

What's New	4
What's new in CCC 5?	5
Carbon Copy Cloner 5 Release Notes	11
Credits	33
Everything you need to know about Carbon Copy Cloner and APFS	35
Working with APFS Volume Groups	39
Upgrading from Carbon Copy Cloner 3.5 to Carbon Copy Cloner 5	42
System Requirements for Carbon Copy Cloner	44
Purchasing CCC	46
Bombich Software Sales Policies and Frequently Asked Questions	47
How much does Carbon Copy Cloner cost and how can I purchase it?	50
Purchasing an Upgrade for Carbon Copy Cloner 5	51
How does the free 30-day trial work?	53
If I pay for CCC now, will I have to pay for future updates?	54
Can I use one license of CCC on multiple Macs in my household?	55
Do you offer an academic discount?	56
Do you offer a volume licensing program?	58
Can I give CCC as a gift?	59
Why isn't CCC on the Mac App Store?	60
Do you offer telephone support?	61
Downloading, Installing and Registering CCC	62
How do I download and install Carbon Copy Cloner?	63
Upgrading from CCC 4 to CCC 5	66
How to Manually Enter a CCC Registration Code	67
Can I download the old versions of Carbon Copy Cloner?	71
How to Register CCC in One Click	72
Trouble Applying Your Registration Information?	74
How do I use one license of CCC on multiple Macs in my household?	76
Oops, that license code is invalid...	78
I already purchased CCC but can't find my registration code. Can you send it to me?	81
Migrating CCC tasks from one system to another	82
Getting Ready to Use CCC	84
Choosing a backup drive	85
Preparing your destination disk for an installation of macOS	89
Best practices for updating your Mac's OS	102
Using CCC	106
How to set up your first backup	107
How to verify or test a bootable backup	113
How to restore from your backup	116
How to set up a scheduled backup	123
How to modify a scheduled backup	127
Monitoring backup tasks with the CCC menubar application	131
Configuring Email Notifications	137
How to find out when a backup last ran: CCC Task History	142
Protecting data that is already on your destination volume: The Carbon Copy Cloner SafetyNet	146
The Disk Center	151
Cloning Apple's Recovery HD partition	154
Leveraging Snapshots on APFS Volumes	157
Simple Mode	168
Notes for VoiceOver users	171
Granting Full Disk Access to CCC and its helper tool	172
Cloning macOS System volumes with Apple Software Restore	175
Creating and restoring data volume backups	178
Sample Usage Scenarios	180

I want to clone my entire hard drive to a new hard drive or a new machine	181
I want to back up my data to a Time Capsule, NAS, or other network volume	183
Restoring an item from a hidden folder	185
Cloning one external hard drive to another external hard drive	190
Folder-to-Folder Backups	193
Backing up and restoring Finder's Trash	198
Refining the scope of a backup task	200
Troubleshooting	201
macOS Big Sur Known Issues	202
macOS Catalina Known Issues	205
How do I get help?	211
Help! My clone won't boot!	213
Keeping CCC up to date	225
Uninstalling CCC	227
Antivirus software may interfere with a backup	229
What criteria does CCC use to determine if a file should be recopied?	232
"CCC found multiple volumes with the same Universally Unique Identifier"	235
Finder or App Store finds other versions of applications on the backup volume	237
Launchpad ignores settings created while booted from another volume	238
"The task was aborted because a subtask did not complete in a reasonable amount of time"	240
Troubleshooting slow performance when copying files to or from a network volume	242
Where can I find CCC's log file?	244
Why can't I eject the destination volume after the backup task has completed?	245
Why does Finder prevent me from viewing the home folder on my backup when it's attached to another Mac?	248
Some third-party storage drivers may cause hardware misbehavior	251
Troubleshooting APFS Replication	253
Coping with errors caused by APFS filesystem corruption	256
Identifying and Troubleshooting Hardware-Related Problems	258
Advanced Topics	262
Excluding files and folders from a backup task	263
Advanced Settings	268
Performance Suggestions	274
Working with FileVault Encryption	277
Some files and folders are automatically excluded from a backup task	280
Performing actions Before and After the backup task	285
Restoring non-system files	292
Backing up to a disk image	293
Restoring from a disk image	298
I have a full-volume backup in a folder or a disk image, but I don't have a bootable backup. How can I restore everything?	301
Using Carbon Copy Cloner to back up to/from another Macintosh on your network	303
A caveat for backing up to a remote Macintosh that has no user logged in	311
Restoring from a backup on a remote Macintosh	312
Task Organization	313
I want to defragment my hard drive	315
Using the ccc Command Line Tool to Start, Stop, and Monitor CCC Backup Tasks	316
Backing up databases on OS X Server	318
Backing up large files, mounted disk images, and Virtual Machine containers	320
Automated maintenance of the CCC SafetyNet folder	321
"My disk is already formatted APFS or HFS+, why am I getting this warning?"	325
Backing up to/from network volumes and other non-macOS-formatted volumes	327
A closer look at how CCC determines the "bootability" of a destination volume	333
Cloning Coach Configuration Concerns	336

Configuring Scheduled Task Runtime Conditions	340
Modifying CCC's Security Configuration	343
Creating a separate task to prevent VM container versions from bloating the SafetyNet	345
Outgoing network connections made by CCC	346
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?	348
Limitations of online-only placeholder files	350
What is CCC's Privileged Helper Tool?	352
Downgrading an APFS-formatted Fusion volume from Mojave	354
Frequently Asked Questions (FAQ)	356
Glossary of Terms	357
The disk usage on the destination doesn't match the source. Did CCC miss some files?	363
I want to back up multiple Macs or source volumes to the same hard drive	365
Can I run a backup while I'm using my computer? If I have open files, will they be backed up?	368
Some applications behave differently or ask for the serial number on the cloned volume. Did CCC miss something?	369
Can I back up one computer and use the clone to restore another computer?	371
I have a clone created by another application. Will CCC recognize that data, or will it want to recopy everything?	374
Can CCC back up my BootCamp (Windows) partition?	375
CCC reported that the destination is full. What can I do to avoid this?	377
Can I use Carbon Copy Cloner to clone a Time Machine backup?	380
Frequently Asked Questions about encrypting the backup volume	381
Frequently asked questions about scheduled tasks	386
Frequently asked questions about the Carbon Copy Cloner SafetyNet folder	389
Frequently Asked Questions about cloning Apple's "Recovery HD" partition	394
Can I run backup tasks while my system is on battery power?	397
Can I run my backups more frequently than Hourly?	398
System problems can lead to a failure to install CCC's helper tool	399
The legacy SafetyNet folder is not used when snapshots are enabled on the destination	400
Why does CCC say that my Mac is booted from a backup volume?	402
Frequently asked questions about CCC and APFS Volume Groups	403
Frequently asked questions about CCC and macOS 11	413

What's New

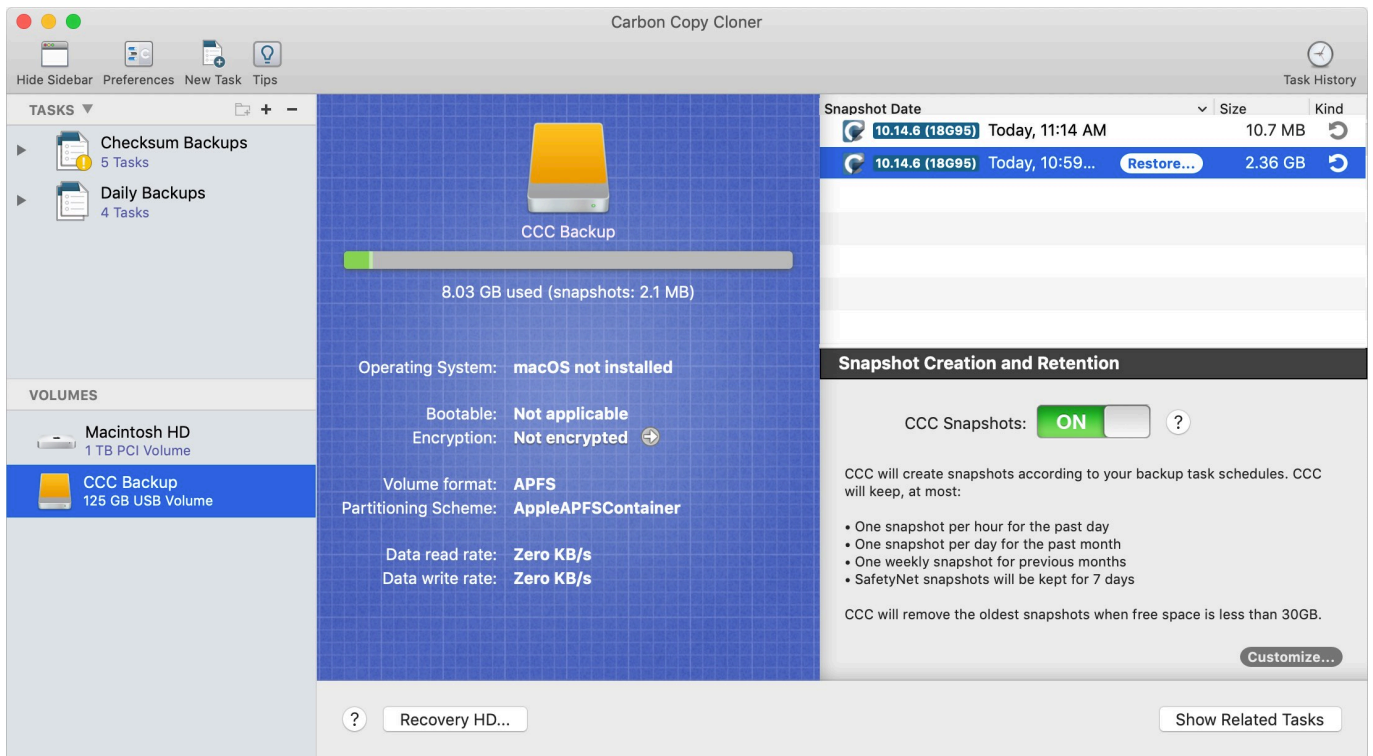
What's new in CCC 5?

Carbon Copy Cloner 5 offers more customization for our advanced users and smarter, more dynamic defaults and extra help for the novice users. There's a little something in here for everyone. If you're still scratching your head over some new functionality, please don't hesitate to [ask us for help](http://bombich.com/software/get_help) <http://bombich.com/software/get_help>.

New in CCC 5.1

Versioned backups with APFS Snapshots

CCC now offers support for point-in-time restores by leveraging the snapshot feature of Apple's new APFS filesystem. CCC is also **the first comprehensive snapshot management utility for macOS**. CCC starts with sensible defaults, but you get to decide how frequently CCC creates snapshots and precisely how CCC will retain snapshots over time. Browsing the contents of any snapshot is just a click away, and should you want to delete a specific snapshot, just select it and press the Delete key. CCC will list each snapshot on a given volume along with its size; select multiple snapshots to see their collective size. No other utility offers this much insight into your APFS volumes' snapshots!



The screenshot displays the Carbon Copy Cloner 5.1 interface. On the left, the 'TASKS' sidebar shows 'Checksum Backups' (5 tasks) and 'Daily Backups' (4 tasks). The 'VOLUMES' sidebar lists 'Macintosh HD' (1 TB PCI Volume) and 'CCC Backup' (125 GB USB Volume). The main area shows a progress bar for 'CCC Backup' at 8.03 GB used (snapshots: 2.1 MB). Below this, system information is displayed: Operating System: macOS not installed; Bootable: Not applicable; Encryption: Not encrypted; Volume format: APFS; Partitioning Scheme: AppleAPFSContainer; Data read rate: Zero KB/s; Data write rate: Zero KB/s. On the right, the 'Task History' table shows two snapshots: '10.14.6 (18G95)' from 'Today, 11:14 AM' (10.7 MB) and '10.14.6 (18G95)' from 'Today, 10:59...' (2.36 GB) with a 'Restore...' button. Below the table, the 'Snapshot Creation and Retention' section has a toggle for 'CCC Snapshots' set to 'ON'. It explains that CCC will create snapshots according to backup task schedules and lists retention rules: one snapshot per hour for the past day, one per day for the past month, one weekly for previous months, and SafetyNet snapshots kept for 7 days. It also notes that CCC will remove the oldest snapshots when free space is less than 30GB. A 'Customize...' button is at the bottom right of this section. At the bottom of the main area, there are buttons for 'Recovery HD...' and 'Show Related Tasks'.

Related Documentation

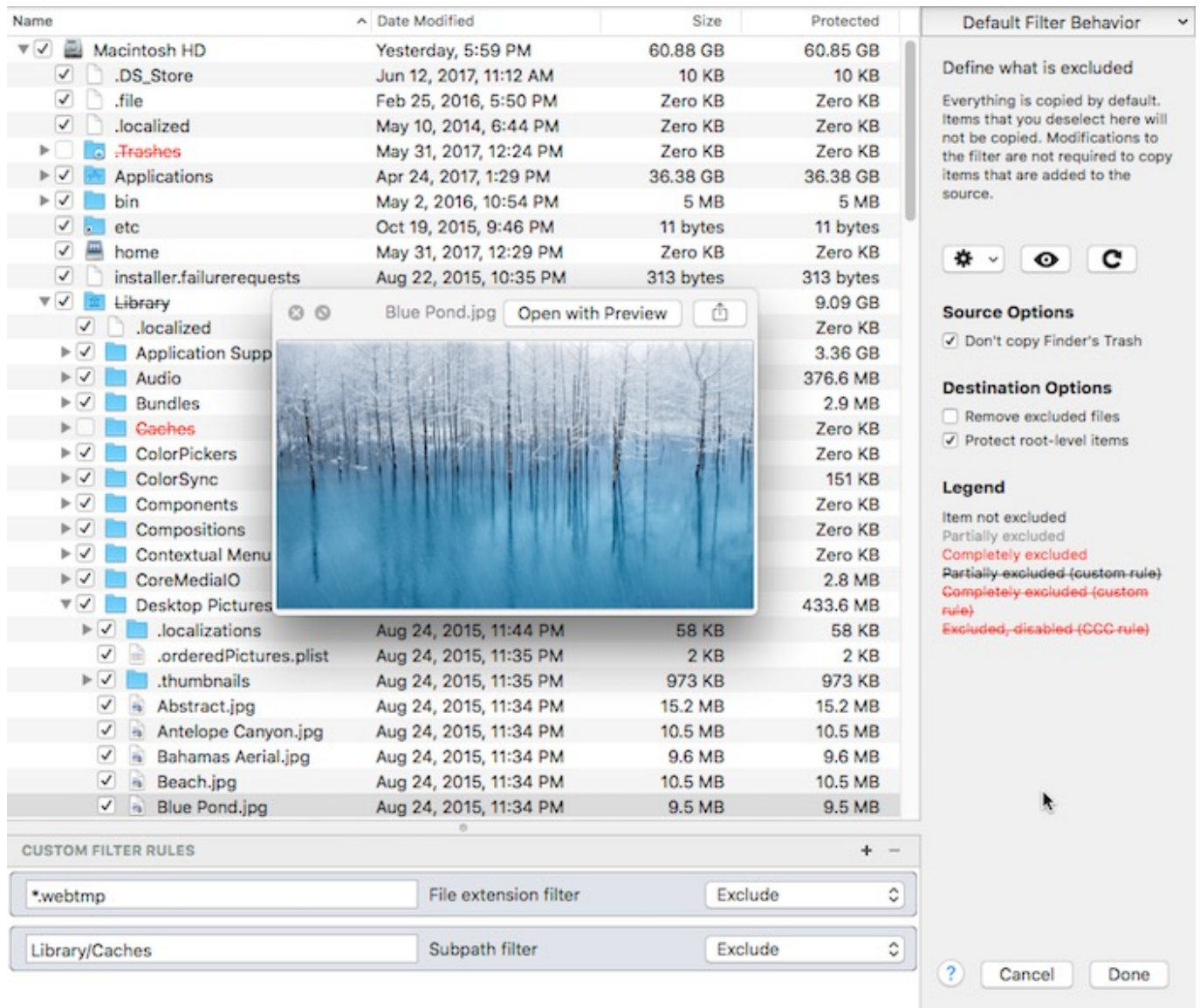
- [Leveraging Snapshots on APFS Volumes](http://bombich.com/kb/ccc5/leveraging-snapshots-on-apfs-volumes) <<http://bombich.com/kb/ccc5/leveraging-snapshots-on-apfs-volumes>>

New interface for defining task filters

Excluding a folder or two from a backup task has always been trivial with CCC. More complex filters

have presented some challenges, though, so by popular request, we have added the following new features:

- CCC can calculate the amount of space consumed by the files on the source. If you exclude items from the task or add custom filters to exclude items based on patterns, CCC will report the total protected size of each folder (and cumulatively).
- The task filter can now exclude everything by default, allowing you to specify only what items should be included in the backup task. This is in contrast to the default behavior in which CCC includes everything by default, allowing you to specify what is excluded from the backup task.
- Filters can be imported and exported. Additionally, when you change the source for your backup task, CCC will now ask you whether you want to reset the task filter (rather than simply resetting it).
- The effects of custom and global filters are immediately apparent.
- A QuickLook panel shows a preview of the selected file.
- Contents can be sorted by name, modification date, or size.
- You can select an item, then Shift+click on the checkbox for another item within the same parent folder to select/deselect all of the items in between.
- If you really want to, you can have CCC copy your Trash. There's a checkbox for that now!



The screenshot displays the Carbon Copy Cloner 5 interface. The main window shows a file list with columns for Name, Date Modified, Size, and Protected. A preview window for 'Blue Pond.jpg' is open, showing a snowy forest scene. The right sidebar contains filter settings, including 'Default Filter Behavior', 'Source Options', 'Destination Options', and a 'Legend'. The bottom section shows 'CUSTOM FILTER RULES' with two rules: '*.webtmp' (File extension filter) and 'Library/Caches' (Subpath filter), both set to 'Exclude'.

Name	Date Modified	Size	Protected
Macintosh HD	Yesterday, 5:59 PM	60.88 GB	60.85 GB
.DS_Store	Jun 12, 2017, 11:12 AM	10 KB	10 KB
.file	Feb 25, 2016, 5:50 PM	Zero KB	Zero KB
.localized	May 10, 2014, 6:44 PM	Zero KB	Zero KB
.Trashes	May 31, 2017, 12:24 PM	Zero KB	Zero KB
Applications	Apr 24, 2017, 1:29 PM	36.38 GB	36.38 GB
bin	May 2, 2016, 10:54 PM	5 MB	5 MB
etc	Oct 19, 2015, 9:46 PM	11 bytes	11 bytes
home	May 31, 2017, 12:29 PM	Zero KB	Zero KB
installer.failurerequests	Aug 22, 2015, 10:35 PM	313 bytes	313 bytes
Library			9.09 GB
.localized			Zero KB
Application Supp			3.36 GB
Audio			376.6 MB
Bundles			2.9 MB
Caches			Zero KB
ColorPickers			Zero KB
ColorSync			151 KB
Components			Zero KB
Compositions			Zero KB
Contextual Menu			Zero KB
CoreMediaIO			2.8 MB
Desktop Pictures			433.6 MB
.localizations	Aug 24, 2015, 11:44 PM	58 KB	58 KB
.orderedPictures.plist	Aug 24, 2015, 11:35 PM	2 KB	2 KB
.thumbnails	Aug 24, 2015, 11:35 PM	973 KB	973 KB
Abstract.jpg	Aug 24, 2015, 11:34 PM	15.2 MB	15.2 MB
Antelope Canyon.jpg	Aug 24, 2015, 11:34 PM	10.5 MB	10.5 MB
Bahamas Aerial.jpg	Aug 24, 2015, 11:34 PM	9.6 MB	9.6 MB
Beach.jpg	Aug 24, 2015, 11:34 PM	10.5 MB	10.5 MB
Blue Pond.jpg	Aug 24, 2015, 11:34 PM	9.5 MB	9.5 MB

CUSTOM FILTER RULES

- *.webtmp File extension filter Exclude
- Library/Caches Subpath filter Exclude

Default Filter Behavior

Define what is excluded

Everything is copied by default. Items that you deselect here will not be copied. Modifications to the filter are not required to copy items that are added to the source.

