source/destination for this task.**
>
> CCC cannot proceed with confidence in having correctly identified the volume you originally chose when you configured this backup task. Unmount one of the conflicting volumes and try the task again, or please choose "Ask a question" from CCC's Help menu to get help resolving the issue.

Most modern operating systems apply a universally unique identifier to a new volume when you format that volume (e.g. in Disk Utility). Volumes should never have the same identifier, these identifiers are called "universally unique" because they're supposed to be unique, universally! Wikipedia <https://en.wikipedia.org/wiki/Universally_unique_identifier#Random_UUID_probability_of_duplicates> notes that, for 122 bit UUIDs, there is a 50/50 chance of having a single duplicate UUID if 600 million UUIDs were allocated to every person on Earth. The chances of two volumes having the same UUID should, then, be slim enough that the UUID can be reliably used to positively identify the source and destination volumes.

Given these odds, it is statistically more likely that CCC's discovery of a duplicate UUID is due to a hardware or software problem rather than to two volumes randomly having the same UUID. Therefore, CCC makes the conservative decision to not back up to either volume if another volume with the same UUID is detected.

Unfortunately, it has come to our attention that some hard drives that are pre-formatted for macOS are stamped with the same UUID at the factory. As a result, this situation can arise if you own and attach two "factory fresh" hard drives to your computer that came from the same manufacturer.

Solution

Reformatting one of the affected volumes will resolve the problem, however there is a non-destructive solution:

1. Hold down Control+Option and click on one of the volumes that was identified as having a non-unique unique identifier in CCC's sidebar
2. Choose the "Reset UUID" contextual menu item
3. Try configuring your backup task again

Note: This procedure may cause bootability problems for a volume that is intended to boot non-Apple computers (aka "Hackintoshes"). Those issues are beyond the scope of our support.

Identity problems specific to Western Digital hard drive enclosures

We have been tracking an issue that can lead to CCC producing the alert described above in cases where a duplicate device is not physically present. Occasionally Western Digital volumes will drop offline (especially during a sleep/wake cycle, and sometimes in the middle of a backup task), but the macOS diskarbitration service errantly retains the virtual device object. When the volume remounts, it is assigned a new device identifier and virtual device object. At that point, any application that asks the macOS diskarbitration service for a list of disks and volumes will get duplicate values for the WD device. Most applications wouldn't care about the duplicate devices, but CCC tracks both mounted and non-mounted devices so that CCC can mount the source and destination at the beginning of the task, if necessary.

CCC works around the underlying macOS issue in every case where it's practical. The one case where it is impossible to reliably work around the issue is in cases where the affected volume is not mounted, but is physically attached to your Mac and currently has duplicate virtual objects on record in the diskarbitration service (both not mounted). If you encounter this scenario, please report this problem to us via the **Report a Problem** menu item in CCC's Help menu so we can add your OS and device details to our open problem report with Apple (rdar://28972958).

If you ever see two **mounted** instances of your Western Digital device in the Finder, you should immediately unmount the device, detach it from your Mac, and then restart your computer. In most of the cases we've seen, the duplicate instances of the device are unmounted and therefore harmless. In a couple cases, however, macOS mounted two instances of the volume and the volume wound up corrupted.

Potential workaround

Western Digital's Support Knowledgebase <https://support.wdc.com/knowledgebase/answer.aspx?ID=18502> states that the **Put hard disks to sleep when possible** setting should be disabled when using their external USB hard drives. If you're using a Western Digital external USB device, open the Energy Saver Preference Pane in the System Preferences application and uncheck the box next to the **Put hard disks to sleep when possible** setting.

Finder or App Store finds other versions of applications on the backup volume

Occasionally we receive reports of odd system behavior, such as:

- When opening a document, the application on the backup volume is opened rather than the version from your startup disk
- When trying to update an application in App Store, the update appears to fail — the older version is always present
- The destination volume cannot be (gracefully) unmounted because various applications or files are in use
- When choosing **Open With...** from a Finder contextual menu, duplicates of your applications appear in the list

These problems consistently go away if the destination volume is ejected.

These problems are ultimately caused by problems with the LaunchServices database, which is an issue outside of the scope of the backup process. There are a few things that you can do to address the problem:

Disable Spotlight on the destination volume

Disabling Spotlight indexing on the destination volume should prevent new additions being made to the LaunchServices database that reference the destination. Open the Spotlight preference pane, click on the Privacy tab, then drag your destination volume into the privacy tab. Check whether applications still open by default from the destination volume, because this step may be enough to address the issue.

Configure CCC to eject the destination volume at the end of the backup task

In the **Postflight** section of CCC's Advanced Settings, you can configure CCC to unmount the destination <https://bombich.com/kb/ccc6/performing-actions-before-and-after-backup-task#dest_postactions> when CCC has finished copying files to it. By keeping the destination volume unmounted, Finder and App Store will be unable to find applications on that volume. You'll save wear and tear on that hard drive by keeping it spun down as well.

Reset the LaunchServices database

macOS maintains a list of application-to-file-type associations in the LaunchServices database. That database is consulted every time you try to open a file or application. Sometimes that database becomes corrupted, or contains outdated or invalid information, and those discrepancies can lead to problems with opening documents or applications. You can use this Reset LaunchServices Register <https://bombich.com/software/files/tools/Reset_LaunchServices_Register.app.zip> application to reset the LaunchServices database, then restart your Mac.

Big Sur+ users: GateKeeper will prevent you from running that script. You can paste the following into the Terminal application instead to reset the LaunchServices database:

sudo /System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/LaunchServices.framework/Versions/A/Support/lsregister -kill -r -domain local -domain system -domain user

Press the Return key after pasting that line into the Terminal window, then authenticate when prompted. Restart your computer for the change to take effect. macOS will automatically rebuild the LaunchServices database.

"The task was aborted because a subtask did not complete in a reasonable amount of time"

Occasionally a backup task can stall if the source or destination stops responding. To avoid waiting indefinitely for a filesystem to start responding again, CCC has a "watchdog" mechanism that it uses to determine if its file copying utility has encountered such a stall. By default, CCC imposes a ten minute timeout on this utility. If ten minutes pass without hearing from the file copying utility, CCC will collect some diagnostics information, then stop the backup task. Our support team can analyze this diagnostic information to determine what led to the stall.

Common factors that lead to stalls

Hardware problems are the most common cause of a stall. There are a few other factors that can lead to a stall, though, depending on how the backup task is configured:

- It can take a really long time to get a folder list from folders with extremely high file counts <https://bombich.com/blog/2023/01/18/folders-high-file-counts>
- Filesystem corruption or media problems on the source or destination can prevent that filesystem from providing a file or folder's filesystem entry
- A firmware problem in an external hard drive enclosure can cause that device to stop responding
- File sharing service errors can lead a network volume to become unresponsive
- Access to a network volume via a wireless connection may become slow enough that the volume stops responding
- Excessive bandwidth competition from other software can cause a volume to appear unresponsive, though it may just be responding very slowly

Troubleshooting suggestions

The first thing you should do if a task ends with this result is to view the event in CCC's Task History window to see if any specific errors are listed in the Errors tab <com.bombich.ccc6.task.history://show?tab=errors>.

If no specific files or folders were called out in the Task History window, reboot your Mac and run the task again. In many cases, an unresponsive filesystem is a transient problem, and the simple act of restarting will get the volume remounted in a better state. If the problem recurs, please choose **Report a problem** from CCC's Help menu and our support team can offer more specific troubleshooting suggestions. Below is a list of some of the troubleshooting suggestions we may offer depending on how your task is configured.

- Use Disk Utility's **First Aid** tool to check for any filesystem problems on the source volume. If any are discovered and the source is your startup disk, reboot while holding down Command+R (Intel Macs) or the Power button (Apple Silicon Macs) to boot in Recovery Mode <https://support.apple.com/en-us/HT201314>, then use Disk Utility to repair the problems. Please note: A report of "No problems found" from Disk Utility does not mean that there are no problems with that volume. There are no hardware diagnostic utilities on the market that will inform you of a problem with a cable, port, or enclosure, or report a bug in the firmware of a hard drive or SSD.

- Exclude a file or folder from the backup task. Click the **Task Filter** button at the bottom of the window, then uncheck the box next to the item that the source filesystem is unable to read.
- Remove a corrupted item from the destination volume.
- Erase the destination volume (we make this recommendation sparingly, and only when the stall can be definitively identified as a filesystem problem on the destination).
- Disable Spotlight on the destination volume to reduce bandwidth competition. To disable Spotlight, open the Spotlight preference pane, click on the Privacy tab, then drag the backup volume into the Privacy table. This only affects the destination volume, and it's reversible, you can remove it from that list should you decide that you want to re-enable indexing.
- If the stalling volume is a network volume, connect your Mac and the host of the network volume to the network via a wired connection (i.e. rather than via a wireless connection, if applicable).
- If the stalling volume is a network volume, eject that volume in the Finder, then remount the volume using a different file sharing protocol <https://bombich.com/kb/ccc6/backing-up-tofrom-network-volumes-and-other-non-hfs-volumes#nas_EINVAL>.
- If you have DriveGenius installed, that software may be performing a verification on the destination that "freezes" the volume for the duration of the verification. DriveGenius support suggests that you create a file in the root of the destination volume with the name ".com.prosofteng.DrivePulse.ignore" (no quotes) to stop Drive Pulse from acting on that volume.
- Hold down the Shift key while rebooting your Mac to boot into Safe Boot mode, then try running the task again. If the stall does not recur, then third-party software may be causing the stall.

Troubleshooting slow performance when copying files to or from a network volume

Network performance is usually the bottleneck of a backup task that copies files to or from a network volume, but there are several other factors that can affect performance as well. Here are some suggestions for improving the performance of your NAS-based backups.

Use ethernet instead of WiFi

Backing up data over a wireless connection will be considerably slower than backing up over an ethernet connection. 802.11n networks support approximately 300 Mb/s of rated (theoretical) bandwidth under the best conditions, but they usually operate at much lower speeds (130 Mbps and below, which is comparable to 16 MB/s). Bandwidth drops considerably as you get further from the base station (a wooden door between your Mac and the router will cut the signal in half), and the file sharing protocol overhead will reduce your achievable bandwidth yet more. So practically speaking, you're lucky to get 8 MB/s over a wireless connection while sitting right next to the base station. That performance can be cut in half due to Apple Wireless Direct Link (AWDL), which causes the Airport card's interface bandwidth to be shared between your ordinary WiFi network and an ad hoc network hosted by your Mac.

We performed a simple bandwidth test to a fourth generation Airport Extreme Base Station (802.11n) to demonstrate the performance decline. We copied a 100MB file to an external hard drive attached to the base station via USB in three scenarios: 1. An ethernet connection to the base station, 2. Sitting a few feet from the base station, and 3. Sitting across the house from the base station (~35 feet, no line of sight to the base station). The results were 6.5s (15.5 MB/s), 18.7s (5.3 MB/s), and 256s (0.39 MB/s) for the three scenarios, respectively. So, before you try to back up over a wireless network, consider running a simple test in the Finder to see just how fast your connection is. If it takes more than a minute to copy a 100MB file, your connection is too slow to be practical for backup purposes.

Use Quick Update after establishing a backup of a local source

Once you have established the initial, complete backup to a destination network volume, you can use CCC's Quick Update feature to greatly reduce the length of subsequent backup tasks. When Quick Update is enabled, CCC queries the FSEvents service for a list of folders that were modified on the source since the last backup event. In many cases, this folder list is just a small fraction of the total number of folders. By limiting the scope of the task to just the modified folders, CCC will have far fewer folders to enumerate on the destination.

Related Documentation

- Use Quick Update when it's possible to collect a list of modified folders from macOS <https://bombich.com/kb/ccc6/advanced-settings#quickupdate>

Exclude unnecessary content from the backup task

The more content you have in your backup task, the longer it will take to copy that content to a NAS and update that data set later. Especially if you're using the NAS as a secondary backup, we

recommend excluding content that is more easily restored from other sources, e.g. applications archives can often be re-downloaded from the App Store faster than the decompressed files can be restored from a NAS backup. Click the Task Filter button at the bottom of the CCC window to exclude content from the backup task <https://bombich.com/kb/ccc6/excluding-files-and-folders-from-backup-task>.

Eject the network volume in the Finder

We have run several tests and positively identified an issue in which the Finder will make repeated and ceaseless access attempts to the items of a folder on your network share if you simply open the network volume in the Finder. This persists even after closing the window. If you eject the network volume(s), then run your CCC backup tasks, CCC will mount the network volume privately such that it is not browsable in the Finder.

Disable support for extended attributes

Most NAS volumes are very slow at working with extended attributes, so we recommend disabling this setting if you do not specifically require them to be backed up. Apple considers extended attributes to be "disposable" because some filesystems cannot support them.

CCC automatically disables this setting when backing up to or from a network volume

1. Open CCC and select your backup task.
2. Click the **Advanced Settings** button.
3. Check the box next to **Don't preserve extended attributes** in the **File Copying Settings** tab.
4. Save and run the task.

Try using AFP instead of SMB to connect to the NAS

Apple deprecated AFP many years ago, but it still remains faster and more reliable than SMB in many cases (moreso on Intel Macs, notsomuch on Apple Silicon Macs). To try AFP instead of SMB:

1. Eject the NAS volume if it's currently mounted
2. Open CCC and select the applicable backup task
3. Click on the Source or Destination selector (whichever references the NAS volume)
4. Hold down the Option key and choose "Switch to AFP" (provide the credentials for the NAS volume again if prompted)
5. Save and run the task

Avoid running tasks simultaneously if they read from or write to the same NAS device

Especially with locally-attached source volumes, CCC won't have any trouble saturating your network connection with a single backup task. If you run more than one task at the same time, especially to the same NAS device, the network connection or the NAS device may not be able to handle the load. Leverage CCC's task chaining functionality <https://bombich.com/kb/ccc6/performing-actions-before-and-after-backup-task#chain_tasks>, or place your tasks into a task group <https://bombich.com/kb/ccc6/task-organization> so that they will be run sequentially instead.

Where can I find CCC's log file?

It is our aim to have the Task History window provide the user with enough information to find and troubleshoot any problems they're having with their backup tasks. For debugging and support purposes, however, CCC logs its activity in the following files:

- Task Activity: /Library/Application Support/com.bombich.ccc/pht_debug.log
- Task Editing: ~/Library/Application Support/com.bombich.ccc/ccc_debug.log
- CCC Dashboard: ~/Library/Application Support/com.bombich.ccc/ua_debug.log
- Remote Mac Authentication Agent: ~/Library/Application Support/com.bombich.ccc/sshauth_debug.log

Tip: Hold down Command+Option and choose **Open Debug Logs** from the Carbon Copy Cloner menu to open these four files in the Console application.

If there's something specific that you're retrieving from the log that is not presented in the Task History window, please let us know <https://bombich.com/software/get_help>. We'd prefer to consider exposing that information in the Task History window so you don't have to dig through the log. Also, note that basic details of task history are exposed in CCC's command-line utility, so that may be an easier way to get the information.

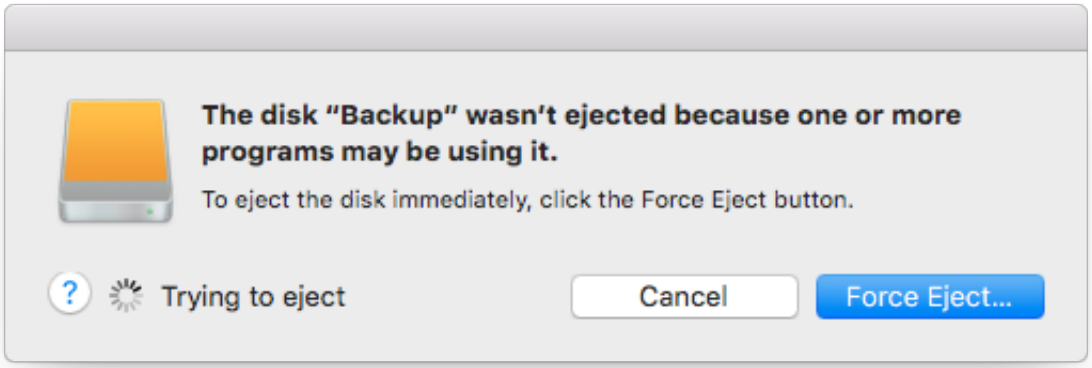
Where can I find a list of every file that CCC has copied?

You can find a transaction list for each task history event in the Audit tab of CCC's Task History window.

Related documentation

- Task Audit: Viewing details about the modifications made by the backup task <https://bombich.com/kb/ccc6/how-find-out-when-backup-last-ran-ccc-task-history#transactions>
- Using the ccc Command Line Tool to Start, Stop, and Monitor CCC Backup Tasks <https://bombich.com/kb/ccc6/using-ccc-command-line-tool-start-stop-and-monitor-ccc-backup-tasks>
- Why is CCC recopying every file during each backup? <https://bombich.com/kb/ccc6/why-ccc-recopying-every-file-during-each-backup>
- How do I get help? <https://bombich.com/kb/ccc6/how-do-i-get-help>

Why can't I eject the destination volume after the backup task has completed?



Occasionally this annoying message comes up when you're trying to eject your destination volume. If CCC is currently using that volume as a source or destination to a **running** backup task, then CCC will effectively prevent the volume from being unmounted. If your backup task is not running, though, CCC isn't preventing the volume from being unmounted. But what application is?

If this occurs within a minute or so after the backup task completes, it's typically caused by a macOS or third party service that is scanning or reindexing content that was just copied to the backup volume. Those processes usually finishes after a minute or two, and usually the destination can be ejected when that completes. If this frequently affects your backup volume, you can ask CCC to unmount the destination after the backup task completes. CCC will make multiple attempts to unmount the destination, resulting in a more reliable (and automated!) ejection of the destination at the end of the backup task:

1. Open CCC and select your backup task
2. Click the **Advanced Settings** button
3. In the **Postflight** tab, choose the option to unmount the destination volume <https://bombich.com/kb/ccc6/performing-actions-before-and-after-backup-task#dest_postactions> after the backup task completes.
4. Click the Done button, save and run your backup task

If the volume cannot be unmounted several minutes after the backup task has completed, or if CCC is also unable to eject the destination, open CCC's Task History window and view the error noted in the Errors tab for more information, if available, about the identity of the dissenting application.

Applications that frequently prevent volumes from unmounting

We've received (and confirmed) reports of the following applications causing trouble with volume

unmounts. If you have one of these applications, you should see if you can add your CCC backup volume to a "whitelist" within that software to avoid the interference it causes. The name of the offending process (which is what you would see in the Console application) is noted in parentheses.

- BitDefender (BDLDaemon)
- Time Machine (backupd)
- Spotlight (mds or mds_stores)
- Disk Drill (cfbackd)
- Retrospect (RetrospectInstantScan)
- CleanMyDrive
- Intego Virus Barrier (virusbarriers)
- AppCleaner (AppCleaner SmartDelete)
- AVG AntiVirus (avgoad)
- ClamXAV

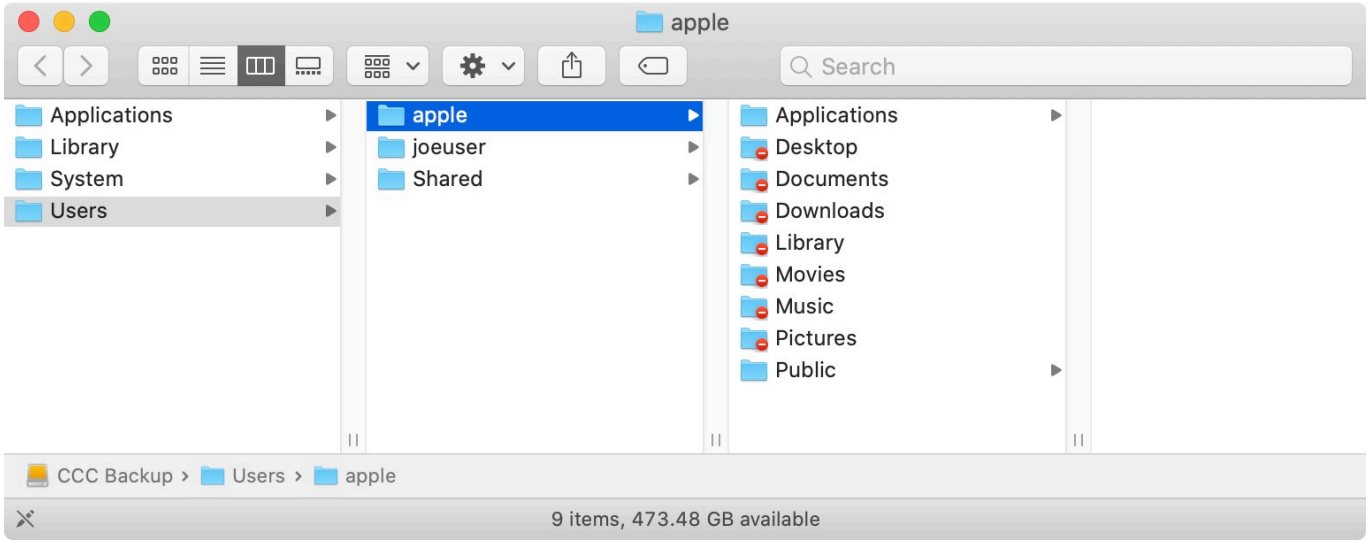
Remove any duplicate keychain entries in the Keychain Access application

Sometimes references to the keychain files on your backup volume can show up in the Keychain Access application. As a result, any application that leverages Keychain Services (e.g. Safari) will maintain an open file handle on the keychains on your backup disk, thus preventing that disk from unmounting. To resolve this, open the Keychain Access application (in /Applications/Utilities) and look for any duplicate keychain references in the sidebar. If you see duplicates, hover your mouse over those item until a tooltip appears revealing the path to the keychain file. If the keychain file is located on your backup disk, click on the keychain, then press the Delete key. When prompted, remove the references to the keychain file, not the file.

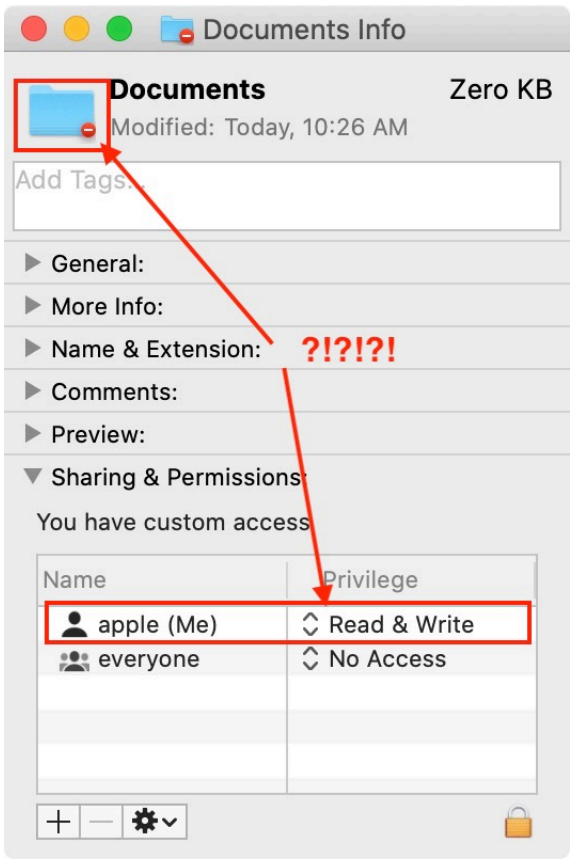
Why does Finder prevent me from viewing the home folder on my backup when it's attached to another Mac?

Note: This problem only affects macOS Catalina

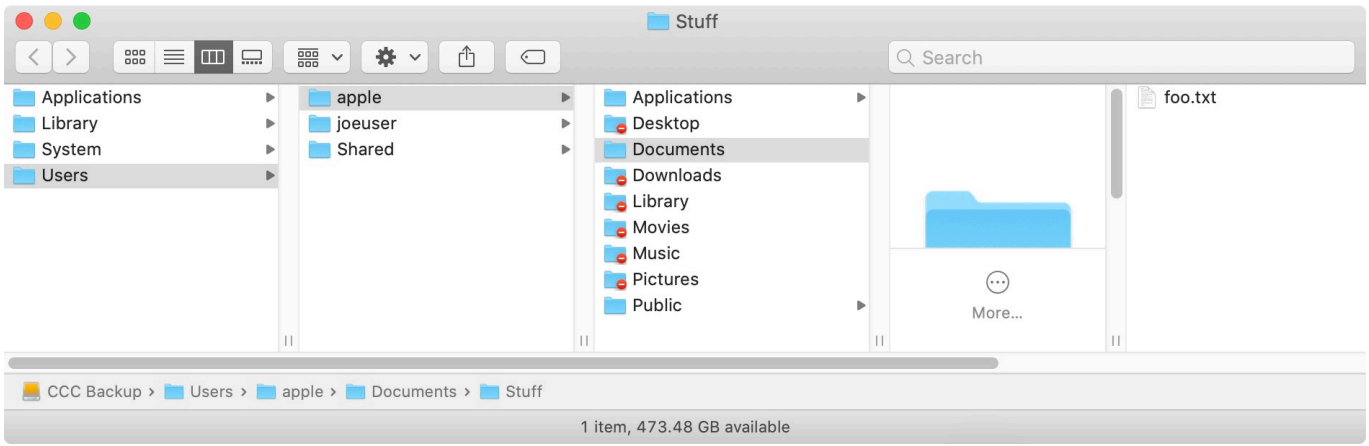
We are currently tracking a Finder bug in which the Finder incorrectly determines your access to some folders. The issue occurs when an "access control list" is applied to a folder and when ownership is disabled on the backup volume. Ownership is disabled by default when you attach your backup volume to a different Mac, and the folders in your home directory each have an access control list, so we often see this problem when trying to access the contents of the home folder on a backup disk when that backup disk is attached to some other Mac. Here's what you might see in the Finder:



Naturally, you might think, "OK, I'll just correct the permissions". But, if you select one of those folders and choose "Get Info" from the Finder's File menu, you'll discover that you already have Read & Write privileges for that folder!



The information in the Get Info panel is contradictory — on one hand, you have no access to the folder (indicated by the universal "no access" badge applied to the folder icon). According to the Sharing & Permissions section, though, you have full read and write access. If you try to access the contents of that folder via the Terminal, you can view and open the folders just fine. In fact, you can even reveal items nested within these folders in the Finder, with a really odd artifact!



There is nothing inherently wrong with these folders on the backup volume — CCC has retained file ownership and permissions such that the backup can be properly restored back to the original Mac. In fact, you shouldn't see this Finder bug if you boot the other Mac from the backup. If you're doing a one-time transfer of files to the other Mac, booting from the backup is one option to avoid this Finder bug.

How can I set up my backup task to regularly share files between two Macs?

If you're trying to set up a backup task that allows you to *regularly* transfer files between two Macs, then a better solution is to set up a folder-to-folder backup:

1. Drag the folder whose contents you'd like to share between Macs to CCC's Source selector
2. Create a **new** folder on the destination volume and drag that new folder onto CCC's Destination selector
3. Click the **Advanced Settings** button
4. Check the box next to **Don't preserve permissions** in the **File Copying Settings** tab
5. Save and run the task

Your account on the second Mac should then have no trouble accessing the contents of that new folder on the backup disk.

Can I keep my backup bootable, yet also occasionally access my files on another Mac?

If your goal is to create a *bootable* backup that you *occasionally* use to transfer files between Macs, and if enabling ownership on the volume does not resolve the access issue, then we have developed a workaround that will avoid this Finder bug. Download this script instead <https://bombich.com/software/files/tools/finder_perms_bug.scpt>, open it in the Script Editor application, then click the Run button in the toolbar. When prompted, select the affected folders (or your entire home folder) from the backup volume. This script will remove the access control entries and set your current user account as the owner. Keep in mind that this change will be reversed when you attach the disk to the original Mac and re-run the backup task, so keep the script handy if you're using this disk between Macs frequently.

Some third-party storage drivers may cause hardware misbehavior

We occasionally receive reports of strange behavior from USB devices, e.g. slow performance, disks dropping offline in the middle of the backup task. In some of those cases we've discovered that third-party storage drivers are causing the problem. In particular, the SAT-SMART drivers and some ancient BlackBerry USB drivers can lead to problems. We have also received a handful of reports indicating that the Samsung SSD storage drivers cause problems booting from their devices.

If you're troubleshooting a USB device behavior or performance problem, we recommend that you consider uninstalling these drivers.

Removing BlackBerry drivers

Assuming you're not actively using any USB BlackBerry devices with your Mac, we recommend uninstalling that old software. BlackBerry doesn't offer an uninstallation guide, but this helpful forum post makes a recommendation <https://superuser.com/questions/647762/how-can-i-remove-blackberry-tools-entirely-from-os-x>. Simplifying those instructions a bit:

Choose "Computer" from the Finder's Go menu, then navigate to these locations to find extension and agent components (you may not have all of these locations on your version of macOS):

Macintosh HD > Library > LaunchAgents
Macintosh HD > Library > LaunchDaemons
Macintosh HD > Library > Extensions
Macintosh HD > System > Library > Extensions
Macintosh HD > Library > StagedExtensions > Library > Extensions ‡

If you find the BlackBerry components in those folders, just drag them to the Trash, authenticating when prompted. When you're done, reboot. Here's a complete list of components that the website recommended that you remove (you may not find all of these components, but hopefully you can at least find and remove the extensions):

/Library/Application Support/BlackBerry
/Library/Application Support/BlackBerryDesktop
/Library/Frameworks/RimBlackBerryUSB.framework
/Library/LaunchAgents/com.rim.BBLaunchAgent.plist
/Library/LaunchDaemons/com.rim.BBDaemon.plist

/System/Library/Extensions/BlackBerryUSBDriverInt.kext
/System/Library/Extensions/RIMBBUSB.kext
/System/Library/Extensions/RIMBBVSP.kext

Removing SAT-SMART drivers

The SAT-SMART drivers <https://github.com/kasbert/OS-X-SAT-SMART-Driver> aim to offer SMART support for USB devices. These drivers have not been actively maintained since late 2016, so their compatibility with newer macOS releases is dubious. Their uninstallation instructions may also be out of date for newer macOS releases, so we offer the following suggestion.

Choose "Computer" from the Finder's Go menu, then navigate to these locations to find extension

components (you may not have all of these locations on your version of macOS):

Macintosh HD > Library > Extensions
Macintosh HD > System > Library > Extensions
Macintosh HD > Library > StagedExtensions > Library > Extensions †

If you find the SAT-SMART components in those folders, just drag them to the Trash, authenticating when prompted. When you're done, reboot. Here's a list of components that may be installed by the SAT-SMART installer in any of the folders noted above (you may not find all of these components, remove as many as you find):

SATSMARTDriver.kext
SATSMARTLib.plugin

Removing staged extensions

System Integrity Protection will prevent the removal of staged extensions, but you can paste this command into the Terminal application to ask the system to clear all staged extensions:

sudo kmutil clear-staging

Removing Samsung drivers

The Samsung FAQ for its Portable SSD products <https://semiconductor.samsung.com/consumer-storage/support/faqs/portable> provides the following instructions for removing their drivers:

> On a Mac PC, remove the Portable SSD from the Thunderbolt port and use the CleanupAll.scpt from the directory where the software is installed (e.g., Home/Library/Application Support/PortableSSD) with osascript to uninstall it (osascript CleanupAll.scpt). For more information, please refer to the User Manual.

A CCC user discovered that this does not remove the entries from the KextPolicy database. We can't recommend that you manually modify the KextPolicy database, however, in the interest of documenting a potential solution, that user indicated that the Samsung kext driver policy could be removed by booting into Recovery Mode, then running the following command in the Terminal application:

/Volumes/Macintosh\ HD/usr/bin/sqlite3 /Volumes/Macintosh\ HD\ -\
Data/private/var/db/SystemPolicyConfiguration/KextPolicy 'delete from kext_policy where team_id = "8S33FS7Q5Q"'

Troubleshooting APFS Replication

Apple's APFS replicator is typically fast and flawless, but it does not handle some conditions with grace (or at all). CCC works to avoid as many of these ungraceful results as possible, but we have the following recommendations for the cases where Apple's APFS replicator flops.

CCC reported that the APFS replication failed

If your first backup attempt failed, try the following steps.

1. Restart your Mac
2. Rule out general hardware problems <https://bombich.com/kb/ccc6/identifying-and-troubleshooting-hardware-related-problems#steps>, and verify that your destination device is attached directly to a USB or Thunderbolt port on your Mac (avoid hubs). Consider removing any potentially-conflicting hardware drivers <https://bombich.com/kb/ccc6/some-third-party-storage-drivers-may-cause-hardware-misbehavior>.
3. Open Disk Utility
4. Choose **Show All Devices** from the View menu
5. Unmount your destination volume – this redundant step is often necessary to avoid failures in step 7.
6. Select the **parent device** of your destination volume in Disk Utility's sidebar †
7. Click the Erase button in the toolbar
8. If you see a volume named "ASRDataVolume_xxx", select that volume and click the **—** button in the toolbar to remove it.
9. Back in CCC, click on the Destination selector box and choose **Choose a different destination**. Choose the freshly-erased volume as the destination.
10. Click on the Destination selector again and choose **Legacy Bootable Copy Assistant**. Choose the option to allow CCC to erase the destination.
11. Click the Start button

† If you have other volumes or partitions on your destination disk that you do not want to lose, do not erase the whole disk. Instead, select the destination volume in this step. Click the "Erase Volume Group" button if it is presented in the Erase Volume panel.

If APFS replication fails repeatedly

Apple's APFS replicator will fail if there are problems with your installation of macOS, filesystem corruption on the source, storage driver conflicts, problems with the hardware, or if there are any media read failures. In short, it's just not very tolerable of real-world conditions. CCC's file copier is battle-tested — we've built years of experience into it to handle all sorts of challenging conditions with grace.

In cases where Apple's APFS replicator simply can't get the job done, we recommend that you configure CCC to perform a Standard Backup. A Standard Backup is a complete backup of all of your data, settings, and applications. This backup will be suitable for migrating all of your applications, data, and settings to a fresh installation of macOS should that ever be required. Creation of the backup alone is sufficient to protect your data, however this will not address any problems with the source.

To proceed with a Standard Backup, click the "X" button in the top-left corner of the destination volume icon in the Destination selector box to clear out the current destination selection. Then click on the Destination selector box again and reselect the destination volume.

Related documentation

- Installing macOS onto a Standard Backup <https://bombich.com/kb/ccc6/cloning-macos-system-volumes-apple-software-restore#install_macos>
- How to restore from your backup <https://bombich.com/kb/ccc6/how-restore-from-your-backup>

I stopped the backup task and now my destination disk is completely unresponsive

Apple's APFS replicator does not gracefully handle the cancelling of a replication task. The destination volume is essentially corrupted, but ASR does not erase the volume to place it back into its pre-task condition. Further, the destination device is not only completely unresponsive, but even Disk Utility cannot load devices and volumes. This is scarier than it looks initially, there is fortunately a simple solution.

Solution: Physically detach the destination device from your Mac, then reattach it. If the destination is an internal device or cannot be easily detached, simply restart your computer. Then choose **Disk Utility** from CCC's Utilities menu and reformat the destination.

We reported this ungraceful result to Apple (FB7324207) in September 2019 and we are still awaiting a response.

CCC reported that my source or destination is reporting read/write errors

Apple's APFS replicator clones the source volume at a very low level. Rather than copying individual files, it copies the filesystem data structures directly. Because this utility is not examining files on an individual basis, it's not able to deal with media failure nor filesystem corruption in a graceful manner (FB7338920). When ASR encounters media failure or filesystem corruption, the cloning task will fail and the destination volume will be in a corrupted state. The presence of media errors makes it very unlikely that ASR will be able to complete the clone, so CCC will not use the ASR utility if the source or destination is reporting read/write errors.

Solution: We recommend that you proceed with a Standard Backup, then address the hardware concern that led to the read/write errors, then restore your data from the backup (if the problem was affecting the source).

Related documentation

- How to restore from your backup <https://bombich.com/kb/ccc6/how-restore-from-your-backup>
- Identifying and Troubleshooting Hardware-Related Problems <https://bombich.com/kb/ccc6/identifying-and-troubleshooting-hardware-related-problems>
- Disk error statistics <https://bombich.com/kb/ccc6/disk-center#errors>

Coping with errors caused by APFS filesystem corruption

We regularly see cases of APFS filesystem corruption that lead to errors during a backup task. This corruption is typically presented in an error like one of these:

readlink_stat("/Photos/Foo/2020_Dumpster_fire.jpg") failed: Illegal byte sequence (92)
rename("/Photos/Foo/.2020_Dumpster_fire_out_of_control.jpg.asdfgh" ->
"/Photos/Foo/2020_Dumpster_fire_out_of_control.jpg") failed: No such file or directory (2)

When CCC encounters these errors, the affected items are listed in CCC's Task History window, often with this advice:

> When an error occurs while trying to read or modify a file or folder's filesystem attributes (e.g. ownership and permissions, modification date, file name, what folder it's in, etc.), that usually suggests that there is some corruption in that item's filesystem entry. The file may need to be deleted and, if applicable, restored from a backup.

In both of the error cases in the above example, the file or the parent folder is corrupted, and the APFS filesystem will not allow any modifications to those items. Sometimes you can simply delete the affected items, but sometimes this is not possible because the Finder does not reveal these corrupted items to you (because they are corrupted). Typically Disk Utility does not even detect this filesystem corruption, and it will never repair the corruption if doing so would require the removal of files or folders. Sadly, lacking any other utilities to repair the damage, your only remaining option for *resolving* the corruption is to erase the affected volume.

The folder swap method

If you are unable to see a corrupted item in the Finder (and therefore unable to delete it to resolve the corruption), there is one alternative that you may be able to consider. Often when errors are encountered while trying to make changes to a file (especially its name or location), the corruption is affecting the parent folder, not the file itself. In those cases you can replace the folder to remove the corruption. Supposing CCC is reporting errors on a file at "My Media Volume" > Photos > Foo > 2020_Dumpster_fire.jpg, you could do the following to replace the folder while retaining the bulk of its content:

1. If the item you're looking for resides in a hidden folder (e.g. "/Users/yourname/Library"), you can press Command+Shift+Period to toggle the Finder's display of hidden items
2. Navigate in the Finder to "My Media Volume" > Photos
3. Create a new folder here named "Foo new"
4. Select all of the items in "Foo" (e.g. Command+A) and drag them into "Foo new"
5. Move "Foo" to the Trash†
6. Rename "Foo new" --> "Foo"

† This does not *solve* the corruption problem, rather it only cordons the corruption off to a separate (and disposable) folder. In most of these cases, you'll find that Finder cannot empty the Trash, claiming that the files are "in use". That's just the Finder's way of expressing that it can't cope with the corrupted content, and has no advice that would actually be helpful. If you are unable to empty the Trash, and you would rather not erase the affected volume to remove the corruption, then you can create a new folder on the affected volume, e.g. "Corrupted Items" and move the items from the Trash into that new folder. You can then exclude that folder from your backup task

<https://bombich.com/kb/ccc6/excluding-files-and-folders-from-backup-task> to avoid the errors that its content would cause.

Preserving Finder comments and tags

CCC copies all of the information required to preserve Finder tags and comments, but the Finder can interfere with the preservation of these data.

Finder tags and comments are stored as extended attributes associated with a file or folder (tags are stored as a "com.apple.metadata:_kMDItemUserTags" extended attribute, comments are stored as a "com.apple.metadata:kMDItemFinderComment" extended attribute). Some associated data related to tags and comments is also stored in the hidden .DS_Store folder-specific Finder preference file. When backing up to a locally-attached volume, CCC will preserve these extended attributes and the .DS_Store files. Whether the Finder accepts these attributes, however, depends on whether the Finder has cached older information for the affected files and folders. If you open the destination in the Finder prior to running your backup task, Finder will cache a bunch of those ".DS_Store" preference files. If you then run the backup task, and then revisit those folders on the destination, Finder will not only present cached .DS_Store content (i.e. content that does not reflect your comments and tags), but it will also replace the .DS_Store files that were copied by CCC with the cached versions. The older .DS_Store files will then conflict with the Finder comment and tag extended attributes, and the Finder will not show the tags and comments despite the data being present on the destination files.

You should be able to do the following to get the Finder comments and tags preserved:

1. Restart your Mac (or log out and log back in)
2. Do not open the destination volume in the Finder (no peeking!)
3. Run the backup task
4. At this point you should be able to view the content on the destination, and the comments and tags should be preserved

Preserving Finder comments and tags on network volume backups

NAS volumes traditionally offer poor performance and reliability for preserving extended attributes, so CCC does not preserve extended attributes by default when backing up to a network volume. As a result, Finder comments and tags are not preserved by default when backing up to a network volume.

To preserve Finder comments and tags on a network volume, click the **Advanced Settings** button, then uncheck the box next to **Don't preserve extended attributes** in the File Copying Settings tab.

Character composition conflicts on NAS volumes

If you copy folders to your NAS device from a Windows system or via SSH (e.g. using rsync) that have accented characters in their names (e.g. é, ö), then you can later run into file or folder name conflicts when you try to access those folders via SMB file sharing. When these conflicts affect a CCC backup task, you'll see errors in CCC suggesting that there is a permissions problem on the NAS volume, or that you should try restarting the the NAS device. This article explains how these conflicts arise, how to spot them in the Finder, and how to ultimately resolve them to achieve error-free backups.

Some brief background about character encoding

The "ASCII" character set is composed of 255 1-byte characters — all of the characters that you'd find in any English word. Non-English languages have numerous other characters, however, that can't possibly fit in a set of just 255 characters. These other characters are defined in the Unicode standard, and typically consume 2 or 3 bytes per "code unit". Most modern filesystems support the Unicode standard, however there are some characters within the Unicode standard that can present challenges to filesystems, and can lead to conflicts when transferring content between filesystems or across a network filesystem protocol.

Let's take the character "é" as an example that can lead to conflicts. This character is described as "Latin small letter e with acute". In the UTF-8 standard, this character can be presented as a single two-byte code unit (0xC3A9), or it can be generated by composition, i.e. by combining "Latin small letter e" (ASCII, 0x65) code unit with a "combining acute accent" (0xCC81) code unit. What individual filesystems do when faced with these ambiguous characters is a potential source of conflict. Some filesystems normalize the characters (i.e. choose one variant when storing file names, e.g. HFS+), some accept both but treat the characters as identical (composition-preserving [usually], composition-insensitive, e.g. APFS), and other filesystems accept both and treat the variants as unique/different characters (composition-sensitive, e.g. EXT4, a common format used on NAS devices).

Network filesystems (AFP, SMB) are in an awkward middle place — they can't dictate how the underlying filesystem behaves, so composition conflicts can place them in an unsupportable position.

Creating conflict

Let's suppose you have a folder named **Beyoncé** in your Music library. Long ago (e.g. prior to macOS High Sierra), your library was on an HFS+ filesystem, so that é character was stored in the composed form, 0x65CC81. Way back then, let's suppose you used rsync to copy this library directly to your NAS via SSH. On the NAS, the backend filesystem is EXT4, which is composition-sensitive. The EXT4 filesystem stored the folder name using the same encoding as on the source — the composed variant. Fast-forward many years later. You have a new Mac and your startup disk is now APFS formatted. You migrated content from an HFS+ volume to an APFS volume, and the é in that Beyoncé folder name was "normalized" to the two-byte, single character variant. You still have the same NAS, but now you're preparing to use CCC to make the backups to that NAS via SMB. Many factors have changed!

If you were to navigate to this Beyoncé folder on the SMB-mounted volume in the Finder, you might

be surprised to find that the folder *appears* to be empty. In fact, the Finder is failing to query the content of that folder, because the macOS SMB client queries the content of the folder using the normalized variant of the name (which the NAS correctly reports as "not there"). If you try to copy content into that folder, Finder will ask you to authenticate, then present an error indicating that you don't have permission to make the change. This is not actually a permissions problem! It's not necessarily a Finder bug either, rather it is an unsupportable configuration — that folder can't be effectively accessed by SMB or AFP. You'll see the same problem if you try to delete that folder in the Finder.

Resolving character encoding conflicts

The correct solution in a case like this is to delete the "old" folder from the NAS. You won't be able to do this in the Finder (nor CCC for that matter), though, because the macOS SMB client normalizes folder names when it makes requests to the NAS. So despite that the SMB client can see the composed variant of a name in the parent folder listing, if we subsequently ask the SMB volume to remove the composed variant of a folder, the SMB client relays that request to the NAS using the normalized variant of the folder name, which doesn't exist on the NAS.