Source Options

- Don't copy Finder's Trash

Destination Options

- Remove excluded files
- Protect root-level items

Legend

- Item not excluded
- Partially excluded
- Completely excluded
- Partially-excluded-(custom-rule)
- Completely-excluded-(custom-rule)
- Excluded,-disabled-(CCC-rule)

Smarter SafetyNet

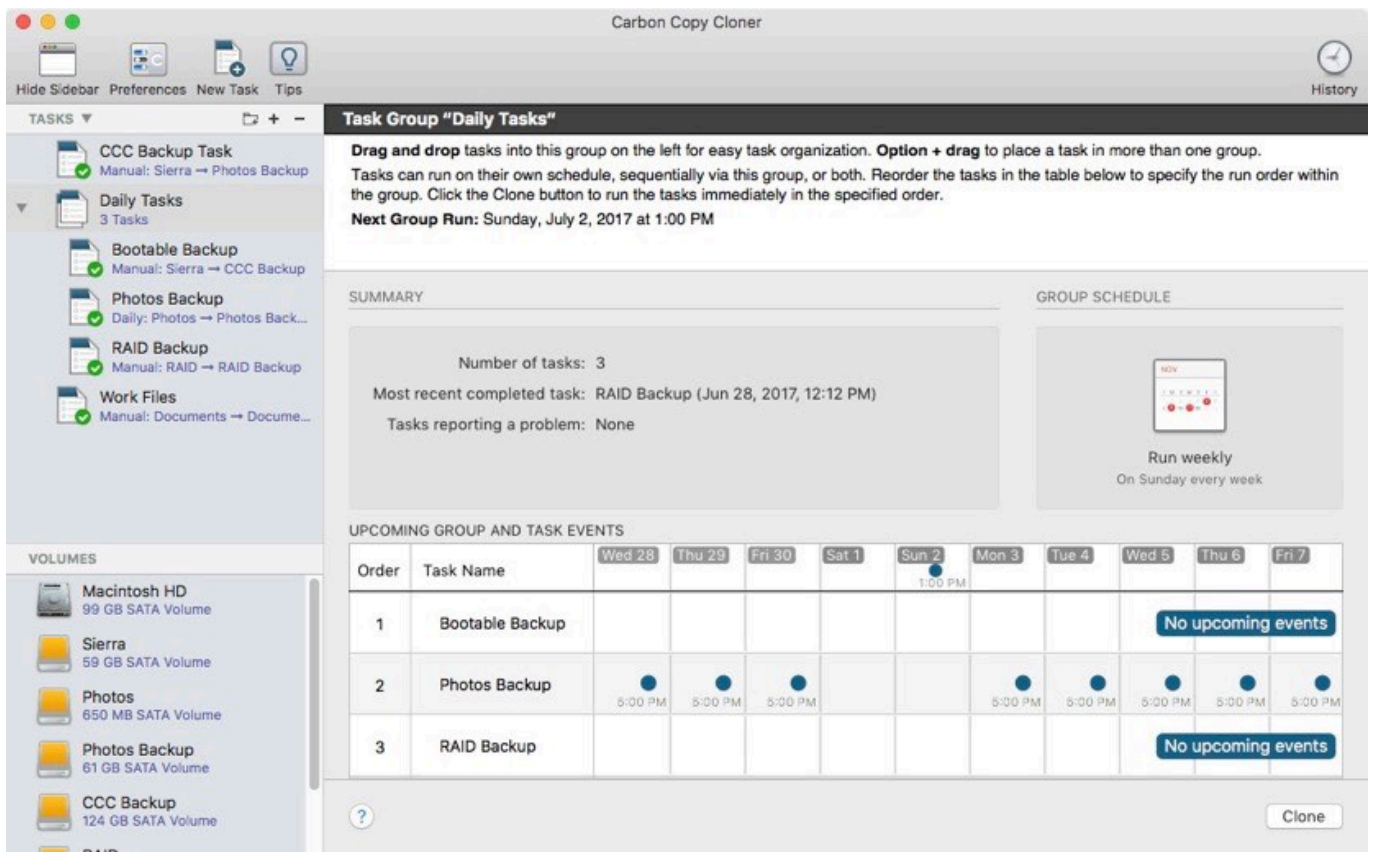
CCC's SafetyNet pruning settings will now automatically adapt to the amount of data your tasks need to copy. If a backup task runs out of space on the destination, CCC will revisit the pruning of the SafetyNet folder, then resume copying. In cases where the SafetyNet feature is impractical due to limited overhead on the destination, CCC will recommend disabling that feature.

Simplified Remote Mac setup

The setup procedure for backing up to a remote Macintosh has been greatly simplified. CCC now presents a browser that shows Macs on your local network that have the remote login service enabled. Upon authenticating, CCC can then retrieve OS version details (to determine compatibility) and a list of volumes and files/folders. This greatly simplifies the specification of the remote host address and the path to the source/destination. This functionality is extended to the task filter as well, where you can choose to exclude specific items that are on a remote Mac source (making remote Mac restores far simpler than they are in CCC v4).

Task Grouping

Many users have asked for more advanced ways to organize their tasks, so in CCC v5 we added task groups that have both organizational and runtime behaviors.



The screenshot shows the Carbon Copy Cloner interface. On the left, there's a sidebar with 'TASKS' and 'VOLUMES'. The 'TASKS' section shows a list of tasks: CCC Backup Task, Daily Tasks (3 tasks), Bootable Backup, Photos Backup, RAID Backup, and Work Files. The 'VOLUMES' section shows Macintosh HD, Sierra, Photos, Photos Backup, CCC Backup, and RAID.

The main window displays a 'Task Group "Daily Tasks"' with the following details:

- Drag and drop tasks into this group on the left for easy task organization. Option + drag to place a task in more than one group. Tasks can run on their own schedule, sequentially via this group, or both. Reorder the tasks in the table below to specify the run order within the group. Click the Clone button to run the tasks immediately in the specified order.**
- Next Group Run: Sunday, July 2, 2017 at 1:00 PM**

SUMMARY

- Number of tasks: 3
- Most recent completed task: RAID Backup (Jun 28, 2017, 12:12 PM)
- Tasks reporting a problem: None

GROUP SCHEDULE

Run weekly
On Sunday every week

UPCOMING GROUP AND TASK EVENTS

Order	Task Name	Wed 28	Thu 29	Fri 30	Sat 1	Sun 2	Mon 3	Tue 4	Wed 5	Thu 6	Fri 7
1	Bootable Backup					1:00 PM					
2	Photos Backup		5:00 PM	5:00 PM	5:00 PM		5:00 PM	5:00 PM	5:00 PM	5:00 PM	5:00 PM
3	RAID Backup										

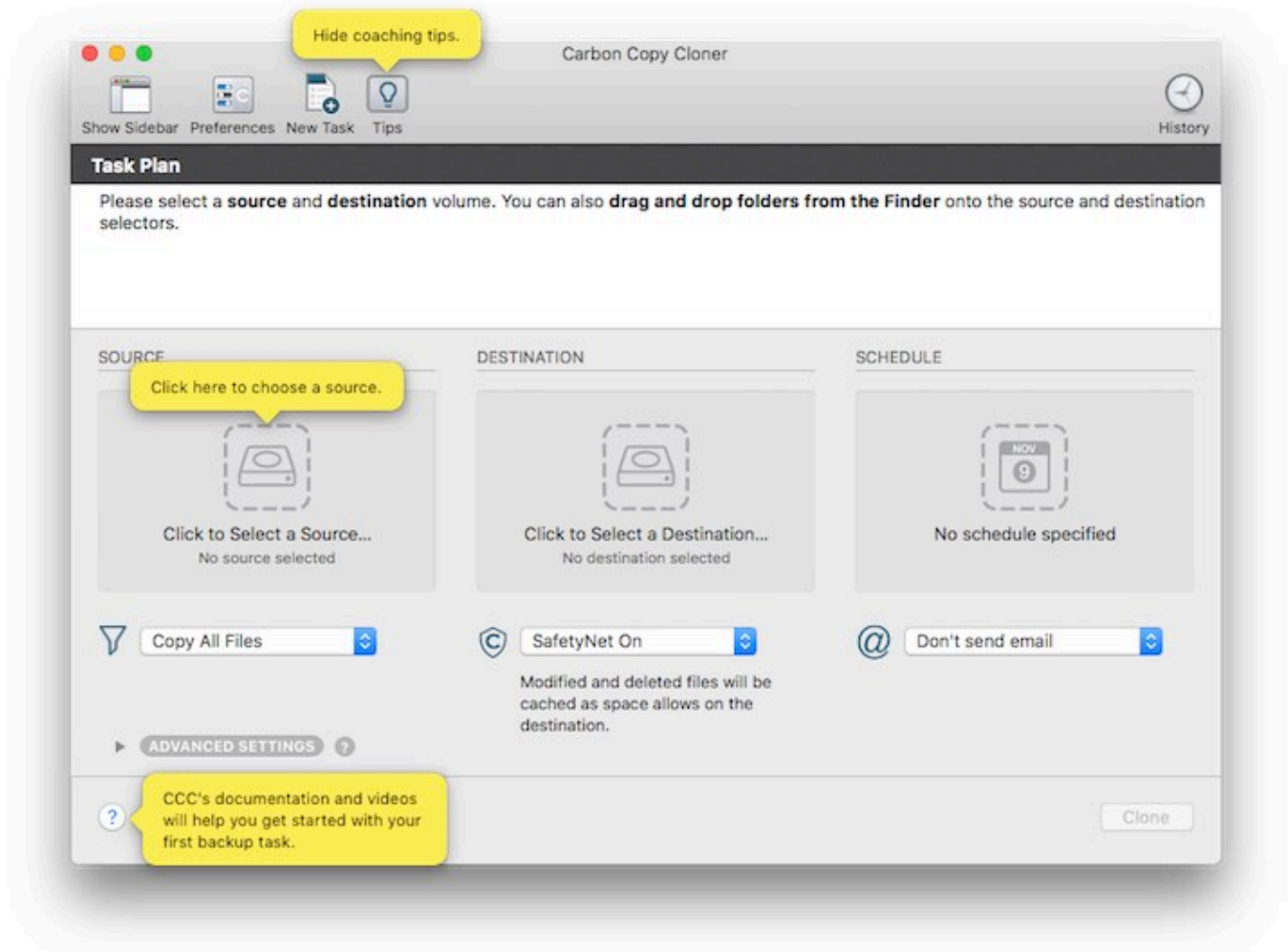
Buttons: Clone

In their simplest form, task groups can be used to organize your tasks in a logical manner. Task groups can also be scheduled, however, and this offers a much simpler way to run a collection of tasks in a specific order. There's a lot of power and flexibility here – individual tasks within the group can be scheduled and run independently of the group, but they can also run on the group schedule. CCC handles conflicts that would arise; for example, a task will skip its own schedule if it's already

running via the group. If you have task-specific postflight power management settings, those are aggregated. CCC will only sleep/restart/shutdown the system at the end of the last backup task that runs within the group.

Guided Setup

CCC now offers coaching tips in "thought bubbles". These tips explain the purpose of various user interface elements. Upon first launch, a few of these tips appear and guide the user through setting up the first backup task. Once that's complete, toggling the Tips via the menubar shows the full collection of tips.



Guided Restore

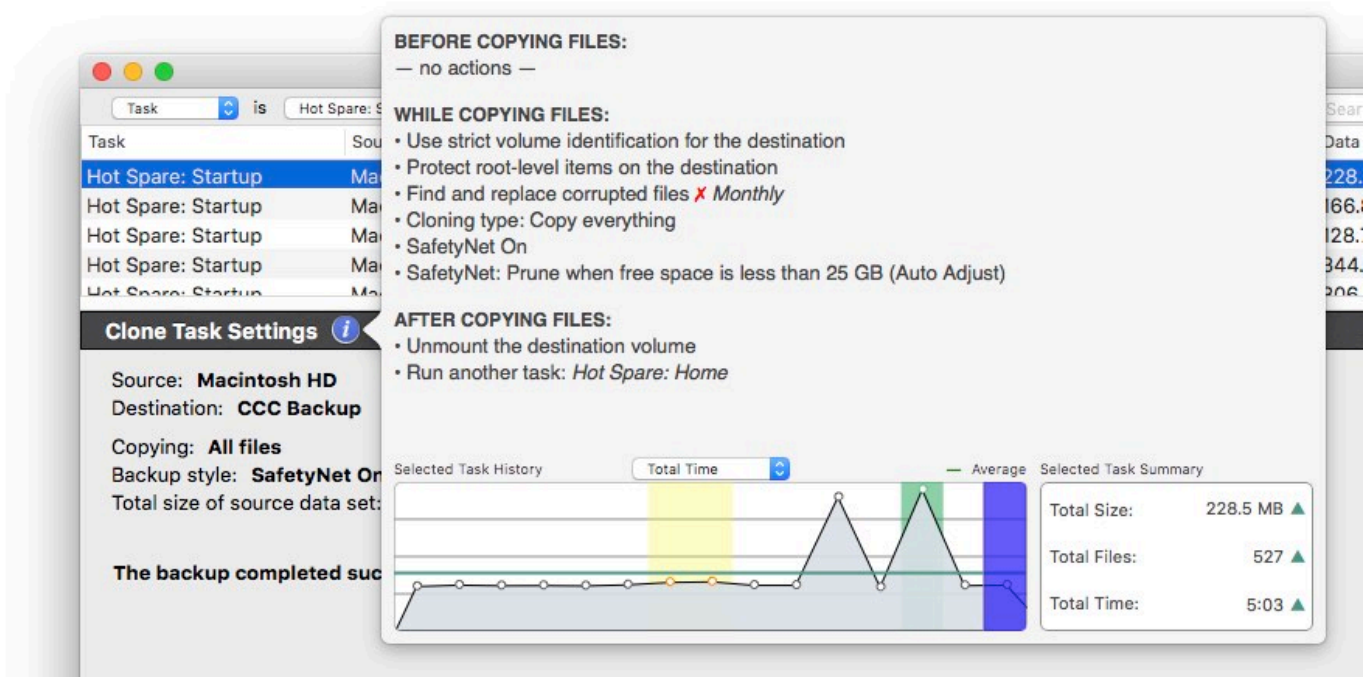
CCC can detect if your Mac is booted from a volume that was previously a CCC destination volume. Upon seeing this on startup, CCC will open and prompt the user to do a guided restore. In the guided restore, CCC will create a new restore task, select the startup disk as the source, then present coaching tips that guide the user through selecting the destination and (optionally) excluding items from the restore task. The Help button will also take the user to restore-specific documentation and videos.

New scheduling options

Tasks can be scheduled to run once at a particular time in the future. After that run, the tasks will revert to run "only when I click the Clone button". We also added hourly runtime limits, allowing the user to limit a task to running only between 5PM and 7AM, for example. Hourly limits will prevent a task from starting if it's outside the specified run time, and if the task runs past the allowed end time, the task will be stopped.

Task History Trends

CCC's Task History window now offers a trend chart. The trend chart shows how your tasks are performing over time, and how many files/how much data gets copied each time your task runs. All of this information was available in the Task History window before, but the chart makes it easy to visualize trends, potential configuration issues and to identify, for example, when a performance issue arose.



Other niceties

Our todo 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 v5:

- SafetyNet generates a lot of questions, so now the SafetyNet popup menu has a "What is SafetyNet?" item.
- Tasks can be sorted by name, exit status, last run date, next run date, or manually.
- The destination selector offers a visual disk usage indicator.
- You can click on a volume (e.g. in the source/destination selectors) to mount or unmount that volume, or to reveal it in the Finder.
- The source and destination selections can be reset to "Choose a source/destination".
- The CCC User Agent will now check for updates on the schedule defined in the main application.
- Some of the the Cloning Coach messages have been aggregated and simplified to seem less daunting to novice users.
- The "Find and replace corrupted files" setting can now be limited to run once per week or

once per month. This simple change will allow many people to drop superfluous task duplicates that have only this option as a difference.

- Tasks can be [imported and exported](http://bombich.com/kb/ccc5/migrating-ccc-tasks-from-one-system-another) <<http://bombich.com/kb/ccc5/migrating-ccc-tasks-from-one-system-another>>.

Upgrading from CCC 4

The upgrade path from CCC 4 to CCC 5 couldn't be simpler. Simply open CCC 5, and it will automatically update your CCC v4 tasks. If you kick the tires for 30 days and decide to stay on CCC 4, simply re-open CCC 4 and choose the option to downgrade. CCC 4 will then reload your original CCC v4 tasks and everything will be as it was prior to your trial of CCC v5.

Related Resources

- [Download CCC 5](http://bombich.com/software/download_ccc.php?v=latest) <http://bombich.com/software/download_ccc.php?v=latest>
- [Download CCC 4](http://bombich.com/download#ccc4) <<http://bombich.com/download#ccc4>>
- [Upgrading from Carbon Copy Cloner 3.5 to Carbon Copy Cloner 5](http://bombich.com/kb/ccc5/upgrading-from-carbon-copy-cloner-3.5-carbon-copy-cloner-5) <<http://bombich.com/kb/ccc5/upgrading-from-carbon-copy-cloner-3.5-carbon-copy-cloner-5>>



Carbon Copy Cloner 5 Release Notes

Carbon Copy Cloner 5.1.25

February 2, 2021

- Fixed an issue that was causing "On Reconnect" tasks to not run when the destination volume was remounted (affecting Catalina and Big Sur volumes).
- Fixed an issue in which the destination volume could be set as the current startup disk at the end of a task on systems with System Integrity Protection disabled.
- Made a handful of VoiceOver-related adjustments.
- Fixed the positioning of CCC's Preferences window, it had a tendency to wander downwards.
- Fixed the appearance of the update notification window in the user agent when Dark Mode is used.
- Fixed an issue in the Task Filter window in which items within a folder would appear to be excluded or re-included automatically as changes were made to that folder in the Finder.
- When applicable, the Backblaze `/Library/Backblaze.bzpkg/bzdata/bzvol_system_volume/bzvol_id.xml` file is now removed at the end of a Full Volume Clone to avoid a "safety freeze" when booting from a Big Sur backup.
- Attempting to clone a Big Sur volume into another volume in the current startup disk's APFS container is now disallowed (because it always fails). CCC offers some better alternatives instead.

Carbon Copy Cloner 5.1.24

December 16, 2020

- Fixed an issue in which CCC was not presenting custom volume icons in the sidebar and source/destination selectors.
- Fixed an issue in which CCC's main window was occasionally not showing task progress for a running task.
- Fixed the functionality of the "Manage snapshots on {volume name}" contextual menu item on the source and destination selectors.
- Improved some error handling when performing a full volume clone with Apple's APFS replication utility.
- Adjusted postflight disk image ejection. We found some cases where CCC had no trouble unmounting the destination disk image, but the eject request initially failed because it was "busy". Patiently waiting a few more seconds avoids a case where the disk image couldn't be remounted (e.g. when the task runs next) without manually ejecting the disk image.
- Resolved a logistical annoyance on Big Sur that can occur if a task is configured to run "On reconnect", the destination volume is a volume group, the Data volume is encrypted (note that the System volume is *not* encrypted on Big Sur), and CCC has not been given the password to that volume. CCC now instead waits for the Data volume's mount event as a trigger to these tasks.
- Time Machine backup volumes are now explicitly disallowed as source or destination selections on Big Sur. We're not planning to offer support for cloning to or from volumes that are flagged as Time Machine volumes.
- The "task started" notification now indicates the user-facing name of the source volume rather than the name of the Data sibling.
- CCC now breaks a cycle in which two tasks can volley back and forth, erring out because their destination folders are absent. This occurs when both tasks are configured to "Defer if



another task is writing to the same destination", and both tasks are configured to back up to a folder on the same NAS volume.

- Addressed a few cases where CCC wasn't requesting the password for an encrypted volume (again, because the System volume on Big Sur is no longer encrypted when FileVault is enabled).
- Fixed an issue that could cause an ASR restore of a read-only disk image to fail. CCC also will automatically scan read-only disk images for ASR when configured to create a read-only disk image.
- Addressed an issue in which tasks were errantly getting marked "Task requires review".
- Fixed an issue regarding restores of Data volume snapshots on Big Sur.
- Made a few tweaks to work around ASR failures that can occur when the destination APFS container has remnants of an older OS.
- Addressed an issue with the CCC update mechanism in which the application doesn't automatically re-open when clicking the "Install and Relaunch" button on macOS Big Sur. The fix won't be realized until you apply the next update after this one, so if this issue was affecting you, you may still have to manually re-open CCC after applying this update.

Carbon Copy Cloner 5.1.23

November 24, 2020

☐ Bootable backups on macOS Big Sur

CCC can now make bootable backups of a Big Sur startup disk on Intel-based Macs. Support for System volume cloning on Apple Silicon Macs is disabled for now because [Apple's APFS replication utility does not currently work on that platform <http://bombich.com/kb/ccc5/macos-big-sur-known-issues#asr_broken_arm>](http://bombich.com/kb/ccc5/macos-big-sur-known-issues#asr_broken_arm). When Apple fixes that, we'll post an update to CCC that restores support for making bootable backups on Apple Silicon Macs.

CCC is a native application on Apple Silicon and is 100% compatible with Apple Silicon Macs

CCC will automatically proceed with a Data Volume backup when backing up an APFS Volume Group on Apple Silicon Macs — that's a complete backup of your data, applications, and system settings. If you would like to make your Apple Silicon Mac backup bootable, you can [install Big Sur onto the CCC Data Volume backup <http://bombich.com/kb/ccc5/creating-and-restoring-data-only-backups#install_macos>](http://bombich.com/kb/ccc5/creating-and-restoring-data-only-backups#install_macos). Please keep in mind, however, that [your CCC backup does not have to be bootable for you to be able to restore data from it. <http://bombich.com/kb/ccc5/creating-and-restoring-data-only-backups#migrate>](http://bombich.com/kb/ccc5/creating-and-restoring-data-only-backups#migrate)

Please take a moment to review the following resources related to macOS Big Sur:

- [macOS Big Sur Known Issues <http://bombich.com/kb/ccc5/macos-big-sur-known-issues>](http://bombich.com/kb/ccc5/macos-big-sur-known-issues)
- [Frequently asked questions about CCC and macOS 11 <http://bombich.com/kb/ccc5/frequently-asked-questions-about-coc-and-macos-11>](http://bombich.com/kb/ccc5/frequently-asked-questions-about-coc-and-macos-11)
- Made several cosmetic adjustments specific to macOS Big Sur.
- Fixed an issue in which "On reconnect" tasks wouldn't run (i.e. when the destination volume is remounted) if the source is a Big Sur startup disk.
- Fixed an issue with unlocking and mounting encrypted APFS volume groups on Big Sur.