Solution: Log in to the NAS device's web admin interface, or connect to it via SSH to remove the affected folders.

Workaround: Alternatively, you can configure CCC to back up to a new folder on the NAS. This alternative approach is ideal if you have non-Mac clients that access the content in the original folders (and therefore tend to just re-introduce the same problem).

For the Terminally-curious

Here is what a pair of composition-conflicting folder names would look like on the backend EXT4 filesystem (i.e. logged in to the NAS via SSH):

```
admin@baltar:/volume2/SynBackup6TB/FunWithEncoding$ ls -li
total 16
30421978 drwxrwxrwx+ 2 admin users 4096 Dec 20 17:31 Beyoncé
30421986 drwxrwxrwx+ 2 admin users 4096 Dec 20 17:31 Beyoncé
```

This would appear to be illegal — two folders cannot coexist in the same folder having the same name. But if we pipe the listing to xxd to see the hexadecimal representation of the characters, we can see that the é characters do actually differ (note, this output is slightly massaged for easier reading):

```
admin@baltar:/volume2/SynBackup6TB/FunWithEncoding$ ls | xxd
4265 796f 6e63 65cc 81  Beyonce..
4265 796f 6e63 c3a9     Beyonc..
```

The first item has the composed é character, the second item has the single-character-two-byte code point. Now suppose each of these folders has a different file within it. Here is the NAS perspective:

```
admin@baltar:/volume2/SynBackup6TB/FunWithEncoding$ ls -l Beyonc*
Beyoncé:
total 0
-rwxrwxrwx+ 1 admin users 0 Dec 20 17:31 composed

Beyoncé:
total 0
```

-rwxrwxrwx+ 1 admin users 0 Dec 20 17:31 single

But the macOS SMB client normalizes the folder listing result and requests, so we see different results from the macOS perspective:

[bombich:/Volumes/SynBackup6TB/FunWithEncoding] ls | xxd
4265 796f 6e63 65cc 81 Beyonce..
4265 796f 6e63 65cc 81 Beyonce..

[bombich:/Volumes/SynBackup6TB/FunWithEncoding] ls -l Beyonc*
Beyoncé:
total 0
-rwx------ 1 bombich staff 0 Dec 20 17:31 single

Beyoncé:
total 0
-rwx------ 1 bombich staff 0 Dec 20 17:31 single

This last result is the most curious. We can see from the parent folder that two separate "Beyoncé" folders exist here, but when we ask for details about each folder and a folder listing of each folder, we only get results pertaining to the folder that has the normalized name. Yet stranger, Finder only presents one of these (although you might catch a glimpse of both folders right before Finder removes one from view!). This is why requests to add files to the folder named with the composed character will fail, and it's also why attempts to delete the folder with the composed character will fail — the SMB client simply will not make the request correctly using the composed variant of the character.

Identifying and Troubleshooting Hardware-Related Problems

There are several behavior patterns that inevitably boil down to a problem with a hardware component between your Mac and the storage. Any time you see random errors, stalls, crashes, the destination volume "disappearing" in the middle of a backup task, reports from the Finder that a disk was ejected improperly, Finder lockups and other unruly behavior, we have to turn to old-fashioned troubleshooting to rule out the problematic component. Everything is on the table – USB ports, cables, plugs, adapters, hubs, hard drive enclosures, storage devices – a problem with any of these components can lead to mayhem.

Many times that hardware problems occur, CCC will get meaningful errors from the filesystem that plainly indicate some sort of hardware problem, and CCC will report these at the end of the backup task. In some cases, however, macOS or CCC will detect a hung filesystem and you will see one of the following messages from CCC:

"The task was aborted because the [source or destination] disappeared."

If you see this message, macOS's kernel recognized that the affected filesystem was not responding and terminated it. While this is obviously an abrupt end to your backup task, it beats the alternative macOS behavior described next.

"The task was aborted because the [source or destination] filesystem is not responding."

CCC will present this message when the source or destination volume hasn't accepted read or write activity in at least ten minutes, and a deliberate followup test verifies that a simple read or write request fails. In these cases, macOS's kernel has failed to take action on the misbehaving filesystem and you can expect to see stalls in any application that attempts to read from or write to the affected volume. To break the stall, the affected disk must be forcibly detached from your Mac or you must reboot by holding down the power button if the disk is internal.

In other cases, you'll see a report from the Finder:

Disk Not Ejected Properly

"Eject 'Your Backup Disk' before disconnecting or turning it off."

Even if this event occurred when a CCC task was running, please note that CCC can *never* be responsible for a device's apparent detachment from the system – CCC never interacts with hardware at that level. CCC is simply copying files from one volume to another. If simple file copying leads to volume disappearance, the most common explanation is that a communication failure occurred due to a crash of the storage device's firmware, or due to the (typically transient) failure of a component between the Mac and the storage (most often it's a USB hub or adapter). These events also may coincide with sleep/wake cycles, e.g. if a device does not handle the power state transition well. Many times these messages will be perplexing because the storage device reboots and then immediately reappears, possibly before you see the message from the Finder. Other times the device may not reappear until it is physically detached and reconnected to your Mac.

When you see these messages – there is a hardware problem or a negative

hardware:macOS interaction afoot. We cannot solve these problems with a change to CCC, but the steps below can help you identify the problematic component.

macOS Monterey ejects the source snapshot on logout

In nearly every case where a task is aborted due to the source or destination disappearing, it's the result of a hardware issue. We have found one exception to this though. When you log out of a macOS Monterey system while a backup task is running, macOS will errantly unmount the source volume snapshot, and will do so despite CCC's dissent of the volume unmount request. This behavior did not occur on macOS Big Sur, and appears to be resolved for macOS Ventura. Note that this only affects a task that is running during a logout event. Tasks run fine when they are started when no user is logged in.

Workaround: On Monterey, avoid logging out while a backup task is running. Go to System Preferences > Security & Privacy > {click the padlock and authenticate} > {click Advanced...} and verify that you do not have the system configured to log you out after a period of inactivity if that may overlap with a scheduled backup of the startup disk.

Solution: Upgrade to macOS Ventura.

Troubleshooting steps

When CCC suggests that you might have a hardware problem, here are the steps that we recommend you take to isolate the problem. Repeat the backup task between each step, and stop if something has resolved the problem:

1. If the affected volume resides on an external hard drive, detach that disk from your Mac, then reattach it. Otherwise, restart your Mac before proceeding. Note that this generally only resolves the acute problem of a filesystem stalling. While the disk may appear to function fine once it is reattached, it's not unlikely for problems to recur.
2. Run Disk Utility's **First Aid** tool on the source and destination volumes. Note that Disk Utility's First Aid will rarely **fix** filesystem corruption. If filesystem corruption is detected, we recommend that you erase the volume to resolve the corruption.
3. If you have any other hardware devices attached to your Mac (e.g. USB webcams, printers, iPhones — anything other than a display, keyboard, mouse, and the source/destination disks), detach them.
4. If your source or destination volume is plugged into a USB hub, keyboard, or display, reconnect it to one of your Mac's built-in ports. **USB hubs are the most common cause of "disk not ejected properly" errors.**
5. Replace the cable that you're using to connect the external hard drive enclosure to your Mac (if applicable). Do not use an adapter to connect the device to your Mac, use a cable that has the correct plugs on each end for the device and your Mac. **USB adapters are another common cause of "disk not ejected properly" errors.**
6. If you have any third-party storage drivers, uninstall them. Especially since macOS Catalina, we have seen numerous reports of problems caused by third-party storage drivers <https://bombich.com/kb/ccc6/some-third-party-storage-drivers-may-cause-hardware-misbehavior>.
7. Try connecting the external hard drive enclosure to your Mac via a different interface (if applicable)
8. Try the same hard drive in a different external hard drive enclosure (we offer some recommendations here <https://bombich.com/kb/ccc6/choosing-backup-drive#recommendations>).
9. Reformat the hard drive in Disk Utility.
10. If none of the previous steps has resolved the problem, then the hard drive is failing or defective. Replace the hard drive.

"Why does CCC eject the destination?" or "Why is CCC making my whole computer stall?"

We hear this one a lot, and we generally reply, "don't shoot the messenger." In most cases, CCC is either the only application copying files to the affected volume, or it is at least the application doing most of the access, so it only seems like the problem is specific to CCC. A typical backup task will make millions of filesystem requests, so it comes as no surprise to us when CCC uncovers hardware problems in a disk. CCC is merely copying files from one disk to another, and this is not the kind of task that should cause a system-wide stall. Whenever multiple applications are stalling while trying to access a volume, the fault lies entirely within the macOS kernel, which is mishandling hardware that is either failing or defective. If you're uncertain of this assessment, please send us a report from CCC's Help window. When CCC detects a stalled filesystem, it collects diagnostic information to determine where the stall is occurring. We're happy to review the diagnostics and confirm or deny the presence of a hardware problem.

"But Disk Utility says that there is nothing wrong with the disk..."

Disk Utility is competent at detecting structural problems with the filesystem, but it can't necessarily detect hardware failures that can cause a filesystem to stop responding to read and write requests. Additionally, even if your disk is SMART capable and "Verified", the attributes that SMART status reports on are weighted, and may not yet indicate that the hardware is in a pre-fail condition. **Disk Utility does not scan for bad sectors, it only checks the health of the filesystem**. **Bad sectors will not be reported by Disk Utility**. Don't take a "Verified" status to indicate that your disk has no hardware problems whatsoever.

"But Disk Warrior/Tech Tool/[other third-party utility] says the hardware is fine, I'm sure the hardware is fine!"

There are no hardware diagnostic utilities on the market that will inform you of a problem with a cable, port, or enclosure, or report a bug in the firmware of a hard drive or SSD. The tools currently available on the Mac platform will inform you of software-based filesystem problems, media failure, and the results of SMART diagnostics which are specific to the hard drive device inside of an enclosure. While these tools are great at identifying the problems within that scope, the inability to detect problems with a cable, port, or enclosure, or a firmware bug on a hard drive, leaves a gaping hole that can only be filled with old-fashioned troubleshooting — isolate components, rule out variables, run multiple tests.

Other factors that can lead to stalls

Hardware is often the culprit when a backup task stalls, but sometimes other software can interfere with a backup task and even cause the whole system to stall. If you are using an external hard drive enclosure that came with custom software, try disabling or uninstalling that software before trying your next backup task. Otherwise, reboot your Mac while holding down the Shift key to boot into Safe Boot mode. Third-party software is disabled in Safe Boot mode, so if the backup task runs successfully in Safe Boot, there is likely a third-party application causing some interference.

Related

- Uninstalling Seagate diagnostic utilities alleviates hangs <https://bombich.com/kb/discussions/cant-restore-image>
- Some third-party storage drivers may cause hardware misbehavior <https://bombich.com/kb/ccc6/some-third-party-storage-drivers-may-cause-hardware-misbehavior>
- We have received several reports that ProSoft's Drive Pulse software can cause the backup task to stall. Disabling scanning of the CCC destination volume should effectively resolve the

problem, however we have received one report in which that was not effective. Uninstalling Drive Pulse did resolve the stall in that case.

Additionally, some hard drive enclosures respond poorly to sleep/wake events. If the problems that you are encountering tend to occur only after your system has slept and woken, you should try a different hard drive enclosure or interface to rule out enclosure-specific sleep problems.

Troubleshooting Media errors

Read errors are typically a result of media damage — some of the sectors on the hard drive have failed and macOS can no longer read data from them. Read errors can occur on the source or destination volume, and they can affect old disks as well as brand-new disks – even SSDs and NVMe storage. **When read errors occur, the file or files that are using the bad sector must be deleted.** Bad sectors are spared out — permanently marked as unusable — only when the files on those sectors are deleted.

If CCC has reported dozens or hundreds of files that are unreadable due to media errors, we recommend replacing the affected hard drive because it is likely failing. Small numbers of unreadable files, however, are not necessarily an indication that a hard drive is failing. The steps below indicate how to resolve media errors.

1. Click on the affected item in the Task History window, then click on the **Reveal in Finder** button.
2. Move the affected files and/or folders to the Trash.
3. Empty the Trash.
4. If you had to delete items from your source volume, locate those items on your backup volume and copy them back to the source (if desired).†
5. If CCC reported problems with more than a few files or folders, we strongly recommend that you reformat the affected disk in Disk Utility.

† If you're looking for an item that is hidden in the Finder, press Command+Shift+Period to toggle the Finder's display of hidden items.

Once you have deleted the affected files, you should be able to re-run your backup task with success.

Note: If you do not have a backup of the affected files, please scroll to the top of this document and exhaust the hardware-based troubleshooting techniques first. As indicated above, read errors are *typically* a result of media damage. In some rare cases, though, media errors can be errantly reported when a hardware-based problem exists (e.g. a bad port, cable, or enclosure). If deleting your only copy of a file is the suggested resolution, then it's prudent to rule out everything else as the cause of an issue before deleting that file.

Errors on read or write that are caused by physical drive malfunction

If your source or destination hard drive is experiencing a significant physical malfunction (errors that go beyond "input/output" read errors described above), you may have a narrow window of opportunity to back up the data from that disk to another hard drive. Time is precious; components could fail at any moment rendering the drive completely unmountable. Read activity is stressful on a dying volume, especially a full-volume backup. We recommend that you immediately back up the files that are most important to you. When you have backed up the most important data, next try to do a full-volume backup. When you have recovered as much data as possible, we recommend that you replace the affected hard drive.

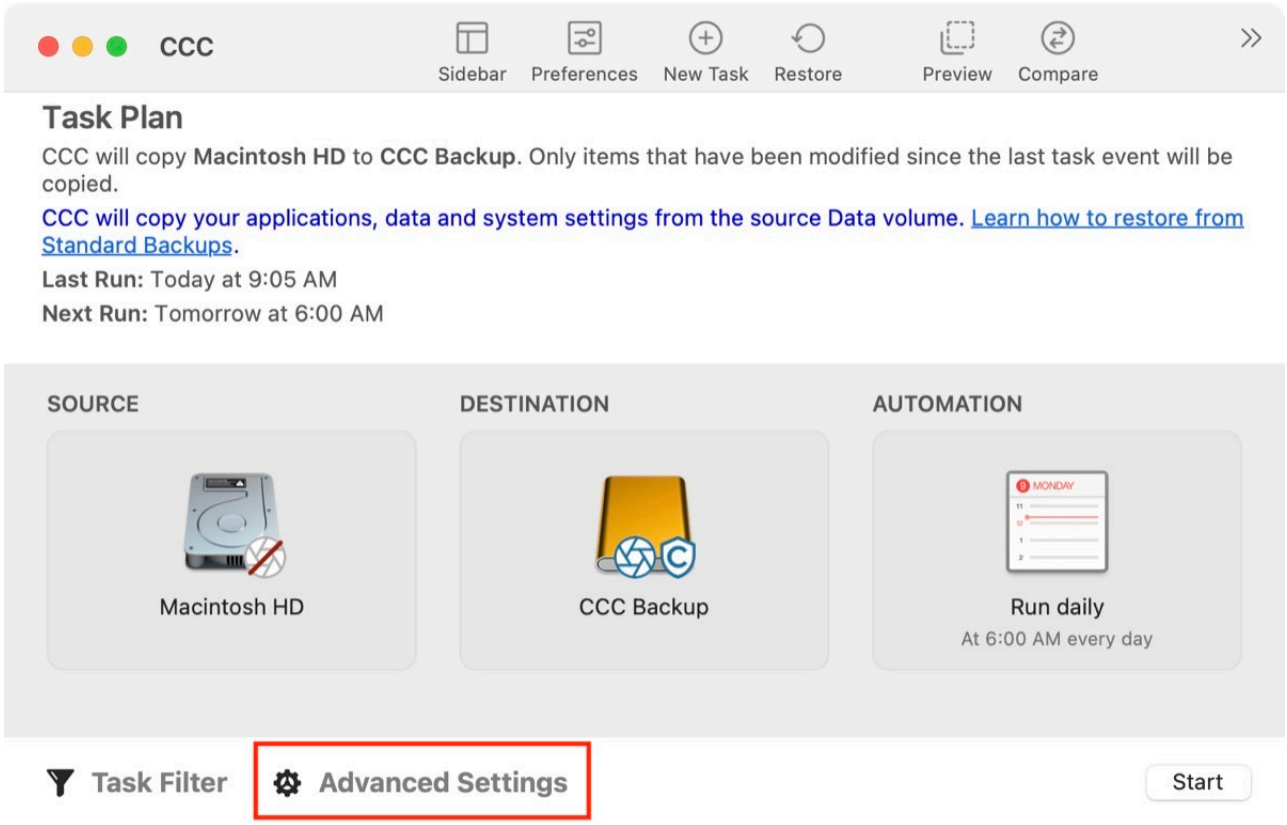
What if the dying drive's volume won't mount?

More often than not, you're completely out of luck. You may be able to revive a hard drive for small amounts of time by letting the drive cool down (somewhere cool and dry, not cold) and then powering it up attached to a service workstation (i.e. don't attempt to boot from it, you may not have enough time).

Advanced Topics

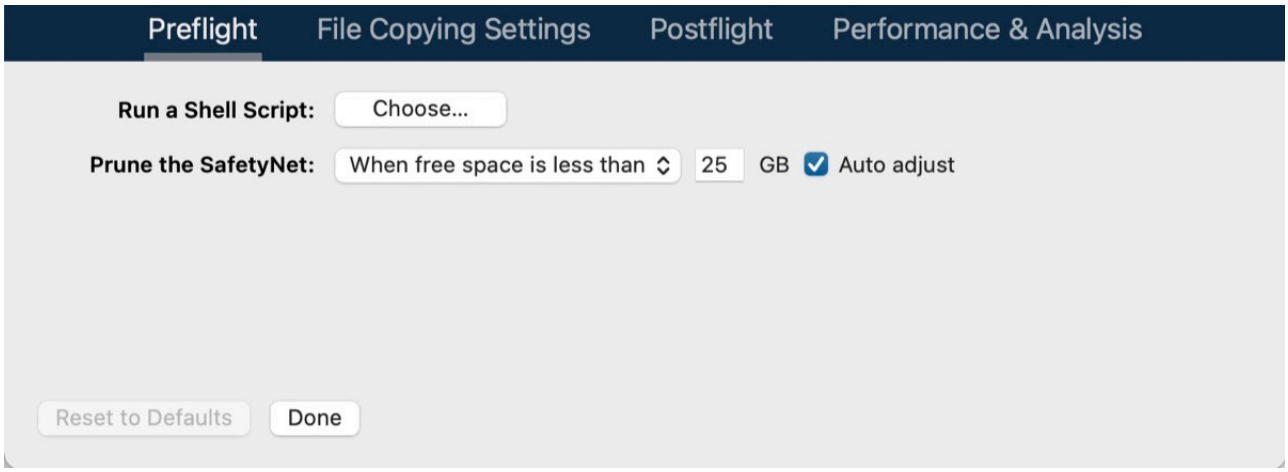
Advanced Settings

To access the advanced settings, click the **Advanced Settings** button at the bottom of the window.



The "gear" icon to the left of the Advanced Settings button will be red if any advanced settings have been customized from the default settings.

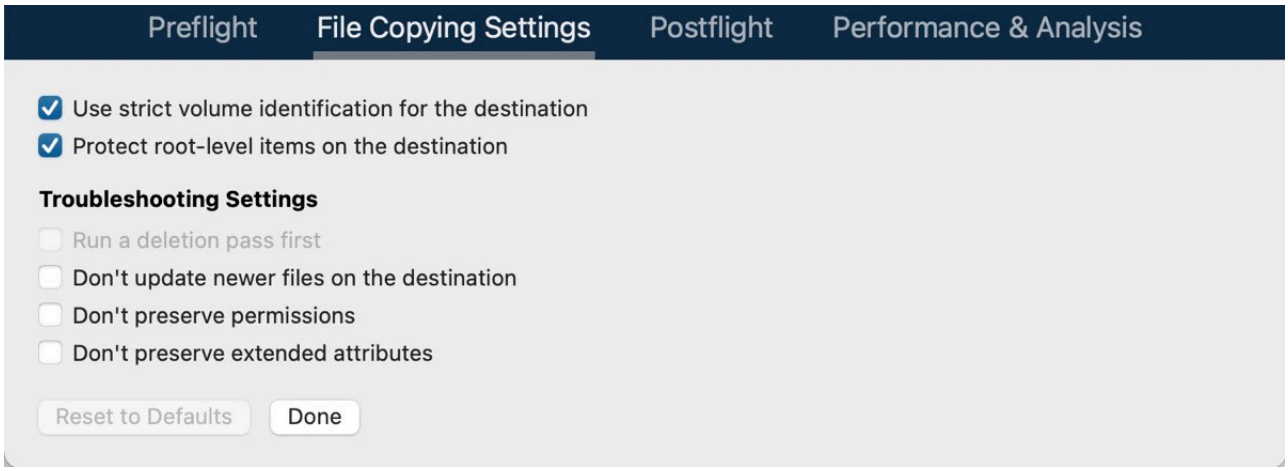
Preflight



See these two sections of documentation for detailed information about the settings available in the Preflight tab:

- Performing actions Before and After the backup task <https://bombich.com/kb/ccc6/performing-actions-before-and-after-backup-task>
- Automated maintenance of the CCC SafetyNet folder <https://bombich.com/kb/ccc6/automated-maintenance-ccc-safetynet-folder>

File Copying Settings



Use strict volume identification

By default, CCC uses the name and Universally Unique Identifier (UUID <https://en.wikipedia.org/wiki/Uuid>) of your source and destination to positively identify those volumes. By verifying both of these identifiers, there is less risk in, for example, backing up to a volume that has the same name as your usual destination but is not actually the destination.

While beneficial, this behavior can sometimes have the wrong result. For example, if you rotate between a pair of external hard drives, CCC will not back up to both of them even though they have the same name (e.g. **Offsite Backup**). CCC will instead claim that the UUID of one of the volumes does not match that of the originally chosen destination.

To accommodate a "rotating pair of backup volumes" solution, you can uncheck this option to indicate that CCC should only use the volume name to identify the destination volume. When deselecting this option, be vigilant that you do not rename your destination volume and that you never attach another non-backup volume to your Mac that is named the same as your destination volume.

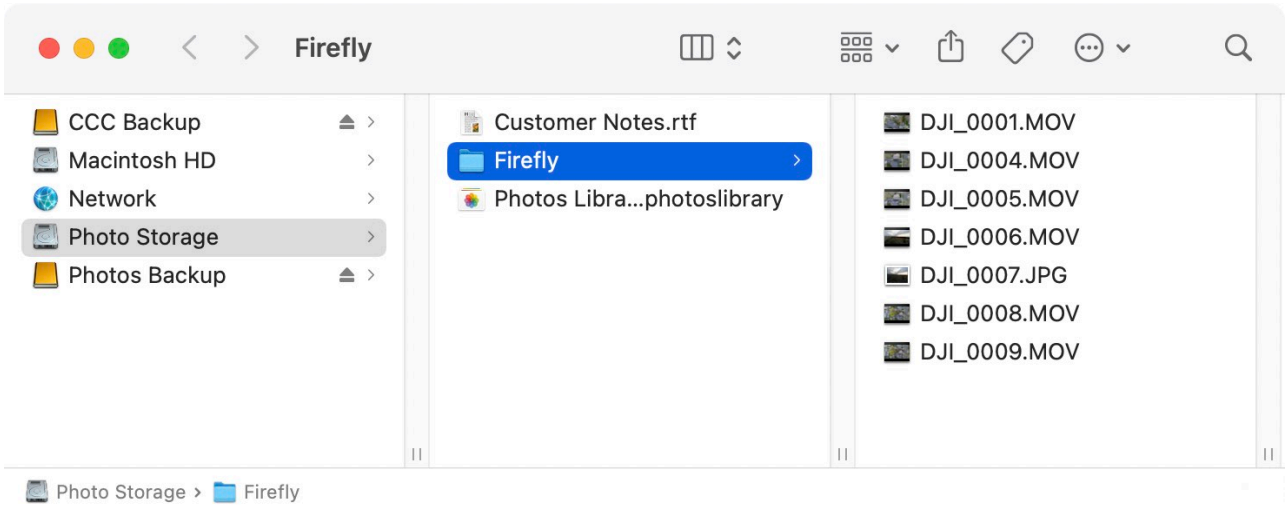
This option is automatically disabled when the destination volume does not have a UUID. Network volumes and some third-party filesystems, for example, do not have volume UUIDs. This option is also disabled if the originally-selected destination device is not attached.

Note: This setting is only applicable to the **destination** volume. CCC **always** uses the name and UUID to positively identify the source volume.

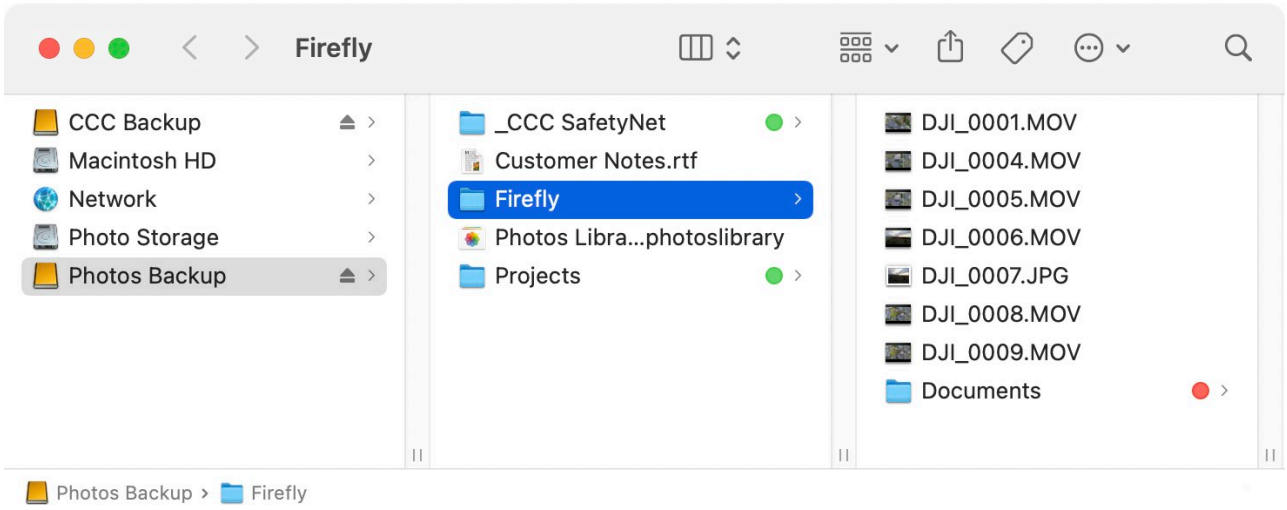
Note: If your rotating destination volumes are encrypted, CCC will only be able to unlock and mount the **original** encrypted volume selected as the destination for your backup task. CCC must have a unique identifier of the destination volume in order to unlock that volume, and CCC will only retain that information about one destination volume for a particular task. If you would like to rotate a pair of backup disks that are encrypted, we recommend using two separate tasks for that purpose; one for each encrypted destination.

Protect root-level items

If you have files and folders that are unique to the root-level on your destination volume and you want them to be left alone, yet you want to keep your backup "clean", use the **Protect root-level items** option. This option is enabled by default when CCC's SafetyNet option is enabled. To understand how this feature works, suppose you have these items on your source volume:



And you have these items on the destination volume:



With the **Protect root-level items** option, the **Projects** folder will **not** be moved to the _CCC SafetyNet folder because it is unique to the root level of the destination. The **Firefly** folder is **not** unique to the root of the destination (it also exists on the source), though, so its contents will be updated to match the source. As a result, the **Documents** folder will be moved to the _CCC SafetyNet folder (or deleted if you have disabled the SafetyNet).

The "root" of the destination refers to the first or top-most folder relative to your **selected** destination. If you selected a volume named **CCC Backup** as the destination, then the root level refers to the root of the volume — what you see when you open that volume in the Finder (the middle pane in the screenshot above). If you selected a folder as the destination for your task, then the "items at the root of the destination" refers to the items that you find in that specific folder that you selected as the destination, not the root of the whole volume. When you select a folder as the destination, anything outside of that folder is completely outside of the scope of the backup task, and will be left alone by that particular backup task.

Run a deletion pass first

This setting is only applicable when using a Remote Macintosh source or destination. In all other cases, CCC will automatically perform a deletion pass when necessary

When the CCC SafetyNet option is disabled, CCC typically deletes unique items from the destination as it encounters them. CCC iterates through the folders on your source alphabetically, so some files are often copied to the destination before all of the files that will be deleted have been deleted from the destination. If your destination volume has very little free space, CCC may not be able to complete a backup to that volume. This option will cause CCC to run a deletion pass through the entire destination before copying files. Use of this option will make your backup task take longer.

This option will only be enabled when the SafetyNet option is disabled.

Don't update newer files on the destination

Files on the source are generally considered to be the authoritative master, and CCC will recopy a file if the modification date is at all different — newer or older — on the source and destination. Occasionally there are circumstances where the modification date of files on the destination is altered after a backup task runs (e.g. by anti-virus applications), and this alteration causes CCC to copy these files every time. This option can work around these circumstances when the root cause of the modification date alteration cannot be addressed.

Don't preserve permissions

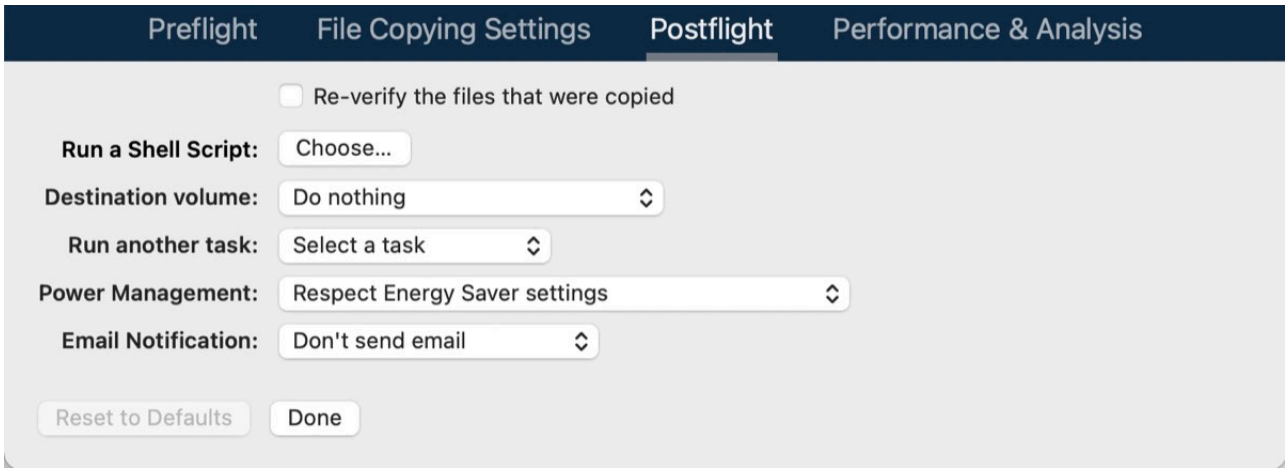
This setting will avoid the errors generated by network volumes that disallow the modification of permissions and ownership on some files. It will also prevent CCC from enabling ownership on the destination volume. Use of this option while backing up applications or macOS system files will prevent those items from working correctly on the destination.

Don't preserve extended attributes

This setting will disable support for reading and writing extended attributes, such as Finder Info, resource forks, and other application-proprietary attributes. Extended attributes store data about the file. Apple explicitly recommends that developers do not store irreplaceable user data in extended attributes when saving a file, because extended attributes are not supported by every filesystem, and could be silently dropped (e.g. by the Finder) when copying a file.

This option is helpful in cases where the source or destination filesystem offers exceptionally poor performance for reading and writing extended attributes, or offers very limited support for macOS native extended attributes such that many errors are reported when trying to copy these metadata.

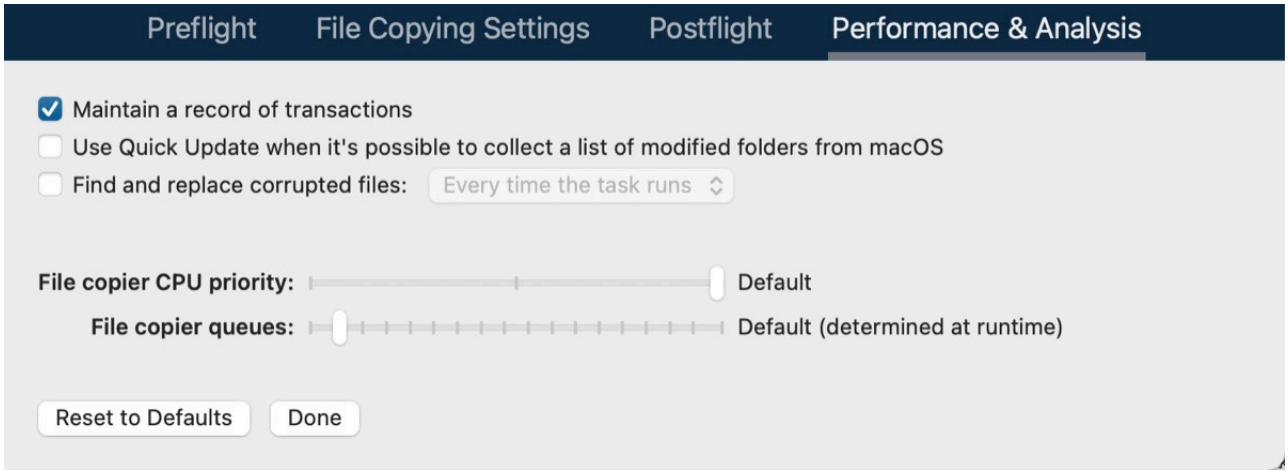
Postflight



See these sections of documentation for detailed information about the settings available in the Postflight tab:

- Postflight verification: Verify files that were copied during the current task event <https://bombich.com/kb/ccc6/how-verify-or-test-your-backup#postflight>
- Performing actions Before and After the backup task <https://bombich.com/kb/ccc6/performing-actions-before-and-after-backup-task>

Performance & Analysis



Maintain a record of transactions

This option enables the collection of a list of files and folders that were modified by each task event. See these articles for more information about CCC's collection and use of transactions:

- Audits: Viewing details about the modifications made by the backup task <https://bombich.com/kb/ccc6/how-find-out-when-backup-last-ran-ccc-task-history#transactions>
- Transaction privacy and disabling transaction collection <https://bombich.com/kb/ccc6/how-verify-or-test-your-backup#disable_transactions>

"Maintain a record of transactions" is not available for "Remote Macintosh" tasks

The collection of transactions relies on functionality that is only available in CCC's new file copier. Remote Macintosh tasks use the legacy file copier, so cannot store records of the files that were copied.

Use Quick Update when it's possible to collect a list of modified folders from macOS

macOS operates a service that tracks filesystem activity on locally-attached volumes. This "FSEvents" service can be queried to get a list of folders that have been modified since a particular time. When this feature is enabled, the CCC task will limit its enumeration of the source to only the folders that were modified since the last time this particular task ran successfully. This feature can greatly decrease the overall run time for each backup task event, especially in cases where your source has a very high file count, and a large number of folders that are not modified frequently.

This feature assumes that the destination is not modified outside of the task's purview. This is not an insignificant assumption, and that's why this feature is disabled by default. You must assess your usage of the destination when deciding whether to use this feature. If you make modifications to the destination outside of CCC, or by another CCC backup task, then those modifications may not be accommodated for (or corrected, for example, if you deleted something from the destination) when this feature is enabled.

If you ever want to verify that the destination is whole, you can click the **Standard Copy** button (adjacent to the **Start** button) to have CCC do a one-time enumeration of the entire source and destination.

Sometimes the Quick Update feature will be overridden in favor of a full audit of the destination

CCC will perform a full audit of the destination in lieu of the Quick Update feature in the following situations:

- If the source or destination selection is modified, or if any changes are made in the Task Filter window
- If the source is unable to produce a list of filesystem change events dating back to the start time of the last successful task event
- If the task has not completed successfully within the last two weeks
- When a backup task ends with errors, CCC will retrieve FSEvents dating back to the start time of the last successful task event.

Tip: Right-click on the table header in the Task History window, then enable the "Settings" column to see an indication of when Quick Update or Backup Health Check was applied to a particular task event.

Quick Update and the "Disable strict volume identification" setting

If you are using a "rotating" pair of backup devices for a single task, i.e. using the "Disable strict volume identification" setting, note that Quick Update will be ignored every time the destination volume's unique identifier has changed since the previous task event. If you would like to use Quick Update with a pair of rotating backup volumes, we recommend that you configure separate tasks for each destination.

Quick Update requires a locally-attached, APFS or HFS+ formatted source, and is not available for "Remote Macintosh" tasks

The Quick Update feature relies on functionality that is only available in CCC's new file copier. Remote Macintosh tasks use the legacy file copier, so cannot take advantage of the Quick Update feature.

Additionally, the Quick Update feature draws information from the macOS FSEvents service. CCC will

only make FSEvents queries to an APFS or HFS+ formatted source volume. Tasks that specify a network volume as a source cannot use the Quick Update feature.

Quick Update can be periodically audited with the "Find and replace corrupted files" setting or a "Standard Copy"

The Quick Update feature and the "Find and replace corrupted files" settings were designed to complement each other. Quick Update provides a way to quickly determine the files that were modified since a previous task – trusting the changes reported by a macOS service, while "Find and replace corrupted files" offers a more thorough, "trust but verify" analysis of changes to both the source and destination. If you use the Quick Update feature, we recommend that you complement this feature with a weekly or monthly audit by the "Find and replace corrupted files" setting (the time-based application of that feature is available in the popup menu to its right), or by periodically clicking the **Standard Copy** button.

Find and replace corrupted files, "Backup Health Check"

See this Kbase article for additional details on the "Find and replace corrupted files" option:

- Backup Health Check: Verify before copying, automatically replace corrupted destination files <https://bombich.com/kb/ccc6/how-verify-or-test-your-backup#bhc>

File copier CPU priority

By default, CCC runs its file copier at the default CPU priority for maximum performance. If you find that your backups have a noticeable impact on system performance, you can either schedule your tasks to run at a more convenient time, or you can reduce the CPU priority of the file copier. This will generally make the task take longer, but the task should have a less noticeable impact on system performance.

File copier queues

When your task runs, CCC decides how much concurrency is appropriate for your selected source and destination devices. If both the source and destination can be identified as Solid State devices, CCC will simultaneously process up to four folders at once, and copy up to eight files at a time. In other cases, CCC will simultaneously process two folders and two files at a time. If you have solid state media in an enclosure that hides the hardware details (or in a NAS device), you may find that you get better performance from your task by increasing the number of file copier queues. See this section of CCC's documentation for additional insight into the File copier queues setting:

- CCC's file copier is tuned for modern, high performance storage <https://bombich.com/kb/ccc6/performance-suggestions#cce>

Addressing Common Performance Problems

There are several factors that affect the performance of your backup tasks. Here we describe the most common conditions that affect backup performance, and offer some suggestions for mitigating the effects of those conditions.

Use CCC's Quick Update feature

The Quick Update <https://bombich.com/kb/ccc6/advanced-settings#quickupdate> feature can greatly reduce the amount of time it takes to compare items on the source and destination. Rather than evaluating all files and folders in the source data set, CCC will collect a list of folders that have been modified since the last backup task from the macOS FSEvents service. Especially for data sets with a lot of small files in folders that are infrequently modified, this feature can improve performance by many orders of magnitude. Click the **Advanced Settings** button at the bottom of the CCC window, then you'll find the Quick Update option in the **Performance & Analysis** tab.

Reduce the number of files considered for backup

If the aforementioned Quick Update feature is not applicable (e.g. because the source volume doesn't support it), and if you have a particularly high number of files on your source volume, you may be able to reorganize your data set and apply some exclusions to improve task performance. For example, if you have a large number of files that never change (perhaps some old, completed projects), you can collect these into a folder named "Archives", back it up once, then exclude it from future backups. CCC will not delete excluded items from your destination (unless you configure the Task Filter to do so), so as long as you keep the original on your source volume, you will always have two copies of your archived content. Because these items are excluded from your daily backups, CCC will not spend time enumerating through those files for changes.

Related Documentation

- Excluding files and folders from a backup task <https://bombich.com/kb/ccc6/excluding-files-and-folders-from-backup-task>
- Folder-to-Folder Backups <https://bombich.com/kb/ccc6/folder-folder-backups>

Trim unnecessary content from the backup task

macOS is constantly touching log and cache files, and those files can add up to a lot of changes for every backup task. Take a moment to review your task audits to see if there is content that doesn't have to be backed up. A few minutes reviewing the audit can add up to lots of time shaved off your regular backups.

1. Click **Task History** in the toolbar to open CCC's Task History window
2. Select one of your regularly-recurring task events
3. Click on the **Audit** tab in the center of the window
4. Sort the list by **Size**, then browse through the changes
5. If you see something in the audit that you don't feel needs to be backed up, especially cache folders with a particularly high file count or a large amount of data, right-click on the item and choose the option to exclude it from the backup task.

Related Documentation

- Audit: Viewing details about the modifications made by the backup task <https://bombich.com/kb/ccc6/how-find-out-when-backup-last-ran-ccc-task-history#audit>

Avoid simultaneous writes to the same destination

When two tasks are writing to the same destination at the same time, the two tasks will typically take more than twice as long to complete when running at the same time vs. when they are run sequentially. This is particularly true when writing to network volumes, the resulting CPU load on the NAS server can be more than it can handle. CCC offers two features to avoid running automated tasks simultaneously to the same destination:

- Click on the Automation selector for each task and check the box next to **Defer if another task is writing to the same destination**
- Rather than scheduling the individual tasks, place the tasks into a task group <https://bombich.com/kb/ccc6/task-organization>, then configure the group to run on a schedule. The group will then run the tasks sequentially.

Hard drive performance and interface bandwidth

Your backups will be no faster than your slowest disk. Performance will be worse for smaller rotational hard drives (e.g. physically smaller, like those in 2.5" hard drive enclosures), for older hard drives, and for hard drives that are nearly full and thus more likely to be fragmented.

You will also get longer copy times when you have lots of small files vs. a volume filled with just a few very large files. Finally, you will see better performance with faster/more efficient interfaces — USB 3.1 is faster than USB 3.0, USB 3.0 is faster than USB 2.0, etc.

Rotational hard drive performance will diminish as the disk fills up

Sectors on the disk are arranged in concentric circles. On the outside edge of the disk (the "beginning" of the disk), the disk spins faster, so data can be read at a faster rate. On a 5400RPM disk, for example, the linear speed of the outside edge of the disk is about 60 miles per hour. At the center of the disk, the linear speed is just 16 miles per hour – 4 times slower. As such, read performance at the end of the disk is considerably slower. You can easily see this performance difference if you partition a disk in half. The first partition will consistently get much faster performance than the second partition.

Another performance-affecting factor comes into play when a rotational disk gets close to its maximum capacity – fragmentation. As the filesystem becomes fuller, it becomes harder for the filesystem to find large, contiguous blocks to place files, so the filesystem starts to become fragmented. That fragmentation causes the disk to spend more time seeking when retrieving any individual file (because the pieces of the file are scattered all over the disk). Often you can hear this "chattiness" from the disk as the drive head darts back and forth across the disk.

If your source volume is nearly full and is a rotational disk, we recommend that you replace it with a larger hard drive to avoid the performance implications of filesystem fragmentation.

Filesystem performance on rotational devices

The filesystem format applied to your disks can also affect the performance of a backup task. Apple's

legacy HFS+ format, for example, was designed specifically to deal with the performance characteristics of rotational devices – storage at the fastest part of the disk is preallocated for the filesystem metadata so that folder enumeration requests aren't negatively affected by seek activity. When Apple designed its newer APFS filesystem, it designed that filesystem to excel on media that has no seek penalty (SSDs). On rotational media, however, APFS has a distinct performance disadvantage <https://bombich.com/blog/2019/09/12/analysis-apfs-enumeration-performance-on-rotational-hard-drives>, and that difference is most acutely noticed on the slowest rotational devices (e.g. 2.5" "slim" disks, and 5400RPM disks – Western Digital My {anything} and many Seagate Backup disks are among these devices).

Unless you are specifically using a disk to share files with a Mac running an OS older than High Sierra, we recommend using APFS for all backup devices – despite any potential performance disadvantage. The information above is not intended to dissuade you from choosing APFS, rather just to set expectations for performance when using an exceptionally slow rotational device. Disks that were noticeably slow on older OSes will be even slower with APFS applied. Despite the slower performance, however, an APFS backup device will offer better compatibility with the file types on your APFS sources, as well as features that are exclusive to APFS (e.g. filesystem snapshots, support for encryption).

If you're finding performance on an older/slower backup disk to be exceptionally poor, we recommend replacing the disk with something faster. An SSD is not required, but when shopping for a rotational disk, we recommend that you avoid the "slim" disks.

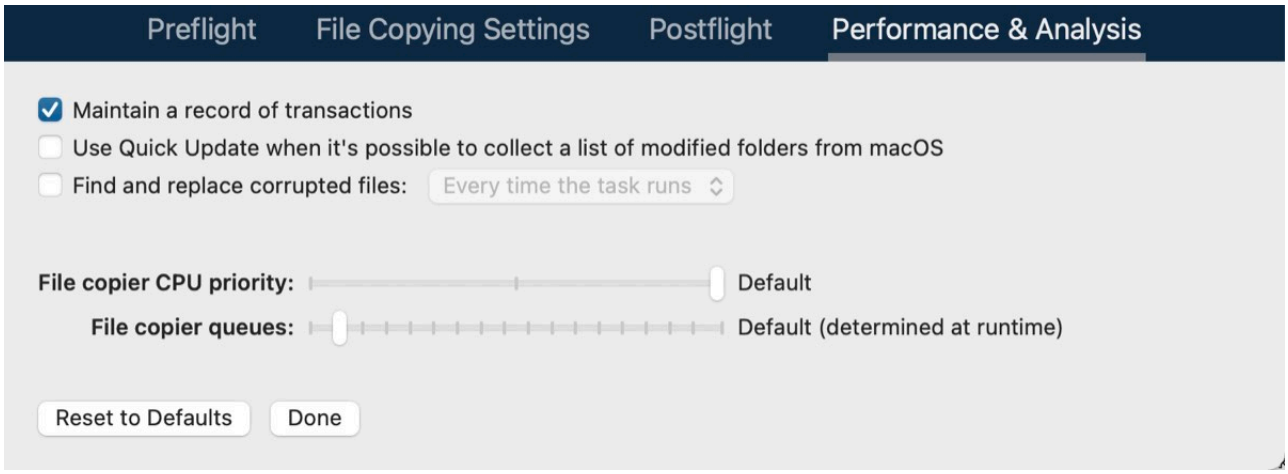
Related Documentation

- Choosing a backup drive: Devices that we recommend <https://bombich.com/kb/ccc6/choosing-backup-drive#recommendations>

CCC's file copier is tuned for modern, high performance storage

When we developed our new file copier in CCC v6, one of our design goals was to take full advantage of the performance that is available from modern SSD and NVMe storage devices. The CCC "Core Copy Engine" will process up to four folders at once, and copy up to eight files at a time by default when both the source and destination devices can be positively identified as APFS-formatted solid state devices. This multi-threaded approach yields blazing-fast transfers of very large amounts of data between fast devices – typically exceeding CCC v5's legacy file copier performance by 50% or more, and meeting or exceeding Finder copying performance.

When CCC cannot identify a device as a solid state device, CCC throttles back the concurrency of its file copier to a default that works better for rotational media. In these cases, CCC will still evaluate up to four folders at once, but it will only copy 1-2 files at a time (depending on file size). If you have a solid state device placed into a generic USB hard drive enclosure, that enclosure won't identify the media type to macOS, and you won't see the full potential of that device when using it with CCC. In those cases, you can improve performance by manually increasing the "File copier concurrency" setting in Advanced Settings > Performance & Analysis:



CCC sometimes uses the APFS clonefile function to use storage space more efficiently

If both the source and destination are APFS-formatted, and CCC can verify that they are both solid state devices, then CCC uses a special procedure to handle updates to files that are larger than 1GB. For this procedure, CCC will create a duplicate of the existing file on the destination using the "clonefile" function of the APFS filesystem. At this point, the duplicate copy doesn't consume any additional disk space because it's a "clone" of the original destination file. CCC will then open the source and cloned destination file and proceed through them one block at a time to compare the blocks. If a block differs, it's copied, if not, the existing block is left in place. When the cloned destination file is completely updated, the original file on the destination is deleted. Any space consumed by blocks that aren't used by the cloned file will be freed (or retained in a snapshot, if applicable).

The benefit of using this procedure can be quite substantial when snapshot support is enabled on the destination volume. Consider two alternatives. Suppose you have a 40GB VM container file that changes every day, but only about 1GB of data within that file changes in any given day. If CCC were to recopy that whole file every time it changes, then every snapshot would uniquely reference at least 40GB of disk space. This will add up quickly, and will impose a lower practical limit on the number of snapshots that can be retained. When using the clonefile procedure, however, only the blocks that have been modified on the source will be modified on the destination, so the 1GB of daily changes to that VM container file will have a very low net impact on snapshot disk usage.

The clonefile procedure has great benefits for using storage space more efficiently, however it is not a *faster* procedure than simply recopying the file. The performance of this procedure on rotational media is poor enough to make it impractical, and even on solid state media, we chose to limit the procedure based on file size so that we're only taking a performance hit when there is a large potential storage efficiency benefit.

Spotlight Indexing

Anything that causes CCC to compete for bandwidth to your source or destination volume will increase the amount of time that it takes to back up your data. Spotlight indexing is one such process that CCC typically must compete with for disk bandwidth. As you copy new data to your destination volume, for example, Spotlight wants to read those "new" files so it can index their contents. Having a Spotlight index of your backup volume may be unnecessary as you probably want to search for files only on your source volume.

To disable Spotlight indexing on a volume that is dedicated to backup, open the **System Settings**

application, select **Siri & Spotlight** in the sidebar, scroll to the bottom of the window and click **Spotlight Privacy…**. Drag the icon of the destination volume into the "Privacy" table. If you do want the backup volume indexed, drag its icon out of the "Privacy" table after the backup completes and indexing will start immediately.

Find and replace corrupted files

CCC offers an advanced option to "Find and replace corrupted files" <https://bombich.com/kb/ccc6/advanced-settings#checksum>. When using this option, CCC will re-read every file on the source and every file on the destination, calculating a checksum of each file. CCC then compares these checksums to see if a file should be recopied. While this is an excellent method for finding unreadable files on the source or destination, it will dramatically increase the amount of time that your backup task takes, and it will also increase CPU and hard drive bandwidth consumption on your Mac. We recommend limiting the use of this option to weekly or monthly, or to one of the other options offered in the popup menu adjacent to that setting.

Other applications and conditions that can lead to performance problems

Over the years we have received numerous queries about poorer performance than what is expected. Careful analysis of the system log and Activity Monitor will usually reveal the culprit. Here are some things that we usually look for:

- Other backup software copying simultaneously to the same volume, a different volume on the same disk, or across the same interface as CCC's destination.
- Utilities that watch filesystem activity and do things when file changes are detected. Antivirus software <https://bombich.com/kb/ccc6/antivirus-software-may-interfere-backup> is a common culprit, but we have also seen problems caused by other watcher applications, such as memeod and Western Digital's SmartWare.
- Slow interfaces — **USB hubs (including the ports on a USB keyboard or display) and even some USB cables can reduce the bandwidth to your disk dramatically**. If you're using USB, be sure that your device is plugged directly into one of the USB ports on your Mac.
- Using a wireless network connection to connect to a network volume. If you're seeing poor performance with a wireless connection, compare the performance when using a wired (ethernet) connection.
- Third-party USB device drivers can reduce the performance and/or reliability of your USB storage devices <https://bombich.com/kb/ccc6/some-third-party-storage-drivers-may-cause-hardware-misbehavior>. Examples include the "SAT-SMART" drivers, as well as some ancient BlackBerry drivers.
- Symantec's Digital Loss Prevention (DLP) can cause performance problems when backing up a specific Microsoft font cache (e.g. /Users/yourname/Library/Containers/com.microsoft.Outlook/Data/Library/Application Support/Microsoft/FontPreviewCache). The problem appears to be specific to DLP's ability to cope with the dorky emojis that Microsoft uses in the file names in this folder (i.e. replacing the word "family" with the family emoji). Exclude that FontPreviewCache folder from your backup task <https://bombich.com/kb/ccc6/excluding-files-and-folders-from-backup-task> to avoid the performance problem.

If you're still having trouble identifying a performance problem, we're here to help <https://bombich.com/software/get_help>.

Related Documentation

- Troubleshooting slow performance when copying files to or from a network volume <https://bombich.com/kb/ccc6/troubleshooting-slow-performance-when-copying-files-or-from-network-volume>...

Using the Dynamic Performance Chart to understand factors that affect performance

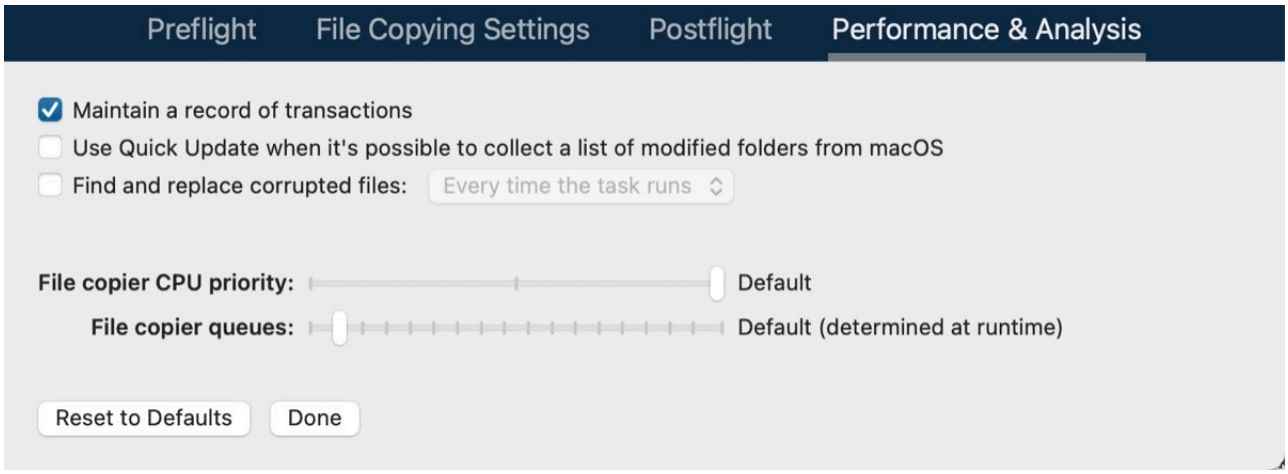
When a task is running, CCC presents a live chart of file evaluation rate (i.e. the number of files compared per second) and data write rate. Hover your mouse over the chart to see the rates at various points on the chart:

File evaluation rate and write rate are often complementary. This dynamic performance chart was designed to show how these two factors relate to each other, and also to show how the characteristics of your source data set interact with the performance characteristics of your source and destination devices. For example, you will find that when CCC is copying very large files, file evaluation rate will be low, but write rate will get very high – close to the maximum bandwidth potential of the destination (if that's slower than the source device's read rate). In contrast, when CCC is processing lots of smaller files, the file evaluation rate will get higher and the write rate will be considerably less than the maximum write rate that is achievable on that device. This is normal – it takes longer to copy a million 1KB files than it would take to copy a single 1GB file, even though you're copying the same amount of data.

The dynamic performance chart will bring NAS protocol performance into sharp focus. While we can typically process thousands of files per second on a locally-attached filesystem, NAS filesystems (e.g. AFP and SMB) can typically process tens or hundreds of files per second. This performance is wholly dependent on the NAS device, its storage, and is also strongly influenced by the overhead of the SMB and AFP protocols. The key to improving performance on a task that involves a NAS device is to reduce the number of filesystem transactions that must occur, and the only way to do that is to reduce the number of files and folders that are compared during the backup task. CCC's Quick Update <https://bombich.com/kb/ccc6/advanced-settings#quickupdate> feature can be instrumental in achieving that goal.

Reducing the impact of a backup task on your Mac's performance and usability

Sometimes backup tasks can have a noticeable impact on system performance. By default, the CPU priority of CCC's file copier will be comparable to that of a foreground application, yielding the fastest possible file copying performance. If you would like to reduce the impact that a particular task has on the system, you can reduce the File copier CPU priority in the **Performance & Analysis** tab of CCC's Advanced Settings.



Pausing a task

If you would like to immediately cease a task's impact on the system without stopping the task altogether, you can pause the task. Click the Pause button adjacent to the Stop button in CCC's main window to pause the task. The CCC Dashboard also offers a Pause button for quicker access to this functionality. Paused tasks will resume automatically after five minutes, or you can click the Continue button to resume the task. The five minute timeout can be adjusted in the Advanced section of CCC's Settings window.

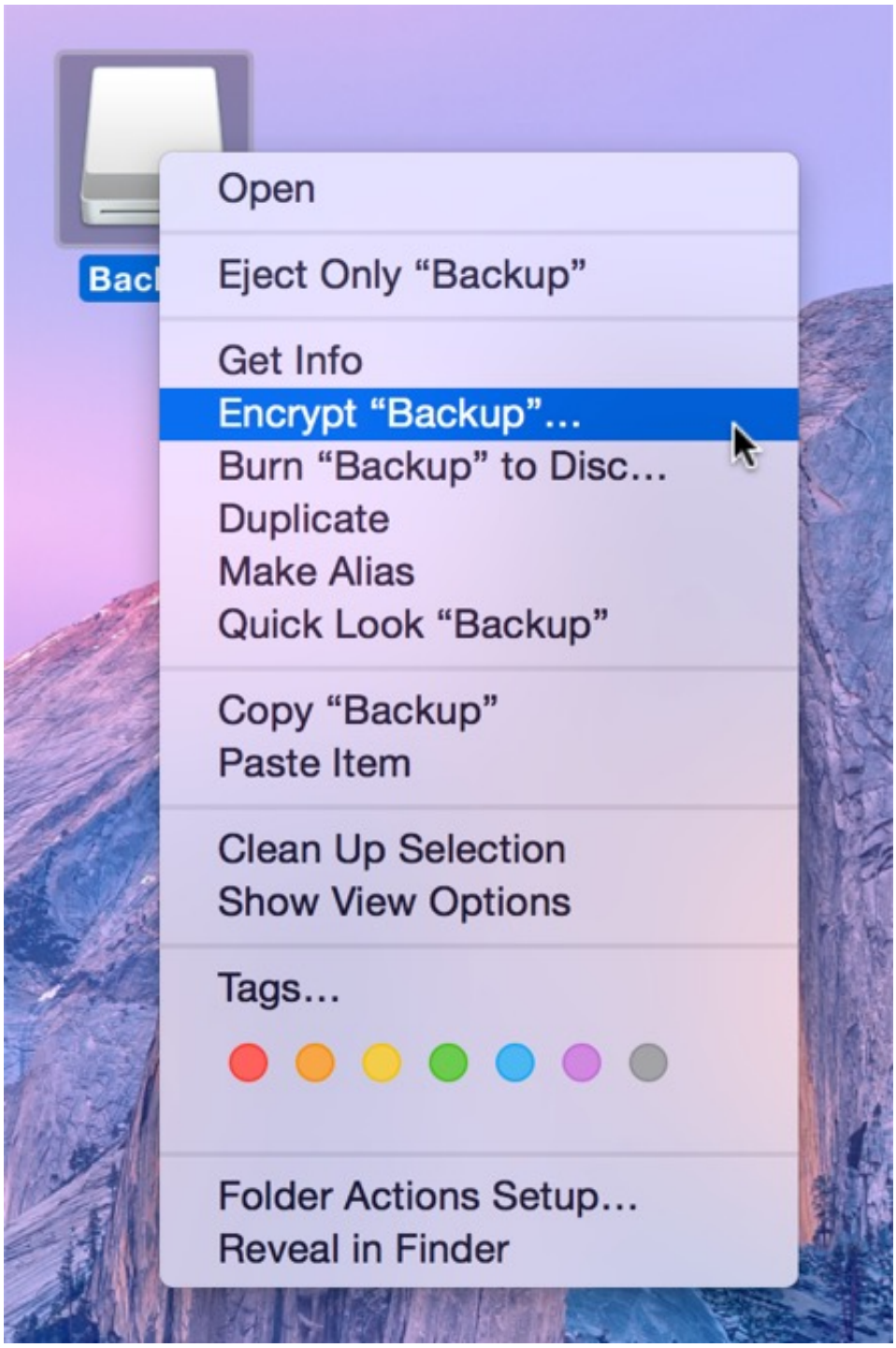
Working with FileVault Encryption

CCC is fully qualified for use with FileVault-protected volumes (HFS+ and APFS, however note that Apple no longer supports creating HFS+ encrypted volumes on Big Sur+).

Standard Backup: Enabling encryption on a volume that will not contain an installation of macOS

If you're not creating a legacy bootable backup, and if you have no intention of installing macOS onto your backup volume, there are two simple options for encrypting the backup:

- New backup: Erase the backup volume as APFS Encrypted in Disk Utility.
- Existing backup: Right-click on the APFS-formatted volume in the Finder and choose the option to encrypt the volume. (Note: If this backup was previously part of a full system backup, Finder will fail with an "Internal error", or indicate "This disk has macOS users". If you see that message, you'll have to erase the volume as APFS Encrypted in Disk Utility instead).



Legacy Bootable Backup: Enabling encryption on a volume that contains (or will contain) an installation of macOS

If your goal is to create a legacy bootable backup that is encrypted, use the following procedure:

1. Follow CCC's documentation to properly format the destination volume <https://bombich.com/kb/ccc6/preparing-your-backup-disk-backup-os-x>. Choose APFS as the format, do **not** format the volume as encrypted.
2. Use CCC to back up your startup disk <https://bombich.com/kb/ccc6/how-set-up-your-first-backup> to the unencrypted destination volume. [Big Sur (and later OS) users, use the

Legacy Bootable Backup Assistant <https://bombich.com/kb/ccc6/cloning-macos-system-volumes-apple-software-restore>]
3. Reboot your Mac while holding down the Option key (Intel Macs) or the Power key (Apple Silicon Macs) and choose your backup disk as the startup disk.
4. Enable FileVault encryption in the **Security & Privacy** preference pane of the System Preferences application.
5. As soon as the encryption conversion procedure begins, you may reboot your Mac — it will automatically reboot from the production startup disk.
6. Configure CCC for regular backups <https://bombich.com/kb/ccc6/how-set-up-scheduled-backup> to your encrypted backup volume.

You do not have to wait for the conversion process to complete before rebooting from your production startup disk

You do not have to wait for the conversion process to complete before using your backup disk. You can simply enable FileVault encryption, then immediately reboot from your primary startup disk and the conversion process will carry on in the background. Encryption will continue as long as the backup disk is attached. macOS doesn't offer a convenient method to see conversion progress, but you can type `fdesetup status -device "/Volumes/CCC Backup" -extended` in the Terminal application to see conversion progress. Some users have found that conversion may not resume until you log in to an admin account while booted from your production startup volume, so try that if conversion appears to be stalled.

Keep your Mac plugged into AC power for the duration of encryption conversion

We have received a handful of reports from macOS Catalina users indicating that encryption conversion remains permanently paused if AC power is removed during the encryption conversion process. We have been unable to reproduce this result in our test lab — typically encryption conversion pauses when AC power is removed, but then resumes when AC power is restored. The number of reports to us, however, suggests that there is some underlying problem that may be new to macOS Catalina. To avoid this result, we recommend that you keep your Mac plugged in to AC power for the duration of encryption conversion. If you see an indication that encryption conversion is paused, try leaving the system plugged into AC overnight.

What if I don't want my personal data to ever be on the destination in unencrypted form?

Enabling FileVault on the destination means that the volume starts out unencrypted, and then over the course of several hours the data is encrypted in place. If the encryption conversion process completes successfully, then for most intents and purposes, no trace of the unencrypted data will be left on that disk. There are some caveats however. If your backup volume is an SSD, and if you **delete** files from the SSD prior to enabling encryption, then the SSD may automatically move the not-yet-encrypted underlying blocks out of rotation (for wear leveling), and those data could be recoverable by experts. Likewise, if the conversion process fails for any reason, then the data on that disk is potentially recoverable. If either of these scenarios is not acceptable, then we recommend that you exclude any sensitive data <https://bombich.com/kb/ccc6/excluding-files-and-folders-from-backup-task> from the initial backup task. Don't exclude your whole home folder — you must include at least one folder from your home directory so that you can log in to that account on the backup.

After you have booted from the backup volume and enabled FileVault, you can then reboot from the production startup disk, remove the exclusions from your backup task, then run the backup task

again to copy the remainder of your data. **Any data that is copied to a volume that is in the midst of encryption conversion will be encrypted immediately.**

Note for Big Sur (and later OSes) users: Do not use the Legacy Bootable Backup Assistant to configure your initial backup task, you will not be able to exclude content from a Full Volume Clone. After the initial Standard Backup has completed, proceed to install macOS onto the destination <https://bombich.com/kb/ccc6/creating-and-restoring-data-only-backups#install_macos>. After installation has completed, enable FileVault, then reboot from your production startup disk and run your CCC backup task again without the exclusions.

Related Documentation

- Frequently Asked Questions about encrypting the backup volume <https://bombich.com/kb/ccc6/frequently-asked-questions-about-encrypting-backup-volume>
- The Disk Center <https://bombich.com/kb/ccc6/disk-center>
- [Apple Kbase] Learn more about FileVault <https://support.apple.com/kb/HT4790>

"A recovery key has been set by your company, school, or institution"

If you migrated data from a Mac that had an institutionally-managed FileVault Recovery key, the presence of that key can prevent you from enabling FileVault. You can remove that key in the Terminal application:

```
sudo rm -f /Library/Keychains/FileVaultMaster.cer /Library/Keychains/FileVaultMaster.keychain
sudo fdesetup removerecovery -institutional
sudo fdesetup changerecovery -personal
```

Then proceed with the instructions above to enable FileVault in System Preferences.

Additionally/alternatively, you can exclude the /Library/Keychains/FileVaultMaster.cer and /Library/Keychains/FileVaultMaster.keychain files from your CCC backup task to avoid copying those to your backup disk.

Some files and folders are automatically excluded from a backup task

CCC maintains a list of certain files and folders that are automatically excluded from a backup task. The contents of this list were determined based on Apple recommendations and years of experience. The following is a list of the items that are excluded along with an explanation of why they are excluded.

Legend:
Items prefixed with a "/" indicate that they will only be ignored if located at the root of the volume.
Items postfixed with a "/*" indicate that only the contents of those folders are ignored, the folders themselves will be copied.
Items postfixed with a "*" indicate that the filename will be matched up to the asterisk.

Filesystem implementation details

- .HFS+ Private Directory Data*
- /.journal
- /.journal_info_block
- .afpDeleted*
- ._*
- .AppleDouble
- .AppleDB
- /lost+found
- Network Trash Folder
- .TemporaryItems

These items only show up if you're running an older OS than what was used to format the source volume, and on some third-party implementations of AFP and SMB network filesystems. These items should never, ever be manipulated by third-party programs.

Volume-specific preferences

- .metadata_never_index
- .metadata_never_index_unless_rootfs
- /.com.apple.timemachine.donotpresent
- .VolumeIcon.icns
- /System/Library/CoreServices/.disk_label*
- /TheVolumeSettingsFolder
- /private/var/db/dslocal/nodes/Default/secureaccesstoken.plist

These items record volume-specific preferences, e.g. for Spotlight, Time Machine, and a custom icon for the volume. Feedback on the exclusion of these items is welcome <https://bombich.com/software/get_help>. Because they are volume-specific preferences, the exclusion of these items from a day-to-day backup seems most appropriate.

Apple-proprietary data stores

- .DocumentRevisions-V100*
- .Spotlight-V100
- Library/Metadata/CoreSpotlight
- /.fseventsd
- /.hotfiles.btree
- /private/var/db/systemstats
- /private/var/db/ConfigurationProfiles/Store
- /private/var/folders/*/*/C
- /private/var/folders/*/*/T
- /Users/*/Library/Caches
- /Users/*/Library/Containers/*/Data/Library/Caches
- /private/var/folders/*/*/0/com.apple.nsurlsessiond
- /System/Library/AssetsV2/analytics
- Library/CloudStorage/*/.tmp

These items are Apple-proprietary data stores that get regenerated when absent. Their respective apps typically reject these items when restored from a backup and will recreate them as necessary.

The DocumentRevisions data store is used by the Versions feature in macOS. The Versions database stored in this folder contains references to the inode of each file that is under version control. File inodes are volume-specific, so this dataset will have no relevance on a backup volume.

Volume-specific cache files

- /private/var/db/dyld/dyld_*
- /System/Library/Caches/com.apple.bootstamps/*
- /System/Library/Caches/com.apple.corestorage/*

Copying these caches to a new volume will render that volume unbootable. The caches must be regenerated on the new volume as the on-disk location of system files and applications will have changed. macOS automatically regenerates the contents of these folders when CCC is finished updating the backup volume.

NetBoot local data store

- /.com.apple.NetBootX

In the unlikely event that your Macintosh is booted from a Network device, macOS will store local modifications to the filesystem in this folder. These local modifications are not stored in a restorable format, therefore should not be backed up. In general, you should not attempt to back up a NetBooted Mac.

Dynamically-generated devices

- /Volumes/*
- /dev/*
- /automount
- /Network
- /.vol/*
- /net

These items represent special types of folders on macOS. These should not be backed up, they are dynamically created every time you start the machine.

Quota real-time data files

- /.quota.user
- /.quota.group

When these files are copied to a destination volume using an atomic file copying procedure, the macOS kernel will prevent the destination from being gracefully unmounted. The contents of these files is never accurate for the destination volume, so given the kernel's unruly behavior with copies of these files, CCC excludes them. According to the quotacheck man page, these files **should** be regenerated every time a quota-enabled volume is mounted (e.g. on startup). We have not found that to be consistently true. If you're using quotas, run sudo quotacheck / after restarting from your backup volume or a restored replacement disk to regenerate these files.

Large datastores that are (or should be) erased on startup

- /private/var/vm/*
- /private/tmp/*
- /cores
- /macOS Install Data
- /.PKInstallSandboxManager
- /Library/InstallerSandboxes/.PKInstallSandboxManager
- /.PKInstallSandboxManager-SystemSoftware

macOS stores virtual memory files and your hibernation image (i.e. the contents of RAM are written to disk prior to sleeping) and temporary items in these folders. Depending on how you use macOS and your hardware configuration, this could be more than 50GB of data, and all of it changes from one hour to the next. Having this data for a full-disk restore does you absolutely no good — it makes the backup and restore processes take longer and the files get deleted the next time you boot macOS.

Trash

- .Trash
- .Trashes

Moving an item to the trash is typically considered to be an indication that you are no longer interested in retaining that item. If you don't want CCC to exclude the contents of the Trash, you can modify each task's filter:

1. Click **Task Filter** at the bototm of the window
2. Uncheck the box in the sidebar next to **Don't copy the Finder's Trash**
3. Click the **Done** button

Time Machine backups

These folders store Time Machine backups. Time Machine uses proprietary filesystem devices that Apple explicitly discourages third-party developers from using. Additionally, Apple does not support using a duplicated Time Machine volume and recommends instead that you start a new Time Machine backup on the new disk.

- /Backups.backupdb
- /.MobileBackups
- /.MobileBackups.trash

- /private/var/db/com.apple.backupd.backupVerification

Corrupted iCloud Local Storage

iCloud leverages folders in your home directory for local, offline storage. When corruption occurs within these local data stores, macOS moves/renames the corrupted items into the folders indicated below. macOS doesn't report these corrupted items to you, nor does it attempt to remove them. CCC can't copy the corrupted items, because they're corrupted. To avoid the errors that would occur when trying to copy these corrupted items, CCC excludes the following items from every backup task:

- Library/Mobile Documents.* [Note: This exclusion is specific to Mobile Documents.{something} folders that have a corruption suffix, not to the non-corrupted "Mobile Documents" folder]
- .webtmp

Special files

Files included in this section are application-specific files that have demonstrated unique behavior. The kacta and kactd files, for example, are created by antivirus software and placed into a special type of sandbox that makes them unreadable by any application other than the antivirus software.

The "com.apple.loginwindow" item can be found in each user home folder. Excluding this item prevents the applications that were open during the backup task from opening when you boot from a restored backup. This seems appropriate considering that Apple intends the feature to be used to open the applications that were in use when you log out, restart or shutdown, not at an arbitrary point during the backup task.

- /private/tmp/kacta.txt
- /private/tmp/kactd.txt
- /private/var/audit/*.crash_recovery
- /private/var/audit/current
- /Library/Caches/CrashPlan
- /PGPWDE01
- /PGPWDE02
- /.bzvol
- /Library/Backblaze.bzpkg/bzdata/bzvol_system_volume/bzvol_id.xml
- /.cleverfiles
- /Library/Application Support/Comodo/AntiVirus/Quarantine
- /private/var/spool/qmaster
- $Recycle.Bin
- @Recycle
- /@Recently-Snapshot
- .Transporter Library
- Library/Preferences/ByHost/com.apple.loginwindow*
- .dropbox.cache <https://www.dropbox.com/help/desktop-web/cache-folder>
- /private/var/db/atpstatdb*
- Library/Logs/Acronis
- .@__thumb
- /.com.prosofteng.DrivePulse.ignore
- com.apple.photolibraryd/tmpoutboundsharing
- /Library/Application Support/Fitbit Connect/Minidumps

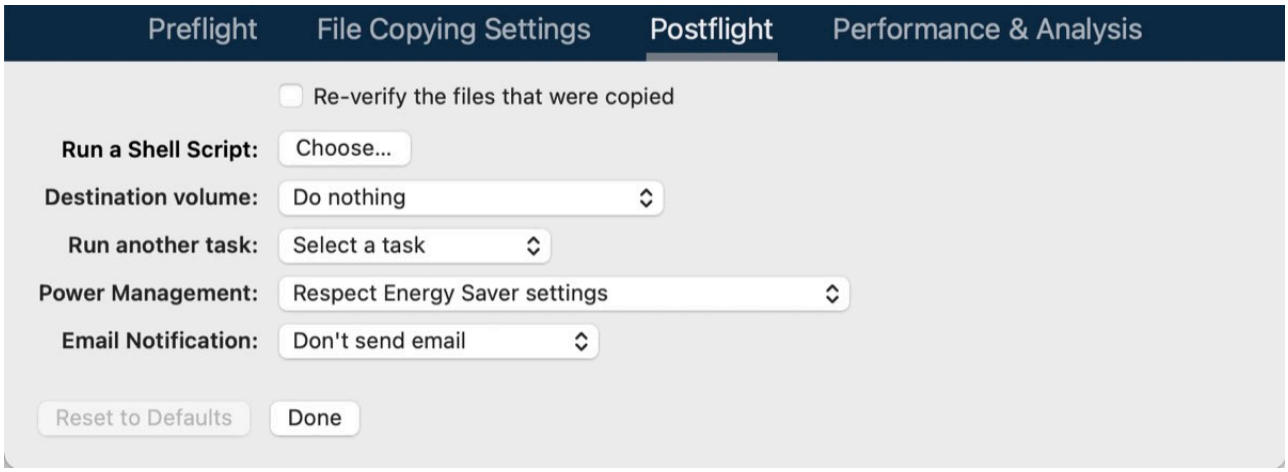
CCC SafetyNet folders

When CCC's SafetyNet feature is enabled, CCC creates a _CCC SafetyNet folder at the root of the selected destination volume or folder. When CCC encounters an item on the destination that does not exist on the source, or an item that will be replaced with an updated item from the source, that item gets placed into the SafetyNet folder rather than being deleted immediately. The SafetyNet folder is literally a safety net for files on your destination. If you accidentally delete a file from the source and you don't realize it until after your backup task runs, you'll find the item in the SafetyNet folder. Likewise, if you accidentally specify the wrong volume as a destination to a CCC backup task, the mistake does not catastrophically delete every file from the selected destination; you simply recover the items from the _CCC SafetyNet folder.

The protection that the SafetyNet folder imparts is specific to the volume upon which the SafetyNet folder resides. As such, CCC never includes the contents of the _CCC SafetyNet folder in a backup task. So, for example, if your hard drive fails and you restore your backup to a replacement disk, the _CCC SafetyNet folder is automatically excluded from that restore task. If you have several tasks backing up to separate folders on a backup volume, for example, the _CCC SafetyNet folders that are created in those subfolders would not be included in a secondary backup task that copies your backup disk to a third disk.

Performing actions Before and After the backup task

Often when you have a backup task that runs on a scheduled basis, there are associated tasks that you would like to perform before or after files are actually copied. CCC offers the option to run shell scripts before and after a backup task, unmount the destination, run another CCC backup task, and power management options such as restart and shutdown. If you would like to perform any of these pre- or postflight tasks, click the **Advanced Settings** button at the bottom of CCC's main window.



Mounting the source or destination volume before a backup task begins

Without any additional configuration, CCC will attempt to mount your source and destination volumes before a backup task begins. This applies to many different volume types — ordinary volumes on locally-attached hard drives, disk images, network volumes, encrypted volumes – even encrypted volumes on remote Macs. If your source or destination volume is on a disk that is physically attached to your Mac (e.g. via Thunderbolt or USB), but it is not mounted, CCC can "see" that device and will attempt to mount it. If your source or destination is a network volume, CCC will obtain the credentials that you use to mount that device when you create the backup task, and will use those credentials to mount the volume before the task begins.

This also applies for nested volumes. For example, suppose you are backing up to a disk image on a network volume. CCC will first attempt to mount the network volume, then it will attempt to mount the disk image. Likewise, suppose you have a task configured to back up the contents of a folder on an encrypted volume. If you have saved the encrypted volume's passphrase in CCC's keychain, CCC will unlock and mount the encrypted volume before the backup task begins.

CCC's attempts to mount the source and destination volumes occur automatically before any other tasks, including preflight shell scripts (described below), therefore **it is not necessary to implement a shell script to pre-mount the source or destination**.

Little Snitch may prevent the automated mounting of network volumes

If you're using Little Snitch to monitor and filter your inbound and outbound network traffic, you may find that CCC has trouble automatically mounting a network volume. If you run into this problem, configure Little Snitch to allow network access to the NetAuthSysAgent system service.

NetAuthSysAgent is the macOS system service that fulfills application requests to mount network volumes.

SafetyNet Pruning

SafetyNet pruning is covered in more detail in this section of CCC's documentation <https://bombich.com/kb/ccc6/automated-maintenance-ccc-safetynet-folder>.

Destination volume options

If you would like CCC to unmount your destination volume at the end of the backup task, choose **Unmount the destination volume** from the Destination volume management menu. If your destination is a folder, the text will be **Unmount the underlying volume**. If the destination is a disk image, CCC always unmounts the disk image volume, so this setting refers to the underlying physical volume upon which the disk image resides.

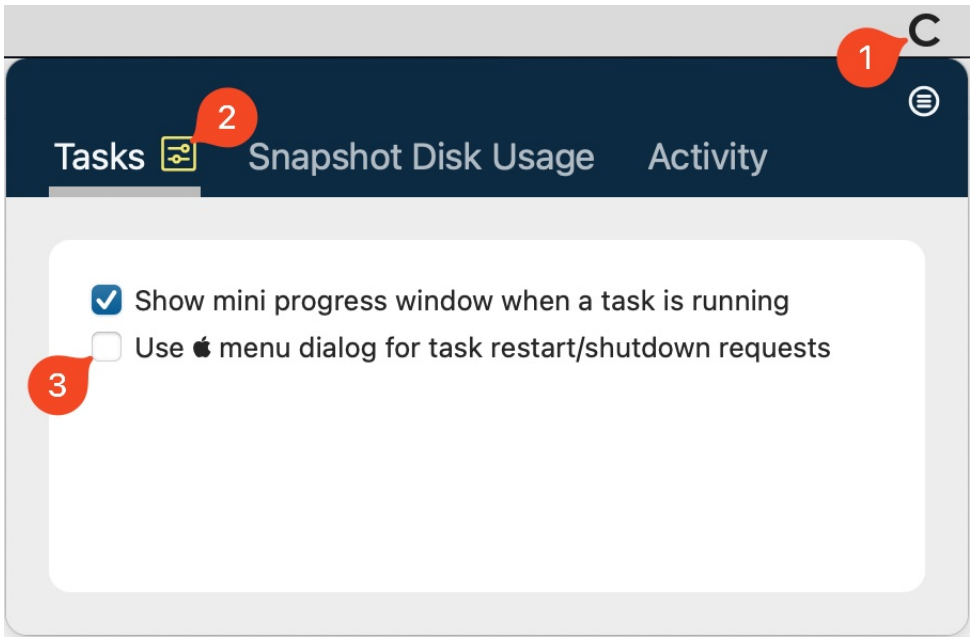
If an application has open files on the destination volume, CCC's attempt to unmount the volume will fail. CCC does not report this as a task failure, though it will make a note of the event in the Errors tab of the Task History window.

Power management options

By default, at the end of a backup task, CCC will not perform any power management tasks. Instead, the system will perform as defined by the settings in the Energy Saver Settings pane. For example, if you have the system configured to idle sleep after 20 minutes, the system will go to sleep if there hasn't been any user activity in the last 20 minutes. CCC activity is not considered user activity, so often the system will go to sleep immediately after CCC finishes a backup task.

If you choose one of the options from the Power management menu, CCC will reboot or shut down your Mac when the backup task finishes. The reboot and shutdown options are not forceful, rather these are "requests". If you have a document open with unsaved modifications, for example, the application would prompt you to save the document. If a save dialog is not attended to, the shutdown or reboot request will time out.

These restart/shutdown requests are made on behalf of the logged-in user by the CCC Dashboard application, which runs in the currently-logged-in user's login session. The CCC Dashboard offers two separate approaches for making these requests. By default, the Dashboard will make the request immediately and directly to macOS. Alternatively, you can have the Dashboard make the request in the same manner as implemented by the options in the Apple (□) menu. Requests made via the Apple menu cause a prompt to appear indicating that the system will shutdown. At that time a 60-second timer will start to count down. The reboot/shutdown request will be made when the timer expires. This option is convenient if you think you might want to cancel the reboot/shutdown request. To change the setting, click the CCC icon in the menu bar to reveal the CCC Dashboard, select the Tasks tab in the Dashboard, then click the settings icon to reveal the setting.



Turn off the computer if it was previously off

If your backup task is scheduled to run on a regular basis, this option will be enabled in the Power Management popup menu. This option is applicable if you would like to have CCC shut down your Mac at the end of the task, but only in cases where the Mac was booted at the task's scheduled run time. If your backup task runs when the system has been on for a while or has been sleeping, CCC will not shut down the Mac when using this option.

Power Management options are ignored in some cases

Power management options will not be applied to backup tasks that are cancelled (e.g. you click the Stop button). Additionally, power management tasks will not be applied if other CCC backup tasks are running or queued to run immediately after the current task finishes running. If your task is running as part of a Task Group, power management options will be deferred to when all tasks within the group have completed.

Power Management options are applied regardless of task success

Power management options will be applied whether the backup task completes successfully or not. If you prefer for a backup task to perform the power management action only when the backup task exits without error, see the pm_on_success.sh postflight script below.

Run another backup task (task chaining)

If you have more than one CCC backup task configured, the other tasks will be listed in this popup menu. To create a task chain (e.g. to run tasks sequentially), simply choose one of these tasks to have that task run automatically after the current task finishes. Tasks run in this manner will start after the current task has finished completely. Chained tasks will run regardless of the exit status of a preceding task in the chain, e.g. if the first task reports errors or fails to run at all, the second task will still run. Only the first task in a chain needs to be scheduled to start the chain.

Note: Postflight tasks will not be started if the current task was started via a task group <https://bombich.com/kb/ccc6/task-organization>. When you run a task group, we're specifically aiming to run exactly the tasks within that task group, and within the order specified. If you run the

task manually, however, or if the task is run separately from the group on its own schedule, then the task's postflight task will be run.

Running shell scripts before and after the backup task

If there is functionality that you need that does not exist within CCC, pre- and postflight shell scripts may be the solution for you. Preflight shell scripts run after CCC has performed "sanity" checks (e.g. are the source and destination volumes present, is connectivity to a remote Macintosh established) but before copying files. **If you need your preflight script to run before CCC does the source/destination sanity checks, specify the preflight script as a global preflight script in the Advanced section of CCC's Settings window.** Note that global preflight scripts run prior to every task, they are not task-specific. Also, please bear in mind that CCC automatically attempts to mount the source and destination at the beginning of the task, you should not be implementing a shell script to achieve that functionality. If you're having trouble with CCC pre-mounting the source and destination, please ask us for help <https://bombich.com/software/get_help> rather than attempt to address the issue with a preflight shell script.

Postflight shell scripts run after CCC has finished copying files and performing its own internal cleanup, but before unmounting any volumes.

CCC passes several parameters to pre- and postflight shell scripts. For example, the following shell script:

```
#!/bin/sh

echo "Running $0"
echo `date`
echo "Source: $1"
echo "Destination: $2"
echo "Third argument: $3" # Exit status for postflight scripts, underlying volume path for a disk image for preflight scripts
echo "Fourth argument: $4" # Destination disk image path, if applicable
```

Would produce the following output (you can redirect this output to a file of your own specification) if implemented as a postflight script:

```
Running /Library/Application Support/com.bombich.ccc/Scripts/postaction.sh
Wed Oct 8 21:55:28 EDT 2014
Source: /
Destination: /Volumes/Offsite Backup
Third argument: 0
Fourth argument:
```

First parameter

The path to the source volume or folder. If the source volume is APFS-formatted, then this path will usually be the path to a temporary, read-only snapshot of the source (or the path to the source folder on the temporary, read-only snapshot). If the source volume is a System volume, CCC will send the path to a snapshot of the Data sibling of the source as the first parameter.

Second parameter

The path to the destination volume or folder. If the destination is a disk image, this is the path to the mounted disk image. On macOS Catalina and later, if the destination volume is a System volume,

CCC will send the path to the Data sibling of the destination as the second parameter, e.g. "/Volumes/CCC Backup - Data".

Third parameter

- Preflight script: The underlying mountpoint for the volume that holds the destination disk image, if applicable.
- Postflight script: The exit status of the file copying phase of the backup task.

Fourth parameter

The path to the destination disk image, if applicable.

Controlling the CCC task via the preflight script exit status

If your preflight script exits with a non-zero exit status, it will cause CCC to abort the backup task. This can be used to your advantage if you want to apply preconditions to your backup operation. If you want to be certain that errors in your preflight shell script never cause the backup task to be aborted, add "exit 0" to the end of your script. If you would like that script to silently cancel the backup task, add "exit 89" to the end of the script. If the script is a global preflight script (specified in the Advanced section of CCC's Settings window), you can add "exit 104" to the end of the script to cancel the backup task **and** to avoid recording a Task History event.

The postflight script will run whether the backup task exits successfully or not. If your script should behave differently depending on the result of the task, you can test whether the third parameter is zero (an exit status of "0" means the task ended successfully). For example:

```
#!/bin/sh

source="$1"
dest="$2"
exitStatus=$3

if [ "$exitStatus" = "0" ]; then
   # task succeeded
else
   # task failed or reported errors
   # Note: Do not assume that $source and $dest are populated
   # These will be empty if source or destination validation fails
fi
```

If your postflight script exits with a non-zero exit status, CCC will not report this as a failure of the backup task. The failure will be noted in the Task History window, however.

Making changes to the source with a preflight script

If the source is an APFS volume, CCC will create a snapshot on that volume prior to running your preflight script, and then pass the path to that mounted snapshot as the first parameter to your shell script. Please bear this in mind if you are implementing a preflight script that makes changes to the source. Those changes will not be reflected in the current backup. *If you need those changes to be reflected in the current backup, specify the preflight script as a global preflight script in the Advanced section of CCC's Settings window*.

Running a preflight script prior to evaluating the source and destination availability

Per-task preflight scripts run after CCC has evaluated the availability of the source and destination. This order is deliberate — CCC passes the path of the source and destination to the preflight script, and we guarantee that these paths are available and correct when your preflight script is called. If you need your preflight script to make changes to the source, or take special measures to make the source or destination available (e.g. establishing a VPN connection), then you can perform those tasks in CCC's Global Preflight Script, specified in CCC Settings > Advanced. If you would like to limit the functionality of your global preflight script to a specific task, you can add logic to your script for that purpose. This example global preflight script <https://bombich.com/software/files/tools/global_pretask_preflight.sh.zip> demonstrates how to do this.