Carbon Copy Cloner 5.1.22

October 16, 2020

- Fixed an issue in which CCC was unable to access a new secret Apple data store in a folder

named "searchparty" that was added in macOS 10.15.7.

- Added a global exclusion for a "com.apple.mediaanalysisd" temporary items folder whose content was leading to stalls on macOS 10.15.7.
- Improved the error message that is presented when CCC is unable to copy the Catalina System volume due to a lack of Full Disk Access (or more precisely, due to the inconsistent manner in which the system grants full disk access to an application's helper tool).
- Fixed a math issue regarding the application of a task time limit when the task starts shortly before midnight and the time limit starts at midnight.
- Made a couple small improvements to the messaging around some exceptional conditions in the Remote Mac setup window (e.g. lack of Full Disk Access on the remote Mac, using an "@" character in a hostname).
- The "If the source or destination is missing" UI in the scheduler is now made available to tasks that are part of a scheduled task group.
- This update includes many changes to accommodate Apple's next OS, macOS "Big Sur". Please take a moment to review the following resources *prior* to upgrading to macOS Big Sur:
 - [Frequently asked questions about CCC and macOS 11](http://bombich.com/kb/ccc5/frequently-asked-questions-about-ccc-and-macos-11) <<http://bombich.com/kb/ccc5/frequently-asked-questions-about-ccc-and-macos-11>>
 - [macOS Big Sur Known Issues](http://bombich.com/kb/ccc5/macos-big-sur-known-issues) <<http://bombich.com/kb/ccc5/macos-big-sur-known-issues>>
 - [Best practices for updating your Mac's OS](http://bombich.com/kb/ccc5/best-practices-updating-your-macs-os) <<http://bombich.com/kb/ccc5/best-practices-updating-your-macs-os>>

Carbon Copy Cloner 5.1.21

August 10, 2020

- Added an exclusion for a system cache folder that has been causing some stalls, affecting primarily 10.15.6 users.
- Addressed an error related to the copying of a "SystemKey" file on a Catalina startup disk.
- Addressed an issue affecting the bootability of Yosemite and El Capitan backups.

Carbon Copy Cloner 5.1.20

July 21, 2020

- In macOS 10.15.6, Apple has resolved the [firmlink creation issue that was introduced in macOS 10.15.5](http://bombich.com/blog/2020/05/27/bug-in-macos-10.15.5-impacts-bootable-backups-weve-got-you-covered) <<http://bombich.com/blog/2020/05/27/bug-in-macos-10.15.5-impacts-bootable-backups-weve-got-you-covered>>. This update to CCC removes the workaround that we added in CCC 5.1.18 to address that issue. For 10.15.6 users, CCC will now revert to using its own file copier for establishing new bootable backups. 10.15.5 users will be encouraged to apply the 10.15.6 update, although the aforementioned workaround will still work for 10.15.5 users.

Carbon Copy Cloner 5.1.19

June 17, 2020

- This update addresses a handful of failure conditions of Apple's APFS replication utility which CCC is using temporarily in response to a bug that Apple introduced in macOS 10.15.5. We have also improved the task configuration workflow for new backup tasks, and we've added some documentation around this functionality: [Cloning macOS System volumes with Apple Software Restore](http://bombich.com/kb/ccc5/cloning-macos-system-volumes-apple-software-restore) <<http://bombich.com/kb/ccc5/cloning-macos-system-volumes-apple-software-restore>>, [Creating and restoring data-only backups](http://bombich.com/kb/ccc5/creating-and-restoring-data-only-backups) <<http://bombich.com/kb/ccc5/creating-and-restoring-data-only-backups>>, [Troubleshooting](http://bombich.com/kb/ccc5/troubleshooting)



[APFS Replication <http://bombich.com/kb/ccc5/troubleshooting-apfs-replication>](http://bombich.com/kb/ccc5/troubleshooting-apfs-replication).

- Orphaned System volumes are now handled more proactively when selected as a source or destination. Orphaned System volumes arise when you either delete or erase the "Backup - Data" volume in Disk Utility without deleting/erasing the whole volume group when prompted. System volumes are unsuitable for user data, but some folks manage to get data onto them anyway (it doesn't help that Finder allows you to copy data to them). CCC can now help you migrate content from an orphaned System volume source, and will insist that you erase an orphaned System destination before proceeding with a task.
- CCC no longer excludes 1Password by default. We added the exclusion in light of a [recommendation by the folks at Agile software <https://support.1password.com/extra-copies-found>](https://support.1password.com/extra-copies-found), however we got some feedback that people would prefer to exclude this manually, if at all.
- The Backblaze ".b2vol" folder is now removed from the root of the destination volumes at the end of an initial APFS replication. This should resolve issues in which Backblaze has identification issues after an initial clone is performed.

Carbon Copy Cloner 5.1.18

May 29, 2020

- Addressed an issue that Apple introduced in 10.15.5 (FB7706647) that will prevent CCC from establishing an initial backup of a macOS Catalina system volume.
- Starting in 10.15.5, CCC will no longer back up a macOS Catalina System volume to a disk image destination (i.e. a sparseimage or sparsebundle disk image file). We're making this change reluctantly, unfortunately we just can't get reliable results when using Apple's proprietary utility with disk images.
- Added a green checkmark emoji to the subject of "task completed successfully" emails.
- Improved upon the previous attempts to suppress VirusBarrier attached-but-not-mounted disk images in CCC's sidebar.
- When backing up to a OneDrive or Dropbox folder, CCC will no longer replace online-only placeholder files with a non-placeholder from the source unless the two files' modification dates differ. This resolves an issue in which a user flags a OneDrive/Dropbox folder as "online only" and CCC replaces the placeholders with real files, causing OneDrive/Dropbox to re-upload the content.
- Addressed an issue in which some sparse files were getting copied during every backup. In some cases this led to a noticeable performance degradation.

Carbon Copy Cloner 5.1.17

May 12, 2020

- Creating a new task via the CCC menubar application now works more consistently.
- Addressed a small logistical change introduced in macOS 10.15.4 that could lead to (harmless, but annoying nonetheless) errors while archiving the Preboot helper volume in a macOS Catalina volume group.
- Addressed a small UI error that occurred when strict volume identification is disabled for a task and a matching volume is present. The issue was specific to APFS volume groups.
- If a scheduled task was missed due to an encrypted volume being physically absent, CCC will now run that task and unlock the applicable volume when the device reappears. Previously the task would only run when the volume was unlocked by the user (and thus mounted), but now CCC will unlock the volume if a scheduled task was missed, or if the task is configured to run when the source or destination reappears.
- Resolved an issue in which CCC would report that it was unable to delete a snapshot on a rotational startup disk while the system was busy defragmenting boot files (another treat



bestowed upon us by Apple's 10.15.4 update!).

- Resolved an issue introduced in CCC 5.1.16 that would cause CCC to fail to perform a task whose destination is a disk image on the startup disk.
- Unmounted disk images that some application left attached (VirusBarrier, I'm looking at you) are no longer listed in CCC's sidebar.
- When enabling the "Find and replace corrupted files" setting for a task that specifies an encrypted APFS volume group as the destination, CCC now presents a dialog requesting the password to that volume (if CCC doesn't already have it). This resolves a situation where the task would fail if CCC is unable to unlock and mount the destination Data volume.
- If CCC establishes a connection to an SMTP server, but the server never responds to CCC's "EHLO" reply, CCC will retry the connection.
- Fixed a crash that can occur in CCC's file copier while looking for case conflicts (only applicable if the source is case-sensitive and the destination is not).
- Support for extended attributes is now disabled by default when the user selects a network volume (or a folder on a NAS volume) as the source or destination to the task. You're welcome to re-enable extended attribute support, but we have found that most NAS devices offer exceptionally poor support for extended attributes, and that disabling them is the best default configuration.

Carbon Copy Cloner 5.1.16

March 31, 2020

- macOS 10.15.4 introduced a small timing issue that can occur when CCC attempts to delete the transient source snapshot at the end of the backup. This error is harmless, and the snapshot is removed automatically later, but this update adds a more aggressive method of removing the snapshot.
- macOS 10.15.4 also introduced a change that can cause trouble for setting up a remote Macintosh source or destination. This update resolves an error indicating that the remote Macintosh could not be reached during the initial setup.
- Fixed a dead end that can occur when a backup task encounters an error that calls for aborting the backup task (e.g. due to a stall, or when the destination volume pops offline in the middle of the task).
- Improved the reliability of the option to reveal an APFS Data volume in the Finder (via the volumes table contextual menu or via the Source/Destination selectors).
- Minor improvement to the handling of sparse files on APFS volumes. Also improved progress indication while copying particularly large sparse files.
- Made a small adjustment to the handling of BoxCryptor volumes.
- The "Defer if another task is writing to the same destination" setting now considers other volumes in the same APFS volume group to be the same destination. This addresses cases where one task is configured with the System volume as the destination (a standard configuration for a bootable backup) and another task is configured to back up to a folder on the Data sibling of the same volume (also a standard configuration for a folder-to-folder backup).
- Improved case conflict detection in cases where the source or destination is a member of an APFS volume group.
- In cases where a task is configured to back up to a disk image on a NAS volume, and the diskimages-helper service dissents the unmount request for the underlying NAS volume at the end of the task, CCC now terminates the offending process to make a followup unmount request more effective.
- The option to suppress the destructive task warning is now reset when resetting a task to default settings.
- Addressed some minor errors related to archiving the source APFS helper partitions that can occur if the source is a read-only device (e.g. a read-only disk image).
- Addressed an issue in which the startup disk setting would be set to the current startup disk

when running a backup task (e.g. in cases where the current startup disk is not actually set as the startup disk selection in the Startup Disk Preference Pane).

- Remote Mac: If CCC's RSA key pair should become corrupted, CCC will now deal with the authentication failures more gracefully.
- Addressed a logic error that can lead CCC to restore items to the root of the selected destination volume rather than to a designated folder on that volume when restoring from a Data volume snapshot.
- Fixed an issue in which tasks that were flagged for review because the HFS+ destination will be converted to APFS were not presenting an APFS conversion dialog if the destination device was not attached.

Carbon Copy Cloner 5.1.15

February 4, 2020

- Added a timeout mechanism to volume unmount requests. The DiskArbitration service should never fail to reply to an unmount request, but we've been seeing those incidents more frequently lately.
- Made some additional tweaks to HFS+ to APFS conversion that should make it more robust.
- Addressed an issue in which an "On reconnect" task would not run when the source or destination was reconnected if the source or destination is a folder on a Data volume in an APFS volume group.
- CCC will now disable Spotlight by default on the destination when making a bootable backup of a macOS Catalina System volume.
- The "task finished with errors" email subject now leads with a "warning" emoji so it's more easily distinguishable from non-erring tasks.
- Fixed a logic issue that caused a selected Task Group to not be marked as selected in the View menu. Fixed a similar issue that caused the "Run Now" menu option in the File menu to be disabled for task groups.
- Fixed some dead ends in the CCC command-line utility that can be encountered when CCC's helper tool has not yet been installed, or when tasks have not yet been saved.
- Fixed a localization issue related to the thousands grouping separator used in numbers presented in various windows, including the Task History window.
- Errors that are produced by Disk Utility on a remote Mac regarding the failure to load unsigned plugins will no longer cause CCC to fail to produce a volume list when configuring a backup task to or from a remote Mac.
- Addressed an issue in which some pre and postflight scripts failed to run, supposedly due to the lack of a shell interpreter line.
- Added more specific handling of a scenario in which Disk Utility fails to create an APFS volume group when a T2 Mac is booted from an encrypted volume.
- Fixed a couple user interface sizing and placement anomalies.
- Improved the accuracy of the "Total data size" value reported in the Task Filter window when an APFS volume group is selected as the source.
- Fixed an issue in which the "Total data size" value that was being reported in the Task History window was incorrect (too low) in cases where the data set had very, very few modified items.
- CCC will no longer add the "About this folder.rtf" file to the SafetyNet folder if "OneDrive" appears anywhere in the folder path. This should avoid complaints from OneDrive that arise due to its 1980s-esque failure to deal with files whose names start with a space character.

Carbon Copy Cloner 5.1.14

November 14, 2019

- Authentication errors that occur when failing to mount the destination Data volume are now handled correctly (i.e. you'll get a "Reset Password" prompt instead of a generic error).
- CCC no longer avoids rebuilding the dynamic linker shared cache on Macs with less than 4GB of RAM. We found that this resolved system performance issues in the past, but now it only exacerbates system performance issues on these anemic systems when running macOS Catalina.
- CCC will now disallow the conversion of an HFS+ formatted Drobo volume to APFS because Drobo does not currently support APFS. This does not prevent you from reformatting a Drobo volume yourself and selecting it as a destination for a Catalina bootable backup, but CCC is no longer going to perform the task that places the Drobo volume in an unsupported configuration. If you want to use your Drobo device as a bootable backup, you should share that feedback with Drobo.
- Catalina: Added a "Reveal Data Volume" button to the source and destination selector when the applicable volume is a mounted System volume.
- Catalina: CCC's Cloning Coach now warns that a FireWire-attached destination is not bootable on Catalina+ (Apple no longer supports this configuration).
- Catalina: Errors encountered during the System volume backup will no longer cause the Data volume backup to fail, and the errors are now presented with more helpful advice.
- High Sierra+: Fixed an issue that resulted in non-bootable clones when specifying a volume other than the current startup disk as the source.
- The task selection in CCC's sidebar is retained more reliably.
- Fixed a logic issue that caused CCC's restart or shutdown requests to fail when no user is logged in.
- Catalina: Addressed a issue where an "On reconnect" task would fail to run when the destination volume was reconnected in cases where the source is the startup disk and the System volume had been replaced entirely during a system software update.
- CCC now works around volume unmount interference caused by CleanMyDrive. That product can still cause trouble for Disk Utility, however, so consider disabling that software if you're having trouble with an HFS+-to-APFS conversion, for example.
- Addressed an issue in which the source and destination selections might not be cleared out in Simple Mode.
- Fixed an issue in which CCC would report that it was unable to collect the details about the underlying volume when selecting a folder on a volume within a volume group, and when that underlying volume's name had a non-ASCII character (e.g. "CCC Backup - Données").

Carbon Copy Cloner 5.1.13

October 17, 2019

- Made an adjustment to how CCC copies the contents of the System volume when that volume is getting updated to avoid removing any content from the destination System volume that doesn't belong there. While it is inappropriate to ever have content on the destination System volume (CCC, for example, would not allow you to configure a task in that manner), Finder allows the modification of that volume, so conceivably someone could copy content to that volume without realizing the error. In general, you should avoid storing anything on your macOS backup volume that is unrelated to the source volume. **If you want to store other content on your backup disk, create a dedicated volume for that content** <http://bombich.com/kb/ccc5/frequently-asked-questions-about-ccc-and-macos-catalina#dedicated_volume>.
- CCC detects a couple more error conditions that are commonly encountered during APFS conversion on macOS Catalina and either works around them to make the conversion succeed or presents them with more accurate advice.

Carbon Copy Cloner 5.1.12

October 10, 2019

- Fixed an issue in which folders in the Task Filter window were missing a disclosure triangle, making it difficult to exclude subfolders.
- Improved OneDrive and Dropbox placeholder file detection.
- If you've deleted a Catalina System volume from a destination volume group, CCC now allows the selection of the orphaned Data volume as a destination, and will recreate the volume group as necessary.
- Made a couple small adjustments that should make HFS+-to-APFS conversions more reliable, particularly for slower destination devices.
- CCC 5.1.10 addressed an issue in which a remote Mac could go to sleep between CCC's archive management and file copying requests, but we found that change to be inadequate. This update improves upon that fix.
- Fixed a race condition in which the sort criteria popup menu in the Task History window wasn't getting populated if the task history window was opened very soon after launching CCC.
- Added "files copied" to the history output of the CCC command-line tool.
- When backing up to a disk image on a network volume, postflight unmounting of the network volume is now a little more reliable in cases where the diskimages-helper service is being stubborn.
- When CCC creates a System volume on the destination, the new System volume is now formatted as case-sensitive if the sibling Data volume is formatted as case-sensitive.

Carbon Copy Cloner 5.1.11

August 30, 2019

- Relaxed the restriction related to cloning a newer OS than what the Mac is currently booted from. CCC issues a warning, indicates clearly that the destination may not be bootable, but now you're welcome to proceed in this scenario if you have a particular need to create a non-bootable backup of the source system.
- Fixed an issue in which you'd be prevented from backing up to a new disk image stored on the startup disk.
- Fixed the "Open Disk Utility" and "Open Terminal" menu items in the Utilities menu for Catalina users.
- Addressed an edge case in which CCC would errantly report that it was unable to bless the destination because it's in the same APFS container as the current startup disk.
- Fixed some quirky behavior of the email password text field in the Preferences window.
- Addressed a couple errant Cloning Coach messages.
- Addressed a race condition that could cause the CCC User Agent to lose its connection to CCC's privileged helper tool after applying an update to CCC. This would lead to an empty task list in the CCC menubar, a lack of task started/finished notifications, and a failure to present the mini task progress window.
- Addressed an issue in which CCC would not create the APFS helper partitions on an APFS destination when restoring from an HFS+ volume, resulting in a non-bootable volume.

Carbon Copy Cloner 5.1.10

August 20, 2019

This update offers qualification against macOS 10.15 Catalina, but also includes improvements for pre-Catalina OSes, so **we recommend this update for all CCC 5 users**. Please follow [macOS Catalina Known Issues <http://bombich.com/kb/ccl5/macOS-catalina-known-issues>](http://bombich.com/kb/ccl5/macOS-catalina-known-issues) for information on issues related to the new OS.



Changes not specific to macOS Catalina

- Addressed an issue introduced in 10.14.6 that prevents the removal of snapshots via CCC's Disk Center (it does not affect the automated removal of snapshots that occurs when backup tasks run).
- Corrected the read/write rate calculation for non-APFS-Fusion volumes.
- Added a button to reveal the password that you're typing into the Email Settings password panel.
- Changed the encoding of postflight emails that are sent by CCC to "quoted printable" (from UTF-8) to address an obscure edge case on some systems.
- CCC no longer automatically enables snapshot support on APFS-formatted volumes unless CCC can positively determine that the underlying device is an SSD. We have been underwhelmed by the performance of APFS on rotational devices, particularly with snapshot-related activities. Users are still welcome to manually enable snapshot support on any volume — simply click on the volume in CCC's sidebar and flip the switch to "on".
- CCC offers more helpful advice in cases where snapshot creation fails due to the destination being a slow, rotational device and also in cases where encryption conversion is preventing the creation of snapshots.
- CCC's privileged helper tool now proactively verifies the code signature of any client that attempts to connect to the helper. This resolves a potential vulnerability in which an application masquerading as CCC could make requests to CCC's helper tool.
- Modification of the name of a source or destination is detected and presented as a review item to the user. Previously we were simply marking the task dirty, and many users found that behavior disconcerting.
- CCC now proactively warns against cloning a volume whose operating system is newer than what the Mac is currently booted from.
- Addressed an issue in which a remote Mac could go to sleep between CCC's archive management and file copying requests.
- Failure to mount an encrypted volume attached to a remote Mac is now handled with a password request and the task's destination specification is updated accordingly.
- Addressed some minor accessibility annoyances in the CCC License window. Added a proper accessibility label to the task status icon in the Task History window.

Catalina-specific changes

- **CCC will make bootable backups of macOS Catalina startup volumes. For most people, that's all you need to know, and you don't have to make any changes to your current tasks to accommodate the upgrade. The logistics of booting macOS are a bit more complicated in macOS Catalina, but we've risen to the challenge, CCC supports it 100%, and nearly all of these complications are dealt with automatically.**
- macOS Catalina requires APFS, it cannot be backed up to a volume formatted with Apple's legacy HFS+ format. When cloning a macOS Catalina system volume, CCC will inform you of this requirement and request your permission to allow conversion of an HFS+ formatted destination to APFS. When you proceed with the task, CCC will automatically convert the destination to APFS (when possible).
- When you upgrade to macOS Catalina, any existing backup tasks that reference your startup disk and a non-APFS destination volume will be disabled and flagged for review. If any scheduled tasks are disabled in this manner, CCC will be opened automatically on startup and these concerns will be raised to your attention.
- CCC will automatically create System and Data volumes on the destination as required to support APFS volume groups.
- When selecting an APFS volume group member as a source (i.e. your current startup disk), CCC will automatically copy the contents of both the System and Data volumes to the corresponding System and Data volumes on the destination. No special configuration is

required for this, you will simply choose a single source and destination as you have in the past.

- CCC's task filter automatically accommodates source volumes that have a System/Data bifurcation.
- CCC fully supports encrypted source and destination APFS volume groups. If you have enabled FileVault on your bootable backup, CCC can automatically unlock and mount both members of the destination volume group as required for your scheduled backups. Please take note, however, of [a kernel panic issue that we have reported to Apple <http://bombich.com/kb/cc5/macos-catalina-known-issues>](http://bombich.com/kb/cc5/macos-catalina-known-issues) that can occur when mounting encrypted volume groups.
- When mounting and unmounting a volume that is a member of a volume group (either by clicking on the volume in CCC's Source/Destination selectors, or by right-clicking on the volume in CCC's sidebar), CCC will automatically apply that action to both members of the volume group.
- Tasks configured to unmount the destination at the end of the task will automatically unmount both members of a destination volume group.
- When backing up an APFS volume group to a disk image, CCC automatically creates System and Data volumes as required on the destination disk image, and copies the source volume group members accordingly.
- CCC has special handling of snapshot retention policies for APFS volume groups. The snapshot retention policy for both group members will be configured via the Data volume member.
- CCC will never create snapshots on source System volumes. These volumes are already read-only so a snapshot is not required. Considering that software updates may delete the snapshots or the System volume altogether, creating snapshots on the source System is futile.
- 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). 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.
- CCC lists the OS version and now also the build number associated with both System and Data volumes in the snapshots table.
- CCC offers great flexibility for restoring from System and Data volume snapshots. For example, you can restore from a newer Data volume snapshot and an older System volume snapshot, allowing you to downgrade the System without losing newer data. However, care should be taken when restoring System and Data volume snapshots that are associated with different OS versions, we don't yet know the implications of mixing these.
- Added a "Reveal in Finder" contextual menu item to the Volumes table so that users can reveal the Data volume in the Finder. That's key if you wanted to access something at the root level of that volume, e.g. the `_CCC SafetyNet` folder.
- CCC no longer limits its requests for full disk access to times that you're saving a task that references the current startup disk. On macOS Catalina, we need full disk access to have access to external volumes and network volumes, so we pretty much need it any time you want to make a backup.
- When selecting a macOS Catalina System volume as the source, CCC's Source selector shows the cumulative disk usage of the System and Data volumes (because that's the value that reflects what will be copied). To see the individual disk usage of each volume separately, you can click on those volumes in CCC's sidebar.

New unsupported configurations in macOS Catalina

- Copying macOS Catalina system volumes to or from a Remote Macintosh is not a supported configuration, nor will CCC copy the contents of a System volume to a subfolder on a locally-attached volume. The logistics of producing a bootable copy of the bifurcated system are too



complex to manage on or from a remote Mac, so we're only going to support making bootable backups of macOS at the root-level of locally-attached volumes.

- Selecting the startup disk of a remote Macintosh as a destination is no longer supported. This rarely works in the way you'd hope it will, typically it just produces lots of errors. You may still select a subfolder on the remote Mac's startup disk as long as it is a writable folder.

Carbon Copy Cloner 5.1.9

May 16, 2019

- Fixed an issue that could lead CCC to incorrectly conclude that a GoogleDrive volume is not mounted or present.
- Improved disk read/write rate calculations for APFS Fusion volumes.
- Minor adjustment to the analysis of permissions errors that occur when trying to access OneDrive placeholder files.
- We've received several reports of long stalls in the "Cleaning up" phase when backing up to a disk image; particularly when that disk image resides on a NAS volume. In most cases this was the result of a filesystem stall while the filesystem was attempting to create a snapshot. Snapshot support is now disabled by default for CCC-created APFS-formatted disk images. You're welcome to enable snapshot support on a disk image manually if you prefer that; double-click the disk image to mount it, then click on the mounted disk image volume in CCC's sidebar to manage the snapshot creation and retention preferences for that volume.
- Minor adjustment to the handling of locked files when trying to create hard links.
- Fixed an edge case in which the "Secure CCC's Scripts Folder" function was not removing non-root-user write privileges on shell scripts.
- The task history sort attribute is now retained as a preference.

Carbon Copy Cloner 5.1.8

February 26, 2019

- When creating a new disk image on a Mojave+ system, CCC will now create APFS-formatted disk images if the source volume is APFS-formatted. All snapshot functionality afforded to APFS-formatted volumes will apply to APFS-formatted disk images as well.
- Hard drives from a popular vendor ship with a rogue "is a bundle" flag set on the root folder. When cloning this volume to a folder, the rogue flag is preserved on the destination folder, which causes the Finder to treat it like a file, making it awkward to see the items that were copied. CCC now strips this rogue flag from the root folder of the selected destination to avoid the annoying result.
- Adjusted the handling of 0-byte "placeholder" files (e.g. Dropbox, GoogleDrive, OneDrive "online only" files) to avoid lengthy delays. These delays were particularly notable when working through Dropbox folders.
- Total snapshot disk usage is presented more prominently in the Disk Center.
- When cloning to an ExFAT or FAT32 volume, custom volume icons are now preserved at the destination.
- Addressed errors that could occur while trying to create hard links in locked folders.
- Resolved an error that can occur when creating read-only disk images on SMB network volumes. Due to a bug in macOS Mojave, sparseimage disk images cannot be created on SMB NAS volumes. Rather than creating a sparseimage intermediate disk image, CCC will now create a sparsebundle intermediate disk image.
- CCC's "trust but verify" case-sensitivity check is now applied to "ufsd_ExtFS" volumes as well, after getting confirmation from a user that these volumes incorrectly report themselves as case-insensitive, when in fact they are case-sensitive.
- To protect against unauthorized modifications, CCC now requires that pre- and postflight

scripts are owned and writable only by the system administrator, and that all parent folders of the scripts are owned and writable only by the system administrator. A new "Secure CCC's Scripts folder" option is available in the Utilities menu to help meet these new requirements.

- Fixed some UI issues around the visibility of the pre/postflight script interface elements.
- Fixed an issue in which other tasks within a group would start to run after the following events: a) start task group, b) stop task group before all tasks complete, c) manually run one of the tasks within the group.
- Fixed an issue in which CCC would errantly report that a destination lacked support for files larger than 4GB.
- Hourly run time limits that have a start or end time at midnight will be applied a little more gracefully, e.g. a task that starts a few seconds prior to midnight will be allowed to run with a midnight start time limit.
- Fixed a password decoding issue that could cause problems while configuring a task with the Remote Macintosh option if the administrator's password on the remote Mac contained 3-byte characters (e.g. €).
- Tasks that failed due to the source or destination being missing will no longer get a "failed" badge in the Tasks table if the task is also configured to not send error notifications when the source or destination is missing. Likewise, the Task Plan will now indicate this condition specifically, rather than offering a generic "Errors occurred during the last run" message.

Carbon Copy Cloner 5.1.7

December 13, 2018

- CCC will now proactively warn about configurations specific to T2 Macs that will produce non-bootable results, and configurations that will lead to problems with enabling encryption or modifying Startup Security settings.
- Addressed an issue in which a Mojave-running remote Macintosh would fail (inconsistently) to correctly validate the code signature of CCC's file copier, thus causing backups to the remote Mac to fail.
- Apple cache files that have been found to degrade task performance are now excluded from backup tasks by default.
- CCC can now distinguish between a volume that is encrypted vs. a volume that has FileVault enabled. This is a subtle difference that is only apparent on T2-based Macs. CCC will no longer ask for a password for encrypted volumes that are not FileVault protected.
- The "Shut down if previously off" setting is now allowed on a non-scheduled task as long as that task is part of a scheduled group.
- Improved compatibility with VeraCrypt volumes.

Carbon Copy Cloner 5.1.6

October 12, 2018

- Improved the handling of Microsoft OneDrive, Google Drive File Stream and Dropbox placeholder files. Please note that if you're using any of these services, files that are marked as "online only" cannot be backed up. [Learn more here](http://bombich.com/kb/cc5/limitations-online-only-placeholder-files) <<http://bombich.com/kb/cc5/limitations-online-only-placeholder-files>>.
- When showing the sidebar, the left side of the window will no longer get place under the Dock if the user has the Dock placed on the left side of the screen.
- Updated the default snapshot retention policy that gets applied to the startup disk. The default settings are now more conservative, so fewer snapshots will be retained on the startup disk. Note that you must apply the new default settings if snapshots are already enabled for your startup disk.
- When deleting the last task, the new task that's created to replace it is now named "CCC



Backup Task" (rather than "Untitled") and it is no longer marked "edited" by default.

- Final Cut Pro "fcpbundle" files are now treated as ordinary folders in the Task Filter window, allowing the user to exclude items within these bundles files from the backup task.
- Addressed an edge case scenario where the permissions of the root folder of the destination could be set to values that prevent the logged-in user from accessing that volume.

Carbon Copy Cloner 5.1.5

September 17, 2018

- CCC now proactively prompts Mojave users to grant Full Disk Access to CCC and its helper tool so CCC can back up all of the user's Application Data.
- Minor improvement to the handling of sparse files.
- When connecting to a remote Mac via the Remote Macintosh option in the Source and Destination selectors, a timeout that might occur due to a firewall or other Remote Login configuration problem is now greeted with more helpful advice (rather than reported as an "internal error").
- Changes to a custom filter expression or rule type now causes the task to be marked as edited.
- CCC now excludes the Dropbox ".dropbox.cache" folder. This folder's volatile content not only contains a bunch of garbage that shouldn't be backed up, but attempting to do so provokes a conflict between Dropbox and various anti-virus applications.
- Fixed the handling of a failure to mount an encrypted volume when clicking on the source or destination selector if the source or destination was a folder on that volume and CCC lacked the password for that volume.
- Fixed an issue in which CCC was sending two email notifications for a task that exceeds a run time limit.
- Fixed an issue in which a task group might run immediately when adding tasks to it.
- The email body template field in CCC's Preferences window now explicitly disallows macOS from performing 'smart quote' replacements. Such replacements resulted in corruption of the tokens in non-English locales, leading to the presence of the tokens in the resulting emails, rather than the substituted text (e.g. "##Nome dell'operazione##" instead of "Backup CCC").

Carbon Copy Cloner 5.1.4

July 27, 2018

- Some performance enhancements added to the previous version of CCC could occasionally lead to errors affecting tasks that specify a remote Macintosh source. This update modifies those performance enhancements to avoid those errors.
- Errors related to being unable to access Apple-private folders in the user home folder are now suppressed.
- Fixed a crashing issue that occurs when clicking on the source or destination selector. This only affects El Capitan users when VoiceOver is enabled.
- Added an option to the 'ccc' command-line utility to print schedule information in CSV format.

Carbon Copy Cloner 5.1.3

July 17, 2018

- Fixed an issue that would prevent CCC's User Agent from finding updates to CCC.
- Minor improvements to error handling related to creating snapshots.
- Animations are now reduced for 10.12+ users that are using the "Reduce motion" setting in



the Accessibility preference pane.

- Improved performance of the "Find and replace corrupted items" checksumming pass on systems that have exceptionally fast storage.
- Fixed a edge-case couple crashing issues.

Carbon Copy Cloner 5.1.2

May 21, 2018

- Addressed a couple more minor, edge case issues related to unmounting a source snapshot at the end of the backup task.
- Fixed an error that occurred when selecting a folder on a remote Macintosh as a source or destination if that folder's name started with a space character.
- Fixed an issue that caused support request submissions to fail (i.e. via the "Ask a question about CCC" menu item in CCC's Help menu).
- Fixed a date math error that occurred when trying to adjust the initial fire date after a time zone change occurred.
- Fixed a drawing anomaly that occurred when selecting multiple rows in the Snapshots or Related Tasks tables.

Carbon Copy Cloner 5.1.1

May 4, 2018

- The "Use strict volume identification" setting has always been disabled when the destination lacks a unique identifier (because the setting isn't applicable in that case). Now we also uncheck that box in those cases to avoid any confusion about whether that setting will be applied.
- Minor adjustments to the timing of snapshot creation on the source at the beginning of the task. These accommodate archiving of the source volume's helper partitions and also resolve potential conflicts when several tasks are started simultaneously that use the same source volume.
- The postflight destination unmount subtask is no longer skipped when a task is aborted due to a time limit overrun.
- Fixed an issue related to manually mounting an encrypted source or destination volume (when clicking on the source/destination selector).
- Fixed a cosmetic issue in which custom filters with multiple suffixes (e.g. '*.tar.gz') would appear to not be applied to matching files in the Task Filter window, despite actually matching those files during task run time.

Carbon Copy Cloner 5.1

April 24, 2018

- Added support for creating a snapshot on an APFS-formatted source at the beginning of the backup task. This snapshot is then mounted and used as the source for copying files. By using a read-only volume as the source, we avoid rare, but potential conflicts that can occur during the backup task if files are modified while being copied.
- CCC's SafetyNet feature is now built on top of APFS snapshots when the destination is an APFS volume and snapshot support is enabled for that volume.
- CCC will create a snapshot on APFS destination volumes at the end of a backup task to establish a point-in-time restore point.
- CCC offers a highly-tunable snapshot retention policy that allows you to define how long snapshots will be retained (hourly, daily, weekly), and also allows you to define a minimum



amount of free space to retain on the volume.

- CCC's Disk Center offers detailed insight into the snapshots that CCC and Time Machine have created on your APFS volumes. Quickly see how much space those snapshots are consuming, and delete one or many snapshots with the press of a button.

Carbon Copy Cloner 5.0.9

February 15, 2018

- This update implements a workaround for [a serious flaw that we've discovered in macOS](http://bombich.com/blog/2018/02/13/macOS-may-lose-data-on-apfs-formatted-disk-images) <<http://bombich.com/blog/2018/02/13/macOS-may-lose-data-on-apfs-formatted-disk-images>> that can lead to data loss when using an APFS-formatted disk image. If you're running macOS High Sierra, please apply this update and review any tasks that back up to a disk image on a network volume. Note: this flaw applies to APFS **disk images** only — ordinary APFS volumes (e.g. your SSD startup disk) are not affected. Disk images are not used for most backup task activity, they are generally only applicable when making backups to network volumes.

Carbon Copy Cloner 5.0.8

February 5, 2018

- Fixed an issue introduced in CCC 5.0.6 in which CCC was mishandling the encoding of a network volume whose username or hostname contained special characters (e.g. "some%20user@Airport%20Base%20Station.local"). That led to errors mounting the affected network volume during an automated backup task.
- Errors related to creating a Recovery HD archive are now suppressed if those errors are the result of the user stopping the backup task while CCC was creating the Recovery HD archive.

Carbon Copy Cloner 5.0.6

January 30, 2018

- We made some improvements to the postflight option that unmounts the destination volume. If the destination is an encrypted volume, the volume will now be immediately locked when unmounted (negating the need for a separate postflight script as referenced in our blog). If the destination is an ordinary volume and the only partition on an external device, the destination device should be more likely to spin down the disk.
- Improved the efficiency of copying sparse files on APFS volumes. Sparse files appear larger than the amount of data they actually contain. In the wild, we've seen sparse files used by VMWare.
- Notifications prompting you to reattach a missing source/destination will now be revoked when the task starts to run next (e.g. when you attach the missing disk).
- Fixed a subtle timing issue that occurs when a scheduled task with an hourly run time limit starts a couple seconds early. A task with such a limit would previously have stopped immediately, claiming that it was running outside of its allowed time window.
- The remote Macintosh option now handles IPv6 addresses more gracefully.
- Addressed an edge-case scenario in which CCC would set overly-restrictive ownership/permissions settings on the destination root folder.
- The Task Filter window now correctly shows the application of a system items exclusion filter when the destination is a NAS volume that is not currently mounted.
- Fixed a behavior problem in the Task Filter window that arose after refreshing the size of a folder that had excluded items.

Carbon Copy Cloner 5.0.5

December 11, 2017

- Fixed a scheduling issue in which tasks would not be scheduled for the original start time hour (in local time) after a time zone switch and a restart.
- Progress indication during a "Backup with Health Check" is no longer errantly indeterminate.
- Addressed an issue that was introduced by the 10.13.2 update which causes Remote Macintosh setup to fail with an internal error.
- Fixed an issue in which CCC was unable to mount the source for an HFS+ Recovery HD cloning task.
- Custom port numbers are now supported for AFP and SMB hosts.
- The task outlook table now correctly displays the run times for tasks configured to run weekly with a repeat interval greater than 1.
- Fixed an issue in which some tasks were getting errantly marked with a "task failed" badge.
- Clicking on a task finished notification will now open the CCC application and select the relevant task.
- Fixed an issue in which a backup task involving a remote Mac would stall if the source or destination volume on the remote Mac was not available.
- ZFS volume mount notifications are now handled more effectively.
- The CCC command line application will now exit immediately after starting a task group.
- Made some minor improvements to CCC's task database that should make it more resilient to corruption.
- Fixed a minor window sizing issue specific to Yosemite and the dialog that is produced when disabling the SafetyNet setting.
- Suppressed an errant error message produced by High Sierra that can occur when converting a sparse disk image to a read-only format.

Carbon Copy Cloner 5.0.4

November 2, 2017

- Fixed the resolution of the task badge on Retina displays on High Sierra.
- When creating a disk image, the disk image is now formatted as APFS if the source is an APFS volume. CCC also creates the Preboot and Recovery volumes on these disk images so that they can be restored using Disk Utility (in addition to being restorable via CCC).
- Items marked as hidden now stay reliably hidden on an HFS+ destination on High Sierra.
- Addressed an issue in which a task that specifies a remote Macintosh as the source or destination would re-try the connection too aggressively if the remote host was unavailable.
- Fixed the free space indicator for APFS volumes when viewing a volume's details in CCC's sidebar.
- Implemented an alternative key installation method for cases where the remote Macintosh cannot accept files via scp.
- Improved the drawing of the task outlook table when viewing a task group.
- Minor enhancements to the CCC command-line utility.
- The source/destination contextual menu items now more consistently refer to the underlying volume for a disk image, and mounting/unmounting the underlying network volume for a disk image now works. Also tweaked the subtitle offered when an underlying network volume is not mounted. Previously it said "'{sharepoint}' is missing', now it says "'{sharepoint}' is not mounted'.
- The "Show Details" button in CCC notifications that are presented as alerts now correctly opens the Task History event in CCC.
- CCC now handles an undocumented Keychain Services error code that was occurring when CCC was trying to open its keychain for the first time (i.e. before the keychain yet exists).



This resolves an issue that some High Sierra users might have encountered when trying to save a password to CCC's keychain.

- Addressed an issue in which a backup task could stall while "Cleaning up" if the task was configured to unmount the destination volume, and Spotlight was dissenting the volume unmount.
- Minor improvements to the Task Trend chart in the Task History window.

Carbon Copy Cloner 5.0.3

September 29, 2017

- Addressed an issue in which task history events weren't getting recorded for a subset of backup tasks.
- Improved the performance of CCC's archive pruning utility.
- Fixed an issue in which CCC may not have presented a dialog to update the HFS+ Recovery HD volume on the destination when the source is an APFS volume.
- Fixed a window resizing issue affecting the "New disk image" Save panel for High Sierra users.
- Fixed issue affecting Yosemite users in which custom filters in the Task Filter window were hidden despite the custom filter table being shown.
- Fixed an issue in which the setting to skip weekend days was getting disabled for tasks configured to run on a daily or weekly basis.

Carbon Copy Cloner 5.0.2

September 21, 2017

- Added a menu option to clear CCC's entire Task History.
- Added Stop Loading, Reload, Make Text Larger, and Make Text Smaller buttons to the Documentation tab of CCC's Help window.
- Added a couple more ways to rename tasks and groups, because a lot of people were having trouble with this. Previously the semantics were similar to that of the Finder, e.g. click on the text of the title, or select the task and press the Return key to make the text editable. Now you can double-click a task in the task list to make the title text editable, or you can right-click on the text and choose the option to rename the task.
- Tasks listed in the CCC menubar application are now sorted in the same manner as defined in the Tasks table of the main application. The same is now true for the View menu in the main application.
- The run time order for grouped tasks is now considered when sorting the Tasks table by next run time.
- Fixed the "failed to set global attribute" error on first launch for upgrading users.
- Fixed a bug that could cause a spin if a CCC v4 imported task had been configured to run weekly, only on Sunday, and also with a runtime limit that prevented it from running on weekends.
- Fixed a condition in which CCC would report that an error occurred while updating the dynamic linker shared cache and kernel extension cache (it wasn't an error, it was just new debug information).
- Resolved some edge cases that caused remote Macintosh authorization setup to fail.
- Connection reset errors (e.g. remote host drops the connection) now cause a remote Mac task to be restarted.
- Imported v4 tasks with a remote Mac destination are no longer prevented from copying system items (i.e. because we don't yet know the destination filesystem).
- Fixed an errant cloning coach message that said the destination on a remote Mac wouldn't be bootable because it wasn't the root of a volume.