AppleScripts are not supported

You cannot specify an AppleScript as a pre- or postflight script, CCC currently only supports running shell scripts.

Shell scripts require a shell interpreter line

CCC does not assume a default shell environment when running your pre- or postflight script. Not doing so gives users a great deal of flexibility; they can choose to write their scripts in any shell or programming language (e.g. bash, python, perl, ruby, C). For CCC to execute a shell script as an application, though, the system needs to know what shell should be used to interpret the script, and that value needs to be defined in your shell script. This is done simply by placing a shell interpreter line at the top of the file, e.g. #!/bin/sh.

Shell scripts run as the root user

CCC's pre- and postflight shell scripts are executed as the System Administrator (aka "root"). As such, any references to your own shell environment will be invalid. When referencing tools that lie outside of the default $PATH, be sure to either specify the full path to the item (e.g. /usr/local/bin/foo), or export your own $PATH at the top of your script. Likewise, if you make relative references to files (e.g. ~/Desktop/foo.log), those files will be created in the root user account, e.g. /var/root/Desktop/foo.log. Use absolute paths for more reliable results.

Another implication of running scripts as the root user is that interaction between the script and applications running via the logged-in user are generally not possible. For example, special steps are required if you want to open or close an application. See the quit_application.sh and open_application.sh scripts at the bottom of this document for an example of how to do this. Interaction with those applications usually will not work.

Security implications of pre- and postflight shell scripts

To prevent unauthorized modifications to your shell scripts, we recommend that you restrict the ownership and permissions of these scripts and to the folder in which they are contained. The parent folder and scripts should be writable only by the root user. For example, running the following in the Terminal application would secure any shell scripts located in the default location for pre- and postflight scripts:

```
sudo chown -R root:wheel /Library/Application\ Support/com.bombich.ccc/Scripts
sudo chmod -R 755 /Library/Application\ Support/com.bombich.ccc/Scripts
```

To further enhance the security of your pre and postflight scripts, CCC will require that scripts stored in the default location are owned by the root user and writable only by the root user, and that the Scripts folder itself is also owned and writable only by the root user. If a script that resides within the default Scripts folder does not meet these requirements, CCC will refuse to execute that script and the associated task will report an error.

After copying scripts into CCC's Scripts folder or making changes to those scripts, you can choose "Secure CCC's Scripts folder" from CCC's Utilities menu to correct any ownership or permissions concerns. Please note that these additional security requirements are only applied to scripts stored within the /Library/Application Support/com.bombich.ccc/Scripts folder. If you prefer to manage the security of your shell scripts on your own, you may store them in another location.

Example pre- and postflight shell scripts

To use any of these example scripts, download the script and place it somewhere on your startup disk. By default, CCC looks in /Library/Application Support/com.bombich.ccc/Scripts.

parallels_pause.sh <https://bombich.com/software/files/tools/parallels_pause.sh.zip>
This is a preflight script that you can use to pause all currently-running Parallels VM containers. This script will also retain state information that can be read by the corresponding parallels_start.sh postflight script to resume these VMs after the backup task has completed. Note: This script relies on command-line tools offered only in Parallels Desktop for Mac Pro or Business Edition.

parallels_start.sh <https://bombich.com/software/files/tools/parallels_start.sh.zip>
This postflight script will resume any Parallels VM containers that were suspended by the parallels_pause.sh preflight script. Note: This script relies on command-line tools offered only in Parallels Desktop for Mac Pro or Business Edition.

play_sound.sh <https://bombich.com/software/files/tools/play_sound.sh.zip>
If you want to play a unique sound, use this script. You can plug in the path to any audio file of your liking or try one of the examples included.

eject_source_and_destination.sh
<https://bombich.com/software/files/tools/eject_source_and_destination.sh.zip>
CCC's option to automatically unmount the destination volume is a volume-level task, not a device task. It's also limited to the destination. If you want to eject the destination device, or if you want to unmount or eject the source, use this postflight script instead. Note that ejecting a device will unmount all volumes on the device. Also note that this example script adds a 60-second delay to accommodate snapshot creation on the destination.

pm_on_success.sh <https://bombich.com/software/files/tools/pm_on_success.sh.zip>
This postflight script will perform the requested power management option (e.g. shutdown, restart, sleep) at the end of the backup task if the backup task completes without errors. Use this in lieu of one of the Power Management postflight options if you prefer the power management action does not occur when a task ends with errors (e.g. if the destination volume is missing).

quit_application.sh and open_application.sh
<https://bombich.com/software/files/tools/quit_and_open_application.zip>
This pair of scripts can be used to quit and open an application before and after the backup task. Open these scripts in a text editor to define the application that should be quit or opened.

post_to_slack.sh <https://bombich.com/software/files/tools/post_to_slack.sh.zip>
This postflight script will post the status of your backup task to a Slack <https://slack.com> channel.

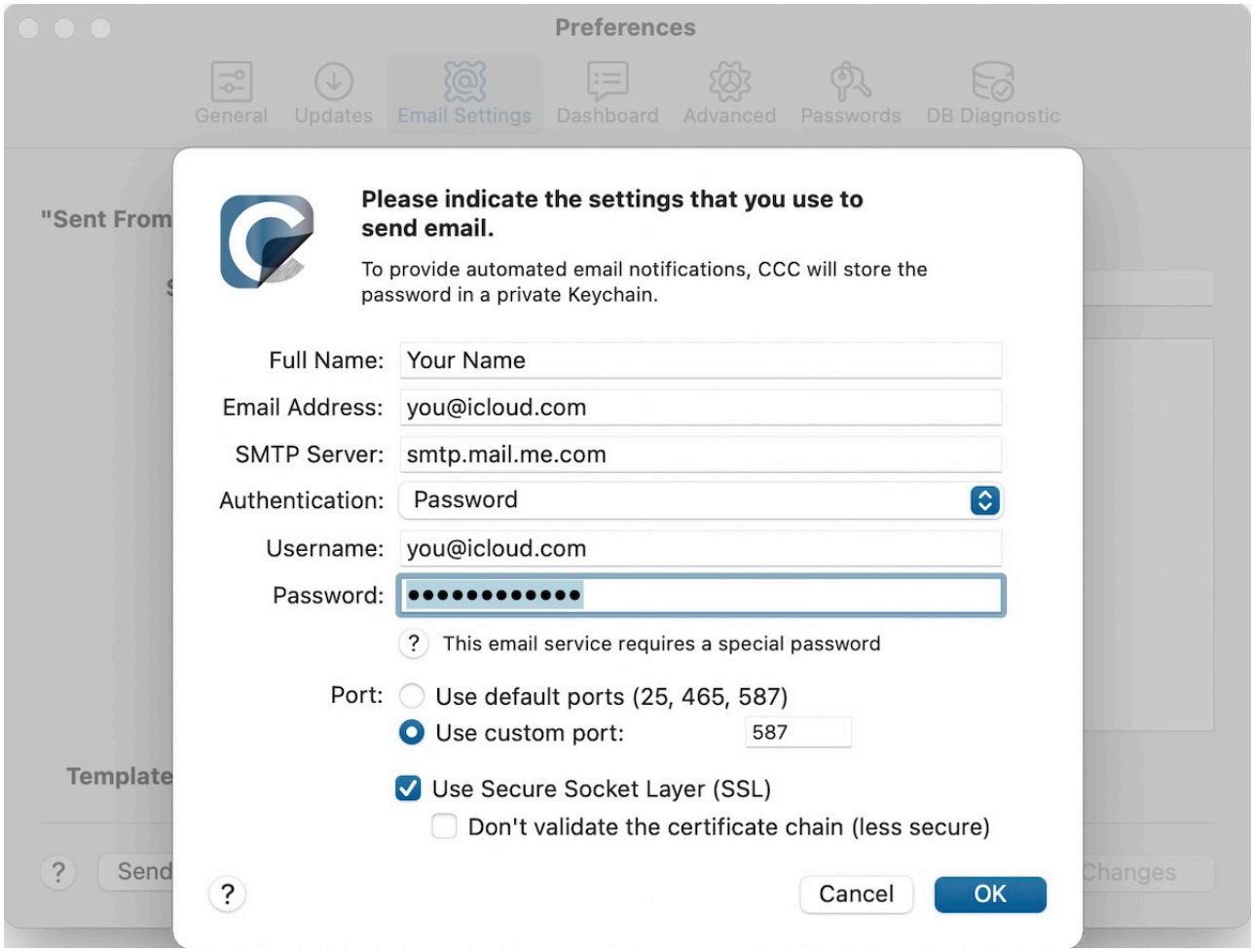
ifttt_maker.sh <https://bombich.com/software/files/tools/ifttt_maker.sh.zip>
This postflight script will post an IFTTT Maker Event <https://ifttt.com/maker_webhooks> of the status of your backup task.

Configuring Email Notifications

If you would like CCC to send your tasks' results via email, you must first configure a sending email account in CCC's Email Settings.

1. Click **Settings** in the CCC toolbar.
2. Click the **Email Settings** button in the toolbar of the Settings window.
3. Choose from one of the accounts imported from Mail in the ***Sent From* Email** popup menu, then verify the details and provide your account credentials in the form that is provided.
4. Click the **OK** button when you are finished entering your account details.

Note for advanced users: If your SMTP server requires SSL and uses a **self-signed** security certificate, check the **Don't validate the certificate chain** checkbox. Alternatively, you can add your server's security certificate to the **System** keychain in the Keychain Access application and explicitly trust that certificate.



[Optional] Modify the email subject and body template

The subject and body of the email that CCC sends upon task completion can be customized. For example, if you want to know which of your Mac's a particular email is coming from, you could customize the subject of the message:

Jon's iMac: ##Task Name##: ##Exit Status##

When CCC sends an email notification, it will replace the template values (enclosed in double # characters) with the attributes of your task, e.g.:

Jon's iMac: Daily Backup: Backup Finished Successfully

Most of the available template values are already present in the default template. You can rearrange the template values and modify the text around them, but do not modify the text inside of the double # characters. If you would like to add a template value:

1. Place the cursor where you would like to place the template value, e.g. in the subject or body text field.
2. Select a template value from the **Template values** popup menu.
3. Click the **Insert** button.

When you are finished making changes to your subject and body templates, click on the **Save Changes** button. This template will be used for all email notifications sent by CCC.

If you have suggestions for additional template values, please let us know <https://bombich.com/software/get_help>!

Send a test email

Click on the **Send Test Email...** button at the bottom of the window. You will be prompted to provide an email address to send the test email to. When CCC indicates that the test email has been sent, check your email to confirm that you can receive it and that the template provides the information you wish to receive when your tasks complete.

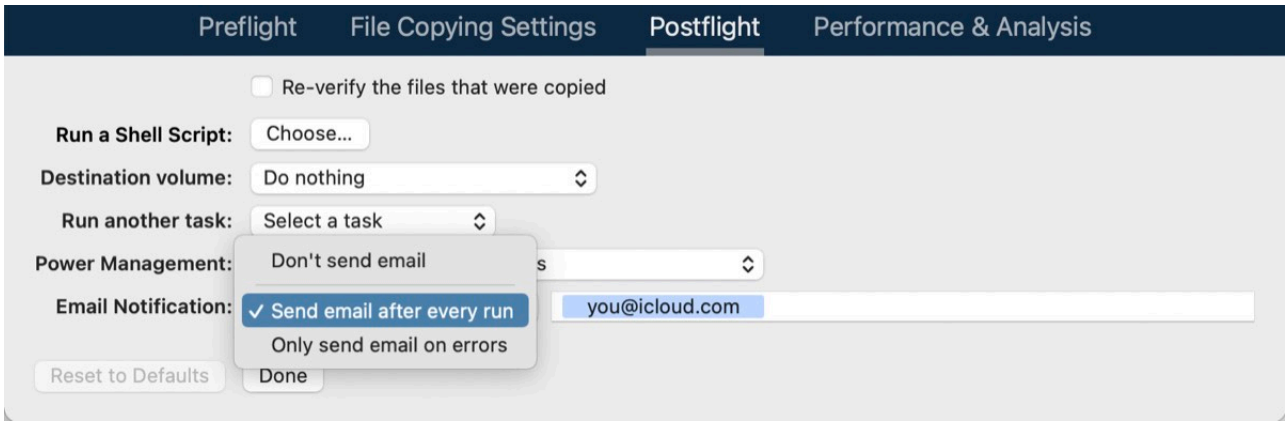
Select a notification level in your backup task

Close the Settings window, then select the task to which you would like to add email notifications. Click the **Advanced Settings** button at the bottom of the window, then select the **Postflight** tab to reveal the email notification option. There are three notification levels:

- Don't send email: CCC will never send an email when this tasks finishes.
- Send after every run: CCC will send an email at the end of every task (i.e. successful tasks and those that report errors).
- Only send on errors: CCC will send an email only when errors occur for this task.

Select a notification level, then specify the email address(es) that you would like CCC to notify when the task completes. If you would like to have emails sent to multiple addresses, separate those addresses with a comma, or simply press the return key after typing in each address. The recipient text field may only show one address at a time. Use the arrow keys to see each address.

Once you have configured a notification level and recipients, choose **Save** from CCC's Task menu to save the changes.



Sending email with an SMTP service that requires an App Password

Because CCC sends emails from a background application, possibly when no user is logged in at all, CCC cannot practically support two-factor authentication. Many applications have this same logistical constraint, and most email providers will allow those applications to use the SMTP service, provided that you have created an application-specific password for that purpose. If you attempted to send an email with your Gmail or iCloud account (for example), and you get an error that "the username and password are invalid", or that "authentication failed", you can resolve the problem by creating an App Password.

Create an App Password for iCloud

Visit your Apple ID account page and create an application-specific password for CCC:

1. Sign in to your Apple ID account page <https://appleid.apple.com/account/home>.
2. In the Security section, click the **Generate Password...** link under the **APP-SPECIFIC PASSWORDS** heading and follow the steps provided.
3. Paste the application-specific password into the Email Settings panel of CCC's Preferences window.
4. Note: Be sure to use an @mac.com, @me.com, or @icloud.com email address for the user name.

Apple's reference: Using app-specific passwords <https://support.apple.com/kb/HT6186>

Ventura users: macOS 13.5 introduces a bug in Safari that prevents it from correctly generating App Passwords. **Workaround**: use a different browser on macOS 13.5 to generate App Passwords.

Create an App Password for Yahoo

Visit your Account Security page to generate an application-specific password for CCC:

1. Visit your Account Security page <https://login.yahoo.com/account/personalinfo>.
2. Click on the **Generate app password** link at the bottom of the page.
3. Click **Select yourapp** and choose **Other App**. Type in CCC as the custom name.
4. Click the **Generate** button.
5. Copy and paste the application-specific password into the Email Settings panel of CCC's Preferences window. Note: We recommend that you **copy and paste** the code. If you choose to transcribe it, take care not to insert spaces. The code is presented in four groups, but it does not actually contain spaces; it should be exactly 16 characters.

Create an App Password for AT&T

Visit your AT&T Profile page to generate an application-specific password for CCC. AT&T does not use the industry standard term "app-specific password" and instead calls this a "secure mail key":

1. Visit your AT&T Profile <https://m.att.com/myatt/native/deepLink.html?action=Profile&appInstall=N> and choose **Sign-in info**.
2. Select the email account that needs a secure mail key. (You'll find a menu at the top if you have multiple accounts.)
3. Scroll to **Secure mail key** and select **Manage secure mail key**.
4. Choose the email address that you'd like to use if you have more than one.
5. Select **Add secure mail key** and then enter a nickname for the secure mail key to make it easier to recognize (Like "CCC").
6. Choose **Create secure mail key**.
7. Select **Copy secure mail key to clipboard**
8. Paste the application-specific password into the Email Settings panel of CCC's Preferences window.

Create a secure mail key <https://www.att.com/support/article/email-support/KM1240308>, Set up or update AT&T email - Apple Mail (OS X) <https://www.att.com/support/article/dsl-high-speed/KM1010489>

Create an App Password for Gmail

Visit your Gmail App Passwords page to generate an application-specific password for CCC:

1. Visit your App passwords page <https://security.google.com/settings/security/apppasswords>.
2. Click **Select app** and choose **Other (custom name)**. Type in CCC.
3. Click the **Generate** button.
4. Paste the application-specific password into the Email Settings panel of CCC's Preferences window. Note: We recommend that you **copy and paste** the code. If you choose to transcribe it, take care not to insert spaces. The code is presented in four groups, but it does not actually contain spaces; it should be exactly 16 characters.
5. Note: Be sure to use an @gmail.com email address for the user name. **G Suite accounts are not supported.**

Google's reference: Sign in using App Passwords <https://support.google.com/accounts/answer/185833>

Create an App Password for Outlook.com

Visit your Outlook.com App Passwords page to generate an application-specific password for CCC:

1. Go to the Security basics <https://account.microsoft.com/security> page and sign in to your Microsoft account.
2. Select **More security options**.
3. Under **App passwords**, select **Create a new app password**. A new app password is generated and appears on your screen
4. Paste the application-specific password into the Email Settings panel of CCC's Preferences window. Note: We recommend that you **copy and paste** the code. If you choose to transcribe it, take care not to insert spaces.

Microsoft's reference: Using app passwords <https://support.microsoft.com/en-us/account-billing/using-app-passwords-with-apps-that-don-t-support-two-step-verification-5896ed9b-4263-e681-128a-a6f2979a7944>

"Your Gmail account will not permit CCC to send email notifications"

Google is very insistent that developers of third-party applications attain a Google Developer Account and subscribe to Google's proprietary APIs so they can use a special form of authentication with Gmail accounts (OAuth2). Developers that choose to use industry-standard authentication mechanisms instead are unjustly deemed as "less secure", and by default, Google will deny authentication requests from these applications. To add insult to injury, when an application attempts to authenticate to Gmail using the industry-standard authentication methods, Google sends you an email that suggests that the requesting application "doesn't meet modern security standards".

CCC absolutely uses modern security standards — TLS, in particular, to secure all traffic to the SMTP server. TLS has and continues to be the modern security standard for securing email communications. If you get a message that your Gmail account won't permit CCC to send email, we have two suggestions:

- Enable two-step verification on your Google account <https://accounts.google.com/b/0/SmsAuthConfig> and then create an application password for CCC [this is our primary recommendation]

— Or —

- Change the settings in your Gmail account <http://www.google.com/settings/security/lesssecureapps> that Google disabled

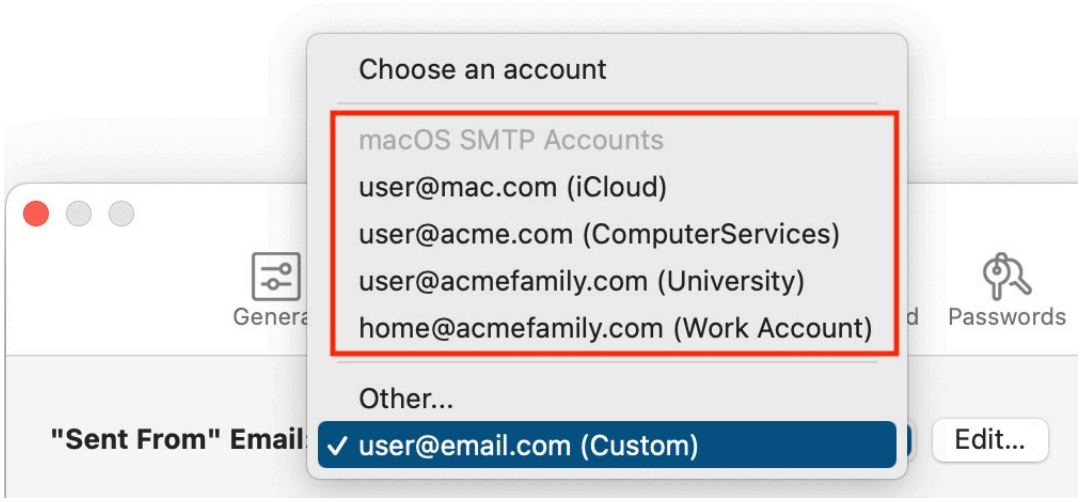
Alternatively, you could just specify a non-Google email account in the Email Settings section of CCC's Settings window.

Update your SMTP credentials after migrating to new Mac

When you provide your SMTP credentials to CCC, CCC stores them securely in a macOS Keychain file. That keychain file is secured in several ways; it is readable only by the macOS system administrator account, it can only be unlocked by CCC, and it can only be unlocked on the Mac upon which it was originally created. As a result, if you purchase a new Mac and migrate your data to the new Mac, CCC's keychain will not work on the new system and CCC will be unable to send email notifications.

After migrating to a new system, open CCC's Email Settings, click the Edit... button, then re-enter your SMTP account credentials.

How can I remove older email accounts listed in CCC's Email Accounts popup menu?



CCC collects email account information from the macOS Accounts service dynamically when you open the Settings window. The email accounts listed under the "macOS SMTP Accounts" heading are not email accounts that CCC retains within its own preferences, rather those come from the Accounts Preference Pane in the System Settings application. These accounts can't be removed from within CCC – again, because CCC doesn't retain information about these accounts. If you would like to remove these accounts from your Mac, you can remove them in the Internet Accounts panel in the System Settings application.

Backing up to a disk image

We discourage the use of writable disk image destinations

Writable sparse disk images are particularly sensitive to connectivity loss between the disk image volume and the disk image file. Reports of disk image corruption have grown steadily worse, especially since the introduction of APFS, and especially when the disk image is hosted on NAS storage. If you're currently using a disk image as part of your backup strategy and it's working for you, you're welcome to continue using it. This functionality is still present within CCC, and we will continue to support it in scenarios where the disk image is working reliably. As you make changes to your backup strategy in the future, however, and especially if you encounter trouble mounting a disk image or accessing its content, we recommend that you migrate away from writable disk images and back up directly to a folder or volume on the underlying storage.

Related documentation

- Folder-to-Folder Backups <https://bombich.com/kb/ccc6/folder-folder-backups>
- Add dedicated volumes to an existing APFS-formatted backup disk <https://bombich.com/kb/ccc6/i-want-back-up-multiple-macs-or-source-volumes-same-hard-drive#apfs_add_volume>
- Encrypting a locally-attached backup volume <https://bombich.com/kb/ccc6/working-filevault-encryption>
- Use Quick Update when it's possible to collect a list of modified folders from macOS <https://bombich.com/kb/ccc6/advanced-settings#quickupdate>

A disk image is a single file that contains the entire contents of another hard drive (except for the free space). When you want to access the contents of that filesystem, you double-click on the disk image to mount the disk image as if it were an external drive attached to the machine.

To back up to a new disk image:

1. Choose your source volume from the Source selector
2. Choose **New disk image...** from the Destination selector
3. Provide a name and choose a location to save your disk image
4. If you plan to back up to this disk image again in the future, set the image format to one of the read/write formats. If you want a read-only disk image for archival purposes, set the image format to one of the read-only formats.

To back up to an existing disk image, select **Choose disk image...** from the Destination selector and locate your disk image, or simply drag and drop the disk image file onto CCC's Destination selector box.

Read/write "sparseimage" disk images

Use of this older disk image format is not recommended, we only make it available as a potential workaround for some SMB NAS devices

A sparseimage disk image is a type of read/write disk image that grows as you copy files to it. In general, sparse disk images only consume as much space as the files they contain consume on disk, making this an ideal format for storing backups. Please note that sparseimage files are monolithic and potentially very large files. If the underlying filesystem has a 2TB file size limit and the sparseimage file reaches that limit, the sparseimage file cannot be grown. In most of these cases the sparseimage file becomes corrupted when the underlying filesystem limit is reached, so we don't

recommend this disk image format for large data sets.

Read/write "sparsebundle" disk images

A sparse bundle disk image is similar to a sparseimage insofar as it grows as you add data to it, but it retains its data in many smaller files inside of a bundle rather than inside a single file.

Running out of space on a sparse disk image

CCC reported that the destination is full, but the underlying disk has plenty of free space. CCC initially sets the capacity of your disk image to the amount of free space on the underlying disk. If you have freed up some space on that disk since you created the disk image, you can manually expand the capacity of the destination disk image in Disk Utility. Choose **Resize...** from the Images menu in Disk Utility, select your destination disk image, then expand it as desired. We recommend that you do not expand the disk image such that it is larger than the capacity of the underlying disk.

The disk image file is larger than the amount of data it contains, why? Sparseimage and sparsebundle disk images grow as you add data to them. They do not, however, automatically shrink when files are deleted from them. As a result, the amount of disk space that the disk image file consumes will not necessarily reflect the amount of data that they consume. To reclaim disk space that is occupied by the free space on your sparse disk image, CCC will compact the disk image before attempting to mount it if the free space on the underlying volume is less than 25GB, or is less than 15% of the total disk capacity. In most cases, you do not need to compact the disk image yourself, but this functionality is documented here so you'll understand why you might see CCC spending time "Compacting the destination disk image" at the beginning of a backup task.

If you would like to compact a disk image manually, drop the disk image file onto this application†: Compact Sparse disk images <https://bombich.com/software/files/tools/Compact_Sparse_Image.app.zip>. Be sure to unmount the disk image volume if it is already mounted. Also, note that the compacting process can take a while (e.g. an hour for a 100GB disk image on a locally-attached volume). Finally, be sure that your system is running on AC power. The system utility that compacts the disk image will refuse to run while the system (e.g. a laptop) is running on battery power.

† Big Sur (and later) users: Right-click on the application and choose "Open" to get past the GateKeeper restriction. Or if you prefer, you can use the command-line hdiutil utility to compact the disk image (e.g. hdiutil compact "/path/to/disk image.sparsebundle").

CCC applies more aggressive SafetyNet pruning to disk image volumes

When you configure a task to back up to a new disk image, CCC will configure the task's SafetyNet pruning to prune anything older than 1 day. You are welcome to change these settings <https://bombich.com/kb/ccc6/automated-maintenance-ccc-safetynet-folder>, but we have found that more aggressive SafetyNet pruning will avoid excessive use of disk space on the underlying device, and will reduce the need to compact the disk image.

Please keep in mind that SafetyNet is not intended to offer access to older versions of your files, it is a safety mechanism that is designed to avoid the loss of data on an errantly-selected destination volume <https://bombich.com/kb/ccc6/protecting-data-already-on-your-destination-volume-carbon-copy-cloner-safetynet>. SafetyNet is generally not applicable to disk image backups because the disk image is typically dedicated to the backup task. However, enabling SafetyNet with even a very aggressive pruning limit does offer a modicum of protection in cases where you've accidentally removed files from the source.

If you're looking for a solution that retains older versions of your files and your source volume is APFS-formatted, consider CCC's snapshot functionality instead. Snapshots are disabled on disk image destinations by default, but you can enable snapshot support <https://bombich.com/kb/ccc6/leveraging-snapshots-on-apfs-volumes> either on the disk image volume or on the source volume.

Read-only disk images

Read-only disk images cannot be modified without invalidating the built-in checksum, therefore they are a good container for storing archived material. Compression rates vary on the content of your source, but you can typically expect to reduce the size of your disk image by about half when using compression. There is a subtle behavior that you should take note of when considering this option as a space-saving measure: CCC will first create a read/write disk image, copy the selected items to it, then convert the disk image to read-only compressed. In this case, you will actually need twice the space on your destination as the items to be copied consume on the source.

Encrypting disk images

If any of the data that you are backing up is sensitive, and if your backup device may be in an insecure location, encrypted disk images can improve the security of your backup. CCC offers 128 bit and 256 bit AES encryption <https://en.wikipedia.org/wiki/Advanced_Encryption_Standard> to encrypt disk images. To create an encrypted disk image, select one of the encryption levels from the Encryption menu. After you click on the OK button, you will be prompted to specify a passphrase for the new disk image, and CCC will give you an opportunity to save the passphrase in your own keychain. CCC will also store the passphrase in a private keychain so the disk image can be mounted automatically during scheduled backup tasks.

Note: If you create a read-only, encrypted disk image, the intermediate disk image that CCC creates is NOT encrypted. This intermediate disk image file is deleted once the final, read-only, encrypted disk image has been created, but it is not shredded. Take this into consideration when choosing your destination media. If the destination may be placed in an insecure location, use Disk Utility to securely erase free space on the underlying destination volume after you have created your encrypted disk image archive.

Running a backup task whose destination is a disk image on the startup disk

If you specify a disk image that resides on your startup disk as the destination to a scheduled task, CCC will impose some more conservative requirements on this task. To proceed with this configuration, **one of the following requirements must be met**:

- The amount of free space on the startup disk is at least 1GB larger than the amount of consumed space on the source volume.
- The disk image won't grow, e.g. it is a .dmg file, not a sparseimage or sparsebundle disk image.

These requirements avoid a scenario in which the startup disk runs out of free space, causing instability on macOS. If you cannot accommodate the free space requirement, we recommend that you create a **.dmg** disk image in Disk Utility (choose File > New... > Blank Disk image, set the image format to **read/write disk image**). Disk Utility will pre-allocate exactly as much space as you request, and CCC will gladly use this disk image without fear of filling up the startup disk.

Snapshots and Disk Images

When creating a new disk image, CCC will format the disk image to match the source volume. For better performance on APFS-formatted disk images, CCC will disable snapshot support on the destination disk image volume if:

- The backup task was originally configured to create a new disk image
- Snapshots are currently enabled for the destination disk image
- The snapshot retention policy limit for SafetyNet snapshots is set to the default value of 7 days

When CCC disables snapshots on that destination disk image volume, it explicitly sets the SafetyNet limit in the snapshot retention policy to 0. If you subsequently re-enable snapshot support on that volume without changing the SafetyNet limit back to the default, then snapshots should remain enabled (because the three logical conditions are no longer matched).

If you would like to enable snapshot support on your disk image and keep it enabled, be sure to either leave the SafetyNet limit set to 0, or change it to anything other than 7. If you ever change the SafetyNet retention value for that disk image back to 7 (or reset the values to defaults), CCC will again disable snapshots on the disk image when the task next runs.

A message for new Mac users coming from the Windows world

Backups on a Windows system are very different from those on a Macintosh. If you're coming from a Windows background, the term "imaging" and the concept of making a disk image backup is probably familiar to you. Restoring from disk image backups is made simpler on Windows because the startup environment is built around them. That's not the case for a Macintosh. When you create a disk image backup of your Mac's startup disk, the logistics of restoring that backup are actually fairly complicated. Due to these complications, **we don't recommend using a disk image as your primary backup on a Mac**. Disk images are useful for storing a backup of your user data on a network volume, but for your Mac's startup disk, we recommend that you back up directly to a disk that is attached to your Mac; not to a disk image.

Related Documentation

- Restoring from a disk image <https://bombich.com/kb/ccc6/restoring-from-disk-image>

Restoring from a disk image

You can access the contents of a disk image the same way that you access other volumes and external hard drives on macOS. Double-click on the disk image file to mount its filesystem, then navigate the filesystem in the Finder to access individual files and folders. If you have the permission to access the files that you would like to restore, simply drag those items to the volume that you would like to restore them to.

Restoring individual items or an entire disk image to another hard drive using CCC

To restore files or an entire filesystem from a disk image:

1. Open CCC
2. Select **Restore from disk image...** from the Source selector and locate your backup disk image. CCC will mount the disk image for you.
3. Choose a volume from the Destination selector. You may not choose the current startup disk as a destination, however you may choose to restore to a folder on the current startup disk.
4. If you do not want to restore everything, click the **Task Filter** button and define a filter to exclude any content that you do not wish to restore.
5. Click the Start button.

Using Migration Assistant to migrate data from a disk image

If you have a clean installation of macOS and want to restore your user data from a full-system backup on a disk image, you can use Migration Assistant for this task. Simply mount the disk image, then open Migration Assistant and proceed as directed, using the mounted disk image as the source. Note that Migration Assistant will only accept a disk image that has a full system backup or a whole Data volume backup, it will not accept a collection of user data (e.g. just a user home folder).

Migration Assistant and the CCC SafetyNet

If your backup volume has a "_CCC SafetyNet" folder, you can move that folder to the Trash before using Migration Assistant to avoid copying that folder during a migration. This is particularly important if that folder has a lot of data in it and you're migrating to a disk that is smaller than the backup volume. If you would like to retain the SafetyNet folder on the backup volume, don't empty the Trash. After Migration Assistant has completed, then you can move the SafetyNet folder back to the root of the backup volume.

Using CCC to back up to/from another Macintosh on your network

CCC offers the option of securely copying your selected data to another Macintosh on your network (or anywhere on the Internet for that matter) via the **Remote Macintosh...** options in the Source and Destination selectors. After a brief setup procedure to establish trust between your Mac and the destination Mac, simply choose the source or destination volume/folder on the remote Mac and CCC will take care of the rest.

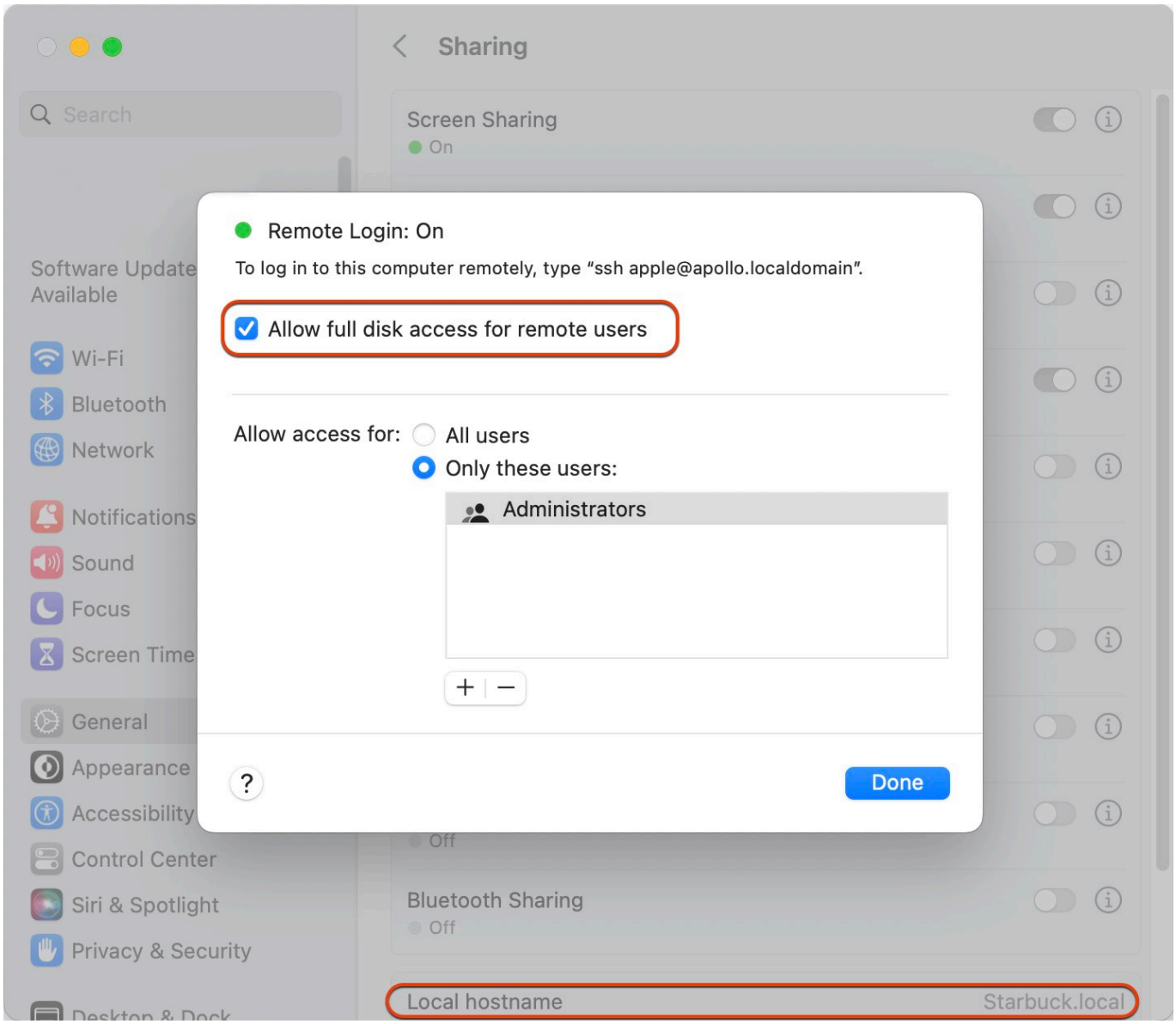
Before setting up CCC to back up to a remote Macintosh, you must:

1. Confirm that the remote Macintosh is running a supported OS (OS X 10.13 or later)
2. Enable Remote Login in the Sharing Preference Pane on the remote Macintosh
3. Verify that any firewalls between the two Macs are permitting "secure shell" traffic over port 22 (or a custom port that you specify).

Enabling Remote Login on the remote Macintosh

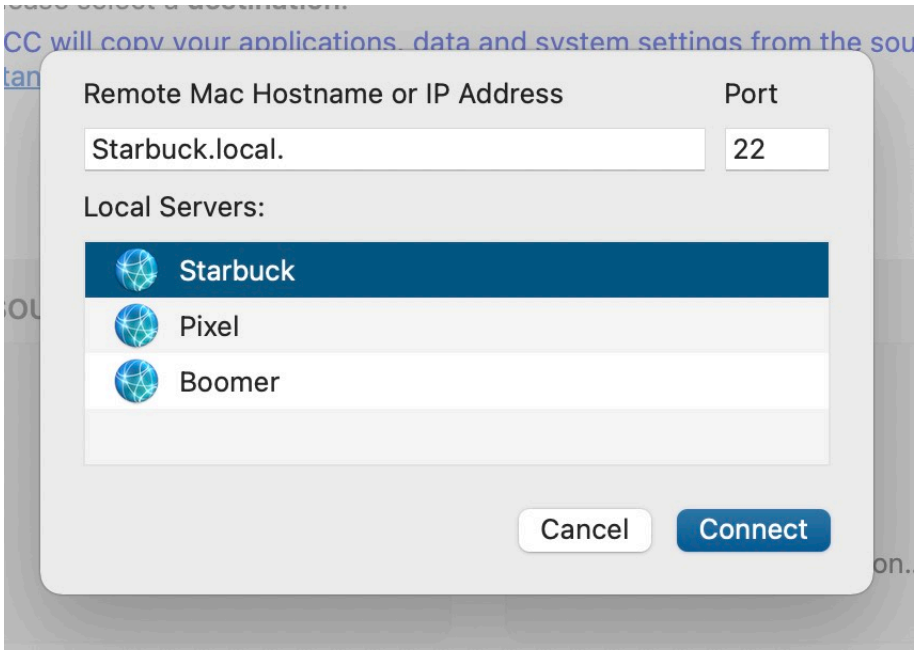
To enable Remote Login on your remote Macintosh:

1. Log in to that machine as an admin user.
2. Open the **System Settings** application.
3. Click **General** in the sidebar, then select the **Sharing** category.
4. Enable the switch next to **Remote Login**.
5. Click the Info button adjacent to Remote Login to reveal the service settings. Be sure to allow access to **All users**, or explicitly add the **Administrators** group to the list of restricted users and groups.
6. Verify that the box next to **Allow full disk access for remote users** is checked, then click **Done**.
7. Make a note of your remote Mac's hostname. The hostname is indicated in the **Local hostname** text field. In the screenshot below, "Starbuck.local" is the hostname of the remote Macintosh.



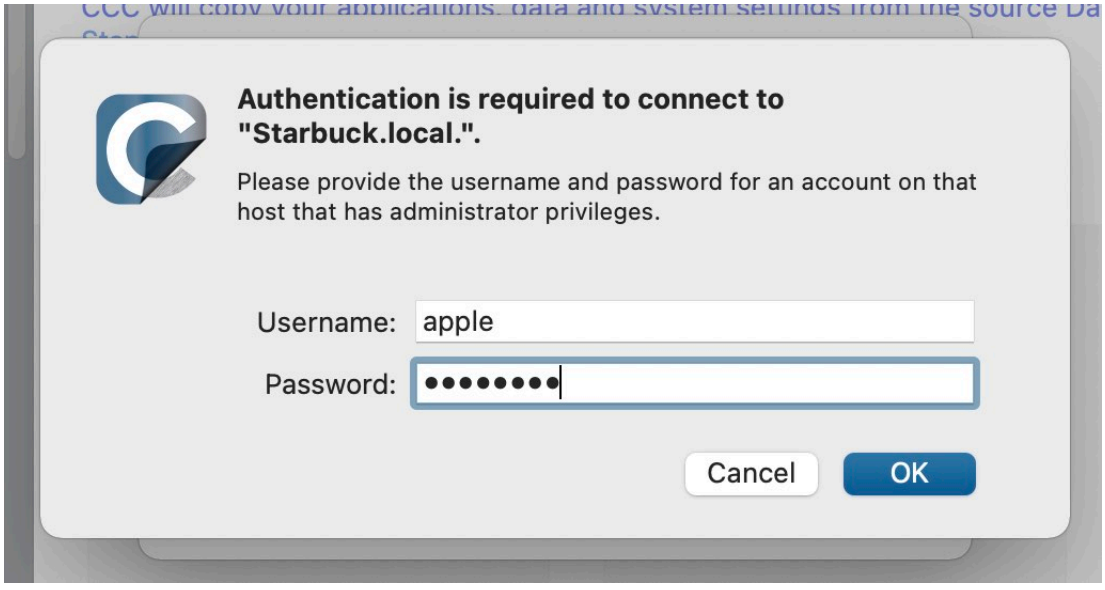
Configuring a Remote Macintosh source or destination

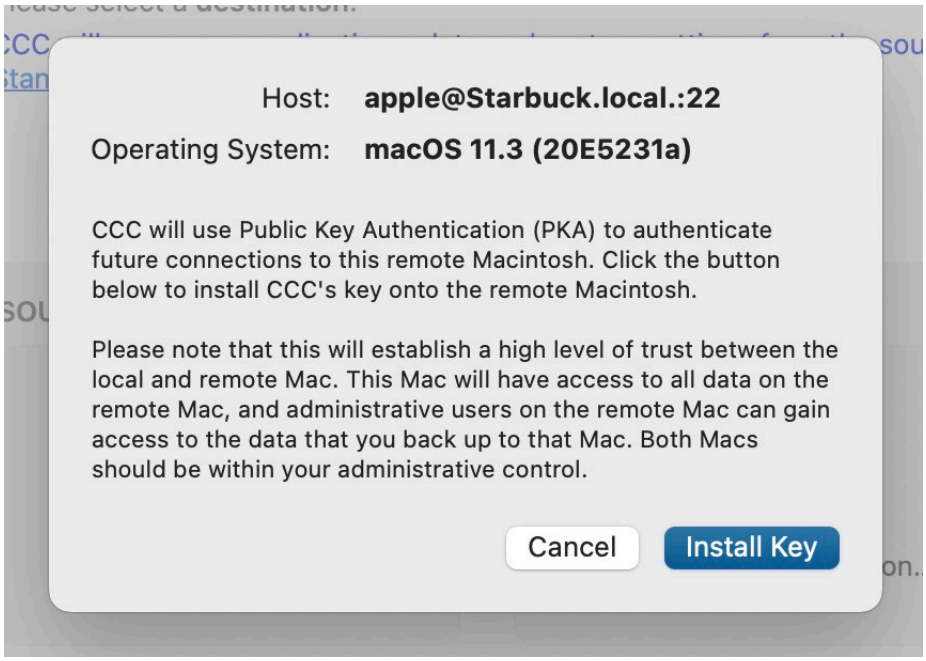
With the Remote Login service enabled on the remote Mac, the next step is to choose **Remote Macintosh...** from CCC's Source or Destination selector. CCC will present a browser that lists any hosts on your local network that advertise the Remote Login service. Find and select your remote Mac in this list, then click the Connect button. If you do not see your Mac listed here, type in the hostname of your remote Mac, then click the Connect button. If the remote Mac is not on your local network, you may need to specify the IP address of the public-facing router that your Mac resides behind. Be sure to configure the router to forward port 22 traffic to the IP address that is assigned to the remote Mac.