- Fixed the source/destination label in cases where the item is a remote Mac. The label wasn't updating consistently, and sometimes was left at the stub text.
- Addressed some cases where CCC would consistently prompt the user for a guided setup when a task with "restore" in its name is present and specifies the current startup disk as the destination, or when the relevant destination volume is named "Macintosh HD".
- Guided Setup and Guided Restore is now disabled if VoiceOver is active. Some VoiceOver users found that these bubble tips were stealing VoiceOver's focus, making task setup more challenging.
- Fixed an issue in which CCC would become unresponsive if you configured a daily or weekly task to start at 7AM, and then checked the box to apply an hourly runtime limit.
- System files are now excluded if the source has an OS older than 10.13 and the destination is APFS. Added a Cloning Coach message to explain the limitation.
- APFS as a system destination is only supported when the running system is 10.13+.
- Fixed the abbreviation for "Monday" that was incorrectly translated in German to "Monat" (rather than "Mo").
- Increased the threshold for system uptime at the time of CCC load to 90 for determining whether the system just restarted. This accommodates slower systems that would otherwise skip a task that was missed while the system was off.
- Write failures on NAS volumes are now more consistently presented as showstoppers that cause the task to fail rather than individual file errors in an otherwise-successful backup task.
- Added some tolerance to the hourly run time limits such that tasks firing a few seconds before the limit window will be allowed to run.
- Fixed an issue in which running a task group could lead to an inability to sleep the system.
- Tasks that are both disabled and suspended now correctly get the "activate/leave suspended" dialog.
- A task can now be moved back outside of a group if there is only one group present and all tasks are part of that group.
- Enabled expansion tooltips for the task name in the task outlook table.
- Fixed an issue in which the destination APFS Preboot volume was not getting properly populated when using an HFS+ source volume.
- The Preferences window is no longer moved to the main screen if its on the secondary screen and the secondary screen is positioned below the main screen.
- Improved some dialog behavior for tasks configured to run on source/destination reconnect, that also are configured to prompt before proceeding and issue a periodic reminder. The CCC User Agent now revokes a reminder prompt if you attach the affected disk before dismissing the reminder prompt.
- Made some minor modifications to CCC's global exclusions list that resolves a startup delay when booting from the backup volume.
- "Delete a SafetyNet folder" now accepts any item that is in the Trash.
- The "Auto adjust" setting being disabled will no longer cause the advanced settings view to be expanded if the SafetyNet is set to Off.
- Fixed an errant Cloning Coach message that said file metadata would not be preserved on a disk image on a network volume.
- Cancelling out of the filter window without making changes will no longer leave the task in the edit state.
- System folders are no longer excluded when copying to or from a folder on the startup disk.
- Fixed a software update issue in which CCC might check for updates on startup if the update interval was set to never check.
- Fixed the calculation of a task's elapsed time as noted in the Task Plan.

Carbon Copy Cloner 5.0

August 24, 2017

- New interface for defining task filters:

- CCC can calculate the amount of space consumed by the files on the source. If you exclude items from the task or add custom filters to exclude items based on patterns, CCC will report the total protected size of each folder (and cumulatively).
- The task filter can now exclude everything by default, allowing you to specify only what items should be included in the backup task. This is in contrast to the default behavior in which CCC includes everything by default, allowing you to specify what is excluded from the backup task.
- Filters can be imported and exported. Additionally, when you change the source for your backup task, CCC will now ask you whether you want to reset the task filter (rather than simply resetting it).
- The effects of custom and global filters are immediately apparent.
- A QuickLook panel shows a preview of the selected file.
- Contents can be sorted by name, modification date, or size.
- You can select an item, then Shift+click on the checkbox for another item within the same parent folder to select/deselect all of the items in between.
- If you really want to, you can have CCC copy your Trash. There's a checkbox for that now!
- CCC's SafetyNet pruning settings will now automatically adapt to the amount of data your tasks need to copy. If a backup task runs out of space on the destination, CCC will revisit the pruning of the SafetyNet folder, then resume copying.
- The SafetyNet pruning feature is now available for Remote Macintosh destinations.
- The setup procedure for backing up to a remote Macintosh has been greatly simplified.
- Task filters can be configured for Remote Macintosh source volumes with the same ease as locally-attached volumes.
- Tasks can be sorted by name, exit status, last run date, next run date, or manually.
- Tasks can be placed into groups for organizational purposes, and also to be run collectively as a group.
- A new Guided Setup feature offers initial task configuration tips for first-time users.
- Upon detecting that your Mac is booted from a CCC backup volume, CCC will present a new Guided Restore option. In the guided restore, CCC will create a new restore task, select the startup disk as the source, then present coaching tips that guide the user through selecting the destination and (optionally) excluding items from the restore task.
- Tasks can be scheduled to run once at a particular time in the future. After that run, the tasks will revert to run "only when I click the Clone button".
- Hourly runtime limits allow the user to limit a task to running only between 5PM and 7AM, for example. Hourly limits will prevent a task from starting if it's outside the specified run time, and if the task runs past the allowed end time, the task will be stopped.
- CCC's Task History window now offers a trend chart. The trend chart shows how your tasks are performing over time, and how many files/how much data gets copied each time your task runs.
- The destination selector offers a visual disk usage indicator.
- You can right-click on a volume (e.g. in the source/destination selectors) to mount or unmount that volume, or to reveal it in the Finder.
- The source and destination selections can be reset to "Choose a source/destination".
- The CCC User Agent will now check for updates on the schedule defined in the main application.
- Some of the the Cloning Coach messages have been aggregated and simplified to seem less daunting to novice users.
- The "Find and replace corrupted files" setting can now be limited to run once per week or once per month.
- Tasks can be imported and exported, making it simpler to migrate task settings to a second Mac.

Carbon Copy Cloner 4.1.24

October 30, 2018

Carbon Copy Cloner 4.1.23

June 21, 2018

Carbon Copy Cloner 4.1.22

May 21, 2018

Carbon Copy Cloner 4.1.21

February 12, 2018

Carbon Copy Cloner 4.1.20

October 25, 2017

Carbon Copy Cloner 4.1.19

September 12, 2017

Carbon Copy Cloner 4.1.18

August 16, 2017

Carbon Copy Cloner 4.1.17

July 19, 2017

Carbon Copy Cloner 4.1.16

June 27, 2017

Carbon Copy Cloner 4.1.15

May 19, 2017

Carbon Copy Cloner 4.1.14

May 11, 2017

Carbon Copy Cloner 4.1.13

January 12, 2017

Carbon Copy Cloner 4.1.12

December 8, 2016

Carbon Copy Cloner 4.1.11

December 6, 2016

Carbon Copy Cloner 4.1.10

September 16, 2016

Carbon Copy Cloner 4.1.9

June 14, 2016

Carbon Copy Cloner 4.1.8

June 6, 2016

Carbon Copy Cloner 4.1.7

February 2, 2016

Carbon Copy Cloner 4.1.6

December 3, 2015

Carbon Copy Cloner 4.1.5

December 2, 2015

Carbon Copy Cloner 4.1.4

September 1, 2015

Carbon Copy Cloner 4.1.3

May 19, 2015

Carbon Copy Cloner 4.1.2

May 6, 2015

Carbon Copy Cloner 4.1.1

May 5, 2015

Carbon Copy Cloner 4.1

April 28, 2015

Carbon Copy Cloner 4.0

October 1, 2014

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



Credits

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

vsdbutil and hfs.util

Carbon Copy Cloner 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) <https://opensource.apple.com/source/diskdev_cmds/diskdev_cmds-332.11.5/vsdbutil.tproj/vsdbutil_main.c.auto.html> (View our modifications: [vsdbutil.h](http://bombich.com/software/opensource/vsdbutil.h) <<http://bombich.com/software/opensource/vsdbutil.h>> and [vsdbutil.c](http://bombich.com/software/opensource/vsdbutil.c) <<http://bombich.com/software/opensource/vsdbutil.c>>)
- [hfs_util](https://opensource.apple.com/source/hfs/hfs-226.1.1/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

Carbon Copy Cloner 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 my 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) <http://bombich.com/software/opensource/rsync_3.0.6-bombich_20190114.diff>
- View the GNU GPL <<http://bombich.com/software/opensource/COPYING.txt>>

Carbon Copy Cloner 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 > MacOS > rsync.

Sparkle

Carbon Copy Cloner leverages [Sparkle](http://sparkle-project.org) <<http://sparkle-project.org>> for handling software updates. 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](http://bombich.com/software/opensource/SparkleLicense.txt)
<<http://bombich.com/software/opensource/SparkleLicense.txt>>

skpsmtplib

The SimpleSMTP framework included with CCC is a derivative work of the [skpsmtplib](https://code.google.com/p/skpsmtplib/) <<https://code.google.com/p/skpsmtplib/>> project. skpsmtplib 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) <<https://pixelespressoapps.com>> for license generation and verification in Carbon Copy Cloner. CocoaFob is distributed under the [BSD License](http://www.opensource.org/licenses/bsd-license.php) <<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 EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Everything you need to know about Carbon Copy Cloner and APFS

Apple introduced a new filesystem in macOS High Sierra, so naturally you may be wondering how Carbon Copy Cloner deals with this and how this new change might affect your backups. You might even be wondering, "What's a filesystem?", so we'll start with that, and gradually move into more technical details.

- [What's a filesystem?](#)
- [Why is Apple introducing a new filesystem?](#)
- [When I upgrade my Mac to High Sierra \(or later\), will my startup disk be converted to APFS?](#)
- [If I first upgrade to High Sierra on an HDD, and then clone to an SSD, will the SSD be converted to APFS?](#)
- [If the OS upgrade converted my startup disk to APFS, what do I need to do to my backup disk? Do I have to erase it as APFS?](#)
- [Can I use CCC to clone an APFS startup disk to another Mac?](#)
- [Does CCC support encrypted APFS volumes?](#)
- [I heard that APFS has a "cloning" feature. Is that the same as what CCC is doing?](#)
- [Why doesn't the disk usage on my backup disk match the disk usage on the source disk?](#)
- [What role does APFS's new snapshot feature play in my backup strategy?](#)
<<http://bombich.com/kb/ccc5/leveraging-snapshots-on-apfs-volumes>>
- [What are these "{volume name} - Data" volumes on macOS Catalina?](#)
<<http://bombich.com/kb/ccc5/working-apfs-volume-groups>>

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.

Why is Apple introducing a new filesystem?

Apple's legacy file system, HFS+, has worked well for almost 20 years, and Apple has made consistent improvements to it over that time. For example, Apple added support for extended attributes, file system compression, file system journaling, and full-disk encryption. All of these new features were added to keep pace with new operating system features and to make the file system more reliable. But that file system was created initially for Mac OS 8, and was designed for platter-based hard drives. Storage technology has changed a lot over the last 20 years, and modifying HFS+ to keep pace with those changes has proven increasingly difficult. To meet the challenges of new OSes and new storage technology, Apple introduced the Apple File System, or "APFS" in High Sierra.

When I upgrade my Mac to High Sierra (or later), will my startup disk be converted to APFS?

When you upgrade to macOS High Sierra, systems with all flash storage configurations are converted automatically. Systems with hard disk drives (HDD) and Fusion drives won't be converted to APFS on macOS High Sierra. When you upgrade to Mojave, HDD and Fusion volumes are also converted to

APFS. [You can't opt-out of the transition to APFS <https://support.apple.com/en-us/HT208018>](https://support.apple.com/en-us/HT208018).

If I first upgrade to High Sierra on an HDD, and then clone to an SSD, will the SSD be converted to APFS?

If you're running macOS High Sierra or Mojave, then neither the HDD nor the SSD will be automatically converted to APFS. You can choose, however, to erase the SSD as APFS prior to cloning to it. Both APFS and HFS are valid destination formats when using Carbon Copy Cloner 5 on High Sierra and Mojave. When making a backup of a macOS Catalina system volume, CCC will [automatically convert the destination volume from HFS+ to APFS <http://bombich.com/kb/ccc5/working-apfs-volume-groups#convert>](http://bombich.com/kb/ccc5/working-apfs-volume-groups#convert), but only after your explicit approval of the action.

If the OS upgrade converted my startup disk to APFS, what do I need to do to my backup disk? Do I have to erase it as APFS?

You don't need to do anything at all to your backup disk after upgrading to macOS High Sierra or Mojave (and again, on macOS Catalina, CCC will automatically convert the destination to APFS, so you still don't have to do anything to the destination volume). Having an HFS+ backup of an APFS-formatted High Sierra or Mojave startup volume is acceptable; that will function just fine for any future restores, even to an APFS-formatted volume. If your backup disk is an SSD, or if you were planning to erase the destination anyway, we do recommend that you erase it as APFS.

I'm running Mojave — can I erase my HDD destination as APFS? Are there any advantages to using APFS on the destination?

If you were planning to erase your destination volume anyway, we recommend that you format the volume as APFS. While [enumeration performance of APFS on a rotational disk is still significantly worse than HFS+ on the same hardware <http://bombich.com/blog/2019/09/12/analysis-apfs-enumeration-performance-on-rotational-hard-drives>](http://bombich.com/blog/2019/09/12/analysis-apfs-enumeration-performance-on-rotational-hard-drives), there are some other advantages to choosing APFS rather than HFS+. For example, an APFS destination can store snapshots from which you can do point-in-time restores. APFS volumes also support [sparse files <http://bombich.com/kb/ccc5/glossary-terms#s>](http://bombich.com/kb/ccc5/glossary-terms#s), and you're less likely to run into name comparison problems (e.g. when files on the source APFS volume have Unicode characters like 'é') when backing up to an APFS-formatted volume. You also cannot boot a T2 Mac from an HFS+ encrypted volume, so if you have a T2 Mac and encryption of the backup is required, you must choose APFS.

Can I use CCC to clone an APFS startup disk to another Mac?

The macOS installer applies a [firmware upgrade <https://support.apple.com/en-us/HT208020>](https://support.apple.com/en-us/HT208020) to your Mac when you install the macOS upgrade. This firmware upgrade cannot be made part of the cloning process. Only the macOS Installer can upgrade a Macintosh to support APFS. If you attempt to clone an APFS volume to a Macintosh that has not yet received the firmware upgrade from the macOS Installer, that Macintosh will not be able to boot from the APFS volume. Once your Mac has received the firmware upgrade via the macOS Installer, your Mac can boot from a CCC bootable backup on an APFS volume. Note, however, that every major macOS upgrade may require a new firmware upgrade to allow use of the newer operating system.

Note that this is also applicable to a Macintosh running in Target Disk Mode. If you upgrade one Mac to High Sierra (or later) via the Installer, you cannot boot a second Mac into Target Disk Mode, attach it to the first, then clone High Sierra (or later) to the Mac in Target Disk Mode. The required firmware upgrade cannot be applied to the Mac that is booted in Target Disk Mode, you must run the macOS Installer on that second Mac. Once the second Mac has received the firmware upgrade via the macOS Installer, you can clone the first Mac to the second Mac booted in Target Disk Mode.

Does CCC support encrypted APFS volumes?

Yes, CCC 5 can clone 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 cloning that CCC performs.

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.

The important take-away is that APFS file cloning can save you space on your startup disk, but CCC cloning 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](http://bombich.com/kb/cc5/some-files-and-folders-are-automatically-excluded-from-backup-task) <<http://bombich.com/kb/cc5/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 (because Apple doesn't offer a way for us to determine that one file is a clone of another). Making matters worse, [Finder does not accurately represent the true disk usage of your files](https://youtu.be/KggyuL8mED0) <<https://youtu.be/KggyuL8mED0>>. Finder doesn't take into consideration whether one file is a clone of another (again, because Apple doesn't provide a way to make that assessment), so 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.

If you convert your Mac's disk to APFS, understand that 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.

Additional Resources

- [Video: Downgrading from High Sierra to Sierra using a CCC bootable backup](https://www.youtube.com/watch?v=UMvSfDTaLwY?t=9m44s) <<https://www.youtube.com/watch?v=UMvSfDTaLwY?t=9m44s>>
- [Preparing your backup volume for an installation of macOS](http://bombich.com/kb/cc5/preparing-your-backup-disk-backup-os-x) <<http://bombich.com/kb/cc5/preparing-your-backup-disk-backup-os-x>>
- [Video: Working with Disk Utility on macOS High Sierra to prepare your CCC backup disk](#)



[<https://youtu.be/oEfqfMf2z9k>](https://youtu.be/oEfqfMf2z9k)

- Testing your CCC backup [<http://bombich.com/kb/ccc5/how-verify-or-test-your-backup>](http://bombich.com/kb/ccc5/how-verify-or-test-your-backup)

We're here to help

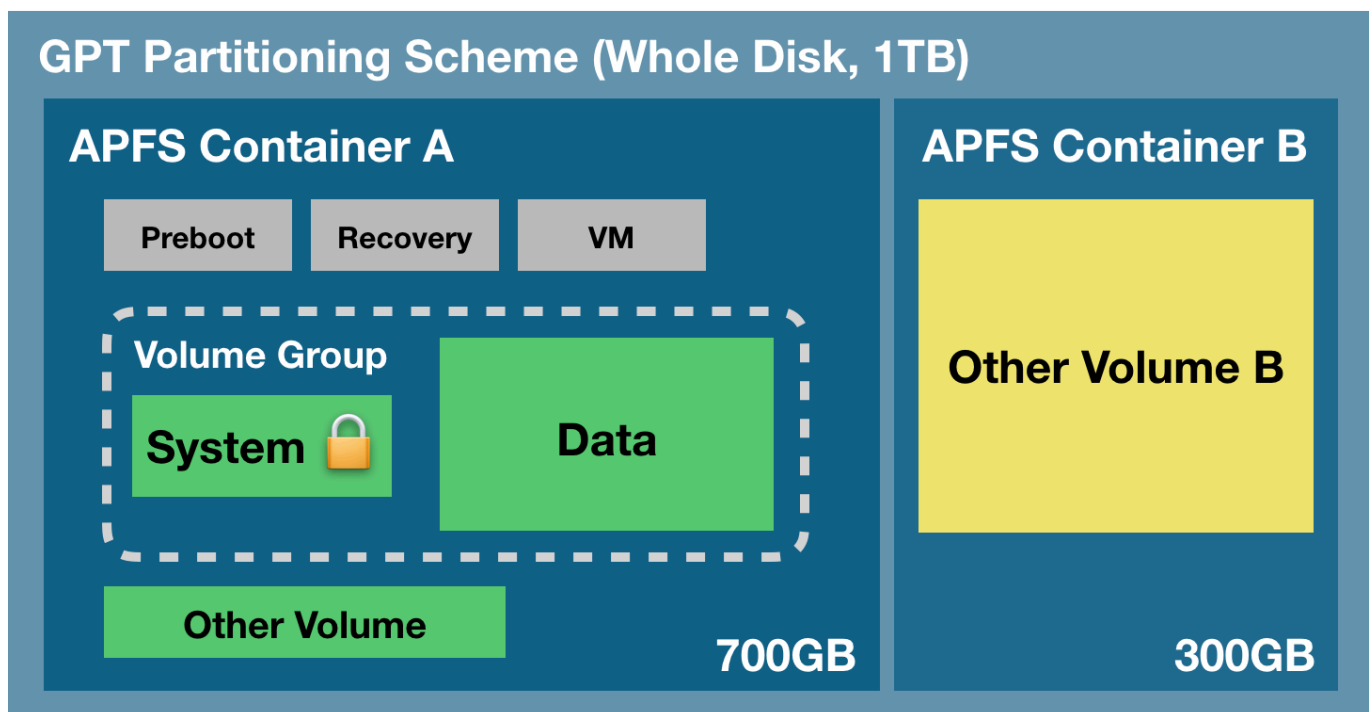
If you get stuck or need some advice, you can get help right from within CCC. Choose "Ask a question" from CCC's Help menu to pose a question to our Help Desk.