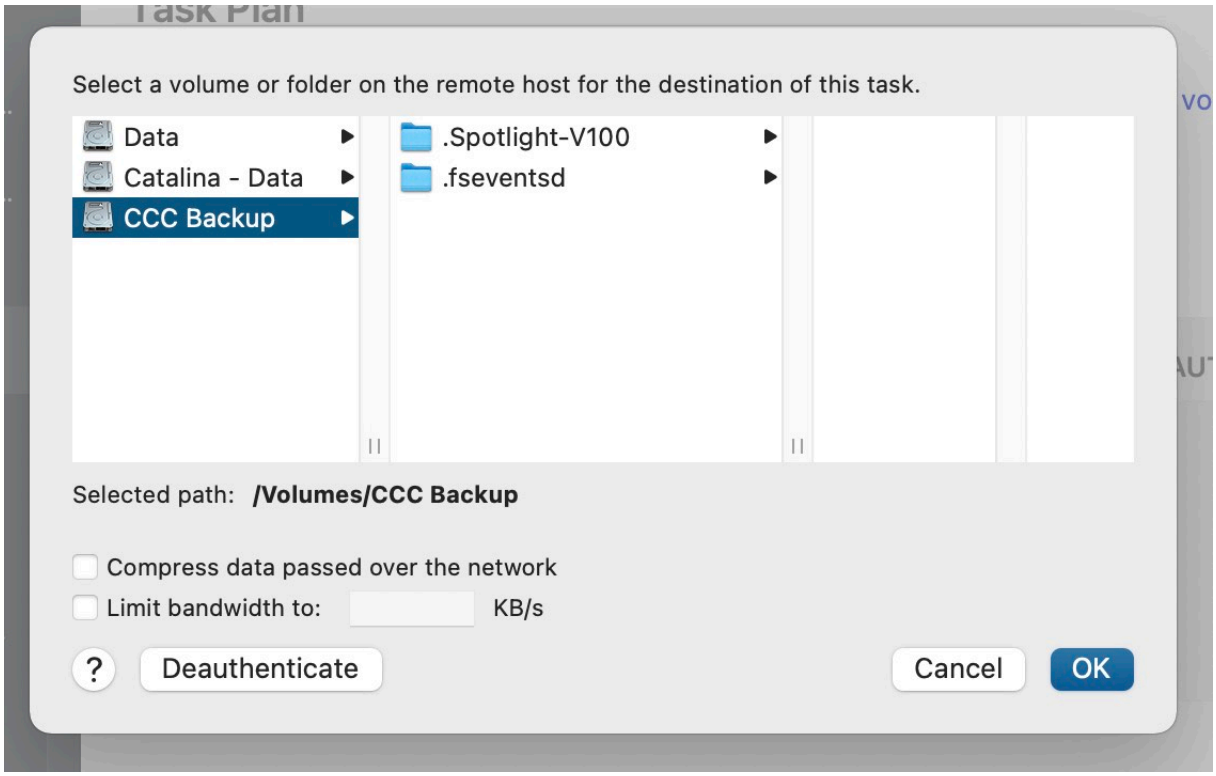
Once CCC has established a connection to the remote Mac, you will be prompted to install a Mac-specific Public Key Authentication (PKA) key pair onto the remote Mac. You must provide the username and password of an admin user on the remote Mac to permit this, and that admin user must have a non-blank password. Those requirements are only for the initial public key installation. For future authentication requests, CCC will use the PKA key pair.

Note: This step establishes a high level of trust between the local and remote Mac; this is required to correctly preserve file ownership. The local Mac will have access to all data on the remote Mac, and administrative users on the remote Mac can gain access to the data that you back up to that Mac. Both Macs should be within your administrative control.





Once you have connected to the remote Mac and installed CCC's key on that system, CCC will present a volume browser. Select the volume or folder to use as the source or destination for your task. Note: avoid selecting a volume or folder that contains an apostrophe (').



Bandwidth management options

CCC offers two options that can help you address bandwidth concerns. The option to **Compress data passed over the network** can greatly reduce your backup time and total bandwidth used. The time savings depend on just how slow the connection is between the two Macs. If you have a connection that is slower than 10MB/s, compression will make the transfer faster. If your bandwidth

is better than that, compression may actually slow down your transfer. CCC will not compress certain file types that are already compressed, such as graphics files, movies, and compressed archives. Specifying the option to compress data passed over the network does not create a proprietary or compressed backup; files are automatically decompressed on the destination volume on the remote Macintosh.

CCC also offers a bandwidth limitation option. If your ISP requires that your transfers stay below a certain rate, you can specify that rate here. Note that CCC errs on the conservative side with this rate, so the average transfer rate may be slightly lower than the limitation that you specify.

De-authenticating a remote Macintosh

If you no longer wish to use a particular remote Macintosh, you can click the **Deauthenticate...** button to remove CCC's PKA key pair from the remote Mac.

Remote Macintosh prerequisites

At this time, CCC requires the use of the root account (though it does not have to be enabled) on both the source and destination Macs. To successfully back up to a remote Macintosh, you must have administrative privileges on both machines.

CCC also requires that the remote Macintosh be running macOS 10.13 or later. Non-Macintosh systems are not supported with the **Remote Macintosh** feature.

Additional pointers for advanced users

CCC's public key-based authentication is designed to work with no additional configuration of the services required for backing up over a network connection. CCC uses rsync over an ssh tunnel to perform the backup. If you do make modifications to the sshd configuration, you should consider how that may affect your backup. For example, CCC requires use of the root account over ssh. If you set the "PermitRootLogin" key in the sshd_config file to "no", you will not be able to use CCC to or from that machine. It's an important distinction to note that the root account does not have to be **enabled**, but sshd must permit the use of the root account. The "PubkeyAuthentication" key must also not be set to "no", because Public Key Authentication is required for CCC to authenticate to the remote Mac. CCC will attempt to proactively present these configuration scenarios to you if authentication problems are encountered.

Additionally, the initial Public Key Authentication (PKA) setup requires the use of an admin user on the remote Macintosh. That admin user account must have a non-blank password, and the Remote Login service must permit password-based authentication. These requirements apply only to the initial installation of CCC's PKA credentials. Once CCC has installed these credentials on the remote Mac, CCC will use PKA for authentication to the remote Mac.

Troubleshooting connectivity problems to a remote Macintosh

Problems connecting to a remote Macintosh generally are caused by configuration problems with the Remote Login service on the remote Macintosh. Try the following if you are having trouble making a backup to a remote Mac:

1. Verify that the Remote Login service is enabled in the Sharing preference pane on the Remote Macintosh.
2. Verify that access to the Remote Login service is allowed for **All users**.
3. Re-select Remote Macintosh from CCC's Source or Destination selector and verify that authentication to the remote Mac is configured.

4. Verify that your firewall and the remote Mac's firewall permits traffic on port 22. If you have an application firewall in place (e.g. Little Snitch), verify that access is granted to CCC's privileged helper tool, "com.bombich.ccchelper".
5. If your local Mac and remote Mac are not on the same network (e.g. you're connecting across a VPN or through a router and over the Internet), confirm that a connection can be established between the two Macs. How you do this will vary from one scenario to the next, but you can generally verify connectivity by typing "ssh root@192.168.1.1" into the Terminal application (replace 192.168.1.1 with the hostname or IP address of your remote Mac). If you see a request for a password, then connectivity is established. If not, your network configuration isn't permitting the traffic, or the hostname that you're connecting to is invalid or unavailable. If you are accessing a remote Mac that is behind a router, consult the router's port forwarding documentation and verify that port 22 traffic is directed to the internal IP address of the remote Mac.

VPN and port forwarding configuration is outside of the scope of support for CCC, though our support staff will make every effort to identify whether problems are occurring within that configuration or within the service configuration on your remote Mac. If you have worked through the troubleshooting steps above and are still having trouble backing up to a remote Macintosh, please choose **Report a problem** from CCC's Help menu and submit a support request.

Meraki router intercepts Secure Shell traffic

Some users that have a Meraki router involved in their configuration have reported that its default configuration will interrupt Secure Shell traffic. The firewall rule that causes interference is in place to protect the network from vulnerabilities that are irrelevant between two modern Macs <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2002-0639>. Nonetheless, the firewall intercepts traffic after initially allowing a connection, which is presented by CCC as a "lost connection" or a failure to authenticate to the remote Mac. The following steps correct the Meraki configuration concern:

1. Log into the Meraki as an administrative user and open the "Security report"
2. Filter the log for SSH events
3. Click the "SSH_EVENT_REPOVERFLOW" event from the list to open it and review the blocked event
4. To allow the blocked traffic of this type, click "Yes" to add this event to the whitelist.

Thomson Gateway router intercepts Secure Shell traffic

Similar to the problem described above for Meraki router, the Thomson Gateway router can also cause interference that appears as an authentication failure. Forwarding traffic to a non-standard secure shell port (e.g. 2222, then be sure to specify that port when connecting to the Remote Macintosh in CCC) resolves the problem.

Norton Security "Connection Blocking" will intercept Secure Shell traffic

If you use this product on the Remote Mac, remove any "Connection Blocking" rules <https://support.norton.com/sp/en/us/home/current/solutions/v137832125> that are applicable to that Mac's Remote Login service, then restart. When prompted to allow a connection on that Mac (i.e. when you run the Remote Mac CCC task), allow the connection to proceed.

A note about access privileges to backed up data

While logged in to your remote Macintosh, you may not have permission to view the contents of your backup in the Finder. Your access to the files will be based on the unique id that is associated with the user account that you're logged in to on the remote Macintosh and the one associated with the

account(s) on the other Mac(s) that you're backing up. The first administrator account always gets a uid of "501", and subsequent accounts are assigned incrementally higher uids — 502, 503, etc. For security and privacy purposes, macOS restricts access to the contents of user home directories to the owners of those home directories, and these restrictions are preserved when your data is backed up to a remote Macintosh.

To learn what user id is associated with your account:

1. Open the **System Settings** application.
2. Click on **Users & Groups** in the sidebar.
3. Control+click on your account and choose "Advanced options...". Authenticate when prompted.

You will see your User ID in the panel that appears.

This may be annoying from the perspective of trying to access those files on your remote Macintosh, but it is important for CCC to preserve the ownership and permissions information when backing up your data. If/when you want to do a restore, you could do either of the following:

a) Attach the external drive directly to the machine that you want to restore files to — the accounts on those systems will be able to access their backed up files.

b) Do a restore directly within CCC <https://bombich.com/kb/ccc6/restoring-from-backup-on-remote-macintosh> from the original source Macintosh.

If you must have read access to some of this data (e.g. the original Mac is gone, the user account changed, etc.), you can change the ownership of the home folder and its contents in the Finder:

1. Choose **Get Info** from Finder's File menu.
2. In the **Sharing and Permissions** section at the bottom, click on the lock icon to make the permissions editable.
3. Click on the **+** button.
4. In the window that appears, select your account, then click the Select button.
5. Set the access privileges to **Read & Write**.
6. Click on the Gear menu and choose to apply the change to enclosed items.

Some CCC features are not supported on remote Macs

CCC uses its legacy file copier when using a Remote Macintosh source or destination. When using the legacy file copier, some features are not supported, e.g. Quick Update <https://bombich.com/kb/ccc6/advanced-settings#qu_remotemac>, transaction support and file copier concurrency. Snapshot support is not available for volumes attached to a remote Macintosh.

Related Documentation

- Restoring from a backup on a remote Macintosh <https://bombich.com/kb/ccc6/restoring-from-backup-on-remote-macintosh>
- A caveat for backing up to a remote Macintosh that has no user logged in <https://bombich.com/kb/ccc6/caveat-backing-up-remote-macintosh-has-no-user-logged-in>

A caveat for backing up to a remote Macintosh that has no user logged in

For improved detachability, macOS will unmount any non-internal volumes that are attached to the system when you log out. So, for example, if you log out of your computer while a USB or Thunderbolt hard drive enclosure is attached, you can detach those hard drive enclosures from the system without having to manually unmount them first. This is a good thing — it would be annoying if you had to log back in to your system just to eject a drive. The downside of this, though, is that if you have a CCC backup task that runs when no user is logged in, the destination volume may be unavailable. For a local backup, CCC will attempt to manually mount the destination volume. When the destination of your backup task is a remote Macintosh, however, CCC will not be able to mount that volume prior to backing up.

If you anticipate backing up to a remote Macintosh that may be sitting at the loginwindow, you can change the behavior of macOS to not unmount detachable volumes. To change this behavior, run this command in the Terminal application on the remote Macintosh:

sudo defaults write /Library/Preferences/SystemConfiguration/autodiskmount AutomountDisksWithoutUserLogin -bool YES

Related Documentation

- Using CCC to backup to another Macintosh on your network <https://bombich.com/kb/ccc6/using-carbon-copy-cloner-back-up-another-macintosh-on-your-network>

Restoring from a backup on a remote Macintosh

Restoring files from a remote Macintosh is nearly the same procedure as backing up to a remote Macintosh:

1. Open CCC
2. Click the **New Task** button in the Toolbar
3. Select **Remote Macintosh...** from the Source selector
4. Configure the hostname of the remote Macintosh and connect to the remote Mac
5. Choose the path to the volume or folder that has the backup.
6. Select a destination volume (do not select a macOS system volume), or a folder
7. Click the **Start** button

Related Documentation

- Using CCC to back up to/from another Macintosh on your network <https://bombich.com/kb/ccc6/using-carbon-copy-cloner-back-up-another-macintosh-on-your-network>

Task Organization

Most organization tasks are available via the Task menu in the menubar, via the Task Actions menu in the Tasks table header (i.e. the "circle with three lines" icon to the left of "Tasks"), or by right-clicking on a task or task group in CCC's sidebar.

Adding a task

Tasks can be added in several different ways. To create a new task with default settings, choose **New Task** from Task Actions menu in the Tasks table header, or choose **New Task** from CCC's Task menu, or click the **New Task** button in CCC's toolbar. You can also duplicate an existing task: select the task in the task list, then choose **Duplicate** from CCC's Task menu, or right-click on the task and choose the option to duplicate it.

If you exported tasks from CCC previously (on your current Mac or on another Mac), double-click the task configuration file to import the task(s) into CCC.

Removing a task

To remove a task, select the task in CCC's sidebar and then choose **Delete Task** from the Task Actions menu in the Tasks table header, or choose **Delete Task...** from CCC's Task menu, or right-click on the task and choose the option to delete the task. Deleting a task only removes the task configuration from CCC's database, it has no effect on any data that the task backed up to a destination volume.

Task Sorting

Tasks are sorted alphabetically in ascending order by default. To change the sort order or criteria, click on the Task Actions menu in the header of the Tasks table. Tasks can be sorted by name, last run time, next run time, last run status, or manually in the order that you define. When defining a manual sort order, simply drag and drop tasks to adjust their order. Note that disabled tasks are always placed last in a list, prior to applying other sort criteria.

Task Groups

Choose Add Task Group from the Task Actions menu in the Tasks table header to create a new task group. Add tasks to the group by dragging a task into the group. If you would like to add a task to multiple groups, hold down the Option key while dragging the task from one group to another. Task groups cannot be modified while the Task Group is running.

In their most basic form, task groups serve to organize your tasks. Each task in the group can be scheduled and configured independently of the other tasks. Task groups can also be used to run the tasks as a collection. You can run all of the tasks within a group by selecting the Task Group and clicking the Start button at the bottom of the window. CCC will run the tasks sequentially in the order defined in the **Upcoming Group and Task Events** table.

Setting the run order of tasks within a group

The order in which tasks will be run within a group is defined in the **Upcoming Group & Task Events** table. Select the Task Group in the sidebar, then click the **Upcoming Group & Task Events** button at the bottom of the window to reveal the task run order. Drag tasks within that table

to set the run order.

Note that this order may differ from the order of the tasks in the Tasks sidebar — task sort order in the sidebar is defined by the sort criteria selection in the "task actions" menu in the top-left corner of the sidebar. There is one exception to that. When the sort criteria for the tasks sidebar is set to "Manually," tasks listed within a group in the Tasks table in the sidebar will be sorted based on the order in which they are set to run (again, based on the order set in the **Upcoming Group & Task Events** table).

Scheduling task groups

Task groups can be scheduled in the same manner as individual tasks; simply click on the Automation selector, choose a scheduling basis, then define when the group should run. Tasks will be run sequentially within the group. If a task has its own schedule configuration, that task will also run independently of the task group. If the task is already running when the task group wants to start it, the task group will move on to the next task in the group. If a task is already running via the task group when its own scheduled run time arrives, the task will continue to run, and will not be run an additional time. Individual task runtime conditions will be taken into account when running the task via the task group. For example, if a task is configured to not run on weekends, that task won't run via the group if the task group runs on the weekend. The only exception to this is when you choose to run a task group manually. In that case, runtime conditions are overridden.

When a task group runs, every non-disabled task will be executed regardless of the success/failure of previous tasks in the group. The only exception is when a task is stopped. If you stop a task that was started via a task group, no more tasks in the group will be executed via the task group.

Exporting tasks and groups

Tasks can be exported individually by right-clicking the task in the Tasks table, then choose the option to export the task. You may also export all of the tasks within a task group by right-clicking the task group and choosing the option to export the group, or by choosing **Export Task Group...** from CCC's Task menu. If you would like to export all of your tasks, choose **Export All Tasks...** from CCC's Task menu.

Using the ccc Command Line Tool to Start, Stop, and Monitor CCC Backup Tasks

CCC includes a command line utility that allows you to start, stop, and monitor the progress of specific CCC backup tasks. The utility is located inside of the CCC application bundle. To get basic usage instructions, invoke the utility without arguments in the Terminal application, e.g.:

```
user@Mac ~ % "/Applications/Carbon Copy Cloner.app/Contents/MacOS/ccc"
ccc -v|--version
  Prints the version of the CCC command-
line utility (this is not the same as the main application version)
ccc -s"Task Name" | --start="My Backup Task" (-w|--watch)
  -w|--watch: Keep running and print task output until the task is finished. Ignored
for task groups.
ccc -x["Task Name"] | --stop[="My Backup Task"] [-r]
  Stop all tasks, or the specified task.
  By default the task is treated as if cancelled.
  Use -r to report the event (e.g. via Notification Center and, if configured, email)
.
  Use another non-zero value if you would like task notifications to be sent.
ccc -h|--history [-c|-d]
  Print a summary of task history, i.e. the data you would see in the table at the to
p of the Task History window.
  -c prints in CSV format
  -d prints dates in seconds since Midnight Jan 1, 1970 (rather than formatting the d
ate)
ccc -p|--print-schedules [-c|-d]
  List each task and when it will next run.
  -c prints in CSV format
  -d prints dates in seconds since Midnight Jan 1, 1970 (rather than formatting the d
ate)
ccc -w["Task Name" | --watch[="Task name"]
  Watch task progress (press Control+C to exit)
  Specify a task name to limit task output to the indicated task
ccc -i|--status
  Print a status line for each task.
ccc -g|--global globalDefaultName [bool|int|float|string] globalDefaultValue
  Set a global default value.
ccc -g|--global globalDefaultName delete
  Delete a global default value.
ccc -n|--notification notificationTitle notificationBody
  Send a notification to the Notification Center.
ccc -z["Task Name"] | --disable[="Task Name"]
ccc -e["Task Name"] | --enable[="Task Name"]
  Disable or enable all tasks [or a specific task].
ccc -u | --uuids
  Print task names and their unique identifiers.
```

Here are some examples of how to use the CCC command-line tool to start and stop a task, and get its last history event:

```
[user:~] cd "/Applications/Carbon Copy Cloner.app/Contents/MacOS"
[user:/Applications/Carbon Copy Cloner.app/Contents/MacOS] ./ccc -s"CCC Backup Task"
-w
04/24 12:52:19 : CCC Backup Task [Data copied: Zero KB, Progress: -1.000000%] Prepari
ng...
04/24 12:52:20 : CCC Backup Task [Data copied: Zero KB, Progress: -1.000000%] Testing
 write responsiveness of the destination...
04/24 12:52:20 : CCC Backup Task [Data copied: 126 bytes, Progress: 0.076235%] Compar
ing and copying files
04/24 12:52:21 : CCC Backup Task [Data copied: 126 bytes, Progress: 1.146266%] Compar
ing and copying files
04/24 12:52:21 : CCC Backup Task [Data copied: 126 bytes, Progress: 1.963699%] Compar
ing and copying files
04/24 12:52:22 : CCC Backup Task [Data copied: 126 bytes, Progress: 3.048320%] Compar
ing and copying files
^C

[user:/Applications/Carbon Copy Cloner.app/Contents/MacOS] ./ccc -x"CCC Backup Task"
Stopping CCC Backup Task

[user:/Applications/Carbon Copy Cloner.app/Contents/MacOS] ./ccc -h | head -n 1
CCC Backup Task|Macintosh HD|SSD Macintosh HD Backup|4/24/20, 12:52 PM|0:19|126 bytes
|Cancelled|0
```

Backing up large files, mounted disk images, and Virtual Machine containers

Note: When backing up an APFS-formatted volume, CCC will copy files from a read-only snapshot of the source volume. The subject of this article is not applicable in those cases.

Mounted disk images and running Virtual Machine container files pose an interesting problem to incremental backup utilities. By simply being mounted and accessed (e.g. via browsing the contents, booting the VM), the content of these large files are subject to modification by the applications that use those files. If you run a CCC backup task while a read/write disk image is mounted or while a VM container's OS is booted, there is a chance that the disk image file or VM container will be modified while it is being backed up, resulting in a corrupted version of the file on your backup volume.

If you have disk image files or VM containers that are regularly in use on your system, you should exclude these items from your backup routine and configure an alternate backup task for these items that runs when they are not in use. Alternatively, you could quit or suspend the applications that modify those files for the duration of the backup (see the "Example pre- and postflight shell scripts" link below for examples of how to automate this).

If errors do occur while backing up large files, quit or suspend the applications that modify those files, then simply run the backup task again to correct the copy of the file on the backup volume.

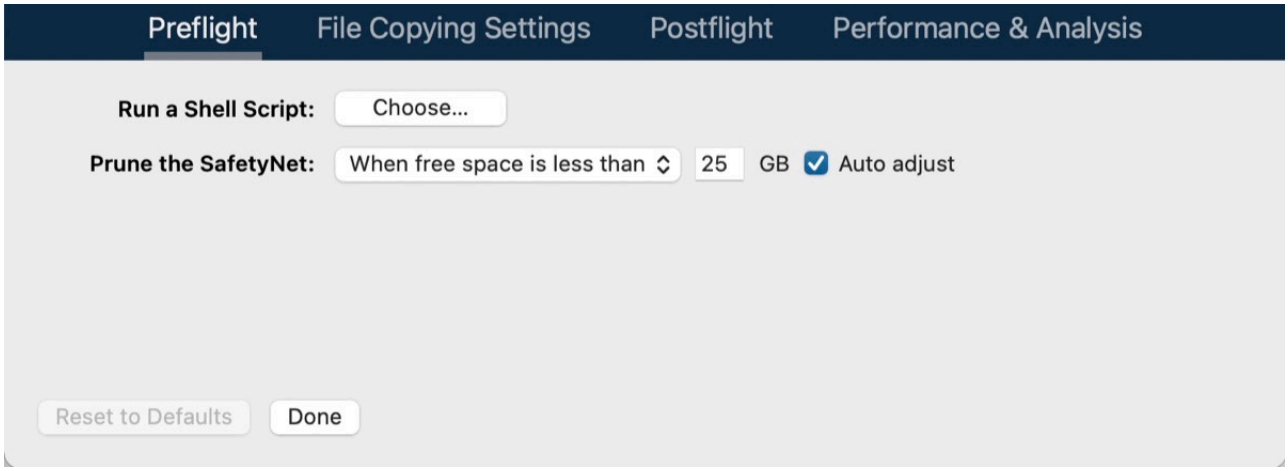
Related Documentation

- Example pre- and postflight shell scripts <https://bombich.com/kb/ccc6/performing-actions-before-and-after-backup-task#examples>
- Creating a separate task to prevent VM container versions from bloating the SafetyNet <https://bombich.com/kb/ccc6/creating-separate-task-prevent-vm-container-versions-from-bloating-safetynet>
- Leveraging Snapshots on APFS Volumes <https://bombich.com/kb/ccc6/leveraging-snapshots-on-apfs-volumes>

Automated maintenance of the CCC SafetyNet folder

This article's content is not relevant when snapshot support is enabled on an APFS-formatted destination volume. See Toggling snapshot support and setting a Snapshot Retention Policy <https://bombich.com/kb/ccc6/leveraging-snapshots-on-apfs-volumes#srp> for more information on SafetyNet Snapshot retention.

CCC will move previous versions of modified files, as well as files deleted since previous backup tasks to a SafetyNet folder at the root of the destination. If left unmanaged, this SafetyNet folder would eventually consume all free space on your destination volume. To prevent that from happening, CCC prunes the contents of the SafetyNet folder at the beginning of each task if free space is less than 25GB. This limit is automatically adjusted if a 25GB limit is too low for a particular source and destination. You can customize these settings by clicking on the **Advanced Settings** button at the bottom of CCC's main window.



SafetyNet pruning occurs at the beginning of a backup task, so CCC will never delete an item that was archived in the current backup task. Additionally, pruning is always limited to the contents of the _CCC SafetyNet folder that is at the root of the destination. CCC's pruner won't delete the current versions of files on your destination, nor anything outside of the scope of the CCC backup task. Lastly, archive pruning works at a macro level. If any portion of an archive pushes past the limit that you have imposed, the entire archive (e.g. the time-stamped folder) will be pruned.

Note for "New disk image" destinations: CCC applies more aggressive SafetyNet pruning to disk image volumes <https://bombich.com/kb/ccc6/backing-up-disk-image#safetynet>. By default, CCC will prune any SafetyNet content older than 1 day.

Automatically prune archived content before copying files

Prune archives in the SafetyNet when free space is less than [xx] GB

If your destination volume has less free space than the limit that you have specified, CCC will prune the oldest archive. CCC will continue to prune the oldest archive until the requested amount of free space has been achieved. Note that if the archives cumulatively consume less space than the limit requested and the destination volume is full, CCC will prune all of the archives.

Auto Adjustment of the SafetyNet Free Space pruning limit

When the Auto Adjust option is enabled (and it's enabled by default), CCC will automatically increase the free space pruning limit if your destination runs out of free space during the backup task. For example, if your pruning limit is set to the default of 25GB, and you have 25GB of free space at the beginning of the backup task, no pruning will be done at the beginning of the task. If that task proceeds to copy more than 25GB of data, however, the destination will become full. CCC will then increase the pruning limit by the larger of either the amount of data copied in the current task, or by the amount of data that was required by the last file CCC attempted to copy. For example, if CCC copied 25GB of data, then the pruning limit would be increased by 25GB. If CCC wanted to copy a 40GB file, however, CCC would not fruitlessly copy 25GB of that file, rather it would immediately increase the pruning limit by 40GB, revisit pruning, and then resume copying.

Prune archives in the SafetyNet when they are older than [xx] days

CCC will prune archives that were created more than "xx" days ago.

Prune archives in the SafetyNet when they are larger than [xx] GB

Starting with the most recent archive, CCC will determine the amount of disk space that each archive consumes. When the cumulative total exceeds the limit that you have imposed, CCC will prune the remaining, older archives. If the newest archive is larger than the limit that you have specified, that archive will be pruned in entirety.

Never prune archives in the SafetyNet

CCC will not automatically prune the contents of the "_CCC SafetyNet" folder at the root of the destination. Archived files may eventually consume all of the free space on the destination, so you should periodically delete older archive folders to maintain enough free space for future backups. You may delete the contents of the SafetyNet folder without harm to the rest of your backup set.

"CCC is pruning my SafetyNet, but the disk is still pretty full at the end of the backup task"

The purpose of CCC's SafetyNet pruning is to make space for additional backups. CCC also avoids pruning items that were very recently archived — after all, it wouldn't make sense to archive an item on the destination, them immediately delete it. To accommodate both of these goals, CCC prunes archives within the SafetyNet before the backup task runs. Pruning the SafetyNet immediately before copying files gives a greater level of assurance that the requested amount of free space (for example) will be available for the current backup. Be sure to consider this detail when specifying your SafetyNet pruning settings. If you want to retain additional space on your backup volume beyond what is required for your CCC backups, specify more liberal limits (e.g. 100GB of free space rather than 25GB).

"Can I use the _CCC SafetyNet folder for long-term archiving of specific items?"

We don't recommend using the SafetyNet for long-term storage. CCC is configured to automatically prune the SafetyNet, by default, when free space on the destination is less than 25GB at the beginning of the backup task, and that limit may increase automatically. CCC doesn't consider whether items in the _CCC SafetyNet folder were placed there by CCC or another application, everything is considered safe to delete when the time is right. If you would like to maintain a permanent archive of items on your backup volume, outside of your CCC backup, we recommend

that you create a separate volume on your backup disk for this purpose <https://bombich.com/kb/ccc6/i-want-back-up-multiple-macs-or-source-volumes-same-hard-drive>.

We also recommend that you maintain a backup of your archived data on another volume! If you don't have a backup of your long-term archived items, you're going to lose them forever if your backup disk fails.

"I manually moved the _CCC SafetyNet folder to the Trash, but now I get an error when trying to empty the Trash"

When CCC backs up your startup disk, it runs with the privileges required to access system files that are not normally accessible to your account. Naturally, some of these files will be updated on the source, and subsequently archived on the destination. When you place these items in the Trash (by placing the _CCC SafetyNet folder in the Trash), and subsequently try to empty the Trash, the Finder typically requests that you authenticate to remove these files. Sometimes the Finder is having a bad day, though, and it simply reports the enlightening "-8003" error when you try to empty the Trash (or something equally obtuse). This error isn't defined or documented anywhere, but through trial and error, we have figured out that it simply means "I can't cope with your request to empty the Trash".

The solution is to avoid using the Finder to delete a CCC SafetyNet folder. Choose **Delete a SafetyNet Folder** from CCC's **Utilities** menu instead and use that interface to manually remove SafetyNet folders.

Related Documentation

- Frequently asked questions about the CCC SafetyNet <https://bombich.com/kb/ccc6/frequently-asked-questions-about-carbon-copy-cloner-safetynet>

Backing up to/from network volumes and other non-macOS-formatted volumes

In addition to backing up to volumes formatted with the macOS standard HFS+ or APFS format (collectively referred to as "macOS-formatted" from here forward), CCC can copy user data files to network volumes (e.g. AFP and SMB via macOS and Windows File Sharing) and to other non-macOS-formatted volumes such as FAT32 or ExFAT. Non-macOS-formatted volumes are presented in CCC's Source and Destination selectors in the same manner as macOS-formatted volumes, so there are no special steps required for backing up to or from these filesystems. However, these filesystems offer limited support for macOS-filesystem features, so special consideration must be given when backing up to these volumes. In general, you can reasonably expect to back up user data — files that belong to your user account — to and from non-macOS-formatted volumes. Specific considerations are noted below.

You can mount network volumes in the Finder, or via the **Mount a network volume...** option in CCC's **Utilities** menu. Please note that network volumes mounted by third-party software is generally not supportable.

CCC will only back up system files to or from locally-attached macOS-formatted filesystems

macOS can only be installed on a macOS-formatted volume. This requirement is also carried to a backup volume. When system files are copied to or from non-macOS filesystems, important metadata are unavoidably lost, resulting in files that cannot be restored to their original functionality. In short, you cannot restore a functional installation of macOS from a backup stored on a non-macOS volume. To prevent any misunderstandings about this result, CCC will exclude system files from a backup task if the destination is not a locally-attached, macOS-formatted volume. Likewise, CCC will not copy system files **from** a network volume, e.g. if you were to mount the startup disk of another Mac via File Sharing, the system files on that network volume cannot be copied in a meaningful way.

Note that the "locally-attached" caveat is an important distinction. Even if your destination volume is macOS-formatted, if it is attached to an Airport Base Station (for example), then you're accessing the volume via file sharing. If you open the Get Info panel for the volume, you will see that the volume format is "AppleShare" or "SMB", not HFS+ or APFS.

Related Documentation

- Preparing your destination disk for a backup or restore <https://bombich.com/kb/ccc6/preparing-your-backup-disk-backup-os-x>

Ownership and permissions concerns

Network filesystems pose some interesting challenges in regards to preserving ownership and permissions. When you connect to another computer that is hosting a shared volume, you usually authenticate by providing a username and password. The account whose credentials you provide is an account on that other computer, and it is this account's privileges that determine what access

you have to files and folders on the shared volume. Additionally, any files that are copied to the shared volume will be owned by that user account, regardless of the ownership of those files on the source volume. This is not a behavior specific to CCC, it is simply the nature of network filesystems.

An example will be very helpful in understanding the implications of this behavior. Suppose Sally would like to back up some Movies from her Mac's home folder to another Mac shared by Bob and Joe. On Sally's Mac, there is a user account named "sally". On Bob and Joe's Mac, File Sharing has been enabled in the Sharing Preference Pane, and there are two user accounts, "joe" and "bob". Bob has attached an external hard drive named "Backup" to his Mac that he and Joe have been using for backup, and he has created a folder named "Sally's Movies" on this volume to which Sally will copy files. Sally does the following to connect to Bob and Joe's Mac:

1. In the Finder, open a new window, then click on "Bob and Joe's Mac" in the Shared section of the sidebar.
2. Click on the **Connect as...** button.
3. In the authentication dialog, provide Bob's username and password, then click on the Connect button.
4. Choose the "Backup" volume from the list of shared volumes.

The Backup volume now appears on Sally's Desktop, and in CCC's Destination selector in the Network Volumes section. Next, Sally chooses **Choose a folder...** from CCC's Source selector and locates the folder of movies that she would like to copy to Bob and Joe's Mac. She then chooses **Choose a folder...** from the Destination selector and locates the "Sally's Movies" folder on the Backup network volume. She clicks the **Start** button and the Movies are backed up.

Later that day, Joe is using his computer and he notices that he can see some of the movies in the "Sally's Movies" folder, but some of the subfolders have a universal "No access" badge and he cannot view those folders' contents. This occurred for two reasons:

1. Sally mounted the network volume using Bob's credentials, so the files and folders created when she copied her files to the Backup volume are now owned by Bob's user account.
2. Some of the folders on Sally's computer prevented access by "other" users.

As a result, the folders on the Backup volume are owned by Bob and some of them limit access to other users (Joe in this case). Joe asks Sally about this and she decides to try copying some of the movies to one of Joe's folders on the backup volume. When she chooses **Choose a folder...** from CCC's Destination menu, however, she sees the same universal "No Access" badge on Joe's folder. Sally can't copy files to this folder (nor can CCC) because the Backup volume was mounted using Bob's credentials, and Joe's backup folder on the backup volume happened to be inaccessible to Bob. Sally unmounts the backup volume and reconnects to it using Joe's credentials, and she is then able to copy files to Joe's private folder.

What can I do when there are permissions or ownership issues that prevent CCC from copying items to/from or updating items on a network volume?

First, it is important to keep in mind that no application can modify the ownership of a file or folder on a network share. Ownership changes must be applied on the computer or device that is hosting the network volume. Additionally, permissions changes can only be made to files and folders owned by the user whose credentials were used to mount the network volume. For this reason, it is generally easier to apply both ownership and permissions changes on the computer or device hosting the network volume.

If the computer hosting the network volume is a Mac, you can modify ownership and permissions in

the Get Info panel for that folder (on the Mac hosting the network volume):

1. In the Finder, click on the folder whose permissions or ownership you would like to change.
2. Choose **Get Info** from the File menu.
3. In the **Sharing & Permissions** section at the bottom, click on the lock icon to make the permissions editable.
4. To change permissions, choose **Read & Write** from the popup menu next to the owner of the file or folder.
5. If the owner of the item is not the user account that you use to connect to this Macintosh, click on the **+** button
6. In the window that appears, select the user account that you use to connect to this Macintosh, then click the Select button.
7. Set the access privileges to **Read & Write**.
8. Click on the "additional actions" menu and choose to apply the change to enclosed items.
9. Try your backup task again.

If the computer or device that is hosting the network volume is not a Macintosh, consult that device's documentation to learn how to change permissions and ownership of files and folders.

Alternative #1: If you have mounted the network volume with **Guest** privileges, unmount and remount the network volume using the credentials of an account on the machine or device hosting the network volume.

Alternative #2: You can create a new folder on the shared volume and specify that folder as the destination in CCC by choosing **Choose a folder...** from the Destination selector.

Alternative #3: You can have CCC create a disk image <https://bombich.com/kb/ccc6/i-want-back-up-my-whole-mac-time-capsule-nas-or-other-network-volume> on the network volume rather than copying files directly to a folder. When CCC creates a disk image on the destination, the disk image is formatted to match the source and attached locally, so CCC can preserve the permissions and ownership of the files that you are copying to it.

Why can't I change the username when CCC prompts for NAS volume credentials?

When you select a NAS volume as the source or destination to a CCC task, CCC will prompt for the credentials that were used to mount that volume. CCC already knows the user name for that volume, that value is published in the "filesystem URL" attribute of the mounted NAS volume (you can type mount into the Terminal application to see that value). CCC asks for the password so that CCC can remount the NAS volume automatically later. In order to avoid ownership or permissions issues, CCC will remount the NAS volume using the exact same user account that was used to mount the NAS volume in the Finder – this is why the username field cannot be modified.

If you would like to use a different user account to mount the NAS volume, then you should eject the NAS volume in the Finder and remount it using the preferred user account. Once the volume is remounted, reselect the NAS volume (or a folder on that NAS volume) as the source or destination to your task. If CCC does not have the credentials for the user account that was used to mount the NAS volume, CCC will again prompt for those credentials.

Limitations of non-macOS-formatted filesystems

When you choose a non-macOS-formatted volume as a destination, CCC's Cloning Coach will proactively warn you of any compatibility issues between the source and destination volumes. You can view the Copy Coach's warnings by clicking on the yellow caution button in the Task Plan box. If

you have selected a source and destination volume, and the caution button is not present, then there are no configuration concerns.

Support for third-party filesystems

CCC offers limited support for third-party filesystems, such as those provided by FUSE for OS X <https://osxfuse.github.io>. Due to the large number of filesystems that can be provided by FUSE, CCC provides generic support for these "userland" filesystems rather than specific support. CCC takes a best effort approach by determining the capabilities of the source and destination filesystems, warns of potential incompatibilities, then presents only unexpected error conditions that arise during a backup.

Backing up to FUSE volumes mounted without the allow_root flag is not currently supported (e.g. Google Drive, BitCasa). Please contact the vendor of your proprietary filesystem to ask that they offer the ability to mount the volume with the allow_root flag if you would like to use that volume as a source or destination to a CCC backup task.

Support for Google Drive is "best effort". We've seen odd behavior when selecting 'Google Drive for desktop' volumes as a whole as the source or destination for a task – CCC is unable to read the root folder during a backup task. CCC explicitly disallows that configuration. Selecting a subfolder on the Google Drive volume often works, and CCC will not disallow that configuration, however we frequently receive reports of inconsistent results when backing up to Google Drive, so we cannot offer support for this configuration.

There is one other notable concern with 'Google Drive for desktop' – Google Drive will download files when they are accessed if they do not currently reside on your Mac's hard drive. If you specify a Google Drive folder as the source to a backup task, you should anticipate that cloud-only files may be downloaded to your Mac during the backup task. That behavior lies outside of CCC's purview, it cannot be modified with a CCC task setting.

The Western Digital MyCloud Home NAS device is another special case. The "Home" model of this NAS device requires the use of WD-proprietary software to access the storage securely; direct access to the storage via SMB is only available with Guest privileges. Users report <https://community.wd.com/t/use-my-cloud-home-with-finder-without-wds-app/216769/4> that performance of the storage while using WD's software is subpar in comparison to Guest access via SMB, and other users have reported to us that macOS is unable to create or mount disk images on the storage when mounted via Western Digital's software. When you mount WD MyCloud Home NAS storage using WD's software, the volume is vended by a 'kddfuse' filesystem. CCC won't allow these volumes as a source or destination device. To back up to a WD MyCloud Home NAS, mount the storage via SMB in the Finder instead <https://support-en.wd.com/app/answers/detail/a_id/24148/kw/smb%20macos#subject1>. Be sure to choose the "Guest" user option when prompted to authenticate, because the MyCloud Home device doesn't support authenticated access via SMB.

Writable NTFS filesystems

We have seen several reports of problems copying large amounts of data (e.g. > 4GB) to writable NTFS filesystems. In most cases, the underlying software that vends the filesystem (e.g. Tuxera, Paragon, and others) crashes and the volume is rendered "mute". While it may be possible to complete a backup to these filesystems in chunks (e.g. 4GB at a time), we recommend using a more reliable, writable filesystem if you encounter these problems.

Related Documentation

- Learn more about formatting volumes on macOS <https://bombich.com/kb/ccc6/preparing-your-backup-disk-backup-os-x>

Backing up a Boot Camp installation of Windows

CCC can back up the user data on a Boot Camp volume, but it cannot make an installation of Windows bootable. If your goal is to back up your user data on the Boot Camp volume, CCC will meet your needs. If you're looking to migrate your Boot Camp volume to a new hard drive, you might consider an alternative solution such as WinClone, or one of the commercial virtualization solutions that offer a migration strategy from Boot Camp.

Backing up the contents of an NTFS volume

The NTFS filesystem supports "named streams", a feature that is comparable to extended attributes on macOS-formatted volumes and many other filesystems. Unlike extended attributes, however, there is no limit to the amount of data that can be stuffed into NTFS named streams (aside from standard file size limitations). Extended attributes on macOS have a 128KB size limit. As a result, any attempts to copy a named stream larger than 128KB to a non-NTFS filesystem will fail. CCC will copy the standard file data just fine, but will not copy named streams larger than 128KB. CCC's Copy Coach will warn of this kind of incompatibility, and any errors related to this limitation will be logged to the CCC log file, however these errors will not be raised to your attention.

This limitation applies when copying files between volumes on Windows as well, so application developers tend to use named streams only for data that can be regenerated (e.g. thumbnail icons, summary or statistical information), not for storage of irreplaceable user data.

NAS service failures can lead to unreliable backups

Access to the contents of a network volume is provided by an application that runs on another computer or Network Attached Storage (NAS) device. Every NAS device and operating system has its own vendor-specific version of the file sharing application, so we occasionally see problems with some NAS devices that don't occur on others. Problems can be minor, such as being unable to set file flags (e.g. hidden, locked) on an item, or more significant, like not being able to store or retrieve resource forks. When these problems are encountered during a backup task, CCC will copy as many files and as much data as possible, then offer a report on the items or attributes that could not be copied.

When you encounter an error caused by the file sharing service that hosts your network volume, there are a few workarounds that you can try to avoid the errors:

- Eject the network volume on your Mac, then restart the computer or NAS device that is hosting the network volume. Reconnect to the network volume and try the backup task again.
- Connect to the network volume using a different protocol. A different application is responsible for each protocol, so if the AFP service on your server has a bug, connecting to the SMB service may work more reliably (and vice versa). Follow these steps to connect to the server using a different protocol:
    1. Eject the NAS volume if it's currently mounted
    2. Open CCC and select the applicable backup task
    3. Click on the Source or Destination selector (whichever is applicable for your particular task)
    4. Hold down the Option key and choose "Switch to {the other protocol}" (provide the credentials for the NAS volume again if prompted)
    5. Save and run the task

- If the errors persist when connecting to the network volume via both AFP and SMB, and restarting the file server does not change the outcome, then we recommend that you back up to locally-attached storage instead.

Some NAS services have obtuse file name restrictions

Some NAS file sharing services will automatically rename files to "DOS compatible" names, or simply issue errors when working with various file names. In particular, files or folders that start or end with a space character, or names that contain a colon (:) or slash (/) character are unacceptable. When the file sharing service encounters files or folders with these disallowed characters, it will either report an "invalid argument" error, or it will automatically rename these items, e.g. " filename.txt" would become "_1CZVG~B". This "mangling" of file and folder names inevitably leads to errors during a backup task.

Non-ASCII characters (e.g. é, ö) can also lead to conflicts on NAS volumes. If you see errors where each "affected item" has a non-ASCII character somewhere in its path, refer to Character composition conflicts on NAS volumes <https://bombich.com/kb/ccc6/character-composition-conflicts-on-nas-volumes> to see how to identify and resolve the issue.

Another common issue that people encounter when copying files to a NAS volume is errors that are the result of a name restriction. For example, Synology NAS devices (and many others) disallow file names <https://kb.synology.com/en-ca/DSM/tutorial/file_or_folder_name_displayed_as_12HWA0_8> that start with .lock, CON, PRN, AUX, NUL, COM0 - COM9, LPT0 - LPT9, _vti_, desktop.ini, any filename starting with ~$. These NAS devices often produce bogus error codes in these cases, e.g. "File name too long". Some NAS devices have specific character restrictions as well, e.g. NAS devices that follow the Microsoft OneDrive naming conventions <https://support.microsoft.com/en-us/office/invalid-file-names-and-file-types-in-onedrive-and-sharepoint-64883a5d-228e-48f5-b3d2-eb39e07630fa>, which exclude " * : < > ? / \ |, and leading and trailing spaces in file or folder names also aren't allowed. Many people run into this same problem when making backups of the GarageBand application because there is a folder in the application bundle named "Aux".

There are three different ways to avoid these errors:

Rename the offending files or folders on the source

If you're only seeing this error on a handful of files, then renaming the files on the source to appease the Windows naming conventions may be the simplest way to resolve the errors. Do not attempt to rename folders that reside inside of an application bundle, though (e.g. GarageBand.app).

Connect to the NAS device using AFP instead

Windows naming conventions are typically only applied by the SMB file sharing service, so you may be able to connect via AFP instead to avoid the NAS limitation. Note that some NAS devices no longer support AFP, so this workaround may not be an option in your case.

1. Eject the NAS volume if it's currently mounted
2. Open CCC and select the applicable backup task
3. Click on the Source or Destination selector (whichever is applicable for your particular task)
4. Hold down the Option key and choose "Switch to AFP" (provide the credentials for the NAS volume again if prompted)
5. Save and run the task

Change the SMB service configuration on the NAS

If your NAS device allows changes to its SMB configuration, you can add "mangled names = no" to

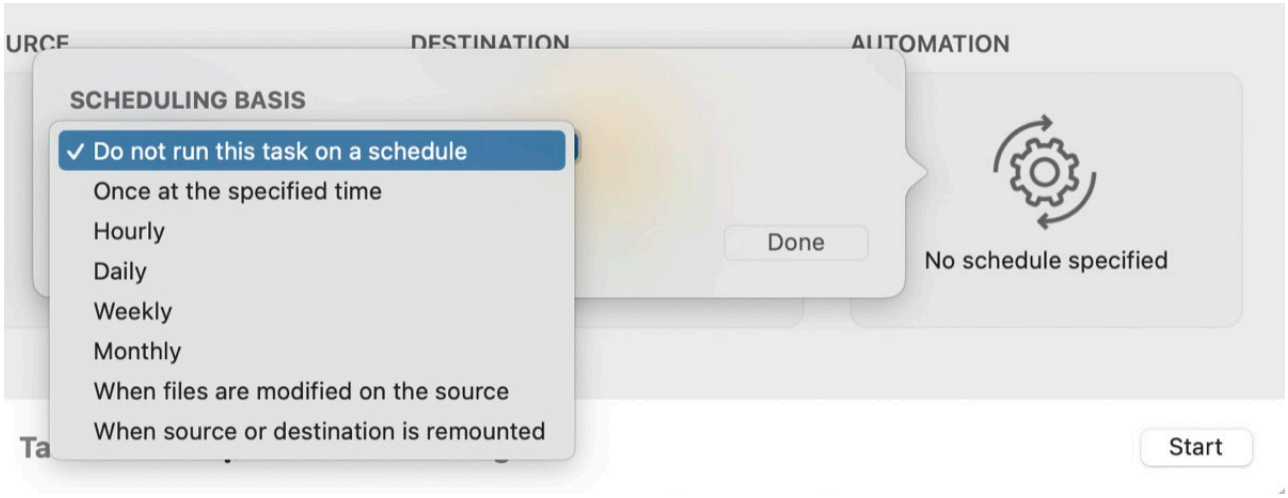
the end of its smb.conf file to disable SMB name mangling (that setting is documented here <https://www.samba.org/samba/samba/docs/man/manpages/smb.conf.5.html#idp60809664>). We can't offer documentation on how to do this for every NAS device available, but we do a fair amount of testing against Synology's DiskStation, and the procedure goes like this:

1. Connect to the DiskStation via ssh (e.g. in Terminal, ssh admin@fileserver.local)
2. Append the smb.conf file:
   sudo -s
   echo "mangled names = no" >> /etc/samba/smb.conf
3. Unmount, then remount your NAS volume, then try running your CCC backup task again

Please note that this change is explicitly not supported by Synology (nor us), so proceed at your own risk. We have, however, submitted a feature request to Synology to add support for changing this setting in the Disk Station Control Panel. It's the 2020s, Windows naming conventions from the 1990s are a bit archaic at this point.

Advanced Scheduling Options

Scheduling Basis



CCC offers seven different bases for automating backup tasks, giving you exceptional control over how and when your backup tasks run.

Do not run this task on a schedule

Select this option when you prefer that the task only run when you click the Start button. Note that you do not have to select this option to prevent a scheduled task from running. If you would like to temporarily disable a task, right-click on the task in CCC's sidebar and choose the option to disable the task. Likewise, you can suspend all tasks via the CCC Dashboard <https://bombich.com/kb/ccc6/monitoring-backup-tasks-ccc-menubar-application#disable_tasks>.

Run once at the specified time

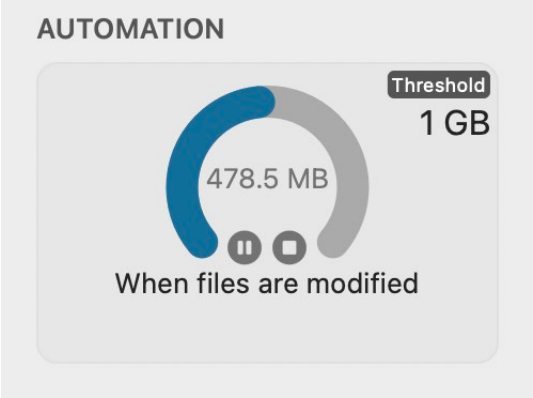
This option is convenient when you would like to run a task in the near future, but not automatically thereafter. When the task completes, it will be reset to "Do not run this task on a schedule".

Hourly, Daily, Weekly, Monthly

When you want your task to run at specific times or intervals, these options give you the most precision.

When files are modified

This setting causes the task to monitor filesystem activity on the source. When folders are modified on the source, CCC will periodically enumerate the changes in those specific folders to determine how much data has been modified on the source since the task's last successful run. When the changes exceed your specified threshold (which is defined in GB, but you can specify 0.01, for example, to specify a lower value than 1GB), the task will run, copying just the items that have changed. This setting also offers a time-based threshold to avoid running the task too frequently.



When a task is actively monitoring the source, the Automation box will present a graphic that indicates how much data has been modified as a percentage of your defined threshold. If the data modification threshold has been reached, but the time threshold has not yet been reached, CCC will indicate that the task will run when the time threshold is met. Data changes are updated approximately every 30 seconds.

When a task is currently monitoring source filesystem activity, task settings cannot be modified (including the thresholds that determine when the task will run). If you would like to make changes to the task settings, click the ⏸ button in the Automation box to temporarily suspend monitoring. If you would like to remove the filesystem monitor altogether, click the ⏹ button in the Automation box.

CCC will suspend source volume monitoring if:

- The task is running and you stop the task (if we don't suspend monitoring, it would simply start running again)
- If the source or destination volume is unmounted

After reviewing any errors and taking any necessary corrective action, you can click the "play" button to resume monitoring. If monitoring was suspended because the source or destination was unmounted, CCC will automatically resume monitoring when the missing volume is remounted as long as no errors occurred during the last task event.

Overriding Quick Update behavior to perform a complete scan of the source: You can click the **Run Now** button any time to immediately update the destination using the Quick Update behavior. If you would like the task to perform a complete scan of the source, click the **Standard Copy** button instead.

This option requires an APFS or HFS+ source volume: Our testing of this functionality has been focused on Apple-formatted filesystems, so it is currently limited to source volumes formatted as APFS or Mac OS Extended, Journaled. We welcome your feedback on this <https://bombich.com/software/get_help>, and we will consider making this option available for other source volume formats in the future.

This option is not available for "transient" destinations: This features relies on the source and destination being reliably available for monitoring. While CCC will accommodate the mounting and unmounting of local volumes for this scheduling option, this option is not available for tasks involving network volumes, nor disk image destinations.

When the source or destination is remounted

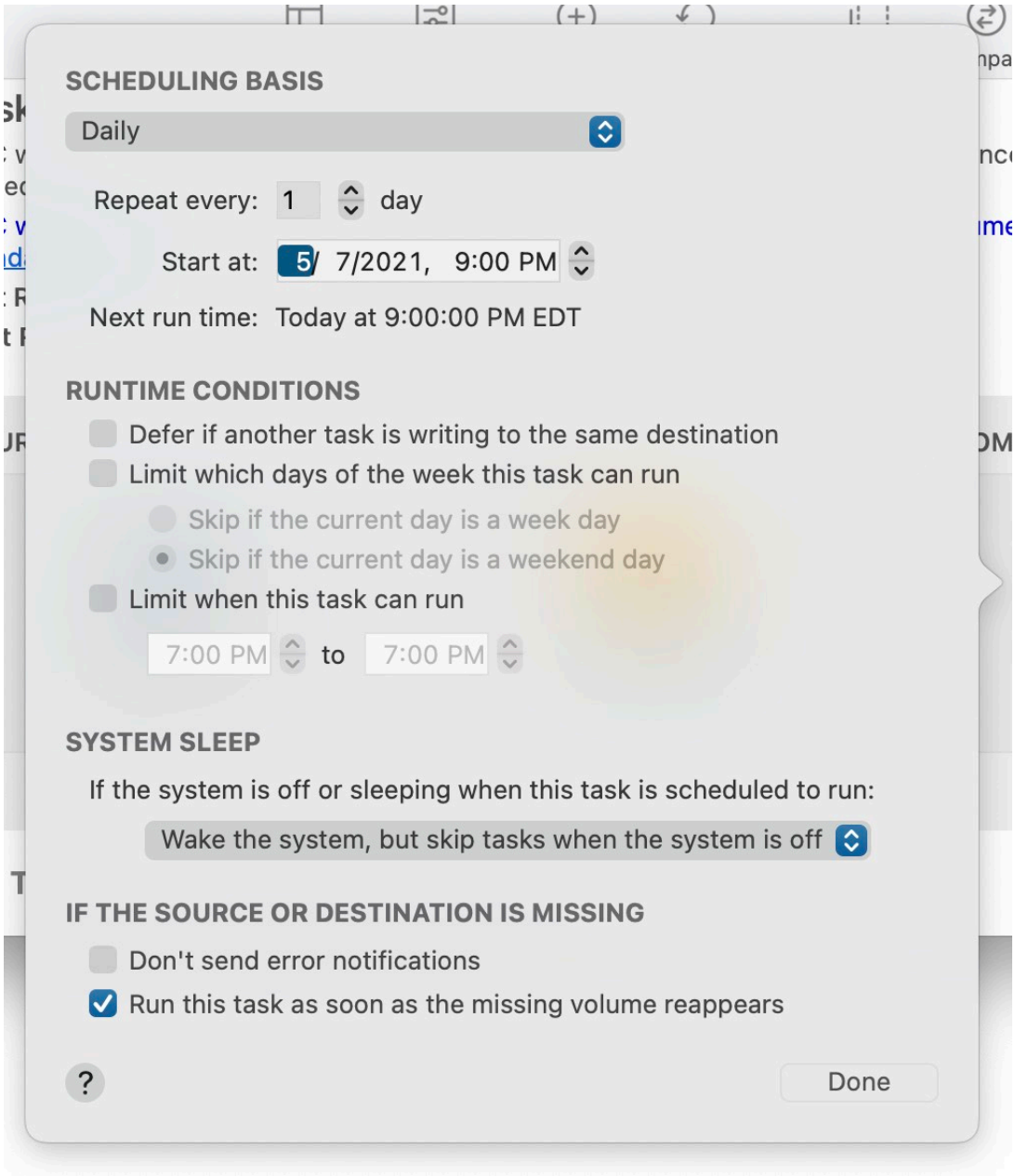
Use this option when you want your task to run when your source or destination volume is remounted. When a task is configured in this manner, volume mount notifications are used to trigger the task. A task will only run when both volumes are present **and mounted**. Note that CCC will not automatically mount the source, for example, if it is not mounted when the destination reappears. Also note that CCC imposes a deliberate 60-second moratorium on task activity when the system is turned on. This task automation option is not designed to run tasks when volumes are mounted on startup.

By default, CCC will immediately run a task configured in this manner when the source or destination reappears. If you prefer, CCC can prompt you to run the task when a volume reappears, and CCC can also present a reminder if the task hasn't run after a particular amount of time. These prompts are presented by the CCC Dashboard <https://bombich.com/kb/ccc6/monitoring-backup-tasks-ccc-menubar-application#activity>, which offers additional settings for how reminders are presented to you. Click on the Activity tab's Settings icon in CCC Dashboard to configure those settings.

Lastly, you can configure a "throttle" to prevent these tasks from running too frequently. If you detach and reattach your backup disk frequently throughout the day, for example, you can configure the task to run no more frequently than once per day. Note that this interval can be specified as a decimal value. For example, if you would like the task to run no more frequently than twice per day, you can configure the threshold as "0.5".

Runtime Conditions

Sometimes time-based scheduling is insufficient to describe exactly how you want your tasks to run. CCC offers **runtime conditions** which allow you to restrict the running of your tasks under certain conditions when the task is normally scheduled to run.



Defer if another task is writing to the same destination

If you have more than one scheduled task that writes to the same destination volume, you may want to configure the tasks to wait for one another such that only one task is writing to the volume at a time. When you configure a task with this setting and the scheduled run time elapses, CCC will place the task into a queue for deferred execution if another task is already writing to that same destination. Assuming another run time condition does not prevent it, CCC will run the deferred task as soon as the first task finishes writing to the shared destination volume.

Limit which days of the week this task can run

This option allows you to limit a task to running only during weekdays or only during weekend days. This option is not applicable to the "weekly" and "monthly" scheduling settings.

Limit when this task can run

This option allows you to limit a task to running during specific hours of the day. For example, if you don't want your hourly task to run in the afternoons, you could set a start limit of 6PM and an end limit of 12PM. This limit would allow the task to start any time after 6PM and any time up to 12PM, thus preventing the task from running between 12PM and 6PM. If the task is already running (e.g. if it started at 11:55AM), CCC will stop the task if it is still running when the end limit is reached.

Note: Set the task start time before you attempt to set time limits. CCC will not allow you to specify a time limit that does not contain the current start time of the task.

Handling system sleep events

By default, CCC will not wake your computer when your tasks are scheduled to run. You can change this setting in the **System Wake or Power On Behavior** section of the Automation popover. There are five options:

Wake the system, but skip tasks when the system is off

CCC will configure a wake event to wake the system shortly before the task runs, so the task should run on schedule. If the system is turned off, this wake event will not turn on the system. When the system is restarted (i.e. after having been turned off for a while), any tasks missed while the system was off will run at the next scheduled run time. This setting wakes the display. If you do not want your display to wake, use the **Run when the system next wakes** setting instead.

Wake or power on the system

CCC will configure a **wake or power on** event to wake the system or turn it on shortly before the task runs, so the task should run on schedule. This setting wakes the display. If you do not want your display to wake, use the **Run when the system next wakes** setting instead.

*Pro tip: You can view scheduled wake/power on events in the System Information application. Choose **About This Mac** from the Apple menu, click **More Info**, scroll down and click on **System Report**, then select the **Power** item in the sidebar.*

Notes: A Mac will not power on automatically if it is not connected to AC power. This setting is not available when FileVault is enabled on the startup disk. When FileVault is enabled, you must enter a password on startup for the system to complete the boot process.

Run when the system next wakes

Upon a wake notification, CCC will run the backup task if its scheduled run time has passed. The task will not run exactly when it is scheduled, though CCC can run tasks during macOS **Dark Wake** events (aka **PowerNap**, aka **Maintenance Wake**), which occur every couple hours. If you want your backup tasks to run in the middle of the night without turning on your display, this is the right option for you.

Run when the system next wakes or powers on

Like the setting above, except that tasks missed when the system was off will start immediately when the system is turned on.

Skip this task

CCC will run the task only at its scheduled run time if the system is awake at that time. Upon a wake event, CCC will not run a backup task if the scheduled run time has passed.

Configuring behavior for when the source or destination is missing at the scheduled run time

Don't send error notifications

By default, CCC will report an error if the source or destination volume is unavailable when the task is scheduled to run. By enabling this option, CCC will suppress these errors. Additionally, if you have configured your task to send an email when errors occur, this option will suppress that email.

This option is not applicable for the **When the source or destination is reconnected** scheduling setting, because a task configured in that manner will only attempt to run if both the source and destination are present.

Run this task as soon as the missing volume reappears

If a backup task is missed because the source or destination was missing at the scheduled run time, this option will cause CCC to run the backup task as soon as that missing volume reappears.

Related Documentation

- Frequently asked questions about scheduled tasks <https://bombich.com/kb/ccc6/frequently-asked-questions-about-scheduled-tasks>

Modifying CCC's Security Configuration

Rather than requiring you to enter admin credentials every time you want to run a task or make changes to a task, CCC only requires users with administrative privileges to authenticate once when CCC is initially installed. While this configuration is easier to use, there are situations where this configuration is not appropriate. If you leave your system unattended with an admin user logged in, someone with physical access to your system can modify or run your CCC backup tasks. If you cannot rely upon the physical security of your Mac to prevent someone from using your Mac, you can use the information below to apply a stricter security policy to CCC.

Require administrator authorization to make changes to tasks and to run or stop tasks

CCC identifies a subset of activity that causes changes to CCC tasks and preferences or that require access to privileged data (e.g. CCC's private keychain). Performing these tasks requires that the user is authorized for the "com.bombich.ccc.helper" privilege. The default rules for this privilege require that the requesting user is either an admin user, or can provide administrator credentials. Once the authorization is obtained, the user is allowed to perform the privileged tasks without additional authorization until the login session ends.

You can modify these rules in several ways. Most commonly, you may want to require the logged-in user to explicitly provide admin credentials to gain this authorization (vs. having the privileged granted simply because the user is an administrator). Additionally, you may want this authorization to expire after a specific amount of time, e.g. 5 minutes (vs. "when the user logs out"). To apply these stricter rules, paste the following into the Terminal application:

```
security authorizationdb read com.bombich.ccc.helper > /tmp/ccc.plist
defaults delete /tmp/ccc "authenticate-user"
defaults write /tmp/ccc "authenticate-admin" -bool YES
defaults write /tmp/ccc timeout -int 300
defaults write /tmp/ccc shared -bool NO
plutil -convert xml1 /tmp/ccc.plist
security authorizationdb write com.bombich.ccc.helper < /tmp/ccc.plist
security authorize -ud com.bombich.ccc.helper
```

Immediately revoking authorization to modify CCC tasks

If you have decided to apply a liberal timeout value to the "com.bombich.ccc.helper" privilege, you may occasionally want to revoke that authorization immediately. To immediately revoke that authorization, paste the following line into the Terminal application:

```
security authorize -ud com.bombich.ccc.helper
```

Resetting CCC's authorization rules back to default values

To reset CCC's authorization rules back to the default values, paste the following into the Terminal application:

```
security authorizationdb remove com.bombich.ccc.helper
```

security authorize -ud com.bombich.ccc.helper

The next time you attempt to modify or run a CCC backup task, CCC will re--apply its default rule set in macOS's Authorization database.

Outgoing network connections made by CCC

If you're using an application firewall such as Little Snitch <https://www.obdev.at>, you will see several outgoing network connections coming from CCC. We explain below what connections you should expect to see, and also explain why some connections that **look** unexpected are simply misreported by Little Snitch.

Ordinary activity

CCC will make external network connections for the following activity:

- † When you launch CCC and it is a scheduled time to check for a software update (bombich.com and mc.bombich.com)
- † When anonymous application usage statistics are submitted
- When you submit a ticket to our help desk (mc.bombich.com and carboncopycloner.zendesk.com)
- When you view the documentation (which takes you to our website, bombich.com)
- When you visit our store (which also takes you to our website, bombich.com and our sales vendor, sites.fastspring.com)
- If you have set up email notifications for completed tasks
- If your backup task specifies a network volume or remote Macintosh as the source or destination

† These activities are enabled only upon your assent when you first start using CCC, and can be suppressed any time later via the Update section of CCC's Settings window. No personal data, nor personally-identifiable data is **ever** sent to these services.

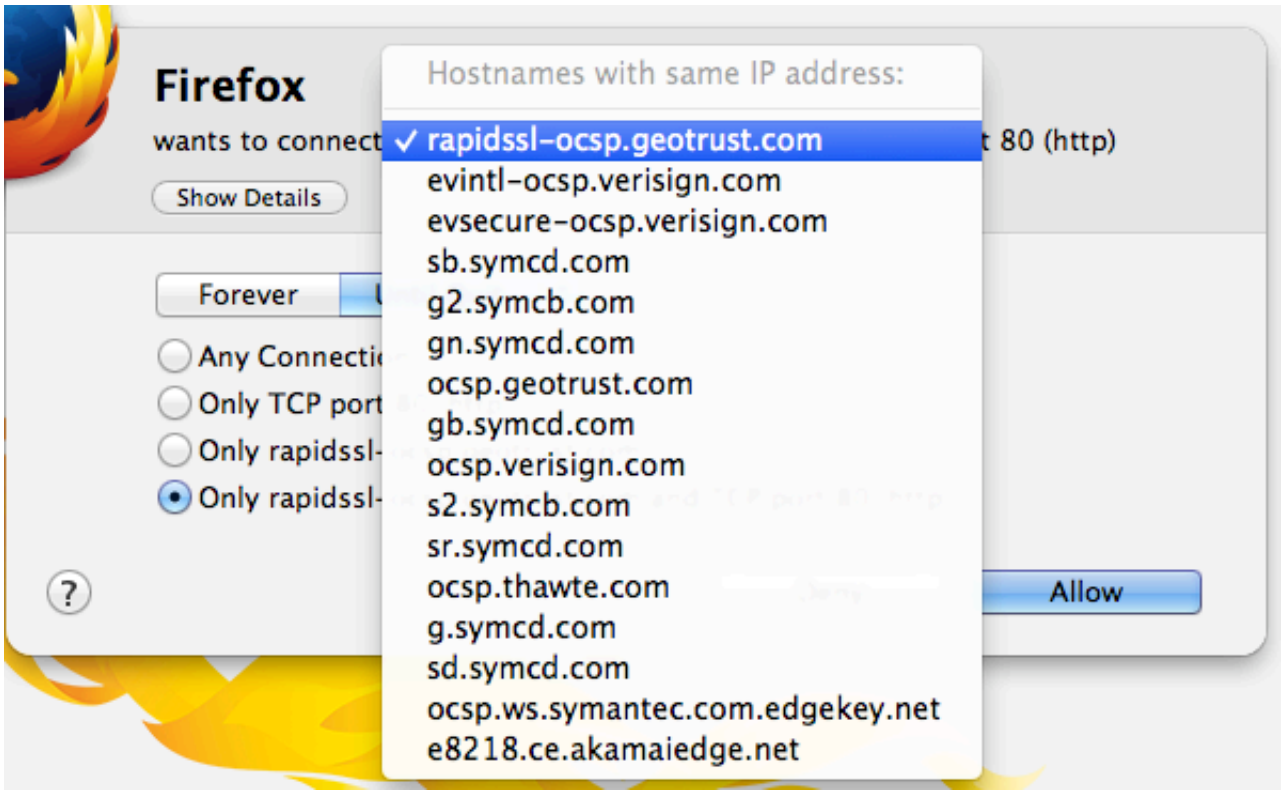
When you view the documentation via CCC, you connect to bombich.com just as you would in your web browser. Like most websites, bombich.com connects to other domains for certain purposes. We use Content Delivery Networks (CDNs) <https://en.wikipedia.org/wiki/Content_delivery_network> to serve our static content, such as file downloads, images, styling, fonts, and so on. The CDNs we use are bootstrapCDN (which is hosted by maxCDN) for styling, jquery and fastly for scripts, Google for fonts, Rackspace (bombich.scdn1.secure.raxcdn.com, hosted by akamai) for files and images, and NewRelic for performance and uptime monitoring (nr-data.net, newrelic.com). CDNs not only provide powerful servers, they also have servers around the world and pick the one nearest to the user so that content can be delivered faster.

FastSpring is our e-commerce partner that handles everything to do with pricing and purchasing. If you go to our store, you are directed to their website. They use Cloudfront, Amazon's CDN service, to host some of their static content.

Why does Little Snitch indicate that CCC is connecting to google.com and other unrelated-seeming domains?

When CCC connects to any server, Little Snitch (or any monitor) sees the IP address only. It then makes a guess as to the domain name associated with that connection, which makes it much easier for the user to recognize. Because CDNs are used to serve files for hundreds of different websites and companies, everything is very interconnected, and sometimes an IP address has dozens of different domain names associated with it. You can actually see Little Snitch's other possible guesses

by clicking the domain name in bold in the Little Snitch window:



It could pull any host name from the list, and we don't know what algorithm Little Snitch uses to decide which one to choose.

The result: google.ca, google.com, googleapis.com, and ytimg.com are all domains associated with Google's servers. We aren't actually connecting to all of these domains, but when we connect to Google Web Fonts, for example, we're accessing some of the same servers.

You can view a list of the CDNs that we use here <http://www.cdnplanet.com/tools/cdnfinder/#site:http://bombich.com> (and also look at any other websites you are curious about).

Backing up the content of cloud storage volumes

There are several cloud storage solutions available that allow you to synchronize content that's stored locally on your Mac with storage hosted on the Internet. Naturally we want to be able to back up all of your data whether it's stored in the cloud or not. The manner in which cloud syncing solutions store data locally, however, can complicate how you go about backing up and restoring that data. There are two complicating factors that we will address in this article:

- The actual location of your locally stored data may be hidden, making it difficult to find the files on your backup.
- Some, or possibly even all, of your cloud-synced files may not be permanently stored on your Mac; content stored only in the cloud is not available for making a local backup.

Local storage of cloud content is kept in a hidden location

You're typically used to accessing your cloud-synced content in the Finder's sidebar. In some cases (e.g., Microsoft OneDrive), the cloud storage solution may place an alias in your home folder that conveniently points to the location of the local copy of your data. Typically, though, that content is not stored in an obvious location, rather it's stored in the hidden "Library" folder in your home folder. Knowing where that data "lives" is key to understanding how to access that content on your backups.

Finding your cloud-synced content on the backup

If you make an ordinary backup of your startup disk, all of your locally-stored cloud content is on the backup. That content is in a hidden location, though, so follow these steps to locate that content on your backup disk:

1. Choose **Computer** from the Finder's Go menu
2. Select your backup disk, then navigate to Users > (yourname)
3. Press **Command+Shift+Period** to toggle the Finder's display of hidden items
4. **iCloud**: Navigate to Library > Mobile Documents
5. **Other cloud storage**: Navigate to Library > CloudStorage

"iCloud Drive" is not a volume nor folder; it's actually a collection of many disparate folders

When you open "iCloud Drive" in the Finder sidebar, you see a simple list of files and folders. Some of those folders may have special icons representing the application that stores data in that folder, e.g. for Preview, Pages, TextEdit, etc. Looking at the content of iCloud Drive in the Finder, you might assume that there is a folder somewhere ("in the sidebar") that has all of those items collected together.

iCloud Drive does not work like that. What you see in the Finder is a Finder trick. iCloud Drive is actually a collection of folders hidden away in the Library folder in your home directory. Files and folders that you manually add to iCloud Drive are stored here:

Macintosh HD --> Users > (yourname) > Library > Mobile Documents > com~apple~CloudDocs

Application storage folders are kept elsewhere. If you have a Pages folder in iCloud Drive, for example, that content would be stored here:

Macintosh HD --> Users > (yourname) > Library > Mobile Documents > com~apple~Pages > Documents

Making matters even more complicated, if you choose to sync your Desktop & Documents folders (i.e., System Settings > Apple ID > iCloud Drive > Options), the Finder will make it appear as if your Desktop and Documents folders actually reside within iCloud Drive. In fact, those folders still exist in their normal locations:

Macintosh HD --> Users > (yourname) > Desktop
Macintosh HD --> Users > (yourname) > Documents

But you won't see those folders in those locations when you navigate there in the Finder — Finder hides them.

Backing up cloud-only content

Some cloud storage service providers offer features that allow (or even encourage/force) you to store your files only online, thus freeing up space on your hard drive. Some services that currently offer this functionality include:

- Dropbox Professional's "Smart Sync" feature
- Microsoft OneDrive's "Free up space" feature
- iCloud Drive's "Optimize Mac Storage" feature
- Google Drive's "File Stream" feature

Files that are only available online will typically have a "cloud" icon or badge in the Finder, e.g., iCloud:  and Dropbox: 

When a file stored by one of these storage services is flagged to reside only online, the local copy of the file is deleted from your Mac and replaced with a 0-byte placeholder file. While this is a convenient feature that allows you to free up some space on your Mac, it imposes a logistical challenge to create a local backup of those files. If you want to have a local backup of these cloud-only files, CCC must temporarily download these files to your startup disk. CCC can do this, but because this involves downloading a potentially large amount of data from the Internet, this functionality is disabled by default. Likewise, allowing this data to co-mingle with your startup disk's backup could lead to a situation where it is impossible to restore your entire backup to the original disk due to space constraints. To avoid that, we recommend making backups of your cloud-only storage to a separate volume on your backup disk.

Best practice for setting up a CCC task to back up cloud-only data

See Preparing your destination disk for a backup or restore <https://bombich.com/kb/ccc6/preparing-your-backup-disk-backup-os-x> for guidance if your backup disk is not APFS-formatted.

1. Open Disk Utility and select your APFS-formatted primary backup volume in the sidebar.
2. Click **+** in the toolbar to add a volume; name it something like "Cloud Storage Backup".
3. Open CCC and click **New Task** in the toolbar; name the new task something like "Local

Backup of Cloud Storage".
4. Click on the Source selector and choose **Cloud Storage**
5. Click on the Destination selector and choose the "Cloud Storage Backup" volume as the destination.
6. Click **Done**, then schedule the task or run it immediately.

When this setting is enabled, CCC will temporarily download cloud-only files that are not yet on the destination, or that are newer than the corresponding file on the destination. After copying the temporarily downloaded files, CCC will "evict" the files to free up the space that they consumed. CCC attempts to retain no more than 100 files and no more than 2GB of temporarily-downloaded content at a time.

This functionality requires macOS Monterey 12.5+.

The Cloud Storage task creates a custom filter

The Cloud Storage source will create a filter that automatically includes the following folders in your home directory:

- Desktop
- Documents
- Library > Mobile Documents
- Library > CloudStorage

The first three folders are specific to iCloud, and the first two folders are only applicable if you have iCloud Drive configured to sync your Desktop and Documents folders. If you don't sync your Desktop and Documents folders to iCloud, you can click **Task Filter** at the bottom of the CCC window, then uncheck the boxes next to your Desktop and Documents folder to not include those folders in this backup task.

Some iCloud cloud-only content will not be temporarily downloaded

Starting in macOS Monterey (12.3, January 2022), Apple disallowed cloud syncing by means of a System Extension. Cloud-syncing service providers like Google, Microsoft, and Dropbox were "encouraged" to adopt the "FileProvider" service within macOS instead. Prior to macOS Sonoma, Apple had not yet adopted that service for their own iCloud Drive cloud syncing solution. Rather, Apple continued to use a proprietary syncing service on macOS Monterey and Ventura that relied on proprietary placeholder files.

Lack of adoption of their own standard leads to some idiosyncrasies when dealing with iCloud cloud-only content on Monterey and Ventura. The only notable problem that proved too difficult for us to work around involves bundle files <https://bombich.com/kb/ccc6/glossary-terms#b>. iCloud uses a single file placeholder for bundle files (vs. dataless folders via FileProvider). This (lack of) structure posed logistical and practical issues that we decided were too costly to resolve, especially in light of the fact that Apple migrated iCloud to FileProvider in macOS Sonoma. As such, cloud-only iCloud files that are bundle files will not be downloaded on Monterey and Ventura, rather the placeholder file will be copied instead.

Other notable caveats regarding the temporary downloading of cloud-only content

CCC's helper tool must have access to icloud.com for the entire duration of the task event

If connectivity is not available or is lost to that host (regardless of the service provider that hosts your cloud-backed content), CCC will suspend downloading activity in the task. We do this because

it's not possible to revoke requests to download files from the cloud. If we plowed through all of the files and requested *all* of them, iCloud/FileProvider would resume downloading all of those files as soon as connectivity was restored. Making matters worse, this would happen outside of the purview of the task, and CCC would not be able to evict the downloaded files, likely leading to space constraints on the startup disk.

CCC's Dashboard application must be running for the entire duration of the backup task

Only the logged-in user is allowed to "evict" file content, so CCC passes those requests to the CCC Dashboard service. If CCC cannot reliably evict files, it will not download files. If/when this occurs, CCC will report an error for the task event.

Verification discrepancies

If you verify a source that has cloud-only content, the cloud-only placeholder files will fail verification. This is the correct result, because the (empty) content of the cloud-only placeholder file does not match the content of the "rehydrated" file that was temporarily downloaded. CCC's transaction only retains a checksum of the actual data that was downloaded, not the empty placeholder file.

Cloud-only placeholder files will not be downloaded for checksum analysis

When using the "Find and replace corrupted files on the destination" setting (aka Backup Health Check), CCC will not download cloud-only placeholder files from the Internet just to calculate their checksums. If CCC copied these files in the past (either via temporary download or prior to eviction), then the task audit will already have the checksum for those files. To verify those files, click on the Destination selector for your dedicated CloudStorage backup task and choose **Verify files copied by this task**.

Ad hoc verification: Verify the source or the destination against the "last known state" <https://bombich.com/kb/ccc6/how-verify-or-test-your-backup#adhoc>

Cloud service problems can prevent CCC from downloading cloud-only files

Naturally your own Internet connectivity problems can prevent CCC from downloading cloud-only files, but so can service problems on the cloud-provider's end. Most cloud-service providers offer a dashboard showing their server status. Here are a few for your convenience:

- Apple System Status [iCloud Drive] <https://www.apple.com/support/systemstatus/>
- Microsoft Office 365 Service Health [OneDrive] <https://portal.office.com/ServiceStatus>
- Dropbox System Status <https://status.dropbox.com>
- Box Status <https://status.box.com>
- Google Workspace Status Dashboard [GoogleDrive] <https://www.google.com/appsstatus/dashboard/>

What is CCC's Privileged Helper Tool?

At its core, CCC is a product that is designed to make backups of your Mac's user data, applications and system settings. In order for CCC to be able to make copies of system files (e.g. user accounts), CCC needs to have the privilege of copying files that can't be read nor written by just any user. Likewise, CCC is often tasked with copying the data associated with multiple users. macOS prevents you from accessing files that belong to other users. If you, as the administrator of the Mac, want CCC to back up everybody's files, then again, CCC requires elevated privileges.

Acquiring elevated privileges on macOS

There are a few different ways to perform a task on macOS with elevated privileges. The simplest – and least secure – method to do this would be to prompt the user to authenticate when he opens the application, and then relaunch the application as the "root" user. The application would then have all of the privileges it needs. This would grant far too much privilege <https://developer.apple.com/library/archive/documentation/Security/Conceptual/SecureCodingGuide/Articles/AccessControl.html#//apple_ref/doc/uid/TP40002589-SW6>, though, because it also gives the user (or malware that is exploiting the application) privileged access to other users' files.

A better way to securely acquire elevated privileges is to isolate the code that requires those privileges into a separate, "faceless" application. This is a common practice known as privilege separation <https://en.wikipedia.org/wiki/Privilege_separation>. Even here, though, there is a right way and a wrong way for the isolated application to gain elevated privileges. The antiquated technique is for the parent application to ask for administrator authentication, then change the owner of the privileged application to the root user, then set a special mode on that application that allows that application to run with the privileges of the owner of the application (root). While this is a popular technique on Linux and much, much older versions of Mac OS X, there is still a significant potential vulnerability with this approach – any user can open that privileged application and potentially use it as a puppet to perform privileged tasks. Apple specifically discourages this practice <https://developer.apple.com/library/archive/documentation/Security/Conceptual/SecureCodingGuide/Articles/AccessControl.html#//apple_ref/doc/uid/TP40002589-SW18>:

Note: Older software sometimes sets the setuid and setgid bits for the executable file, and sets the owner and group of the file to the privilege level it needs (often with the root user and the wheel group). Then when the user runs that tool, it runs with the elevated privileges of the tool’s owner and group rather than with the privileges of the user who executed it. This technique is strongly discouraged because the user has the ability to manipulate the execution environment by creating additional file descriptors, changing environment variables, and so on, making it relatively difficult to do in a safe way.

Adhering to a higher standard of security

Starting in Mac OS X 10.6 (Snow Leopard), Apple introduced a more secure paradigm for performing tasks with elevated privileges <https://developer.apple.com/documentation/servicemanagement/1431078-smjobbless?language=objc>. Rather than blindly granting privileged access to an application, developers can ask the system to install a "privileged helper tool". macOS then invokes the privileged helper tool on demand, and the calling application can only communicate with the helper when it has met stringent requirements:

- The calling application and the privileged helper tool must be code signed (and valid)
- The calling application must be one of the applications that is specifically approved to make

requests to that specific helper
- The calling application must have a valid authorization reference

These requirements prevent unauthorized use of the helper tool and they prevent maliciously modified applications from making requests to the helper tool.

CCC has leveraged a privileged helper tool since version 3 and Mac OS X Snow Leopard – right from the start. This architecture is not only more secure and future-proof than using setuid binaries, it also affords us, for example, the ability to perform backup tasks when no users are logged in to the system.

Related Documentation

- Modifying CCC's Security Configuration <https://bombich.com/kb/ccc6/modifying-cccs-security-configuration>
- Uninstalling CCC <https://bombich.com/kb/ccc6/uninstalling-ccc>
- Granting Full Disk Access to CCC and its helper tool <https://bombich.com/kb/ccc6/granting-full-disk-access-ccc-and-its-helper-tool>
- System problems can lead to a failure to install CCC's helper tool <https://bombich.com/kb/ccc6/carbon-copy-cloners-privileged-helper-tool>

The CCC Private Keychain

CCC creates a private keychain on your startup disk for the purpose of storing authentication credentials that facilitate automated backup tasks. Specifically, CCC will store these sorts of credentials:

- SMTP account settings that you define in CCC's Preferences > Email Settings
- NAS device username/password for mounting NAS volumes specified as a source or destination to a CCC task
- Encrypted volume passwords that you ask CCC to store
- Encrypted disk image passphrases for disk images that you ask CCC to create

To protect these credentials, CCC stores them in a standard macOS keychain file <https://support.apple.com/guide/security/keychain-data-protection-secb0694df1a/web> on your startup disk at Macintosh HD > Library > Application Support > com.bombich.ccc > CCC-global.keychain. Beyond the protections provided by the macOS keychain, CCC applies the following restrictions on the CCC keychain file:

- The keychain file is readable only by the macOS system administrator account (i.e. the "root" user)
- The keychain file can only be unlocked by CCC (specifically, by CCC's privileged helper tool <https://bombich.com/kb/ccc6/what-cccs-privileged-helper-tool>)
- The keychain file can only be unlocked on the Mac upon which it was originally created — it is purposefully Mac-specific

You can remove individual keychain entries, or reset the CCC private keychain

If you would like to see and/or remove individual keychain entries, open CCC's Preferences and click **Passwords** in the toolbar. To remove a keychain entry, simply select the entry and press the Delete key.

CCC never reveals passwords stored in its keychain

Alongside the security measures applied to CCC's keychain file, CCC will never reveal a password entry once it is stored in the keychain. That's a deliberate security measure. If you have lost/forgotten a password and it is retained in CCC's keychain, you will not be able to recover that password from CCC's keychain. You may, however, be able to use CCC to unlock and mount the associated encrypted volume or disk image, then copy the content of that volume to other storage.

The CCC private keychain is not transferrable to other Macs

If you purchase a new Mac and migrate your data to the new Mac, CCC's keychain will not work on the new system. If you configured CCC to send email notifications, open CCC Preferences > Email Settings, then click the **Edit** button to re-enter your SMTP account password (or "App Password"). If any backup tasks run that require NAS volume or encrypted volume passwords, those tasks will fail, and then CCC will prompt for those credentials. You may provide those passwords proactively after migration; hold down the Command key and click on the Destination selector to be prompted for the destination volume's credentials.

Most passwords that CCC retains are created outside of CCC (e.g. SMTP passwords, NAS device

credentials, and encrypted volume passwords), so you'll typically have a copy of that password stored elsewhere (e.g. your login keychain or another password manager). Bear this in mind, however, when creating encrypted disk images. CCC offers an option to store the password that you specify in your login keychain (and that option is enabled by default). If you do not store the password in your login keychain, however, and if you migrate to a new Mac and forget the password, you will not be able to open the disk image.

Frequently Asked Questions (FAQ)

Glossary of Terms

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

A

Apple File System (APFS) — APFS is a new filesystem introduced by Apple in macOS High Sierra as a replacement for the legacy HFS+ filesystem. See also: Everything you need to know about CCC and APFS <https://bombich.com/kb/ccc6/everything-you-need-know-about-carbon-copy-cloner-and-apfs>

Apple Filing Protocol (AFP) — AFP is a file sharing protocol that allows you to access the files on other computers and NAS devices on your network. CCC can copy files to and from folders and sharepoints on SMB and AFP sharepoints. AFP is deprecated in favor of the SMB protocol starting with OS X Yosemite.

B

Backup — A backup <https://en.wikipedia.org/wiki/Backup>, or the process of backing up, refers to the copying and archiving of computer data so it may be used to restore the original after a data loss event. The verb form is *back up,* in two words, whereas the noun is *backup*. In other words, you back up your data using CCC. When you have done that, you have a backup of your data on physically disparate media.

Bootable backup — Same as backup, but a backup of a volume that contains an operating system that can be used to boot the computer if the primary startup volume fails.

Boot selector — See Startup Manager.

Bundle file — Bundle files are actually folders that the Finder presents as a single file. Application files (e.g. Safari.app) and various library files (e.g. Photos Library files) are bundle files; you can right-click on a bundle file and choose "Show Package Contents" to see the internal structure of a bundle file.

C

Checksumming or "Find and replace corrupted items" — With this option, CCC will calculate a checksum of every file on the source and every corresponding file on the destination. CCC then uses these checksums to determine if a file should be copied. This option will increase your backup time, but it will expose any corrupted files within your backup set on the source and destination. This is a reliable method of verifying that the files that have been copied to your destination volume actually match the contents of the files on the source volume.

Clone (CCC) — A copy of a folder or volume; a non-proprietary backup. Clone is a common word used (historically) for a CCC backup, although it is not a term that we use any more due to the ambiguity introduced by the "cloning" feature that Apple introduced in the APFS filesystem.

Clone (APFS) — APFS cloning allows the user to instantly create copies of files on the same volume without consuming extra storage space. When cloning a file, the file system doesn’t create copies of the data, rather it creates a second reference to the file that can be modified independently of the first file. The two files will share storage on the disk for portions of the files that remain identical, but changes to either file will be written to different parts of the disk.

Container (APFS) — A container on an APFS formatted drive is similar to a partition, but allow several volumes to share the space in the container more flexibly. See: Working with APFS Volume Groups <https://bombich.com/kb/ccc6/working-apfs-volume-groups>

Cruft — Another term for digital detritus, e.g. files that could (should) be deleted because they're no longer needed nor desired by the user. This term was coined to describe the large collections of technical equipment piled in the corridors of the Cruft lab at MIT <https://en.wikipedia.org/wiki/Cruft> in the 1980s and 90s.

D

Destination — The location where files from the source are copied. The destination can be a disk attached directly to your Mac, a network location (e.g. a NAS or a share from another computer), or a disk image file. Destination is a relative term. When making an ordinary backup, the destination is your backup volume. When restoring, however, the destination is your original volume, or a replacement device.

Differential backup — A differential backup is a type of data backup that preserves data, saving only the difference in the data since the last full backup. CCC uses a differential backup method, but does not store the differential data in a proprietary manner. Rather, the files are copied to the destination among the already-up-to-date items such that the destination is a b ackupof the source.

Disk image — Disk images are data containers that emulate disks. When you open a disk image file, a virtual volume is mounted that allows you to browse the files held by the disk image – as if you were browsing a physical disk device. Disk images are recommended only when backing up to a network destination to protect attributes that are not supported by the network volume. Disk images are not bootable. Backing up to a disk image <https://bombich.com/kb/ccc6/backing-up-disk-image>

E

EFI Partition — The EFI partition is an Apple-proprietary partition. That partition is created automatically when a disk is partitioned with the GUID partition scheme, and its contents are managed internally by OS X. Third-party applications shouldn't attempt to modify, nor copy that volume.