Working with APFS Volume Groups

When Apple introduced the APFS filesystem several years ago, 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 clone 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, if you navigate to your startup disk > System > Volumes > Data > Applications, you'll notice that the bulk of the Applications are not there. Yet when you look at the Applications folder on the System volume, they are all there! 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. 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. your backup disk). 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). **Rest assured, though, that all of the applications are backed up when CCC is making a bootable backup of your startup disk! You'll find them at System > Applications on the backup volume.**

Related Documentation

- [What will CCC do to my bootable backup disk when I run it for the first time? <http://bombich.com/kb/cc5/frequently-asked-questions-about-ccc-and-macos-catalina#convert>](http://bombich.com/kb/cc5/frequently-asked-questions-about-ccc-and-macos-catalina#convert)
- [Will my encrypted backup volume be automatically converted to an APFS volume group? <http://bombich.com/kb/cc5/frequently-asked-questions-about-ccc-and-macos-catalina#conversion_encrypted>](http://bombich.com/kb/cc5/frequently-asked-questions-about-ccc-and-macos-catalina#conversion_encrypted)
- [Frequently asked questions about CCC and macOS Catalina <http://bombich.com/kb/cc5/frequently-asked-questions-about-ccc-and-macos-catalina>](http://bombich.com/kb/cc5/frequently-asked-questions-about-ccc-and-macos-catalina)
- [Working with FileVault Encryption <http://bombich.com/kb/cc5/working-filevault-encryption>](http://bombich.com/kb/cc5/working-filevault-encryption)
- [Frequently Asked Questions about encrypting the backup volume <http://bombich.com/kb/cc5/frequently-asked-questions-about-encrypting-backup-volume>](http://bombich.com/kb/cc5/frequently-asked-questions-about-encrypting-backup-volume)
- [Everything you need to know about Carbon Copy Cloner and APFS <http://bombich.com/kb/cc5/everything-you-need-know-about-carbon-copy-cloner-and-apfs>](http://bombich.com/kb/cc5/everything-you-need-know-about-carbon-copy-cloner-and-apfs)

Upgrading from Carbon Copy Cloner 3.5 to Carbon Copy Cloner 5

Installing Carbon Copy Cloner 5

If you have not yet installed Carbon Copy Cloner 5 and CCC 3.5 is not prompting you to upgrade, you can manually download and install Carbon Copy Cloner 5. For illustrated directions, please see [How do I download and install Carbon Copy Cloner?](http://bombich.com/kb/ccc5/how-do-i-download-and-install-carbon-copy-cloner) <<http://bombich.com/kb/ccc5/how-do-i-download-and-install-carbon-copy-cloner>>

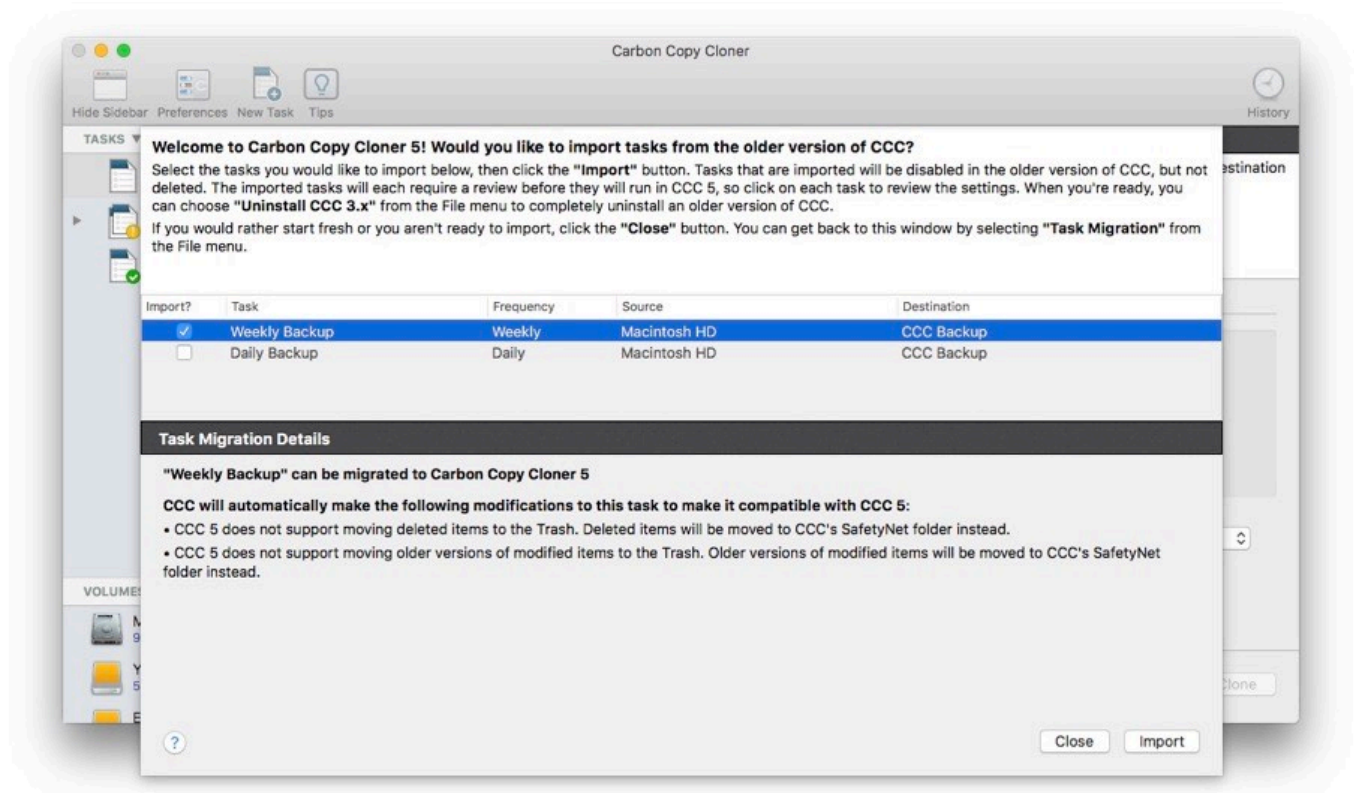
Task Migration Assistant

If you created scheduled tasks with Carbon Copy Cloner 3.5 or later, you will be greeted by the Task Migration Assistant when you open Carbon Copy Cloner 5 for the first time. You can also choose **Task Migration** from CCC's **File** menu to see the Task Migration Assistant.

Click on each task to see notes about changes that CCC will make to the task to ensure its compatibility with CCC 5. Check the box in the **Import** column next to each task that you would like to migrate to CCC 5, then click the **Import** button.

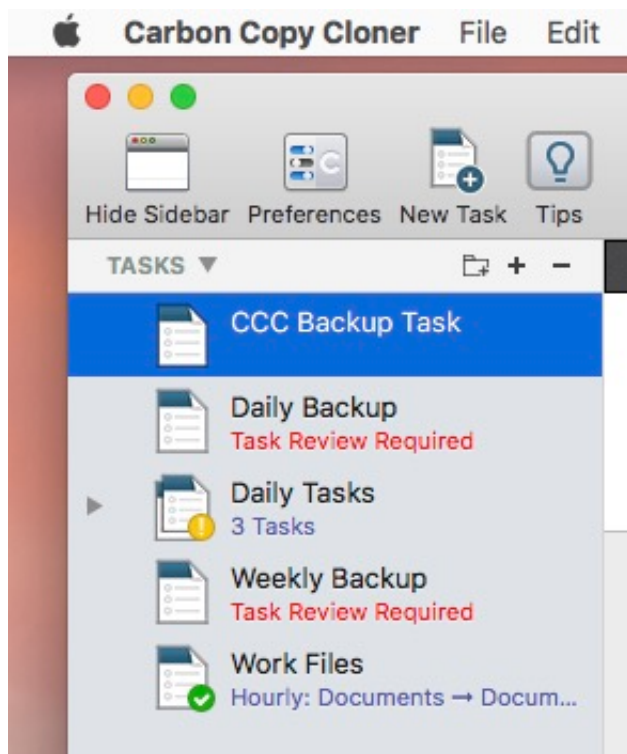
Note: Tasks that are migrated to CCC 5 will be disabled in CCC 3.5.

If you would like to immediately and permanently delete one or more of your older tasks without importing them, simply select those tasks (Command+click to select multiple tasks), then press the **Delete** key.



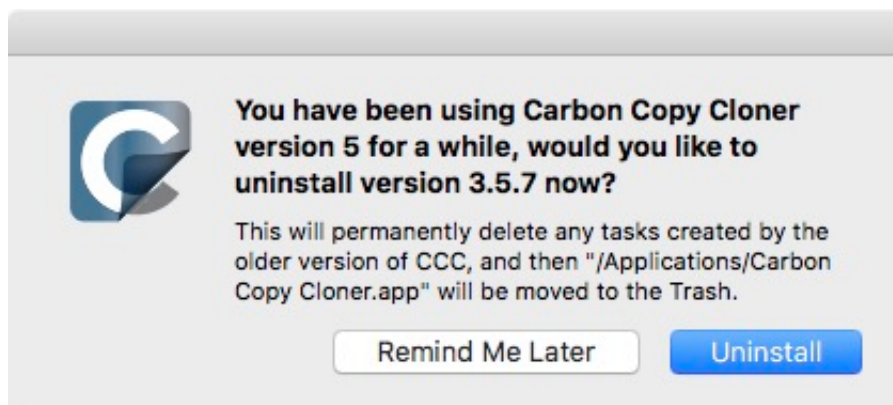
Imported tasks require review

After you have migrated tasks, CCC will indicate that these tasks require review. Click on each task in the sidebar and review the settings. When you are satisfied that the task is configured as desired, click the **Save** button, or choose **Save** from CCC's **File** menu.



Uninstalling the older version of Carbon Copy Cloner

When you import tasks via the Task Migration Assistant, CCC will automatically schedule a 30-day reminder to uninstall the older version of CCC. You can wait for this reminder to appear, or you can choose **Uninstall CCC 3.x...** from CCC's **File** menu to uninstall the older version of CCC immediately.





System Requirements for Carbon Copy Cloner

System Requirements

- OS X 10.10 Yosemite
- OS X 10.11 El Capitan
- macOS 10.12 Sierra
- macOS 10.13 High Sierra
- macOS 10.14 Mojave
- macOS 10.15 Catalina
- macOS 11 Big Sur

Older versions of CCC <<http://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

- HFS+ formatted volume is required for a bootable backup of macOS 10.10 through 10.12.
- APFS or HFS+ formatted volume is required for a bootable backup of macOS 10.13 High Sierra and Mojave
- APFS formatted volume is required for a bootable backup of macOS 10.15 Catalina and later
- APFS source and destination volumes are only supported on macOS 10.13 High Sierra and later
- Backup of user data is supported on some non-Apple-formatted (i.e. not HFS+ or APFS) filesystems
- SSDs and hard disk drives¹ in Firewire², Thunderbolt and USB enclosures³
- CCC is supported only on Apple Macintoshes that officially support OS X 10.10 Yosemite (or higher)
- A minimum screen resolution of 1024x768 is required

1: APFS performs poorly on HDDs with a rotational speed of less than 7200RPM

2: macOS Catalina+ does not support booting a Mac via a FireWire-attached device

3: Not all hard drive enclosures are capable of booting macOS. See the [Preparing a hard drive for use with Carbon Copy Cloner](http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x) <<http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x>> and [Help! My clone won't boot](http://bombich.com/kb/ccc5/help-my-clone-wont-boot) <<http://bombich.com/kb/ccc5/help-my-clone-wont-boot>> sections of the CCC documentation for more information on disk formatting, partitioning, and general bootability concerns. These restrictions apply to the ability of the device to boot a Mac, any of these devices are suitable for general backup.

Configurations that are not supported

- CCC will not clone to or from an unformatted or unmounted device — the source and destination must have a filesystem recognized by macOS and visible in the Finder
- [Cloning Windows system files is not a supported configuration](http://bombich.com/kb/ccc5/can-ccc-back-up-my-bootcamp-windows-partition) <<http://bombich.com/kb/ccc5/can-ccc-back-up-my-bootcamp-windows-partition>>
- CCC will not backup directly to optical media (e.g. CD-ROM or DVD-ROM)
- WebDAV, FTP, NFS and other "cloud" destinations are not supported
- macOS Mojave and later cannot boot from a RAID device



- 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>](https://support.apple.com/en-us/HT208020) and [offers additional resources here <https://help.apple.com/deployment/macOS>](https://help.apple.com/deployment/macOS/), and there are [alternative solutions to consider. <https://twocanoes.com/products/mac/mac-deploy-stick>](https://twocanoes.com/products/mac/mac-deploy-stick)
- We can only support cloning versions 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 clone Mojave onto a 2019 MacBook Pro that shipped with Catalina. 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 5 \(or 4\)?](#)
- [What is your return policy?](#)
- [Need help?](#)
- [What are the terms of sale?](#)
- [How is CCC delivered?](#)
- [Which payment types do you accept?](#)
- [Do you accept purchase orders?](#)
- [Do you charge tax, such as VAT, or other duties?](#)
- [What kind of e-commerce security do you use?](#)
- [Where can I download your W-9 form?](#)
- [Frequently Asked Questions](#)

How can I purchase CCC?

Bombich Software products are available directly through our [online store](http://bombich.com/store) <<http://bombich.com/store>>, hosted by [FastSpring](http://www.fastspring.com) <<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://cccseller.com/redeem) <<https://cccseller.com/redeem>>.

Licenses are valid for prior versions of CCC. (e.g. If you purchase a CCC 5 license, it can be used with CCC 4.) For more info about purchasing CCC, see [How much does Carbon Copy Cloner cost and how can I purchase it?](http://bombich.com/kb/cc5/how-much-does-carbon-copy-cloner-cost-and-how-can-i-purchase-it) <<http://bombich.com/kb/cc5/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 Carbon Copy Cloner](http://bombich.com/download) <<http://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) <<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 Carbon Copy Cloner'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 <http://bombich.com/download>](http://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 <http://bombich.com/store>](http://bombich.com/store), hosted by [FastSpring <http://www.fastspring.com>](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 <http://bombich.com/software/CCC_EULA.rtf>](http://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>](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>](http://www.fastspring.com).

[Review FastSpring's Privacy Policy <http://www.fastspring.com/privacy.php>](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>](http://www.fastspring.com/w9.pdf)

Frequently Asked Questions

- [How does the free 30-day trial work? <http://bombich.com/kb/ccc5/how-does-free-30-day-trial-work>](http://bombich.com/kb/ccc5/how-does-free-30-day-trial-work)
- [How much does Carbon Copy Cloner cost and how can I purchase it? <http://bombich.com/kb/ccc5/how-much-does-carbon-copy-cloner-cost-and-how-can-i-purchase-it>](http://bombich.com/kb/ccc5/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? <http://bombich.com/kb/ccc5/if-i-pay-ccc-now-will-i-have-pay-future-updates>](http://bombich.com/kb/ccc5/if-i-pay-ccc-now-will-i-have-pay-future-updates)
- [Purchasing an Upgrade for CCC 5 <http://bombich.com/kb/ccc5/purchasing-upgrade-carbon-copy-cloner-5>](http://bombich.com/kb/ccc5/purchasing-upgrade-carbon-copy-cloner-5)
- [Can I use one license of CCC on multiple Macs in my household? <http://bombich.com/kb/ccc5/can-i-use-one-license-ccc-on-multiple-macs-in-my-household>](http://bombich.com/kb/ccc5/can-i-use-one-license-ccc-on-multiple-macs-in-my-household)
- [Do you offer an academic discount? <http://bombich.com/kb/ccc5/do-you-offer-academic-discount>](http://bombich.com/kb/ccc5/do-you-offer-academic-discount)
- [Can I give CCC as a gift? <http://bombich.com/kb/ccc5/can-i-give-ccc-gift>](http://bombich.com/kb/ccc5/can-i-give-ccc-gift)
- [Do you offer a volume licensing program? <http://bombich.com/kb/ccc5/do-you-offer-volume-licensing-program>](http://bombich.com/kb/ccc5/do-you-offer-volume-licensing-program)
- [Why isn't CCC on the Mac App Store? <http://bombich.com/kb/ccc5/why-isnt-ccc-on-mac-app-store>](http://bombich.com/kb/ccc5/why-isnt-ccc-on-mac-app-store)
- [Do you offer telephone support? <http://bombich.com/kb/ccc5/do-you-offer-telephone-support>](http://bombich.com/kb/ccc5/do-you-offer-telephone-support)

How much does Carbon Copy Cloner cost and how can I purchase it?

Pricing

A household license of Carbon Copy Cloner 5 costs \$39.99 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** <<http://bombich.com/store/corporate>>.

Bombich Software products are available directly through our [online store](http://bombich.com/store) <<http://bombich.com/store>>, hosted by [FastSpring](http://fastspring.com) <<http://fastspring.com>>, our e-commerce partner and Seller of Record. Carbon Copy Cloner 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](http://bombich.com/download) <<http://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://ccreseller.com/redeem) <<https://ccreseller.com/redeem>>.

Upgrade Pricing

If you own a CCC 3.5 or 4.0 household license, you can receive a discount when purchasing CCC 5.

If you have used CCC 1, 2, 3 or 3.3.....no discount is offered.

If you own CCC 3.5.....your discount is 25%.

If you own CCC 4.....your discount is 50%.

Please [visit our upgrade page to determine your discount offer](http://bombich.com/store/upgrade) <<http://bombich.com/store/upgrade>>

Note: If you purchased CCC 4 between May 22 and August 21, you already have a free CCC 5 license. [Retrieve it here](http://bombich.com/forgot) <<http://bombich.com/forgot>>.

Additional Resources

- [Purchasing an Upgrade for Carbon Copy Cloner](http://bombich.com/kb/ccc5/purchasing-upgrade-carbon-copy-cloner-5) <<http://bombich.com/kb/ccc5/purchasing-upgrade-carbon-copy-cloner-5>>
- [Upgrading from Carbon Copy Cloner 3.5 to Carbon Copy Cloner 5](http://bombich.com/kb/ccc5/upgrading-from-carbon-copy-cloner-3.5-carbon-copy-cloner-5) <<http://bombich.com/kb/ccc5/upgrading-from-carbon-copy-cloner-3.5-carbon-copy-cloner-5>>
- [Contact Sales Support](mailto:sales@bombich.com?subject=Upgrade%20Eligibility%20Question) <<mailto:sales@bombich.com?subject=Upgrade%20Eligibility%20Question>>

Purchasing an Upgrade for Carbon Copy Cloner 5

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

No, CCC 5 requires a new license. However, **if you purchased a CCC 4 license on or after May 22, 2017, we will grant you a FREE license for CCC 5.** Household and Pro licenses purchased prior to May 22, 2017 are eligible for upgrade pricing.

I purchased a license for CCC 4 on or after May 22, 2017. How do I get my FREE CCC 5 license?

When you open CCC 5 for the first time, it will attempt to retrieve your new license using the details from your CCC 4 license. If this succeeds, you will receive an email containing your new license and details for applying the new license to CCC 5. 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 <http://bombich.com/forgot>](http://bombich.com/forgot).

What licenses are eligible for online upgrade pricing?

CCC 3.5 and CCC 4 Household and Pro licenses are eligible for the following upgrade pricing:

If you have used CCC 1, 2, 3, or 3.3.....no discount is offered.

If you own a CCC 3.5 Personal & Household or Pro license.....your discount is 25%.

If you own a CCC 4 Personal & Household or Pro license.....your discount is 50%.

Corporate and Institutional Licenses (Volume License Program) are eligible for an upgrade discount of 25% off [the current corresponding price tier <http://bombich.com/store/corporate>](http://bombich.com/store/corporate). If you own a Corporate and Institutional License, please [contact us <mailto:sales@bombich.com?subject=CCC%20Upgrade%20Quote%20Request>](mailto:sales@bombich.com?subject=CCC%20Upgrade%20Quote%20Request) so that we can create a custom upgrade offer for you. Upgrades are free if Maintenance has been purchased and is currently active.

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.

How do I purchase a license for CCC 5 at upgrade pricing?

If you are (or were) using a registered copy of CCC 4, download and open CCC 5. CCC 5 will recognize your CCC 4 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 wish to upgrade CCC 3.5, you must [request your upgrade offer via our website](#)

<http://bombich.com/store/upgrade>. You can also use our [upgrade offer request form](#) <http://bombich.com/store/upgrade> for CCC 4 if you have any trouble upgrading in-app. 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>.

If you own a Corporate and Institutional License, please [contact us](#) <mailto:sales@bombich.com?subject=CCC%20Upgrade%20Quote%20Request> so that we can create a custom upgrade offer for you.

My Mac is too old for CCC 5. If I purchase a license for CCC 5, will that work with CCC 4 or 3.5?

Yes! If you purchase a license for CCC 5, that license will be recognized by CCC 3.5.7 or later. If you upgrade your Mac at a later date, you can upgrade to CCC 5 and begin using your CCC 5 license.

Additional Resources

- [What's New in CCC 5](http://bombich.com/kb/ccc5/whats-new-in-ccc) <http://bombich.com/kb/ccc5/whats-new-in-ccc>
- [System Requirements for Carbon Copy Cloner](http://bombich.com/kb/ccc5/system-requirements-carbon-copy-cloner) <http://bombich.com/kb/ccc5/system-requirements-carbon-copy-cloner>
- [Upgrading from Carbon Copy Cloner 3.5 to Carbon Copy Cloner 5](http://bombich.com/kb/ccc5/upgrading-from-carbon-copy-cloner-3.5-carbon-copy-cloner-5) <http://bombich.com/kb/ccc5/upgrading-from-carbon-copy-cloner-3.5-carbon-copy-cloner-5>
- [Contact Sales Support](#) <mailto:sales@bombich.com?subject=Upgrade%20Eligibility%20Question>
- [Download CCC](http://bombich.com/download) <http://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 make a bootable backup.

[Download the latest and greatest version of Carbon Copy Cloner <http://bombich.com/download>](http://bombich.com/download).

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

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 5.0 to 5.1, 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 4 to 5) 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](http://bombich.com/download) <<http://bombich.com/download>>.

For more information about our current upgrade pricing options, please see [How much does Carbon Copy Cloner cost and how can I purchase it?](http://bombich.com/kb/ccc5/how-much-does-carbon-copy-cloner-cost-and-how-can-i-purchase-it) <<http://bombich.com/kb/ccc5/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 <http://bombich.com/software/CCC_EULA.rtf>](http://bombich.com/software/CCC_EULA.rtf) allows you to install and use Carbon Copy Cloner on any computer that you own or control for personal, noncommercial use. If you're using CCC commercially or institutionally, check out our [Corporate <http://bombich.com/store/corporate>](http://bombich.com/store/corporate) or [Academic <http://bombich.com/edu>](http://bombich.com/edu) purchasing options.