Extended Attribute — Extra data that is associated with a file. Extended attributes typically contain non-user-created data that was placed there by the application that created the file. For example, photo applications may place thumbnail icon data into an extended attribute. CCC attempts to copy extended attributes when possible, but extended attribute data is generally considered to be disposable because it can be regenerated by the application that created it.
Advanced Settings: Don't preserve extended attributes <https://bombich.com/kb/ccc6/advanced-settings#ignore_xattrs>

F

Filesystem, or file system — A volume's filesystem controls how files and folders on that volume are stored and retrieved, and also controls who can access those items.

FileVault Encryption — Volume level encryption built into the macOS. When enabled on a volume, a password is required to unlock and mount that volume. Unlike ownership-based restrictions, FileVault protection persists when attaching the disk to another computer.
Apple Kbase #HT204837: Use FileVault to encrypt the startup disk on your Mac <https://support.apple.com/en-us/HT204837>

Firewire — Firewire is an interface standard developed by Apple that allows the connection of external peripherals to a computer. Firewire devices provide reliable bootability and excellent performance that rivals USB 3. This interface has largely been supplanted by Thunderbolt on newer Macs.

Firmlink — A firmlink is described by Apple as a "bi-directional wormhole" between two filesystems. A firmlink transparently redirects the navigator from a read-only folder on a System volume to a writable folder on a Data volume. These are similar to aliases, but they are only applicable to folders, and they cannot be created by the user.

H

HFS+, or "OS X Extended, Journaled" — The default filesystem format used for macOS system volumes. First introduced for Mac OS 8, HFS+ has been updated for many years to support new features of macOS. Apple introduced a replacement for HFS+ in macOS High Sierra: Apple File System.

I

Incremental backup — An incremental backup is one that provides a backup of files that have changed or are new since the last backup; it is one that backs up only the data that has changed since the last backup. When making a backup for the first time, an incremental backup copies all files.

M

Migration Assistant — A tool from Apple that allows you to migrate applications, settings, and documents from a backup or older computer to a new computer or fresh installation of the OS. You can use a CCC bootable backup as a source for Migration Assistant.
Apple Kbase #HT204350: How to move your content to a new Mac <https://support.apple.com/en-us/HT204350>

N

Network Attached Storage (NAS) — NAS systems are networked appliances (e.g. a router or a specialized storage device that connects to your router) that contain one or more hard drives. They typically use SMB add/or AFP networking protocols to make sharepoints available to macOS, Windows, and Linux clients.

P

Partition — In verb form, partition refers to the process of creating a division on a hard drive that defines one or more volumes. When you purchase a new hard drive, it often must be partitioned to make it suitable for use on your Macintosh. In noun form, partition is colloquially used in the same manner as a volume. A partition table refers to a hidden structure on a disk that defines the size and position of the volumes on a disk. CCC does not copy the partition table, nor multiple partitions on a disk. Rather, a CCC backup task is defined with one source volume and one destination volume.
Preparing your backup disk for a backup of OS X <https://bombich.com/kb/ccc6/preparing-your-backup-disk-backup-os-x>

Production startup disk, or Production backup disk — This refers to the disk that you ordinarily use for that purpose. For most users, "Macintosh HD" is the "production" startup disk. Antonyms: "rescue startup disk", or "testing backup disk".

Prune — Remove older, archived material that was cached on the destination volume. Automated maintenance of the CCC SafetyNet folder <https://bombich.com/kb/ccc6/automated-maintenance-ccc-safetynet-folder>

Permissions — A file and folder specification that defines the access that various users and groups will have with regard to reading or modifying that item.

Preflight/Postflight script — An advanced feature; shell scripts that can be added to the beginning or end of a CCC backup task to extend the task's functionality. Running shell scripts before and after the backup task <https://bombich.com/kb/ccc6/performing-actions-before-and-after-backup-task#scheduler_shell_scripts>

R

RAID ("**Redundant Array of Inexpensive Disks" or "Redundant Array of Independent Disks")** — A collection of hard drives that using software or hardware are presented as one or more volumes. There are several levels of RAID that balance speed and redundancy. See this Wikipedia article <https://en.wikipedia.org/wiki/RAID> for more details.

Root — the root folder (also known as the root directory) is the first or top-most folder in a hierarchy. When you double-click on a hard drive icon in the Finder, the folder that appears first is the root-level folder.

S

SafetyNet — A feature in CCC that protects files on the destination from being accidentally deleted. If you have files on your destination device that don't exist on the source, those files get placed in the SafetyNet. CCC will also place the older version of modified files into the SafetyNet. The SafetyNet is a *temporary* safe haven for files unique to the destination. When space is constrained on the destination, CCC will start to remove older items from the SafetyNet. Protecting data that is already on your destination volume: The CCC SafetyNet <https://bombich.com/kb/ccc6/protecting-data-already-on-your-destination-volume-carbon-copy-cloner-safetynet>

Seed — Initially populating a destination volume while it is attached directly to your Mac. This "seeded" volume can then be attached to a remote Macintosh at a distant location, and subsequent backups will be faster because less data will be copied over the Internet.

Server Message Block (SMB) — SMB is a file sharing protocol that allows you to access the files on other computers and NAS devices on your network. CCC can copy files to and from folders and sharepoints on SMB and AFP sharepoints.

Shell Script — A text file containing command-line arguments that can automate tedious tasks. CCC backups can be configured with pre and postflight shell scripts to extend the functionality of the backup task. For example, you could implement a postflight script to unmount the source volume. Running shell scripts before and after the backup task <https://bombich.com/kb/ccc6/performing-actions-before-and-after-backup-task#scheduler_shell_scripts>

Sidebar — An interface element that appears on the left side of CCC's main window when you click the **Show Sidebar** button in CCC's toolbar. A table at the top of CCC's sidebar lists your CCC backup tasks, while a table at the bottom of the sidebar lists all of the locally-attached volumes that are

currently mounted on your Mac. The contents of the sidebar are also accessible via CCC's **View** menu.

Simple Mode — A simplified user interface. Simple Mode significantly reduces the number of user interface elements — the sidebar, toolbar, scheduling selector, and advanced settings are all suppressed, leaving the user with only three primary controls: Source, Destination, Start button.
Simple Mode <https://bombich.com/kb/ccc6/simple-mode>

Snapshot — A snapshot is a representation of a volume at a particular point in time. Similar to how a photograph captures a moment in time, a snapshot preserves the state of every file on a volume at the very moment that the snapshot was created.

Source — The folder or volume that holds the data that you want CCC to copy.

Span — When a backup extends past a destination for more room. CCC does not support spanning multiple destinations.

Sparse file — Sparse files consume less space on disk than their file size would suggest. Sparse files are occasionally used for log files, databases and virtual machine files. CCC can preserve sparse files between APFS volumes, but HFS+ does not support sparse files, so these files consume more space on an HFS+ formatted backup disk.

Startup Manager — A system tool from Apple that allows you to select a startup volume as the Mac is starting up. The Startup Manager is part of your Mac's firmware; hold down the Option key while turning on your Mac to bring up the Startup Manager.
Apple Kbase #HT204417: How to select a different startup disk <https://support.apple.com/en-us/HT204417>

T

Target Disk Mode — An alternate startup configuration in which the computer does not boot to the loginwindow nor Finder. Rather, a Firewire, USB, or Thunderbolt icon appears on the Mac's screen, and when you attach the Mac to another Mac via Firewire, USB or Thunderbolt, the internal storage of the Mac in Target Disk Mode appears on the Desktop of the other Mac. In other words, Target Disk Mode makes your Mac behave like an ordinary external hard drive enclosure.
Apple Kbase #HT201255: Mac startup key combinations <https://support.apple.com/en-eg/HT201255>

Task — A collection of settings in CCC that define a source, destination, items to be copied, and automation.

Task chaining — A feature in CCC that allows you to run another task at the end of a task, see: Performing actions Before and After the backup task: Run another backup task (task chaining) <https://bombich.com/kb/ccc6/performing-actions-before-and-after-backup-task#chain_tasks>.

Thunderbolt — Thunderbolt is a hardware interface developed by Intel that allows the connection of external peripherals to a computer. Thunderbolt is a popular, albeit pricier interface for connecting external hard drives to your Mac. Thunderbolt devices provide excellent performance and reliable bootability.

U

Universally Unique Identifier (UUID) — A 36-character hexadecimal code (characters A-F, 0-9) that uniquely identifies a volume, e.g. "F5B1D7B0-66EC-4082-A34C-86FFD294FA61". When you erase a volume with Disk Utility, the new volume gets a new unique identifier. CCC uses this

identifier, along with the name of the volume, to positively identify the source and destination before copying any files. Due to the unique nature of these identifiers, they prove more reliable than volume name when identifying a volume, because there's nothing stopping you from naming all of your disks "Macintosh HD".

Universal Serial Bus (USB) — An industry standard for cables, connectors, and communication between a computer and some external devices like a hard drive, keyboard, or mouse. Macs and USB devices can adhere to the USB 2 or USB 3 versions of the protocol, depending on when the device was manufactured. USB 3 is considerably faster than USB 2. Macs produced before 2012 do not have native support for USB 3. USB 3 devices can be used with those Macs, but will be connected at USB 2 speeds.

V

Volume — The terms "disk" and "volume" are often used interchangeably. Ambiguity arises, however, when you modify the partitioning of a disk such that it has multiple volumes. The term "disk" refers to the physical, whole device. A disk contains volumes, and its a volume that you see in the Finder (frequently with a hard disk icon, bringing the confusion full circle). A helpful graphic is available in this section of CCC's documentation. <https://bombich.com/kb/ccc6/working-apfs-volume-groups>

Why doesn't the disk usage on my backup disk match the disk usage on the source disk?

The disk usage on your startup disk does not reflect the amount of data that needs to be backed up; disk usage on the destination should be lower than disk usage on the source after making an initial backup of your startup disk. Special filesystem devices (e.g. filesystem snapshots) and some macOS service data either cannot or should not be copied to another volume. CCC automatically excludes these items to avoid problems while booting from the backup and to avoid unnecessary disk usage. That list of exclusions is documented here: Some files and folders are automatically excluded from a backup task <https://bombich.com/kb/ccc6/some-files-and-folders-are-automatically-excluded-from-backup-task>.

CCC doesn't copy virtual memory, Trash, nor snapshots

The largest and most notable excluded item is the /private/var/vm/sleepimage file. The sleepimage file contains the live state of your Mac's RAM, so it will be as large as the amount of RAM that you have installed. This file is potentially very large, changes constantly and it gets recreated on startup, so CCC excludes this file from every backup task.

CCC also excludes the contents of the Trash, so you may want to empty the Trash, then compare again the source and destination.

Lastly, filesystem snapshots may consume a considerable amount of space on your source volume. Select the source volume in CCC's sidebar to see snapshot-related disk usage. Snapshots retain references to files that have been deleted or modified, they are not a representation of your current data set, and cannot be copied from one volume to another.

Disk usage math is not straightforward

Disk usage is not a simple matter of adding the size of every file on a volume. Special filesystem devices (e.g. hard links) have always complicated this math, but more recently Apple has introduced more special filesystem devices that complicate this even further. The cloning feature in Apple's new APFS filesystem can lead to a scenario where it appears that you have more data on the disk than it can possibly contain, and the filesystem snapshots feature can lead to scenarios where disk usage is higher than the total size of the files on that volume. APFS also supports "sparse" files, which consume less space on disk than their file size would suggest. CCC can preserve sparse files between APFS volumes, but HFS+ does not support sparse files, so these files consume more space on an HFS+ formatted backup disk. See these sections of CCC's documentation for additional details on working with these challenges:

- I heard that APFS has a "cloning" feature. Is that the same as what CCC is doing? <https://bombich.com/kb/ccc6/everything-you-need-know-about-carbon-copy-cloner-and-apfs#math>
- Finder does not accurately represent the true disk usage of your files <https://youtu.be/KggyuL8mED0>
- Understanding disk usage when using snapshots <https://www.youtube.com/watch?v=4wqAC4YXiaY>

So how can I tell that all of my data was actually copied?

Click the **Compare** button in CCC's toolbar to perform a comparison of the currently-selected task's source and destination. This comparison will help visualize any actual differences between the two volumes.

Related Documentation

- Common explanations for differences between the source and destination <https://bombich.com/kb/ccc6/comparing-source-and-destination#common>

I want to back up multiple Macs or source volumes to the same hard drive

Backing up multiple volumes or multiple Macs to a single hard drive can be a messy proposition. If you back up each source volume to the same destination volume without some pre-planning, data from each source volume will be merged in a heap on the backup volume. Additionally, your tasks will archive or delete each other's backed up content.

Add dedicated volumes to an existing APFS-formatted backup disk

When you're backing up multiple volumes to the same APFS-formatted backup disk, create a dedicated volume on that backup disk for each source volume:

1. Open Disk Utility
2. Choose "Show all devices" from the View menu
3. Select your current CCC destination volume in the sidebar
4. Choose **Add APFS Volume...** from the Edit menu
5. Name your new volume and click the Add button
6. Configure each of your CCC backup tasks to back up to its own dedicated volume on the destination

Related Documentation

- Partitioning a new hard drive with APFS <https://youtu.be/5mBO3o570Ak>

Add dedicated partitions to an HFS+ formatted backup disk

Partitioning is similar to adding volumes like the procedure described above, but a little less flexible:

1. Open Disk Utility
2. Choose "Show all devices" from the View menu
3. Click on the top-most parent device of your backup disk
4. Click the "Partition" button in the toolbar
5. Click the "+" button to add a second partition to the backup disk
6. Set the format of the new partition to **APFS** or **APFS (Encrypted)**
7. Configure each of your CCC backup tasks to back up to its own dedicated volume on the destination (see the section above for adding additional volumes)

Related Documentation

- Preparing your destination disk for a backup or restore <https://bombich.com/kb/ccc6/preparing-your-backup-disk-backup-os-x>

Backing up multiple data volumes to a non-APFS formatted disk

The easiest way to back up multiple data-only volumes to the same non-APFS formatted backup disk

is to create a folder on the backup disk for each volume that you want to back up. Then you'll configure a task for each source volume that you want to back up, setting the destination to that disk's dedicated folder on the backup disk.

1. Click the **New Task** button in CCC's toolbar.
2. Choose your data volume from CCC's Source selector.
3. Create a new folder on the destination volume in the Finder, then drag that folder onto CCC's Destination selector.
4. Schedule the task, if desired, or choose **Save** from CCC's Task menu. You can run this task immediately or let it run on schedule later.
5. Repeat the steps above for other source volumes, creating a new folder for each at the root level of the destination volume.

Can I run a backup while I'm using my computer? If I have open files, will they be backed up?

Generally, yes. Performance will be affected during the backup task (especially the first one) as CCC reads the entire source volume and writes to the destination volume. If your work is "disk bound" — that is your applications are reading or writing to either the source or destination, then you'll notice a performance hit. If you're just reading email or writing a document, then you probably won't notice the performance hit.

What happens if files are modified while they're being copied?

If your source volume is an APFS volume, then CCC will create a read-only snapshot of that volume and use that snapshot as a source for the backup task. With this configuration, any changes that you make to files on the source during the backup task will have no effect on the backup process. Likewise, those changes will not be part of the backup – expect the backup to contain exactly what was on the source at the moment that the backup task started.

If the source volume is not APFS-formatted, then some consideration should be given to the modification of files on the source during the backup task. Typically it's OK to work from the source volume while you're copying it, with the understanding that if CCC copied a file, then you open it, make changes, save it, then CCC completes the backup task, the modified version of your document is not backed up (this time around). Typically that's no big deal, the modifications will get backed up the next time the backup task runs. More importantly, though, if you're working with large files <https://bombich.com/kb/ccc6/backing-up-large-files-mounted-disk-images-and-virtual-machine-containers> (mounted disk image, Entourage email database, VMWare/Parallels container) during the backup operation, it is possible that those large files could be modified while CCC is backing up that file. This won't affect the source file, but there's a good chance that the backup version of that file will be corrupt. For this reason it is a good idea to stop using applications that may be modifying large files for the duration of the backup task. Again, keep in mind that this is only applicable for non-APFS source volumes.

Related Documentation

- Backing up large files, mounted disk images, and Virtual Machine containers <https://bombich.com/kb/ccc6/backing-up-large-files-mounted-disk-images-and-virtual-machine-containers>
- Leveraging Snapshots on APFS Volumes <https://bombich.com/kb/ccc6/leveraging-snapshots-on-apfs-volumes>

Why do some applications behave differently or ask for the serial number after restoring from the backup?

Some applications won't work when transferred to a new disk or when run on a different Mac. This has nothing to do with whether or how CCC backs up your data, it comes down to the serialization requirements imposed by the software vendor (i.e. their anti-piracy strategy). Some applications will work just fine, some will simply require that you re-enter your serial number (Microsoft Office and Adobe apps frequently fall in this category), while other applications will require a reinstallation from the original install media or online reactivation via the vendor's website. **CCC cannot (technically or legally) subvert activation requirements imposed by other software vendors.**

Also note that some applications consider the presence or absence of peripherals as well as other hardware characteristics during the installation process. If these conditions are different when running the application on a new hard drive or Macintosh, you may encounter problems. We have seen these types of problems with some high-end audio software packages in the past, particularly with the installation or configuration of various plugins.

We recommend that you always retain a copy of your applications' installers and serial numbers in case the applications have special serialization or installation requirements.

Non-registration-related, application-specific oddities

In addition to application registration issues that occur when running your apps on a new volume, there are occasionally other oddities that you may encounter after restoring from a backup (any backup, even Time Machine backups). The following is a list of potentially unexpected behavior that has been reported to us that a) appears to be a consequence of running an application from a different volume or on a different Macintosh and b) does not appear to be or cannot be accommodated/resolved in the backup process:

- Dropbox may ask you to reconfigure your account settings
- GateKeeper may reverify non-notarized applications that were previously verified on the source (e.g. you will see a dialog "Verifying iMovie.app" when opening that item).
- Time Machine may no longer recognize your original source volume because the UUID has changed
- **Google Drive** must be disconnected, then reconnected to your account. Details here <https://bombich.com/kb/discussions/google-drive-reports-google-drive-folder-missing>
- Finder preferences may not be respected (e.g. whether to show disks on the Desktop, the contents of the "All my files" item may be empty)
- Photoshop may require that you reset the Scratch Disk preference
- Finder may not resolve aliases to files on a backup volume. Finder will give you the opportunity to "readdress" these aliases when you try to open them.
- Network settings may not be respected on (or even migrated to) another Macintosh. If you have an extensive VPN configuration that you want to preserve, we recommend that you export those settings to a file before you lose access to the original Mac.
- The **Prevent App Nap** setting applies to specific instances of applications, so this setting will not be applied to copies of an application (e.g. on a backup volume).

- The **Local Items** Keychain is a local repository of passwords and other form data eligible to be synced via iCloud to your other devices running iOS 7 or newer. Safari and Mail store passwords in the Local Items keychain. Some items in **Local Items** Keychain cannot be migrated to another Mac (this setting cannot be overidden, even by the user), and the rest can only be migrated to another Mac if your backup volume is encrypted.
- If you open an Adobe Lightroom catalog from a restored volume, Lightroom may indicate that your photos cannot be found because the catalog references the name and path of the original source volume. See this Adobe support article <https://helpx.adobe.com/lightroom/help/locate-missing-photos.html> for instructions on how to re-link your catalog to the photo folders on your restored volume, or watch this video on our YouTube channel <https://youtu.be/vZEdy_aVbeo> to see a demonstration of the problem and solution. **Another tip**: renaming the restored volume the same as the original volume name may help Lightroom resolve catalog links to the media.
- TeamViewer Product Support recommends that TeamViewer be reinstalled when restoring a backup to a different Macintosh.
- If configured to start on login, the Box Sync application will delete the contents of your Box Sync folder, then re-download all of the content from Box.com (i.e. after you have restored data from a backup or migrated to a new Mac). The Box Sync application uses a folder inode number to identify the Box Sync folder, and that attribute cannot be preserved during a backup or a restore.
- Signatures in the Preview application won't be recognized when migrating data to another Mac, they're only recognized on the Mac upon which they were created.
- **Apple Pay** may function incorrectly after migrating data from a backup. Apple documents some suggestions here <https://support.apple.com/en-us/HT209016>, but we have found that simply creating a new admin account, then logging in to your iCloud account in the new account will work around the issue. You do not have to use the new account regularly, just create it and log in to Apple ID, then go back to using your production account. Apple is apparently aware of the awkwardness (and it is actually unrelated to migrating data from a backup) and have intentions to resolve it in a future OS update.

References to third-party solutions/workarounds are provided as information only. We have not tested these solutions and we cannot endorse them.

Can I restore my Mac's backup to another Mac?

Yes! You can use Migration Assistant to migrate data from your CCC backup to another Mac. <https://bombich.com/kb/ccc6/i-want-clone-my-entire-hard-drive-new-hard-drive-or-new-machine> We do not recommend using CCC to restore the data in this particular scenario. Migration Assistant has the privilege to "adopt" the user accounts on the other Mac, so Migration Assistant should be used when restoring a backup to another Mac.

Related Documentation

- I want to migrate data to a new Mac <https://bombich.com/kb/ccc6/i-want-clone-my-entire-hard-drive-new-hard-drive-or-new-machine>

I have a backup created by another application or an older version of CCC. Can CCC update my existing backup?

CCC always examines the files on the destination to determine if they already match those on the source. If you have a volume that is virtually identical to your source, CCC will copy only the items that are different between the two volumes.

Scenario 1: Backup created by a cloning utility

If the software you used previously created a non-proprietary copy of your source to the destination, then CCC will copy only the items that have changed since you created the backup. CCC doesn't care what application you used to copy the files previously, only whether the files match based on name, path, and modification date.

Scenario 2: I replaced my hard drive with an SSD, and now I want to use the HDD as my backup

Whether you copied your HDD to the SSD or used Migration Assistant to get your data there, the bulk of the data on your HDD and SSD are identical. Once again, CCC doesn't care how the data got there or what application put it there, CCC will copy only the items that are different between the two volumes.

Scenario 3: I created my backup with an older version of CCC. Will it still work with CCC 6?

Yes. CCC backups are non-proprietary copies of your source. Any older backup will continue to work with newer versions of CCC.

Can CCC back up my BootCamp (Windows) partition?

CCC is not designed to work with Windows. CCC can back up data from a Boot Camp partition, but it should not be used to make copies of Windows system files. If your goal is to back up your user data on the Boot Camp partition, CCC will meet your needs. If you're looking to migrate your Boot Camp partition to a new hard drive, you might consider an alternative solution such as WinClone <https://twocanoes.com/products/mac/winclone>, or one of the commercial virtualization solutions that offer a migration strategy from Boot Camp. **CCC is not designed to accommodate backing up or restoring Windows system files or applications.**

Avoid copying Windows System files

We have received some reports that macOS will crash when Windows system files are accessed on an NTFS volume. If you encounter this problem, exclude the Windows system files from your backup task:

1. Open CCC and select the relevant backup task
2. Click the **Task Filter** button at the bottom of the window
3. Exclude **WINDOWS** and **Program Files**
4. Click the Done button
5. Click the Save button or choose **Save** from CCC's **Task** menu

Will CCC copy both my macOS and Windows partition at the same time?

No, CCC will copy only one volume at a time, and CCC will not modify the partitioning of the destination disk. You should apply your custom partitioning prior to restoring anything to your new disk.

I'm migrating to a larger disk, will CCC work for my Windows volume?

No, CCC will not create a bootable backup of your Windows volume.

Will CCC copy my Parallels/VMWare virtual machine containers?

Yes! These are just ordinary files as far as CCC is concerned, CCC can copy these just fine. Note that these files can be quite large, so occasionally problems are encountered when these files are in use or when the destination volume does not have sufficient space to accommodate the updated copy of the VM container file.

Related Documentation

- Can I run a backup while I'm using my computer? If I have open files, will they be backed up? <https://bombich.com/kb/ccc6/can-i-run-backup-while-im-using-my-computer-if-i-have-open-files-will-they-be-backed-up>
- My destination has exactly enough space to accommodate the data on the source, why can't CCC complete the backup task?" <https://bombich.com/kb/ccc6/ccc-reported-destination-

full.-what-can-i-do-avoid#destination_is_tight_on_space>

- Example pre and postflight shell scripts (e.g. how to automatically suspend Parallels) <https://bombich.com/kb/ccc6/performing-actions-before-and-after-backup-task#examples>

Can I use CCC to copy a Time Machine backup?

No. Copying a Time Machine backup volume with anything other than the Finder is not supported (by us, nor Apple); CCC specifically disallows copying anything to or from a Time Machine backup volume. Apple does not document a procedure for making copies of Time Machine volumes.

Can I use CCC to restore content from a Time Machine backup?

Generally, no. If you want to restore content from a Time Machine backup, you should use Apple's Time Machine interface for that purpose. If you see a Time Machine snapshot in CCC's Snapshots table, however, you may restore files from that snapshot <https://bombich.com/kb/ccc6/how-restore-from-your-backup#restore_snapshot>.

Can I use the same backup disk for both CCC and Time Machine backups?

Yes, you may use the same physical device, however you should created dedicated volumes on the device for each backup <https://bombich.com/kb/ccc6/i-want-back-up-multiple-macs-or-source-volumes-same-hard-drive>.

CCC reported that the destination is full. What can I do to avoid this?

By default, CCC attempts to be fairly conservative about deleting content from the destination. In most cases CCC will effectively make enough room on the destination by deleting older, out of date content, but depending on the settings you're using, that may not be possible or practical. Here are some things you can do to get past a "destination is full" error.

Use default SafetyNet settings

By default, CCC tasks have SafetyNet enabled, and CCC starts with a SafetyNet pruning limit that will establish 25GB of free space on the destination at the beginning of each backup task. CCC will increase that limit automatically as necessary if the task finds more than 25GB of files to update. If you have customized CCC's SafetyNet setting or the SafetyNet pruning settings, try setting them back to the default values:

1. Select your task in CCC's main application window.
2. Click on the Destination selector and choose **SafetyNet On** from the SafetyNet submenu.
3. Click the **Advanced Settings** button at the bottom of the window.
4. Set the **Prune the SafetyNet** setting to **When free space is less than**.
5. Set the pruning limit to 25 (or a larger value).
6. Check the **Auto adjust** checkbox so CCC can manage this value for you automatically.
7. Click the **Done** button, then run the backup task again.

If snapshots are enabled on your destination volume, you won't configure per-task pruning settings, rather you will adjust the SafetyNet retention settings in the Snapshot Retention Policy for the volume. Follow the steps above, but click on the **Snapshot Pruning Settings** button at step 3 to find those settings.

Disable the SafetyNet feature, and disable "Protect root-level items on the destination"

If your source data set is very close to the capacity of the destination volume, then it may not be practical to use the SafetyNet feature.

1. Select your task in CCC's main application window.
2. Click on the Destination selector and choose **SafetyNet Off** from the SafetyNet sub menu.
3. If prompted, choose the **Remove SafetyNet** option to have the existing SafetyNet folder deleted from the destination immediately.
4. Click on the Destination selector again and select the SafetyNet submenu. If the Protect root-level items on the destination <https://bombich.com/kb/ccc6/advanced-settings#protect> menu item is checked, select that item to disable that setting.
5. If applicable, empty the Trash in the Finder.
6. Save and run the backup task.

When you disable the SafetyNet, all files on the destination are subject to permanent removal – any file that does not exist on the source will be deleted. If you have any doubt about whether content on the destination may be removed, click the **Preview** button in CCC's toolbar to preview the changes before running the task.

Use a larger destination

Ideally, your destination volume will have about twice the capacity as space consumed on the source. That allows ample room for data growth and snapshot retention. If your source data set is larger than, or very close to the capacity of the destination, then it may not be possible to perform safe updates to files on the destination, even with the SafetyNet feature disabled.

Choosing a backup drive: Devices that we recommend <https://bombich.com/kb/ccc6/choosing-backup-drive#recommendations>

Related Documentation

- Where is the CCC SafetyNet folder on the destination? <https://bombich.com/kb/ccc6/frequently-asked-questions-about-ccc-and-macos-catalina#safetynet>
- Snapshots and space concerns; Deleting snapshots <https://bombich.com/kb/ccc6/leveraging-snapshots-on-apfs-volumes#space>
- Why is disk usage different between the source and destination? <https://bombich.com/kb/ccc6/disk-usage-on-destination-doesnt-match-source.-did-ccc-miss-some-files>
- Automated maintenance of the CCC SafetyNet <https://bombich.com/kb/ccc6/automated-maintenance-ccc-safetynet-folder>
- Mail's "Log Connection Activity" setting creates enormous files <https://bombich.com/kb/ccc6/why-ccc-recopying-every-file-during-each-backup#mail_cd_log>

I have a full-volume backup in a folder, but it's not accepted by Migration Assistant. How can I restore everything?

When you configure CCC to back up your startup disk directly to a locally-attached backup volume, that backup is automatically compatible with Migration Assistant. Occasionally people get into this sticky situation though -- "I have a backup of everything in a folder on the backup volume, I have a clean installation of macOS, now how do I get everything back to the way that it was before?"

This situation requires an intermediary restore to a new, empty volume.

Add a volume to your current startup disk

1. Open Disk Utility and select the **Macintosh HD** volume.
2. Click the **+** button in the toolbar.
3. Name the new volume something like **Macintosh HD Restore** (you can rename this later)

Restore your backup to the new volume

1. Open CCC and click **Restore** in the toolbar to create a new Restore task.
2. Drag the folder that contains the complete backup of your previous startup disk onto CCC's Source selector.
3. Select the new **Macintosh HD Restore** volume as the destination.
4. Click the Start button.

Install macOS onto the new volume

1. Boot your Mac while holding down Command+R (Intel Macs) or the Power button (Apple Silicon Macs) to boot into Recovery Mode <https://support.apple.com/en-us/HT204904>.
2. Select the **Reinstall macOS** option and proceed to install macOS onto the **Macintosh HD Restore** volume.

When the installation is complete, you should be able to log in to your restored account, which was adopted by the macOS Installer.

Clean up

1. Open Disk Utility
2. Select the **Macintosh HD** volume in the sidebar.
3. Click the - button in the toolbar. When prompted, choose the **Delete Volume Group** button.
4. Right-click on **Macintosh HD Restore** and choose the option to rename it; rename it to **Macintosh HD**.

Reconfigure your backup strategy to create a Migration Assistant-compatible backup

Finally, make a new backup of your startup disk <https://bombich.com/kb/ccc6/how-set-up-your-first-backup> directly to the root of a locally-attached backup disk so you'll have a Migration Assistant-compatible backup from here forward. If you have other data on that backup disk that you want to leave in place, add a new volume to the backup disk <https://bombich.com/kb/ccc6/i-want-back-up-multiple-macs-or-source-volumes-same-hard-drive#apfs_add_volume> for your CCC backup.

Frequently Asked Questions about encrypting the backup volume

Can I back up an encrypted volume to a non-encrypted volume?

Yes.

If I back up an encrypted volume to a non-encrypted volume, will the copied files be encrypted on the destination?

No, encryption occurs at a much lower level than copying files. When an application reads a file from the encrypted source volume, macOS decrypts the file on-the-fly, so the application only ever has access to the decrypted contents of the file. Whether your backed-up files are encrypted on the destination depends on whether encryption is enabled on the destination volume. If you want the contents of your backup volume to be encrypted, follow the procedure documented here <https://bombich.com/kb/ccc6/working-filevault-encryption> to enable encryption.

Will CCC enable encryption on my backup volume?

No. You can enable encryption in the Security & Privacy preference pane while booted from your bootable backup, or in the Finder by right-clicking on your backup volume (for a backup volume that does not have an installation of macOS).

Do I have to wait for encryption to complete before rebooting from my production volume?

No. Once you have enabled encryption on the backup volume, you can reboot from your production startup disk and the encryption process will continue in the background.

What password do I use to unlock my encrypted volume?

When you boot your Mac from the backup volume and enable FileVault in System Preferences, you explicitly choose which user accounts will be allowed to unlock that volume. To unlock the volume in the future, enter the password to any of those user accounts. Do not attempt to use the Recovery Key or your Apple ID account password to unlock the volume — those passwords will not unlock the volume.

If you erased your backup volume as encrypted in Disk Utility, then you will use the password that you specified in Disk Utility to unlock the volume.

What happens if I change my account password on the source volume? Does the encryption password on the backup volume get updated automatically?

The encryption password(s) on the backup volume will **not** be automatically updated when you change the password for an account on the source volume. When you boot from the backup volume, you may notice that your user account icon is a generic icon, and the text indicates "[Update needed]". The update that is required is within the proprietary encryption key bundle that macOS maintains for your encrypted volume. This encryption key is not maintained on the backup volume, and it is Apple-proprietary, so it isn't something that CCC can or should modify. To update the encryption password on the destination volume:

1. Choose the backup volume as the startup disk in the Startup Disk preference pane and restart your computer. You will be required to provide the old password to unlock the volume on startup.
2. Open the Users & Groups preference pane in the System preferences application.
3. Click on the user whose password was reset on the source volume and reset that user's password again. Resetting the password while booted from the backup volume will update the encryption key for that user on the backup volume.
4. Reset the password for any other user accounts whose password was reset on the original source.

Can I create a bootable backup on a pre-encrypted volume? Why do you recommend copying to a non-encrypted volume first?

It is not possible to **create** a bootable backup on a pre-encrypted backup disk, Apple's tools just don't permit this <https://bombich.com/kb/ccc6/macos-catalina-known-issues#diskutil_addvolume_encryption>. You can enable FileVault after establishing your initial backup, and then CCC can **maintain** a bootable backup on your FileVault-encrypted backup volume.

I restored my backup to another Mac that had FileVault enabled, and now I can't unlock the restored volume.

Encryption is a volume-specific endeavor, and when it's enabled via FileVault, it's also tied to the user accounts on that specific installation of macOS. If you copy another installation of macOS onto a volume that has FileVault enabled, the user accounts from the "foreign" (source) OS will not be able to unlock the FileVault-encrypted destination volume. To avoid this scenario, you should erase the destination volume as a non-encrypted volume. When erasing an APFS volume, be careful to erase the whole APFS container, not just the encrypted volume within the container <https://bombich.com/kb/ccc6/preparing-your-backup-disk-backup-os-x#erase_apfs_container>.

Please note that this concern is not applicable to restoring a backup to the original source volume. In

that case, the OS on the backup volume is not foreign; the user accounts on the backup volume match the user accounts on the original source. In that scenario, FileVault will continue to function normally.

I can't enable FileVault, I'm told that my account cannot be used to manage encryption on this Mac

The Startup Security Utility reports that authentication is needed, but no administrators can be found

After backing up to an APFS volume that previously had FileVault enabled, the destination can't be unlocked on startup

After backing up to an APFS Encrypted volume there is a 24-second stall during startup

All of these conditions are caused by the same underlying problem: users on the affected volume do not have access to the volume's Secure Token. There are generally two ways to get to this result:

- The volume was erased as an encrypted volume, thus no user account was associated with the unlocking of that volume, or
- The user accounts that are allowed to unlock the disk belonged to some previous installation of macOS on that volume

Solution: Erase the destination in Disk Utility before proceeding with the backup task. You should erase the destination as "APFS", not "APFS (Encrypted)". For more technical users, we offer some additional background information below.

APFS volumes that contain an installation of macOS will each have a unique "secure access token". Access to this token allows users to do things like unlock the volume (e.g. if FileVault is enabled) and to change startup security settings. Because this token is volume-specific, it can't be copied to another volume; it has to be regenerated. In addition to this Secure Token, APFS volumes also have a list of users or keys that are "bound" to the volume. These "cryptographic users" are defined within the volume metadata, not within any particular file on the volume. As a result, these bound cryptographic users cannot be modified by CCC nor transferred from one volume to another. This cryptographic user list is proprietary to Apple; only Apple tools can modify the list, and only Apple tools can generate a SecureToken.

While the SecureToken-endowed users and the cryptographic users are usually in sync on a particular volume, these lists are decoupled, and it is possible to get them out of sync. If you copy a system to a pre-encrypted APFS volume, for example, the destination has only one "Disk" crypto user. None of the user accounts on the system that you copied will be (nor can be) included in the crypto users list of that volume. Likewise, if you copy an installation of macOS to a volume that already has an installation of macOS, then you will be overwriting the user accounts that are currently in the crypto user list with new, foreign user accounts. Those new user accounts are not only missing from the crypto user list, but it will be impossible to add them to the crypto user list if all of the previous crypto users were deleted. To avoid both of these scenarios, it's important to copy to a volume that has either crypto users that match those users that exist on the source, or to a destination that has no crypto users at all (e.g. a freshly erased, non-encrypted volume).

Manually regenerating a SecureToken

Apple does not offer a method for creating a SecureToken for a user on a volume that is not the current startup disk, so CCC cannot offer a postflight method that automatically creates that token.

Apple does, however, offer a utility for granting access to the secure token for specific users on the current startup disk *in a very limited number of circumstances*. If the current startup disk has no crypto users (diskutil ap listUsers / returns "No cryptographic users"), or if one of the crypto users is still present on the current startup disk, then you can use the sysadminctl utility to generate a SecureToken for your administrator account, e.g. in the Terminal application:

sysadminctl interactive -secureTokenOn yourname -password -

I don't want to erase my destination again, is there any way to fix this?

If you can't unlock the backup volume on startup, then you can decrypt the destination volume using the diskutil command-line utility. For example, running the following command in the Terminal application would decrypt a volume named "CCC Backup":

diskutil ap decrypt "/Volumes/CCC Backup"

After decrypting the backup volume, you can then boot from it and enable FileVault in the Security & Privacy Preference Pane in the System Preferences application.

If you can boot your Mac from the backup, but you're seeing a stall during startup, you can resolve that matter by decrypting the volume as indicated above, or by creating a new user account that has a Secure Access Token. Only the macOS Setup Assistant has the ability to create the first secure access token, so follow these steps while booted from the volume you're trying to repair:

1. Grant Full Disk Access to the Terminal application
2. Open the Terminal application and run the following commands, substituting your own volume name as applicable:
   sudo rm "/var/db/.AppleSetupDone"
   sudo rm "/var/db/dslocal/nodes/Default/secureaccesstoken.plist"
3. Restart the system
4. Setup Assistant will ask you to create a new user. Create the new user account with default settings. A simple name like "tokenuser" will do, don't login with an Apple ID.
5. Immediately log out of the new user account, and log in using one of your own admin user accounts.
6. Open the Terminal application and run the following commands, substituting your own user names as applicable:
   sysadminctl -secureTokenOn youraccount -password - -adminUser tokenuser -adminPassword -
   sysadminctl interactive -deleteUser tokenuser

Related Apple Bug Reports

- rdar://46168739 — diskutil updatePreboot doesn't remove deleted crypto users

My YubiKey authentication device can't unlock my encrypted backup volume on startup

YubiKey users discovered that the default keystroke input speed of the Yubikey is too fast <https://forum.yubico.com/viewtopicb4e5.html?f=16&t=1142> for the Mac's firmware, resulting in dropped characters. You can solve this by decreasing the key input rate using the YubiKey Manager <https://www.yubico.com/products/services-software/download/yubikey-manager/>.

Frequently asked questions about scheduled tasks

Does CCC have to be running for a scheduled task to run?

No. Once you have saved your tasks, you can quit CCC. Even if tasks are running, it's OK to quit CCC -- they will continue to run. A helper application, named "com.bombich.ccchelper" will be running quietly in the background, handling task operations. This helper application also loads automatically when you restart your computer, so you don't have to launch CCC again unless you want to make changes to your task configurations or scheduling.

What happens if no one is logged in when a task is scheduled to run?

The scheduled task will run whether someone is logged in to the machine or not. You can also log in or log out while tasks are running and the tasks will continue to run.

Will CCC run when the computer is turned off?

If your backup task is configured to "Wake or power on the system", CCC will schedule a "Wake or power on" event with the Power Management service and your system will turn on shortly before the task is scheduled to run.

FileVault exception

There is one notable exception to powering on the system for a scheduled task: **If you have FileVault enabled on your startup disk, your computer would turn on, but it would not proceed past the FileVault authentication prompt.** It is not possible for CCC to subvert this security feature, so the **Wake or power on the system** option will be disabled if FileVault is enabled on your startup disk. This limitation is applicable only when the system is turned off; CCC can wake a system with FileVault protection enabled and proceed to run a backup task.

Related Documentation

- How to modify a scheduled backup <https://bombich.com/kb/ccc6/how-modify-scheduled-backup>

Will CCC run when my laptop's lid is closed?

If your laptop is running on battery power, the system will not wake while the lid is closed and CCC backup tasks will not run. If your laptop is plugged into AC power, then CCC can wake the system to start your scheduled task if the lid is closed. See the section above for the settings that indicate whether a task can wake the system.

How is system sleep handled?

By default, CCC will not wake your computer when your tasks are scheduled to run. You can change this setting in the **System Wake or Power On Behavior** section of the Automation popover.

Once your task is running, CCC will prevent the system from sleeping for the duration of a backup task as long as your Mac is running on AC power.

Related Documentation

- Handling system sleep events <https://bombich.com/kb/ccc6/configuring-scheduled-task-runtime-conditions#sleep>
- How to modify a scheduled backup <https://bombich.com/kb/ccc6/how-modify-scheduled-backup>

Why does my laptop sometimes go to sleep during a backup task?

If your Mac is a laptop, note that CCC will only be able to wake the system or prevent idle sleep if the system is running on AC power. CCC will attempt to thwart sleep while the system is running on battery power, but macOS may sleep the system anyway if there is no user activity while running on battery power.

Why does my screen turn on shortly before a backup task starts?

If your task is configured with one of the **Wake the system** options, CCC will schedule a wake event to occur 20 seconds before the task is scheduled to run. Whether the system is sleeping or not, macOS turns on the display when a scheduled wake event occurs, and there is nothing that CCC can do to prevent this. Additionally, note that if macOS detects an Apple Watch in the vicinity of the computer, it will attempt to use that watch to unlock the screen.

If you prefer that your display does not turn on, e.g. in the middle of the night, use one of the **Run when the system next wakes** settings instead to have CCC tasks run during macOS **Dark Wake** cycles (aka **PowerNap**, aka **Maintenance Wake**).

What if the backup disk is not available when a task is scheduled to run?

If your backup disk is attached to your Mac and unmounted, CCC will attempt to mount the backup volume, then proceed with the backup task if that is successful. If the volume cannot be mounted or is not attached to your Mac, CCC will, by default, report an error, then run the task immediately when the backup disk is reattached to your Mac. You can fine-tune CCC's handling of this scenario using the options at the bottom of the Scheduler panel.

Can I stop a backup task before it finishes?

Yes, you can stop the backup task at any time. The next time you run the backup task, CCC will copy only the files that have changed or were missed since the last backup task.

How can I disable/suspend a task?

If CCC's sidebar is not revealed, reveal it by choosing **Show Sidebar** from CCC's View menu. To disable a task, right-click on that task in the sidebar and choose **Disable** from the contextual menu. Use the same procedure to re-enable the task. If you would like to disable all tasks, choose **Disable all tasks...** from the CCC menubar application, or hold down Command+Option and choose **Disable All Tasks & Quit** from the Carbon Copy Cloner menu.

Can I configure a task to run immediately after the computer is turned on?

CCC doesn't offer an option specifically to run tasks on startup. Running a task immediately after the system is turned on often introduces a lot of extra disk activity that will compete with the disk activity that occurs normally during system startup. Also, it makes less sense to run backup tasks after the computer has been off, because no files have been modified while the system was off. We recommend configuring backup tasks to run sometime toward the end of your work day instead. You can also configure the task to shut down your Mac when the task completes <https://bombich.com/kb/ccc6/performing-actions-before-and-after-backup-task#power_mgmt_options>.

If your work day does not end at a regular time but begins at a fairly consistent time, then there may be one other option available to you. You can configure a backup task to run before your work day begins, and then configure that task to "Wake or power on the system". CCC will then schedule a "wake or power on" energy saver event, and then after the system powers on at that time, CCC will run your scheduled task. Note that this option is not available if you have FileVault enabled on your Mac's startup disk.

Related Documentation

- How do I schedule a backup task? <https://bombich.com/kb/ccc6/how-set-up-scheduled-backup>
- Advanced scheduling options <https://bombich.com/kb/ccc6/advanced-scheduling-options>
- Configuring Scheduled Task Runtime Conditions <https://bombich.com/kb/ccc6/configuring-scheduled-task-runtime-conditions>

Frequently asked questions about the CCC SafetyNet folder

Note: The topics in this article are not relevant to APFS-formatted destination volumes that have CCC snapshot support enabled <https://bombich.com/kb/ccc6/leveraging-snapshots-on-apfs-volumes>. For those volumes, CCC leverages snapshots to implement the SafetyNet functionality, and the snapshots aren't affected by any of the shortcomings described here.

How do I restore files from the _CCC SafetyNet folder?

CCC's SafetyNet folder ("_CCC SafetyNet") is excluded from CCC's backup tasks by default because it contains older versions of modified files, and files that were deleted from the source volume. Typically when you restore data from your backup volume, you will want to avoid restoring the items in this folder, choosing instead to restore the most recent backup of your files.

If there is something that you would like to restore from the CCC SafetyNet folder, a drag and drop restore in the Finder is usually the easiest way to do so. If you would like to restore many items, or merge them into an existing folder, choose **Choose a folder...** from CCC's Source selector and choose the folder from which you would like to restore. If you choose the _CCC SafetyNet folder as the source, note that the full path to your archived files will be preserved, e.g. 2021-07-27 (July 27) 14-11-18/Users/fred/Documents/some file.pdf. In most cases, you will want to choose a subfolder within the archives folder as your source. Likewise, choose **Choose a folder...** from CCC's Destination selector and select the specific folder that you want to restore items into.

Why can't I open some files in the _CCC SafetyNet folder?

When CCC evaluates the items on your destination and determines whether they should be archived or left in place, it does so on a file-by-file basis. This poses a challenge for bundle files — files that are actually a folder of files, but presented by the Finder as a single file. As a result, bundle files (e.g. applications, some types of libraries, some custom file types) may appear in an incomplete form within the CCC SafetyNet folder.

Unless all of the components within a bundle file are modified, only the items that have been updated will be present. Incomplete bundle files are generally not useful on their own, but their contents can be. For example, if you accidentally deleted a photo from your iPhoto library, you would be able to recover that lost photo from the archived iPhoto library bundle. To reveal the content of

an incomplete bundle file in a CCC SafetyNet folder, right-click (or Control+click) on the item and choose **Show package contents** from the contextual menu.

SafetyNet is a safety mechanism, it was not designed for providing access to older versions of files. If you would like access to older versions of files on your APFS-formatted backup disk, we recommend that you enable snapshot support on that volume <https://bombich.com/kb/ccc6/leveraging-snapshots-on-apfs-volumes#srp>.

Can I restore a previous version of the OS using one of the archives in the _CCC SafetyNet folder?

No. CCC's SafetyNet folder is not intended to offer a method for rolling back software updates, OS restores should always be done from the complete backup at the root level of your destination.

I deleted files from my startup disk to make more room, but now it's hard to find some of those files on my backup volume

This generally isn't a concern for ordinary "flat" file types, but it it can be a concern for certain applications that store lots of files in a single, monolithic-appearing container file. Some applications offer highly customized interfaces to access a specific file type. Photos, for example, allows you to manage tens of thousands of photo files. These files are all stored in a proprietary bundle file in your home folder, but because photos are so easy to organize within Photos, many people don't consider how those files are organized on the hard drive. Usually you really don't have to either. That is, of course, until you can no longer use Photos to access your photo files, and that's exactly what happens when you delete files from your Photos library, abandoning them to the SafetyNet folder on your backup volume.

If you have a habit of periodically deleting photos, music, or movies from Photos, iTunes, Aperture, or any other application that uses a proprietary bundle file format so that you can "free up some space on your startup disk", consider how those files will be organized on the destination. Specifically, keep in mind that you use a very elaborate application to access these files on the source volume, but you will only have the Finder to access these files on the backup volume.

CCC can't reorganize your deleted files in a way that's logical to you, it can only place them at the same path in the _CCC SafetyNet folder as they were on the source volume. For files buried in a bundle file on the source (as is the case for Photos, for example), this means that the files will be buried in bundle files in various time-stamped archive folders on the destination. These files will also be subject to deletion if you configure CCC to periodically prune the contents of the SafetyNet. In short, simply archiving deleted files from applications such as these isn't going to be the best way to store these items long-term if your goal is ultimately to keep them.

When you want to free up some space on your startup disk, consider this approach instead, using Photos as an example:

1. Create a new folder at the root level of your backup volume, named something like "Archived Photos 2016".
2. In Photos, delete all of the photos that you want to remove from your source volume. When you delete these items, they are placed in the **Recently Deleted** album.
3. Click on the **Recently Deleted** album in the Photos sidebar and select all of the photos in that folder.
4. Drag all of the selected photos from the **Recently Deleted** album to the "Archived Photos 2016" folder on the backup volume.
5. Once the photos are safely copied to and neatly organized on the backup volume (and

ideally, after you have made a second backup of these precious files on some other volume), go ahead and click the **Delete All** button in the **Recently Deleted** album.

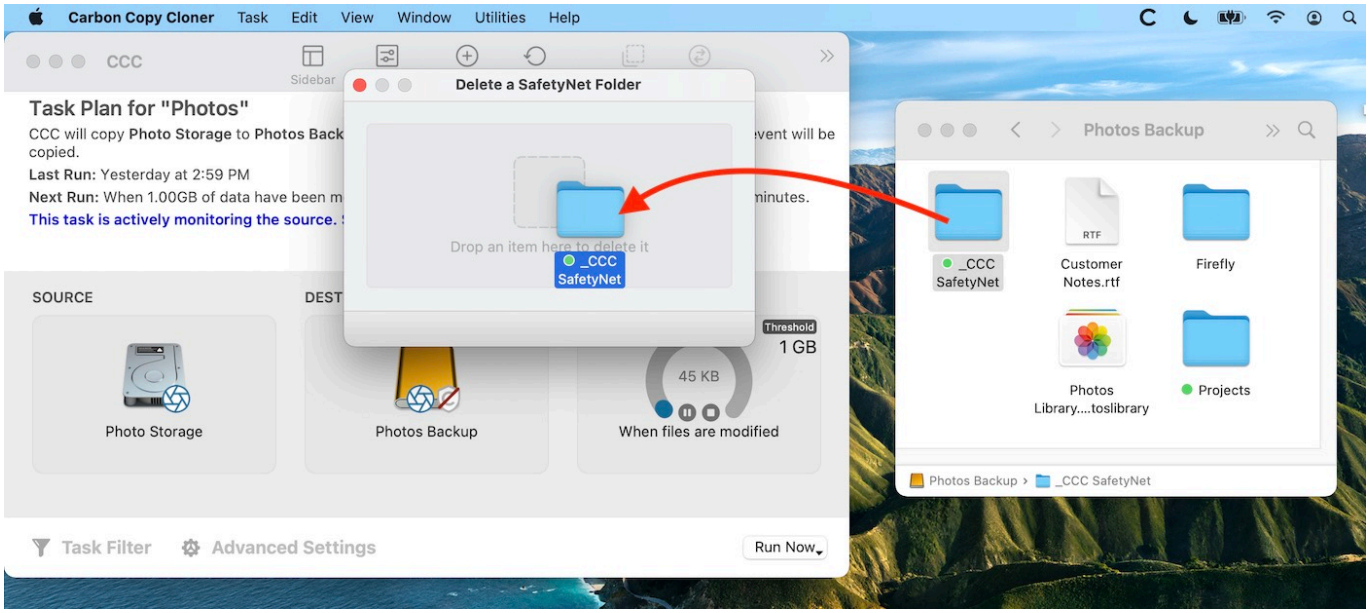
Not all applications have this kind of internal Trash folder, so be sure to see how it works for other applications before applying these exact steps. The general idea, though, is that you should deliberately archive the items that you're removing from your source volume in a way that makes sense to you rather than passively allowing CCC to archive them in a manner that makes sense to the computer.

Why can't I delete some items from the SafetyNet folder? The Finder says that some items are in use.

System Integrity Protection (SIP) and filesystem problems will occasionally cause Finder to report that files in the Trash cannot be deleted because they are in use, or because they are protected. If you try to delete these items in the Terminal application, you'll get a more distinct error message, "Operation not permitted".

CCC won't have any trouble pruning the SafetyNet folder on its own during ordinary backup tasks. If you would like to remove an item from the SafetyNet manually, however, or if you would like to remove the entire folder:

1. Choose **Delete a SafetyNet folder** from CCC's Utilities menu
2. Drag the folder you want to delete onto the window that is presented. Alternatively, you can click on the drop zone in the window that is presented to make your selection from a navigation panel.



If you're still having trouble after trying that, don't hesitate to ask us for help <https://bombich.com/software/get_help>.

How can I prevent Migration Assistant from copying the CCC SafetyNet folder during a migration?

If your backup volume has a "_CCC SafetyNet" folder, you can move that folder to the Trash before using Migration Assistant to avoid copying that folder during a migration. This is particularly important if that folder has a lot of data in it and you're migrating to a disk that is smaller than the backup volume. If you would like to retain the SafetyNet folder on the backup volume, don't empty the Trash. After Migration Assistant has completed, then you can move the SafetyNet folder back to the root of the backup volume.

I have SafetyNet enabled, why can't I find a "_CCC SafetyNet" folder on the destination?

There are three primary reasons that the SafetyNet folder will be missing or difficult to find on the destination:

An empty SafetyNet folder will be removed at the end of the backup task

If CCC finds nothing to archive over the course of the backup task, the SafetyNet archive will be empty at the end of the backup task. If CCC finds that the SafetyNet archive is empty at the end of the task, CCC will remove it. Likewise, if the "_CCC SafetyNet" folder is subsequently empty, that folder will also be removed at the end of the backup task.

The Legacy SafetyNet folder is not used when snapshots are enabled on the destination

When snapshots are enabled on an APFS-formatted destination volume, CCC will implement the SafetyNet feature using snapshots rather than placing files into a separate folder on the destination. Select your destination volume in CCC's sidebar to find these SafetyNet snapshots.

The root level of an APFS Data volume is not visible in the Finder

CCC stores the SafetyNet at the root level of the destination. When you're making a backup of macOS Catalina or later, the destination will be an APFS Volume Group <https://bombich.com/kb/ccc6/working-apfs-volume-groups>, and the SafetyNet will be placed at the root level of the Data member of that group. Root-level items of the Data volume are not immediately visible in the Finder. To reveal the SafetyNet folder on an APFS volume group, right-click on your **CCC Backup - Data** volume (for example) in CCC's sidebar and choose the **Reveal in Finder** option.

Related documentation

- The legacy SafetyNet folder is not used when snapshots are enabled on the destination <https://bombich.com/kb/ccc6/legacy-safetynet-folder-not-used-when-snapshots-are-enabled-on-destination>
- SafetyNet snapshots vs. Backup snapshots <https://bombich.com/kb/ccc6/leveraging-snapshots-on-apfs-volumes#safetynet_vs_backup>
- Where did the CCC SafetyNet folder go after upgrading to Catalina? <https://bombich.com/kb/ccc6/frequently-asked-questions-about-ccc-and-macos-catalina#safetynet>

I selected "Don't delete anything", why is CCC placing items in the "_CCC SafetyNet" folder on the destination?

When you select the **Don't delete anything** SafetyNet setting, CCC applies that setting very literally. If CCC encounters a file on the destination that must be replaced with a newer version from the source, CCC cannot delete the older version of that file that is on the destination. That older file is instead placed into the "_CCC SafetyNet" folder on the destination.

Can I run backup tasks while my system is on battery power?

CCC **can** run backup tasks while the system is running on battery power, but will not (by default) start **automated** tasks when your laptop is running on battery power. Backup tasks generate a lot of disk read and write activity, and that can run your battery down. Additionally, macOS tends to aggressively put the system to sleep when it's on battery power, causing task completion to be deferred until the system is awoken. For the best performance of your backup tasks and your battery, we recommend running your backup tasks when the system is attached to an AC power supply.

Can I configure CCC to start automated tasks when the system is running on battery power?

Yes. Click the **Settings** button in CCC's toolbar to access settings related to running tasks while on battery power.

System problems can lead to a failure to install CCC's helper tool

Configuration files for privileged helper tools are placed in the /Library/LaunchDaemons folder on your startup disk. CCC never touches this folder directly, rather it uses the macOS "Service Management" service to install and load its helper tool configuration. If the permissions or ownership of this folder are incorrect, however, the Service Management daemon (smd) will fail to install the helper tool configuration, and this service offers no recourse. Often the helper tool installation will fail with a nondescript error, e.g. "CFErrorDomainLaunchd error 2". In most cases, reinstalling macOS does not repair the affected system folders. We have reported this system problem to Apple (FB11188842) and we are currently waiting for a response, but there are a handful of options that you can leverage to resolve this permissions problem.

Preliminary troubleshooting of helper tool installation failures

Reboot

The first troubleshooting step is always "**Reboot your Mac**". After rebooting, open CCC to see if you are still prompted to load CCC's helper tool.

Toggle the CCC background item

If the problem persists after rebooting:

1. Quit CCC
2. Open the System Settings applications
3. Navigate to General > Login Items
4. Toggle the switch next to "Carbon Copy Cloner" (On, or if it's already on, toggle it off, then back on).
5. Open CCC to see if you are still prompted to load CCC's helper tool

Force-load the helper tool via the legacy system interface

If the problem still persists, then you can try forcefully loading CCC's helper tool in case some application used an older macOS interface to disable it. Paste the following into the Terminal application:

sudo launchctl load -w /Library/LaunchDaemons/com.bombich.ccchelper.plist

Press the Return key, then authenticate when prompted, then try again to open CCC and save/run a backup task.

Advanced troubleshooting when more serious system problems are present

Remove the contents of the affected folders, then correct their ownership and permissions

If the problem persists after trying the steps above, then the next troubleshooting step is to remove the affected system folders and recreate them with the correct ownership and permissions. To avoid

exposing yourself to potential security vulnerabilities, it is imperative that you **remove** the content of these folders rather than simply correcting the ownership and permissions. Make a note of any applications listed in these folders – those applications should later be re-opened so they have an opportunity to reinstall their helper tools.

Paste the following into the Terminal one line at a time. Press the Return key at the end of each line, authenticate when prompted:

```
cd /Library
sudo rm LaunchDaemons/*
sudo rm PrivilegedHelperTools/*
sudo chown root:wheel LaunchDaemons
sudo chmod 755 LaunchDaemons
sudo chown root:wheel PrivilegedHelperTools
sudo chmod 1755 PrivilegedHelperTools
```

If any of these commands produces an "Operation not permitted" error, or if you are still unable to save a task in CCC, then proceed to the next section.

Replace the folders via Recovery Mode

If macOS security and privacy restrictions prevent you from correcting the issue while booted from your Mac's production startup disk, you can perform the tasks in the Terminal application while your Mac is booted in Recovery mode.

1. Intel Macs: Hold down Command+R while rebooting. Apple Silicon Macs: Shut down, hold down the Power button until the startup options appear, then select **Options**.
2. Choose **Terminal** from the Utilities menu in the menubar.
3. Type the following into the Terminal one line at a time, pressing the Return key at the end of each line:

```
cd "/Volumes/Macintosh HD/Library"
rm -rf LaunchDaemons
rm -rf PrivilegedHelperTools
mkdir LaunchDaemons
chown root:wheel LaunchDaemons
chmod 755 LaunchDaemons
mkdir PrivilegedHelperTools
chown root:wheel PrivilegedHelperTools
chmod 1755 PrivilegedHelperTools
```

Note: If your production startup disk's name is not "Macintosh HD", substitute the correct name in the first line above.

After you have completed those steps, reboot your Mac, open CCC, and try again to save or run a backup task.

Related Documentation

- What is CCC's Privileged Helper Tool? <https://bombich.com/kb/ccc6/what-cccs-privileged-helper-tool>

The legacy SafetyNet folder is not used when snapshots are enabled on the destination

SafetyNet is a feature unique to CCC that aims to protect data on your destination volumes. The most common scenario for which this feature was designed was to protect the contents of a volume that was errantly selected as a destination volume. Rather than immediately deleting the contents of that volume, CCC would place that content into a folder named "_CCC SafetyNet". When you realize the configuration mistake, you simply recover the files from the SafetyNet folder and then correct your backup task configuration.

The SafetyNet feature does not know the difference between "old data that needs to be archived" vs. "data on the destination that has nothing to do with the source data set". Because these files are offered the same protection, many users have leveraged the SafetyNet feature as a means for recovering older versions of their files. The SafetyNet folder was never designed for this, and has many shortcomings when used in that regard <https://bombich.com/kb/ccc6/frequently-asked-questions-about-carbon-copy-cloner-safetynet>. Nevertheless, many users have grown used to looking for the older versions of their files in this SafetyNet folder.

To avoid filling up the destination with older, unnecessary data, CCC would prune the contents of the SafetyNet folder when free space drops below a certain threshold (or based on age, or archive size, if you have modified this behavior). When CCC prunes the content of that folder, the space that those files occupies is immediately freed.

Snapshots and the legacy SafetyNet folder are mutually exclusive

When you enable snapshot support on a destination volume that contains a legacy SafetyNet folder, we have a dilemma to resolve. When you create a snapshot on the destination, the traditional pruning becomes completely ineffective at freeing up disk space. Because your oldest snapshot retains a reference to all of the files in the SafetyNet folder, the space that they consume will never be freed until that oldest snapshot is deleted, which may not occur until the destination reaches the free space limit defined in your snapshot retention policy.

To resolve this dilemma, CCC leverages a snapshot to implement the SafetyNet feature when snapshots are enabled on the destination. If you have a legacy "_CCC SafetyNet" folder on the destination, CCC will create a SafetyNet Snapshot of the destination (thus retaining references to every file in the SafetyNet folder), then delete the legacy SafetyNet folder. The files in the SafetyNet folder are not immediately lost because they are retained within the SafetyNet snapshot, however that SafetyNet Snapshot is now subject to the SafetyNet retention limit specified in your destination volume's Snapshot Retention Policy (by default it will be deleted after one week).

Advantages of snapshots over the legacy SafetyNet folder

Leveraging snapshots on the destination resolves several shortcomings of the folder-based SafetyNet with regard to using the SafetyNet for recovering older versions of your files. Please note that these are not advantages specific to the SafetyNet, however, these are general advantages of using snapshots. If you decide to use snapshots on your destination, you should try to avoid thinking about the SafetyNet as your mechanism for restoring older versions of files. When you want to recover older versions of your files, you'll use Backup Snapshots for that purpose. SafetyNet is a

safety mechanism that should only be used when something was deleted from the destination that had nothing to do with the source data set.

If you have used the SafetyNet in the past for recovering files, consider the following advantages to using snapshots to recover older versions of your files:

- Bundle files (e.g. your Photos Library) in the snapshot are whole. If you deleted several albums from your Photos Library, you'll have a hard time recovering those from the legacy SafetyNet folder. With snapshots, you don't even need the SafetyNet, because those files are retained in Backup Snapshots.
- Deleting snapshots is really simple, you'll never run into permissions problems or failures of the Finder to empty the Trash.
- Past versions of your files can be easily navigated via CCC's Snapshot Navigator <https://bombich.com/kb/ccc6/how-restore-from-your-backup#restore_snapshot>, whereas dumpster-diving through the "_CCC SafetyNet" folder was always a laborious chore.

Disadvantages of the snapshot-based SafetyNet

While snapshots do offer significant advantages to users that want to restore older versions of their files, these come at a small cost to the original purpose of the SafetyNet feature. When items are moved to the legacy SafetyNet folder on the destination, they're still immediately visible to you in the Finder, and you can restore them **immediately** to their original location via a simple drag and drop procedure. When snapshots are enabled, however, those items are retained by a snapshot, but then deleted from the destination. To restore those items, you must reveal the SafetyNet Snapshot in the Finder, then **copy** those items back to the destination. That copying procedure will not only take quite a bit longer than a simple move, but it also may be logistically difficult if your destination volume is particularly full. In those cases, you may have to recover the files to a separate volume, delete the SafetyNet snapshot to free space, then copy the files back to the original volume.

While this is not an insignificant drawback of snapshots, we felt that the benefits of point-in-time restores far outweighs this disadvantage as long as the SafetyNet retains its ability to offer protection for files that are unique to the destination.

How do I choose which approach is best for me?

The choice comes down to whether you leverage the SafetyNet feature more as a safety mechanism that protects against configuration mistakes (like picking the wrong destination or accidentally storing stuff on your backup disk thinking it would be "safe" there) vs. using it as a means to recover older versions of your files. If you rarely look to your backups for recovering the older version of a file (or the OS), then enabling snapshots on your backup disk won't offer a lot of benefit over the legacy SafetyNet mechanism. If you've found yourself looking into the SafetyNet for older versions of your files, however, then enabling snapshots on the destination will provide much more reliable results for retrieving older versions of your files.

Why does CCC say that my Mac is booted from a backup volume?

If you boot your Mac from a backup volume, CCC will be started upon login to ask whether you'd like help restoring from that backup volume. Sometimes, though, this offer is made when you're booted from a production volume, not a backup. CCC makes this assessment based on your currently-defined backup tasks. If you used CCC to migrate from one drive to another, then the task that you used to perform that backup will still be present on your new startup disk. When you boot your Mac from the new disk, CCC will see that you have a suspended task that specifies the current startup disk as the destination, thus giving the appearance that your Mac is booted from a backup.

If you migrated to a new disk and you'd like to avoid CCC opening on startup and offering restore guidance, open CCC and delete the task that you used to restore to your current startup disk.

Frequently asked questions about CCC and macOS Catalina

If you have applied the macOS Catalina, Big Sur or Monterey upgrade, you may have noticed a new volume on your Mac, "Macintosh HD - Data". This new volume is part of a volume group, which is a new concept that Apple introduced in macOS Catalina. We discuss volume groups in detail here <https://bombich.com/kb/ccc6/working-apfs-volume-groups>, but the remainder of this article aims to answer your questions about how CCC handles this new volume structure and what you have to do, if anything, to adjust your backups for Apple's latest OSes.

Maybe. If you are making a simple backup of your startup disk to a dedicated backup disk, then no, you do not have to make any changes to the destination unless CCC specifically recommends it. **CCC will automatically make the changes required for your destination to be a bootable backup of your startup disk**. If your destination volume is encrypted, however, see the question later in this document for information specific to encrypted destinations.

If you have multiple tasks that back up to the same destination, however, then now is a good time to revisit your backup "hygiene". Ideally, each source that you back up will have a dedicated volume on the destination. This is particularly important when one of the sources is a Catalina or Big Sur startup disk. See this section of CCC's documentation for guidance on how to configure your destination device to accommodate backups of multiple source volumes:

I want to back up multiple Macs or source volumes to the same hard drive <https://bombich.com/kb/ccc6/i-want-back-up-multiple-macs-or-source-volumes-same-hard-drive>
Video: Preparing a disk for backup or restore <https://youtu.be/5mBO3o570Ak>

No. When you select your startup disk (e.g. Macintosh HD) as the source for your backup task, CCC will automatically back up both volumes in that volume group.

CCC says that the partitioning scheme of my backup disk is wrong. How do I fix that?

Many external hard drives are shipped with a Windows-centric format and partitioning scheme. That partitioning scheme can't accommodate Apple's APFS filesystem, so before you can use your backup disk for making a bootable backup of your startup disk, you must make sure that it is partitioned with the correct partitioning scheme. This section of CCC's documentation walks you through the steps for configuring your backup disk:

Preparing your destination disk for a backup or restore <https://bombich.com/kb/ccc6/preparing-your-backup-disk-backup-os-x>

Disk Utility's interface for performing this simple task is surprisingly unintuitive, so here is a summary of the process with some emphasis on the steps where people often go awry:

1. Open Disk Utility
2. Choose **Show all devices** from Disk Utility's View menu. *This is a very important step!*
3. Choose the **parent device** of your destination volume in the sidebar – don't click on the backup volume itself, click on its parent device. If you don't click on the parent device, you won't be able to change the partition scheme.
4. Click on the **Erase** button in the toolbar. *Don't click on the Partition button!* That would seem like the obvious choice, but you cannot actually change the partitioning scheme in the Partition interface.
5. Set the Scheme to **GUID Partition Map** and the Format to **APFS**, then click the **Erase** button.

If you're still having trouble correcting the partition scheme, you may find this video demonstration <https://youtu.be/5mBO3o570Ak?t=40> helpful.

What will CCC do to my bootable backup disk when I run it for the first time?

Because macOS leverages volume groups for the startup volume, creating a bootable backup requires an APFS formatted destination volume. HFS+ is no longer an option for booting macOS starting with macOS Catalina. For your convenience, **CCC will automatically convert your HFS+ formatted backup volume to APFS** as necessary and create a volume group on the destination. This conversion is the same conversion that took place on your startup disk when you upgraded to High Sierra or Mojave, with one notable exception: CCC tells you that it's going to convert the

destination, and gives you the opportunity to decline the conversion. The conversion is non-destructive — any data that you have on the destination volume will remain in place, the only thing that changes is the format of the volume.

Why might I not want to allow the conversion of my destination volume?

Typically there is no reason to decline the conversion. The conversion is non-destructive, and it's required for making a backup of the system. If your backup volume is dedicated to your CCC backup task, then converting the destination to APFS is the right choice.

However, if your destination volume is not dedicated to your CCC backup task or if you're not intending to back up the macOS System files, you should consider how the other uses of your destination might be affected by the conversion. For example, Time Machine is not currently compatible with APFS as a destination, so converting a destination volume that contains a Time Machine backup would break the Time Machine backup. CCC specifically avoids converting Time Machine backup volumes. Another example – **if you're only backing up a single folder or handful of folders from your startup disk**, you should configure a folder-to-folder backup <https://bombich.com/kb/ccc6/folder-folder-backups> instead, which won't require any conversion of the destination.

You should also avoid the conversion **if your destination device is a slower 2.5" rotational HDD**, i.e. with a rotational speed of 5400RPM (or slower!). APFS does not perform well on HDD devices <https://bombich.com/blog/2019/09/12/analysis-apfs-enumeration-performance-on-rotational-hard-drives>, and that performance is unacceptable on these slowest HDD devices due to their much slower seek performance. Keep these slower disks formatted as Mac OS Extended, Journaled. These devices are suitable for Data-only backups, but you should acquire an SSD for making bootable backups <https://bombich.com/kb/ccc6/choosing-backup-drive#recommendations>.

Can I keep other data at the root of my bootable backup volume?

No. In particular, you should not use the Finder to copy items to the root level of your bootable backup disk. Finder will copy that data to System volume within the group, and when the System

volume is subsequently updated, any non-system files could be permanently deleted from that System volume. If you want to store other items on your backup disk that are unrelated to the backup of the system, create a separate volume on that disk for that purpose (see the following question for instructions).

I already have other stuff on my destination. How can I avoid affecting that content?

Video: Backing up multiple sources to a single APFS-formatted device <https://youtu.be/MXHNeCHnpnI>

If your destination volume is already APFS formatted, but you do not want to make your bootable backup **in that volume**, you can simply add a new volume to the existing APFS container:

1. Open Disk Utility
2. Select your destination disk in Disk Utility's sidebar
3. Click the "+" button in the toolbar

If your destination volume is not APFS formatted, and you cannot or prefer to not convert the volume to APFS, you can create a dedicated partition on your destination disk for CCC to use. To create the partition:

1. Open Disk Utility
2. Select your destination disk in Disk Utility's sidebar
3. Click the Partition button in the toolbar
4. Click the "+" button to add a partition to the disk
5. Set the name and size of the partition to your preference
6. Choose APFS as the format
7. Click the Apply button

I had other stuff at the root of my destination, now I can't see it. How do I find it?

If you were keeping other data at the root level of your backup disk that isn't on your startup disk, then that data is still on your backup disk, but it will be harder to find in the Finder due to the volume

group changes that are applied for a backup of the startup disk. If your backup disk is named "CCC Backup", right-click on the "CCC Backup - Data" volume in CCC's sidebar and select Reveal in Finder to reveal that content.

Video: Backing up multiple sources to a single APFS-formatted device <https://youtu.be/MXHNeCHnpnI>

How long will the conversion process take?

It depends on how much data you have on your destination volume, the performance of the destination device, and the degree to which the destination volume is fragmented. It can take a while, but CCC won't wait for more than two hours for the conversion to complete. If it's taking longer than two hours, then CCC will recommend that you erase the destination volume instead, which will resolve any performance issues that are directly caused by filesystem fragmentation. If CCC issues this recommendation and you prefer to wait out the conversion rather than erase the volume, you're welcome to convert the volume in Disk Utility instead (the option is in the Edit Menu).

Will my encrypted backup volume be automatically converted to an APFS volume group?

Unfortunately that is not possible due to a macOS limitation, Disk Utility cannot add an encrypted volume to an APFS volume group <https://bombich.com/kb/ccc6/macos-catalina-known-issues#diskutil_addvolume_encryption>. When you select a Catalina+ startup disk as a source and an encrypted volume as a destination, CCC will disallow the selection and suggest that you erase or decrypt the destination volume.

Fastest and easiest solution: Erase the destination as APFS (not encrypted)

Erasing the destination volume is the simplest and fastest way to resume your bootable backups, and you can find detailed instructions for doing that here: Preparing your destination disk for a backup or restore <https://bombich.com/kb/ccc6/preparing-your-backup-disk-backup-os-x>.

After you have run your backup task to a non-encrypted volume, you can then boot from the backup and re-enable FileVault in the Security & Privacy Preference Pane.

Related Documentation

- Can I temporarily decrypt my destination volume instead of erasing it? <https://bombich.com/kb/ccc6/frequently-asked-questions-about-ccc-and-macos-catalina#conversion_encrypted_decrypt>
- Can I make a non-bootable backup on an HFS+ formatted or APFS encrypted volume? <https://bombich.com/kb/ccc6/frequently-asked-questions-about-ccc-and-macos-catalina#encrypted_non_bootable>
- Working with FileVault Encryption <https://bombich.com/kb/ccc6/working-filevault-encryption>
- Frequently Asked Questions about encrypting the backup volume <https://bombich.com/kb/ccc6/frequently-asked-questions-about-encrypting-backup-volume>

Can I temporarily decrypt my destination volume instead of erasing it?

Decrypting the destination volume will take considerably more time (possibly days) and effort, but you can decrypt the destination volume with one of the following methods:

A: Boot from the backup volume, open the Security Preference Pane, disable FileVault

B: Decrypt the volume in the Terminal application. E.g. for an HFS+ formatted destination:
diskutil cs decryptVolume "/Volumes/CCC Backup"

Or for an APFS-formatted destination, get a list of user IDs associated with the encrypted volume, then use one of the "Local Open Directory User" UUIDs from the output of the first command with the second command:
diskutil ap listUsers "/Volumes/CCC Backup"
diskutil ap decryptVolume "/Volumes/CCC Backup" -user B44348A3-68DF-4B7B-800D-47FE38711178

Replace "B44348A3-68DF-4B7B-800D-47FE38711178" with a UUID produced by the first command.

Wait for decryption to complete

You'll have to wait for the decryption process to complete before you proceed with your backup task. Decryption will continue in the background while you're booted from your production startup disk. macOS doesn't offer a convenient method to see conversion progress, but you can type `diskutil apfs list` (or `diskutil cs list` if the applicable volume is HFS+ formatted) in the Terminal application to see conversion progress.

Re-enabling FileVault on your bootable backup volume

After you have run your backup task to a non-encrypted volume, you can then boot from the backup and re-enable FileVault in the Security & Privacy Preference Pane.

Related Documentation

- Can I make a non-bootable backup on an HFS+ or APFS encrypted volume? <https://bombich.com/kb/ccc6/frequently-asked-questions-about-ccc-and-macos-catalina#encrypted_non_bootable>
- Working with FileVault Encryption <https://bombich.com/kb/ccc6/working-filevault-encryption>
- Frequently Asked Questions about encrypting the backup volume <https://bombich.com/kb/ccc6/frequently-asked-questions-about-encrypting-backup-volume>
- Catalina Known Issue: Apple's volume group manipulation tool doesn't work with encrypted volumes <https://bombich.com/kb/ccc6/macos-catalina-known-issues#diskutil_addvolume_encryption>

If I decrypt or erase the destination, then reenable it later, will I have to do this again for future backups?

No, this is a one-time task that is required for CCC to be able to make adjustments to the destination volume that are required for APFS volume groups. Once you have established a bootable backup, you can reenable FileVault and your future backups will work without any additional intervention.

Can I make a non-bootable backup on an HFS+ or APFS encrypted volume?

If you are willing to forgo the creation of a bootable backup of your startup disk, you can configure your backup task to back up only the Data volume of your startup disk:

1. Open CCC and click the Show Sidebar button in CCC's toolbar if it is not already visible
2. Select your backup task in the sidebar
3. Click the "Volumes" header in the sidebar
4. Drag the "Macintosh HD - Data" volume from CCC's sidebar into the Source selector
5. Save the task

With this configuration, CCC will not impose any requirements on the format or encrypted nature of the destination volume. Because this destination will not be bootable, we recommend that you

remove any existing System folders from the destination volume to avoid any ambiguity about the functionality that this volume provides.

CCC was copying the System volume, and then started copying everything a second time. Is this normal?

Yes. Your startup disk has two separate volumes, a read-only System volume, and a writable Data volume where all of your data is kept. The System volume has about 10GB of content, and CCC will back that up first. When CCC has finished copying the System volume, CCC will then proceed to back up the contents of your Data volume. The System volume will only get modified when you apply macOS updates, though, so you won't see this volume getting copied frequently — CCC will only update the System volume on the destination when the System volume on the source has been modified.

Can I undo the volume group changes that CCC applied to the backup disk?

Watch a video of this tutorial on YouTube <https://youtu.be/MXHNeCHnpnI>

Yes, you can dismantle a volume group in Disk Utility. You may want to do this if, for example, you backed up your startup disk to a volume that was not intended to be dedicated to your backup task. The procedure is relatively simple — you simply delete the System volume, then rename the Data volume, then remount the volume. If your backup disk was named "CCC Backup", for example, you would do the following:

1. Open Disk Utility
2. Choose **Show all devices** from the View menu
3. Select the **CCC Backup** volume in the sidebar — this is the System volume in the group.
4. Click the **—** button in the toolbar to delete that volume
5. Select the **CCC Backup - Data** volume
6. Click the **Unmount** button in the toolbar
7. Click the **Mount** button in the toolbar to remount that volume
8. Change the name of the volume back to **CCC Backup**

Where is the CCC SafetyNet folder on the destination?

You won't find a legacy _CCC SafetyNet folder on the destination if snapshot support is enabled on that volume <https://bombich.com/kb/ccc6/legacy-safetynet-folder-not-used-when-snapshots-are-enabled-on-destination>. Instead, select the destination Data volume in CCC's sidebar to see a list of SafetyNet snapshots.

If snapshot support is not enabled on your destination volume, then the SafetyNet folder can be difficult to navigate to in the Finder. It's still located at the root level of your destination's Data volume, but the Data volume is hidden by default in the Finder. To reveal it in the Finder, click on CCC's Destination selector and choose the **Reveal Data Volume** option.

I can't delete the SafetyNet folder in "Relocated Items", Finder says they are in use.

If you have ever restored content back to your production startup disk while booted from a CCC backup, then there may have been a _CCC SafetyNet folder placed at the root of that volume. When you upgrade to Catalina or Big Sur, the macOS installer will relocate any content that is at the root of the startup disk to Users > Shared > Relocated Items > Security. You will also find a PDF in that folder explaining why the content was moved there. In short, the content was moved there because it is very difficult to find content at the root level of the Data volume of your startup disk.

If you attempt to delete that SafetyNet folder (and you certainly **may** delete that folder), the Finder may claim — **falsely** — that the folder cannot be deleted because some items are in use. In fact, nothing in that folder is in use, but some of the older system items may be protected by System Integrity Protection. You can learn how to dispose of this content in this section of CCC's documentation:

Why can't I delete some items from the SafetyNet folder? The Finder says that some items are in use. <https://bombich.com/kb/ccc6/frequently-asked-questions-about-carbon-copy-cloner-safetynet#sip_prevents_delete>

Frequently asked questions about CCC and macOS 11 (and later OSes)

With the announcement of macOS Big Sur, Apple has retired Mac OS X (10) and replaced it with macOS 11. As the numeric change would suggest, this is the biggest change to macOS since Apple introduced Mac OS X roughly 20 years ago. The system now resides on a cryptographically sealed "Signed System Volume" <https://developer.apple.com/news/?id=3xpv8r2m>. That seal can only be applied by Apple; ordinary copies of the System volume are non-bootable without Apple's seal. To create a functional copy of the macOS 11 System volume, we have to use an Apple tool to copy the system, or install macOS onto the backup. CCC 6 will not attempt to create a bootable backup of Big Sur by default, however the functionality is available via the Legacy Bootable Backup Assistant.

How are bootable copies made differently on macOS Big Sur?

When configured via the Legacy Bootable Copy Assistant, CCC will use Apple's APFS replication utility, "ASR", to establish a bootable copy of your startup disk. Apple's utility does not offer as much flexibility as you've grown accustomed to with CCC on older OSes, in particular it requires that the destination is erased and that everything is copied from the source to the destination. When you configure a legacy bootable copy of your startup disk on Big Sur, CCC will offer a few options, depending on the size and current format of your destination device:

- Allow CCC to erase the destination to make a bootable backup
- Add a new, dedicated backup volume to an existing APFS destination (if there is enough free space)
- Proceed with a Standard Backup (this is a complete backup of all of your data, applications, and system settings)

To learn more about these options, and what to expect when running your first "Full Volume Backup" see Creating legacy bootable copies of macOS (Big Sur and later) <https://bombich.com/kb/ccc6/cloning-macos-system-volumes-apple-software-restore>.

Does my CCC backup have to be bootable for me to restore data from it?

No, in fact we no longer recommend that you attempt to make your backup bootable. Bootability is a convenience that allows you to continue working if your startup disk fails, but it is not required for restoring data from a CCC backup. You can restore individual folders and older versions of files (i.e. from snapshots) using CCC while booted from your production startup disk. CCC backups are also compatible with Migration Assistant, so you can use Migration Assistant to restore all of your data to a clean installation of macOS (e.g. on a replacement disk).

Related resources

- How to restore from your backup <https://bombich.com/kb/ccc6/how-restore-from-your-backup>

After CCC has established an initial bootable copy, will it keep the destination System volume up to date?

No. We would like to offer this functionality, but doing so involves some unacceptable compromises. Due to an inflexibility in Apple's APFS replication utility (ASR) <https://bombich.com/kb/ccc6/macos-

big-sur-known-issues#asr_volume_group>, we can only update the destination System volume by cloning both the System and Data volumes together with ASR, and that involves erasing the destination every time an OS update is applied to the source. Doing so would remove all snapshots on the destination, and would take quite a bit longer than an ordinary incremental backup.

How do I upgrade my Catalina (or older) backup to Big Sur?

After you upgrade your Mac to Big Sur, and only after you have decided to commit to the Big Sur OS <https://bombich.com/kb/ccc6/best-practices-updating-your-macs-os#commit>, you may resume the backup of your startup disk to your CCC backup volume. Open CCC and review each of your backup tasks to see if any adjustments are required for the first backup on the new OS.

Related resources

- Creating legacy bootable backups of macOS Big Sur <https://bombich.com/kb/ccc6/cloning-macos-system-volumes-apple-software-restore>
- How to restore from your backup <https://bombich.com/kb/ccc6/how-restore-from-your-backup>
- Using Migration Assistant to restore your startup disk from a CCC backup <https://bombich.com/kb/ccc6/how-restore-from-your-backup#install_then_migrate>
- Frequently asked questions about CCC and macOS Catalina <https://bombich.com/kb/ccc6/frequently-asked-questions-about-ccc-and-macos-catalina> (many of these are also applicable to Big Sur)
- Best practices for updating your Mac's OS <https://bombich.com/kb/ccc6/best-practices-updating-your-macs-os>
- macOS Big Sur Known Issues <https://bombich.com/kb/ccc6/macos-big-sur-known-issues>

When I boot from my backup, Little Snitch reports that its rules have been replaced by a different version. Why, and how can I avoid this?

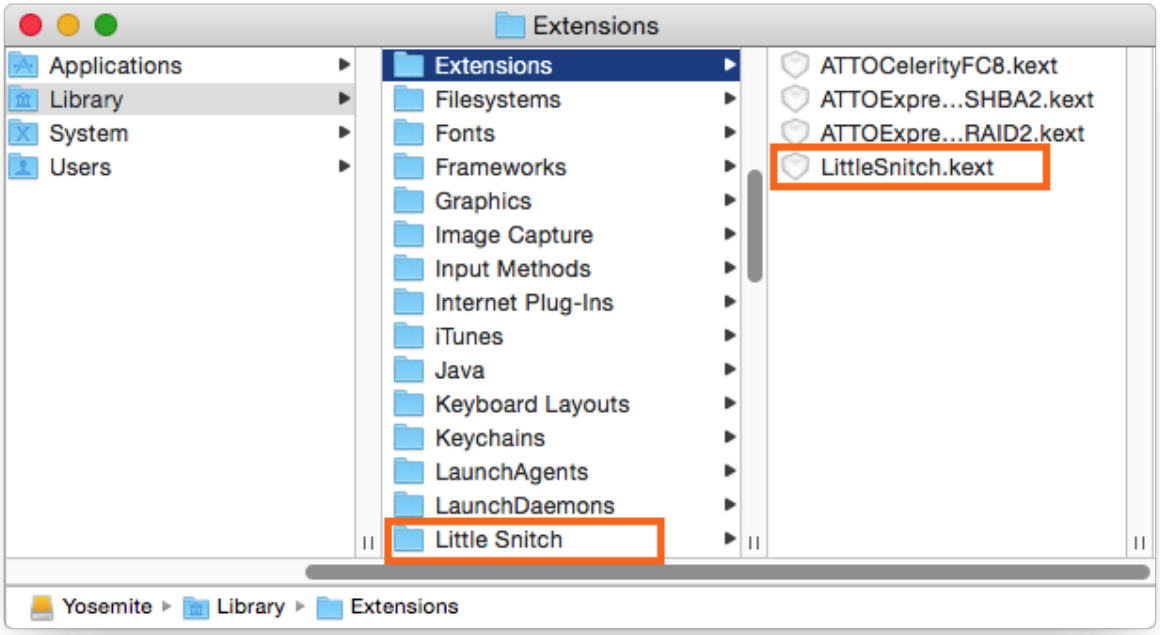
According to ObDev developers, it is crucial for Little Snitch to avoid unnoticed ruleset changes. Little Snitch therefore has numerous mechanisms to detect whether it is using the **exact** same ruleset file, as in, on the same volume and at the same physical address on that disk. This sort of mechanism makes it impossible for Little Snitch to use the ruleset on the booted backup volume without physical intervention from a user at the system (thus the dialog asking if it's OK to use the current version of rules or to use a default ruleset).

In cases where you have physical access to your computer while booting from the backup, the solution is straightforward — simply click the button to use the current rule set and everything behaves as normal.

In cases where you do not have physical access to the system, e.g. you have a server in a colocation facility, there is a logistical challenge. While Little Snitch is reporting that the ruleset doesn't match, it's also preventing network connectivity to and from the server. If you rely on VNC screen sharing to access the system, you will be unable to access the system to accept the current version of the Little Snitch ruleset.

According to ObDev developers, you can avoid this logistical lockout by removing the following two items from your backup volume before rebooting from it:

/Library/Extensions/LittleSnitch.kext
/Library/Little Snitch



Once rebooted, reinstall Little Snitch to regain the application firewall and all is well.

While that method works fine for cases in which you plan to reboot from the backup volume, you're potentially in a lurch if you have an **unplanned** incident, e.g. the server's hard drive fails. To avoid encountering this problem altogether, you can exclude those files from your backup task <https://bombich.com/kb/ccc6/excluding-files-and-folders-from-backup-task>.

CCC does not delete files from the destination that are excluded from the backup task <https://bombich.com/kb/ccc6/excluding-files-and-folders-from-backup-task#delete_excluded>, so be sure to remove those items from your destination if you have already established your backup.

Can I pause a CCC task?

Most tasks can be paused during the "Comparing and copying files" phase of the task. When a task is in a pausable phase, the Pause button will be enabled in CCC's main window, and the button with the "media pause" icon will be enabled in CCC's Dashboard application. Click the Pause button to temporarily pause the task. Click the Continue button to resume the task.

Paused tasks will resume automatically after 5 minutes

After 5 minutes, a paused task will automatically resume. You can change that period in CCC Settings > Advanced, although we recommend that you avoid setting that to very large values. Pausing a task will only pause the task's filesystem activity, it will not pause other filesystem activity on the source and destination volumes. The longer a task is paused, the greater chance there is of state inconsistencies arising between the filesystem and CCC's file copier.

Paused tasks are aborted when the computer is shut down.

A paused task will not resume after a restart or shutdown.