A CCC 5 license will also be accepted by CCC 3.5.7 and CCC 4. If you have multiple Macs in your household and some do not meet the requirements for CCC 5, you can use the same license on all of your Macs with CCC 3.5.7, CCC 4 and CCC 5. You can download all available versions of CCC at any time from our [download page <http://bombich.com/download>](http://bombich.com/download). Misplaced your license? Request the registration key from within CCC or [via our website <http://bombich.com/forgot>](http://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? <http://bombich.com/kb/cc5/how-do-i-use-one-license-ccc-on-multiple-macs-in-my-household>](http://bombich.com/kb/cc5/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 <http://bombich.com/edu>](http://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 <http://bombich.com/edu>](http://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 Carbon Copy Cloner. Volume licensing is open to anyone purchasing 5 or more licenses of Carbon Copy Cloner. A volume license agreement includes:

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

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

Product Delivery and Ordering

We offer Carbon Copy Cloner 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](http://bombich.com/store/corporate) <<http://bombich.com/store/corporate>>. To learn about our education discounts or place a discounted education order, please read about our [Education Pricing](http://bombich.com/edu) <<http://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%20CC%20License) <<mailto:sales@bombich.com?subject=Add%20Volume%20License%20Seats%20to%20CC%20License>> for a custom quote.

Software Maintenance

Volume licenses offer the option of including software maintenance, a service which provides all updates to Carbon Copy Cloner at no additional charge beyond the subscription fee. Maintenance subscriptions can be cancelled at any time via a link found in your Carbon Copy Cloner volume license delivery email. For additional details, please see the [Carbon Copy Cloner Maintenance Terms](http://bombich.com/software/maintenance_terms_2014.pdf) <http://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](http://bombich.com/sales-terms-and-conditions) <<http://bombich.com/sales-terms-and-conditions>>.

If Carbon Copy Cloner 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). <<mailto:sales@bombich.com>>



Can I give CCC as a gift?

Yes, using our [Online Gift Store <http://sites.fastspring.com/bombich/product/ccc?option=gift>](http://sites.fastspring.com/bombich/product/ccc?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>](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 utility that can make a bootable backup of macOS on the Mac App Store. You can [send Apple some feedback <https://www.apple.com/feedback/>](https://www.apple.com/feedback/) about this policy, but judging from the absence of the Mac App Store from Apple's Feedback page, 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 Carbon Copy Cloner'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://ccreseller.com/redeem>](https://ccreseller.com/redeem) can offer that level of assistance.

Related Documentation

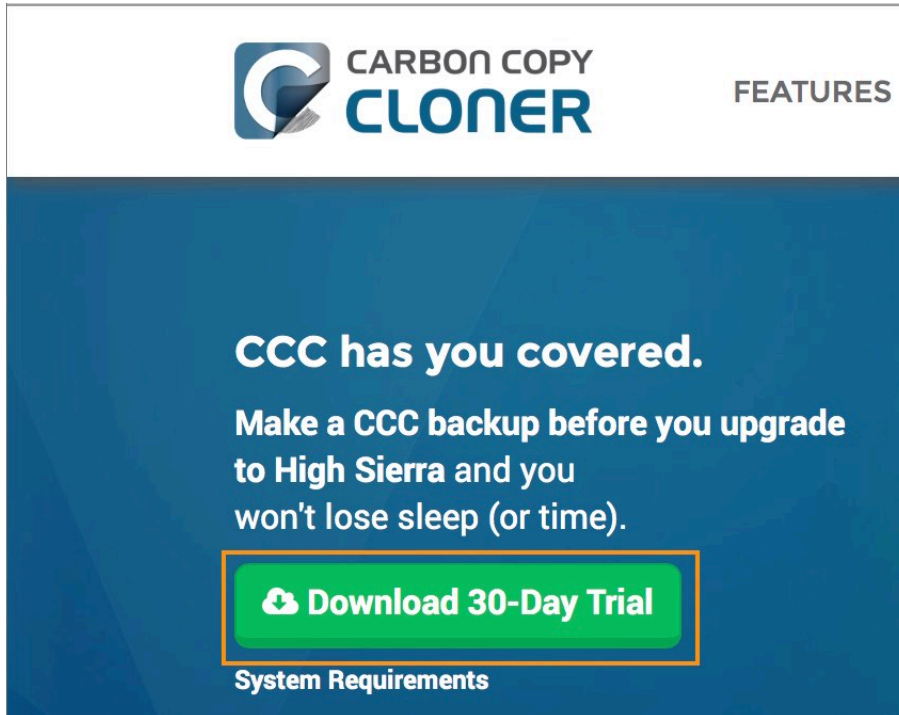
- [Establishing an initial backup <http://bombich.com/kb/ccc5/how-set-up-your-first-backup>](http://bombich.com/kb/ccc5/how-set-up-your-first-backup)
- [How do I get help? <http://bombich.com/kb/ccc5/how-do-i-get-help>](http://bombich.com/kb/ccc5/how-do-i-get-help)
- [About Us <http://bombich.com/about>](http://bombich.com/about)

Downloading, Installing and Registering CCC

How do I download and install Carbon Copy Cloner?

Watch a video of this tutorial on YouTube <<https://www.youtube.com/watch?v=vi1p-aM0gxc>>

Visit **bombich.com**



The screenshot shows the Carbon Copy Cloner website. At the top left is the logo with the text "CARBON COPY CLONER". To the right of the logo is the word "FEATURES". Below this is a dark blue banner with white text that reads: "CCC has you covered. Make a CCC backup before you upgrade to High Sierra and you won't lose sleep (or time)." Below the text is a green button with a white download icon and the text "Download 30-Day Trial". Below the button is the text "System Requirements".

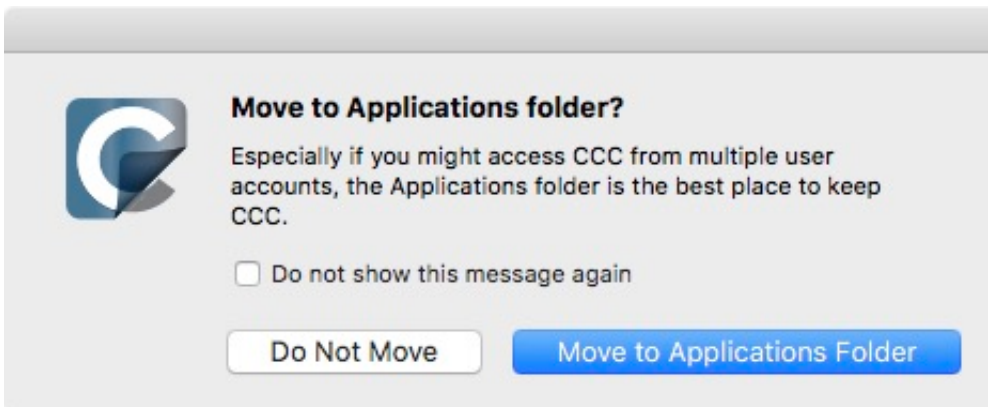
Go to <https://bombich.com> <<https://bombich.com>> and click on the **Download** button.

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. Note: If you have an older version of CCC in your Applications folder already, CCC 5 will not overwrite that, and won't produce this prompt. That's OK, CCC will prompt to move itself after you have proceeded with migrating CCC 3 tasks (if applicable) and then uninstalled CCC 3.

(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 4 to CCC 5

If you download CCC 5 via the upgrade interface in CCC 4, CCC 5 will be downloaded to your Mac and placed adjacent to CCC 4. When CCC 5 opens for the first time, you will begin a full-featured, 30-day trial. Please take all of that time to evaluate CCC 5. When you're ready to purchase CCC 5, 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 5 upgrade?"

Yes, CCC 5 is a paid upgrade. However, CCC 3 or 4 license may be eligible for upgrade pricing. [Check here for eligibility <http://bombich.com/store/upgrade>](http://bombich.com/store/upgrade).

"If I decide to not purchase the CCC 5 upgrade, can I downgrade to CCC 4?"

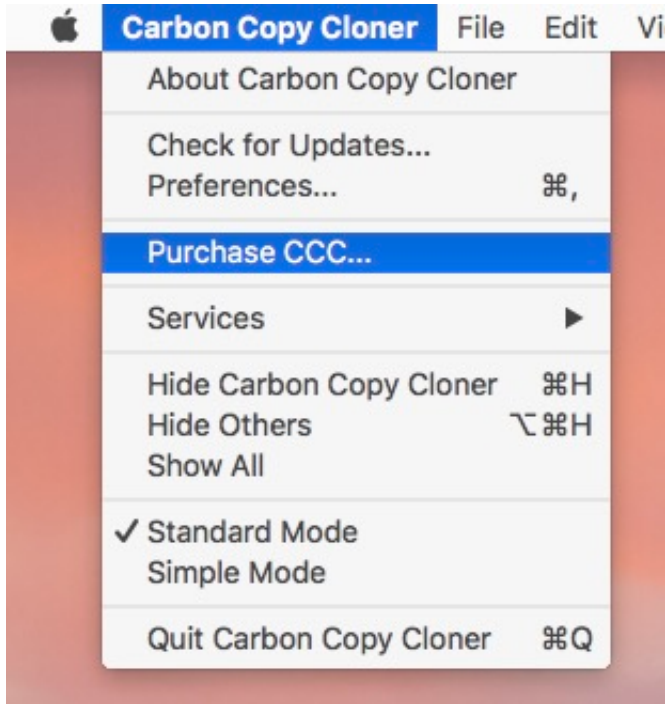
Yes. Downgrading to CCC 4 restores your tasks as they were prior to upgrading. If you still have CCC 4 in your Applications folder, simply open it and choose the option to **Downgrade**. If you downloaded CCC 5 from our website and replaced your copy of CCC 4, you can [re-download CCC 4 from our website <http://bombich.com/download#ccc4>](http://bombich.com/download#ccc4).

Additional Resources

- [Purchasing an Upgrade for Carbon Copy Cloner 5 <http://bombich.com/kb/ccc5/purchasing-upgrade-carbon-copy-cloner-5>](http://bombich.com/kb/ccc5/purchasing-upgrade-carbon-copy-cloner-5)
- [How does the free 30-day trial work? <http://bombich.com/kb/ccc5/how-does-free-30-day-trial-work>](http://bombich.com/kb/ccc5/how-does-free-30-day-trial-work)
- [What's new in CCC 5? <http://bombich.com/kb/ccc5/whats-new-in-ccc>](http://bombich.com/kb/ccc5/whats-new-in-ccc)
- [System Requirements for Carbon Copy Cloner 5 <http://bombich.com/kb/ccc5/system-requirements-carbon-copy-cloner>](http://bombich.com/kb/ccc5/system-requirements-carbon-copy-cloner)
- [Carbon Copy Cloner 5 Release Notes <http://bombich.com/kb/ccc5/release-notes>](http://bombich.com/kb/ccc5/release-notes)
- [Report a problem or ask a question about Carbon Copy Cloner 5 <http://bombich.com/software/get_help>](http://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



Welcome to Carbon Copy Cloner

Thanks for trying Carbon Copy Cloner! You can try the complete feature set of CCC for 30 days before purchasing a license. Use that time to explore CCC's automated, incremental backup functionality, make a bootable backup, move your digital life to a new hard drive and get peace of mind.

I already have a license 

Trial

Purchase CCC

The trial period ends on Jul 20, 2017, 7:19 AM

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

Copy and Paste in Registration Codes



Carbon Copy Cloner Registration

Retrieve Registration


Back

Register

The trial period ends on Jul 20, 2017, 7:19 AM

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



Carbon Copy Cloner Registration

Your Name
name@email.com
GAWQE-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-X

Retrieve Registration

Back Register

The trial period ends on Jul 20, 2017, 7:19 AM

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



Thanks for registering!

Carbon Copy Cloner 5

Your Name

name@email.com

Retrieve Registration Via Email

Change Registration

Close

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



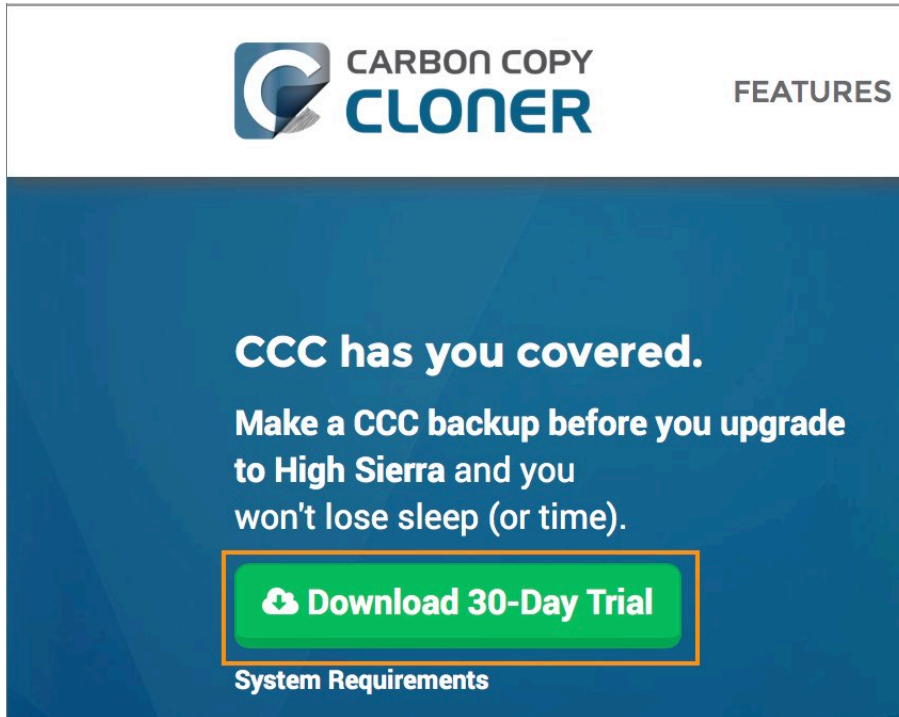
Can I download the old versions of Carbon Copy Cloner?

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

We do not sell CCC 4 and CCC 3.5 licenses. To use CCC 4 or 3.5, please purchase a CCC 5 license. **CCC 5 licenses can be used to register CCC 3.5 and CCC 4.**

How to Register CCC in One Click

Install and Launch Carbon Copy Cloner



The screenshot shows the Carbon Copy Cloner website interface. At the top left is the logo with the text "CARBON COPY CLONER". To the right of the logo is the word "FEATURES". The main content area has a dark blue background with white text that reads: "CCC has you covered. Make a CCC backup before you upgrade to High Sierra and you won't lose sleep (or time)." Below this text is a prominent green button with a white download icon and the text "Download 30-Day Trial". Underneath the button, the text "System Requirements" is visible.

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

Open Your Registration Email

Carbon Copy Cloner

Registration name: Your Name
Registration email: Your Email Address
Registration code:

Number of licenses: [1]

Registering Carbon Copy Cloner

Please resist the temptation to type in that really long registration code. If you're reading this email on your Mac and you already have CCC installed*, just click on this great big button:



[Click Here to Register CCC](#)

We suggest that you do this right now, while you're online. As long as you already have CCC installed on your Mac, clicking the magic button should instantly apply the registration settings to CCC. If you don't already have Carbon Copy Cloner installed, do this first:

1. [Download the latest version of CCC \[Alternate\]](#)
2. Double-click the downloaded zip file and drag the Carbon Copy Cloner icon into your Applications folder.
3. Launch Carbon Copy Cloner, then go back to this email and click the registration button above to apply your registration settings

*** Not on your Mac right now?** If you want to apply this registration code to another Macintosh covered under the same license, drag the big registration button to your Desktop, then distribute the bookmark file to the other Macs and open it there.

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 OS X 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 <http://bombich.com/kb/ccc5/how-manually-enter-ccc-registration-code>](http://bombich.com/kb/ccc5/how-manually-enter-ccc-registration-code), or [contact us for assistance <http://bombich.com/software/get_help>](http://bombich.com/software/get_help).

Trouble Applying Your Registration Information?

Frequently Asked Questions

1. [How do I retrieve my registration information? I paid for CCC in the past, but now I'm trying to use CCC under another user account.](#)
2. [What if I can't retrieve my registration information?](#)
3. [When I click on the button to apply my registration settings, my browser says that it can't open this weird-looking URL.](#)
4. [Why did Firefox report "Corrupted Content Error" when I clicked on the button to apply my registration settings?](#)
5. [How do I register CCC in one click?](#)
6. [How do I manually enter a CCC registration code?](#)
7. [I'm still having trouble. How do I get someone to help me?](#)

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 <http://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 \(no copying/pasting of registration codes is required\) <http://bombich.com/kb/ccc5/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 <http://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 (3.5 or



later) and you're still getting this message, try [entering the registration values manually <http://bombich.com/kb/ccc5/how-manually-enter-ccc-registration-code>](http://bombich.com/kb/ccc5/how-manually-enter-ccc-registration-code), or [contact us for assistance <http://bombich.com/forgot>](http://bombich.com/forgot).

How do I register CCC in one click?

View [step-by-step one-click registration directions, complete with pictures. <http://bombich.com/kb/ccc5/how-register-ccc-in-one-click>](http://bombich.com/kb/ccc5/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. <http://bombich.com/kb/ccc5/how-manually-enter-ccc-registration-code>](http://bombich.com/kb/ccc5/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 <http://bombich.com/forgot?found=0>](http://bombich.com/forgot?found=0), and we will help you sort it out as quickly as possible.

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

The CCC license allows you to install and use Carbon Copy Cloner 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](http://bombich.com/store/corporate) <<http://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 <http://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 Carbon Copy Cloner?](http://bombich.com/kb/ccc5/how-do-i-download-and-install-carbon-copy-cloner) <<http://bombich.com/kb/ccc5/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](http://bombich.com/kb/ccc5/how-register-ccc-in-one-click) <<http://bombich.com/kb/ccc5/how-register-ccc-in-one-click>>. Misplaced your registration email? [Request a new one via our website](http://bombich.com/forgot) <<http://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.

Registering Carbon Copy Cloner

Please resist the temptation to type in that really long registration code. If you're reading this email on your Mac and you already have CCC installed*, just click on this great big button:

Click Here to Register CCC

Click Here to Register CCC
<https://mew.bombich.com/li...RB-XNPZ8-WC3NL-CEMAF-8K8M>

We suggest that you do this right now, while you're online. As long as you already have CCC installed on your Mac, clicking the magic button should instantly apply the registration settings to CCC. If you don't already have Carbon Copy Cloner installed, do this first:

1. [Download the latest version of CCC \[Alternate\]](#)
2. Double-click the downloaded zip file and drag the Carbon Copy Cloner icon into your Applications folder.
3. Launch Carbon Copy Cloner, then go back to this email and click the registration button above to apply your registration settings

*** Not on your Mac right now?** If you want to apply this registration code to another Macintosh covered under the same license, drag the big registration button to your Desktop, then distribute the bookmark file to the other Macs and open it there.

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> <<http://bombich.com/download>>.

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



The screenshot shows the Carbon Copy Cloner error dialog box. At the top left is the Carbon Copy Cloner logo. The main text reads "Oops, that license code is invalid...". Below this, it says "To avoid typos, click on the 'Apply registration settings in CCC' link that was sent to you via email." At the bottom, there are three buttons: "Help Me!", "Back", and "Purchase CCC". A grey bar at the very bottom of the dialog box contains the text "The trial period ends on Jul 20, 2017, 12:08 PM".

Registration Details

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



Carbon Copy Cloner Registration

The trial period ends on Jul 20, 2017, 7:19 AM

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.

Carbon Copy Cloner

Purchase Date: September 30, 2017

Name: CCC User

Email: user@email.com

Code: XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

Automatically apply these registration settings in CCC:

Successful registration

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



Thanks for registering!

Carbon Copy Cloner 5

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 <http://bombich.com/forgot>](http://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 <http://bombich.com/forgot>](http://bombich.com/forgot).

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 File 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. Quit CCC if it is running.
2. Choose **Computer** from the Finder's Go menu.
3. Click on your startup disk (often named **Macintosh HD**)
4. Navigate to /Library/Application Support/
5. Move the com.bombich.ccc folder to the Trash (**note:** doing so will remove any saved tasks on that volume). This folder may not be present, and that's OK.
6. Open a new Finder window (e.g. **File > New Finder Window**).
7. Choose **Computer** from the Finder's Go menu.
8. Click on the backup disk
9. Navigate to /Library/Application Support/
10. Copy the com.bombich.ccc folder to /Library/Application Support/ on your startup disk.
11. Open the Activity Monitor application (Applications > Utilities)
12. Choose **All Processes** from the View menu
13. Find and quit the **com.bombich.ccchelper** application.
14. Open CCC — your tasks should now be restored.

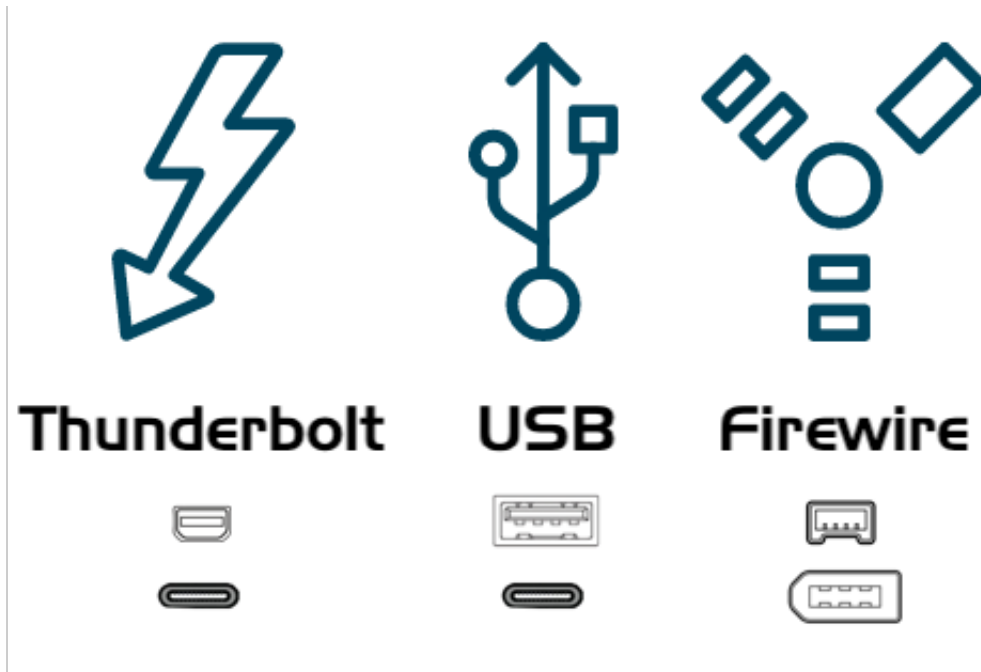
Note that you may have to activate suspended tasks, and/or reselect the source or destination volumes in your tasks.

Also, please note that you must move 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, Firewire, Thunderbolt?



Many hard drive enclosures have Firewire, USB, 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).** If your Mac does not offer native USB 3.0 support (e.g. it's older than 2012), a USB device may boot your Mac, but performance will be considerably slower than your Mac's internal hard drive.

Catalina users: Apple no longer supports booting a Mac from a FireWire-attached device. Backing up to a FireWire device is fine, but if you need a bootable backup, you should use a device that can be attached to your Mac via USB or Thunderbolt.

Specific hard drive recommendations

Most hard drive enclosures will work just fine for your backups, however, [some cannot function as a bootable device](http://bombich.com/kb/ccc5/help-my-clone-wont-boot#known_issues). It would be nearly impossible for us to curate an exhaustive list of every enclosure/Mac combination that does and does not work. However, we frequently get asked for a recommendation, so here's a list of some hard drive enclosures that we have tested with good results. Performance and price go hand-in-hand. If you opt for a USB-only device, pre-2015 Macs will be slower when booting from that device. USB-C equipped Macs can work well from a USB-C (USB 3.1) equipped hard drive, especially if the disk inside of the enclosure is an SSD.

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 bootable backup device:

Oyen Digital U32 Shadow External SSD USB-C (1-4TB) <<https://amzn.to/2CVG23q>> (UK <<https://alteredimagesltd.com/product/u32-shadow-dura-usb-c-rugged-portable-ssd/>>)
Oyen Helix NVMe USB-C (250GB-2TB) <<https://amzn.to/2MdGemO>>
Samsung T5 Portable SSD (1TB & 2 TB) - Recommended only for macOS 10.15 Catalina and newer. <https://www.amazon.com/Samsung-T5-Portable-SSD-MU-PA1T0B/dp/B073H552FJ/ref=as_li_qf_asin_il_tl?ie=UTF8&tag=bombich>

USB 3.1, Gen 2 Desktop External Hard Drive (7,200 RPM 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)

HighPoint RocketStor RS5212 Thunderbolt Storage Dock <https://www.bhphotovideo.com/c/product/985459-REG/highpoint_5212_2_bay_thunderbolt_10gb_s_storage.html/BI/20458/KBID/15280/kw/HIRS5212/DFF/d10-v21-t1-x451315>

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 Dura 2.5" SATA to USB 3.1 external Hard Drive/SSD Enclosure <<https://amzn.to/2Pdkc0m>>

Bare mechanical drive (SATA) 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" <<http://www.amazon.com/Black-4TB-Performance-Hard-Drive/dp/B00FJRS6FU/?tag=bombich-20&creative=9325&linkCode=as2&creativeASIN=B07G3LYX3M&linkId=0561481c219dc81a5c076d88092b4ffa>>

Not Recommended

Before purchasing any enclosure, be sure to check whether any [known compatibility issues](http://bombich.com/kb/ccc5/help-my-clone-wont-boot#known_issues) <http://bombich.com/kb/ccc5/help-my-clone-wont-boot#known_issues> pertain to that device. We offer some general advice here, though, and a small collection of specific devices that are very *popular*, but known to not serve well as bootable backup disks for macOS.

Avoid disks that use Shingled Magnetic Recording

Several years ago Seagate introduced [Shingled Magnetic Recording](https://www.seagate.com/tech-insights/breaking-areal-density-barriers-with-seagate-smr-master-ti/) <<https://www.seagate.com/tech-insights/breaking-areal-density-barriers-with-seagate-smr-master-ti/>> 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>>

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

These disks are cheap and can be acquired by the palette at your local Costco. Unfortunately, [APFS is not tuned to perform well on rotational disks <http://bombich.com/blog/2019/09/12/analysis-apfs-enumeration-performance-on-rotational-hard-drives>](#), and that performance is just unacceptable on these "slowest of the slow" rotational disks. The following disks are examples of these slower devices, and **we do not recommend using these for macOS bootable backups**:

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

If you have one of these devices you can [format the device with Apple's legacy "Mac OS Extended, Journaled" format <http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x#choose_format>](#) instead of APFS, and use it for [data-only backups <http://bombich.com/kb/ccc5/frequently-asked-questions-about-ccc-and-macos-catalina#encrypted_non_bootable>](#).

Samsung T5 Portable SSD and Transcend StoreJet SSD [when using High Sierra and Mojave only]:

The Samsung T5 and the Transcend StoreJet SSD [introduce a lengthy delay to the beginning of the startup process <http://bombich.com/kb/ccc5/help-my-clone-wont-boot#known_issues>](#) when High Sierra or Mojave is installed onto them and when they are APFS formatted. This delay can occur whether you're trying to boot your Mac from the external SSD, or even when you're booting your Mac from its internal disk. Especially if you were planning to use an external SSD as a primary startup disk, or if you tend to reboot your Mac a lot, we recommend that you avoid using these two external SSDs with High Sierra and Mojave.

macOS Catalina and newer: We have seen good results with the Samsung T5 Portable SSD on macOS Catalina. Our internal testing has been 100% successful and we have received several reports that corroborate our results.

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, and [definitely not for creating a bootable backup of your startup disk <http://bombich.com/kb/ccc5/help-my-clone-wont-boot#known_issues>](#).

Western Digital My Passport HDD

We have received several reports that [some Macs are unable to boot macOS Catalina from a Western Digital My Passport enclosure <http://bombich.com/kb/ccc5/macos-catalina-known-issues#wd_bootability>](#).

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 50% larger than the amount of data that you're initially backing up** to it. This allows for a modest amount of data growth and room for temporary archiving of modified and deleted files.

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 Carbon Copy Cloner, 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.

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 bootable backup on that locally-attached disk. **Local, bootable backups are much simpler and more reliable**, and a lot easier to restore from should your Mac's startup disk fail. The logistics of restoring the operating system from a disk image on a network volume are pretty complicated if you don't have a functional startup disk. Providing that functional startup disk is the primary appeal of the CCC backup solution.

NAS devices that we specifically do not recommend

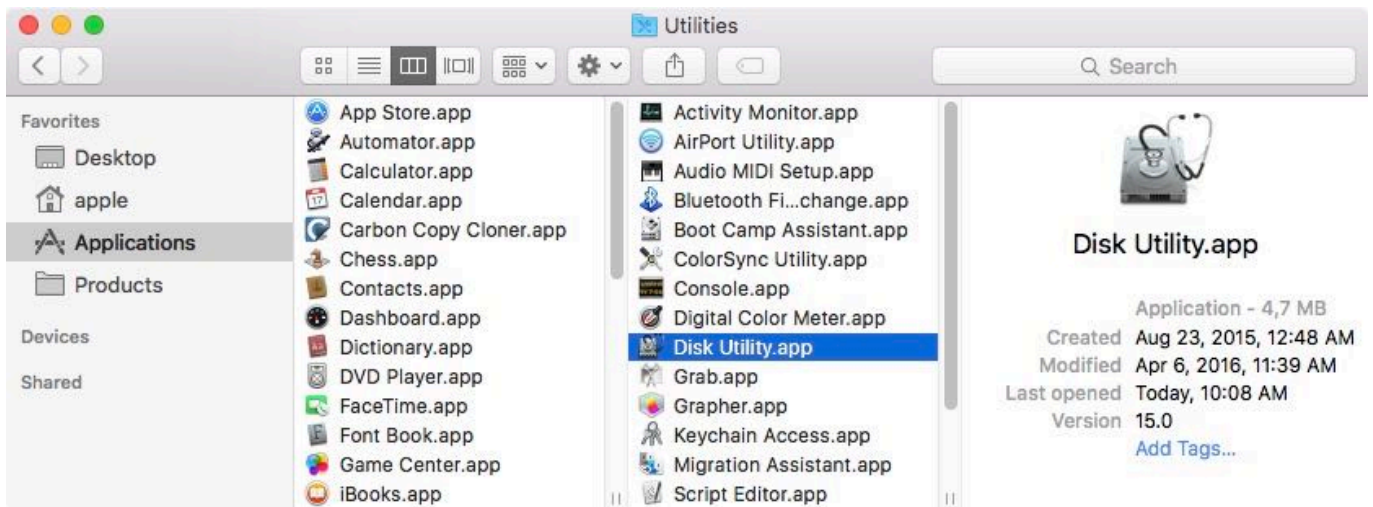
Western Digital MyCloud Home: The "Home" model of this NAS device requires the use of WD-proprietary software to access the storage securely; direct access to the storage via SMB is only available with Guest privileges. [Users report <https://community.wd.com/t/use-my-cloud-home-with-finder-without-wds-app/216769/4>](https://community.wd.com/t/use-my-cloud-home-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 your destination disk for an installation of macOS

Note: This will erase all data on the specified disk

Launch Apple's Disk Utility

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



The remaining steps vary considerably depending on the operating system you are running. Choose **About This Mac** from the Apple menu to determine your current OS, then make a selection below.

- [macOS 11 Big Sur, 10.15 Catalina, 10.14 Mojave, and 10.13 High Sierra](#)
- [macOS 10.12 Sierra and OS X 10.11 El Capitan](#)
- [OS X 10.10 Yosemite](#)

Instructions for Big Sur, Catalina, Mojave, and High Sierra

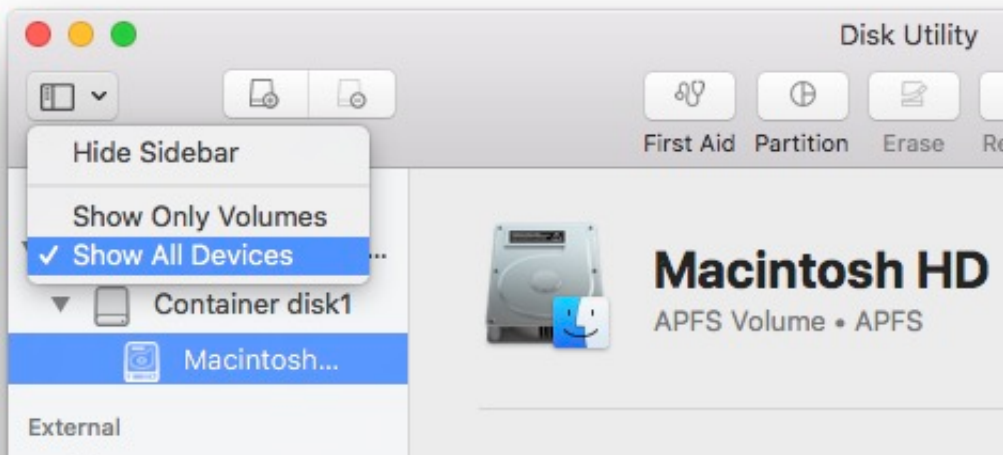
Watch a video of this tutorial on YouTube <https://youtu.be/n_arMTq3d58>

Watch a longer, in-depth tutorial about using Disk Utility

<<https://www.youtube.com/watch?v=oEfqMf2z9k>>

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 task. This disk should not be the same as your startup disk.

The name of a new disk will often include the manufacturer's name (e.g. WD My Book 111D Media...). A startup disk will often include the manufacturer's serial number in the title (e.g. TOSHIBA MK50...). 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. If your disk is a Fusion device, you may erase the "container" within it instead.



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 on 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 set the Scheme to **GUID Partition Map**. If you do not see the **Scheme** option, 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

If your destination device is an HDD with a rotational speed of 5400RPM (or slower): (e.g. "Slim" backup devices, 2.5" disks) **APFS is not designed for these devices** <<http://bombich.com/blog/2019/09/12/analysis-apfs-enumeration-performance-on-rotational-hard-drives>>, **macOS boot performance may be poor** <<http://bombich.com/kb/ccc5/help-my-clone-wont-boot#performance>>. You can format these devices as APFS and try to make a bootable backup, but if the performance of the device is too slow to be practical, then we recommend you choose **Mac OS Extended (Journaled)** for the format. If you are making a backup of a Big Sur or Catalina startup disk, you should **create a Data-only backup** <http://bombich.com/kb/ccc5/frequently-asked-questions-about-ccc-and-macos-catalina#encrypted_non_bootable> to avoid the conversion of the destination filesystem to APFS.

Big Sur, Catalina, and Mojave: Choose **APFS** if you are backing up your startup disk or another installation of macOS. **Do not choose APFS Encrypted**. You can encrypt your backup by **enabling FileVault while booted from the backup volume** <<http://bombich.com/kb/ccc5/working-filevault-encryption>>.

High Sierra: both **APFS** and **Mac OS Extended (Journaled)** are acceptable formats for a backup of the system. **Mirroring Apple's recommendations** <<https://support.apple.com/en-us/HT208033>>, we recommend that you choose **APFS** if your destination device is an SSD and will be used to back up macOS, or if you are backing up a T2-based Mac and you intend to enable encryption on the backup. Choose **Mac OS Extended (Journaled)** if your destination device is a spinning-platter-based device (i.e. a hard disk drive, or HDD), or if you are backing up an operating system older than 10.13.

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.

Your new hard drive is now ready to accept backups created by Carbon Copy Cloner!

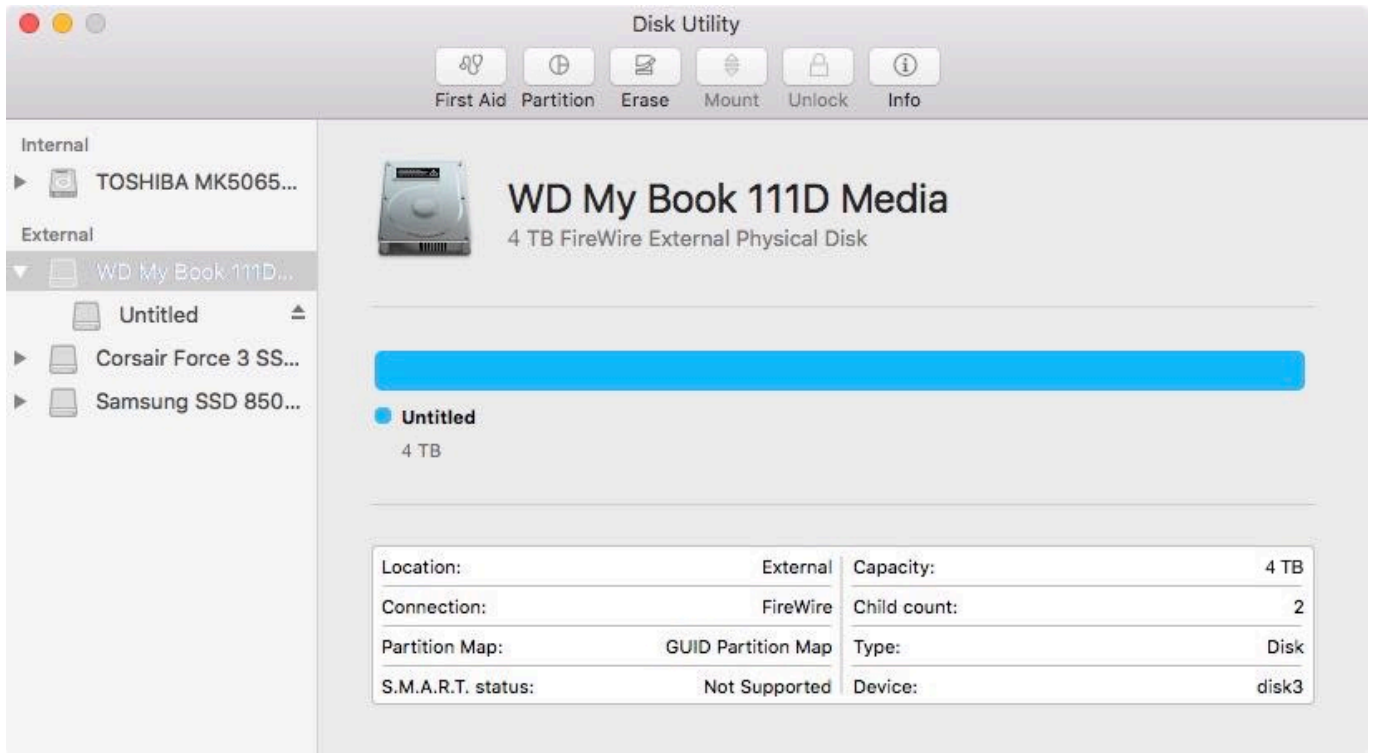
Instructions for El Capitan and Sierra

Watch a video of this tutorial on YouTube <<https://www.youtube.com/watch?v=3AUXkwaVVFQ>>

Select the destination disk

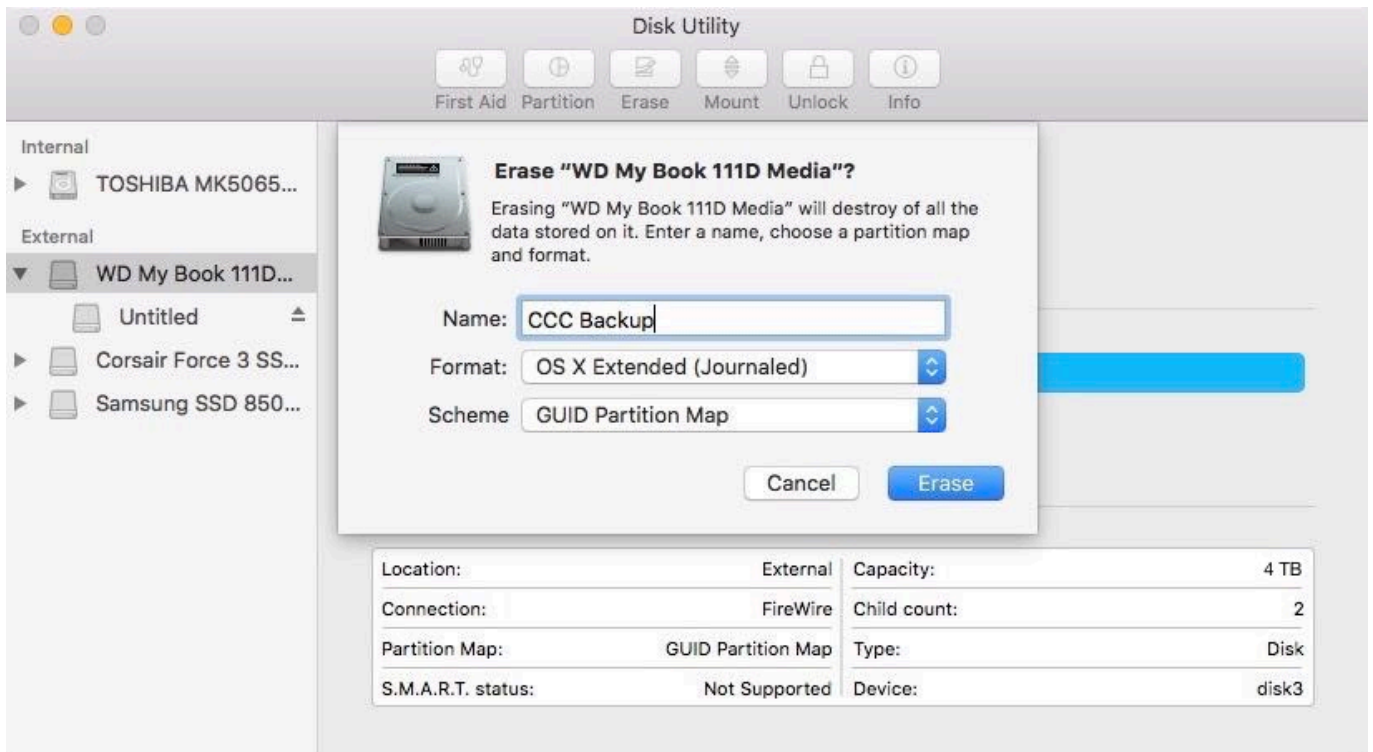
Click to select the disk that you would like to use as the destination for your CCC task. This disk should not be the same as your startup disk.

The name of a new disk will often include the manufacturer's name (e.g. WD My Book 111D Media...). A startup disk will often include the manufacturer's serial number in the title (e.g. TOSHIBA MK50...).



Erase the specified disk

Click on 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 set the Format to **Mac OS Extended (Journaled)** and set the Scheme to **GUID Partition Map**, then click the **Erase** button.



Don't Use 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. 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 to accept backups created by Carbon Copy Cloner!

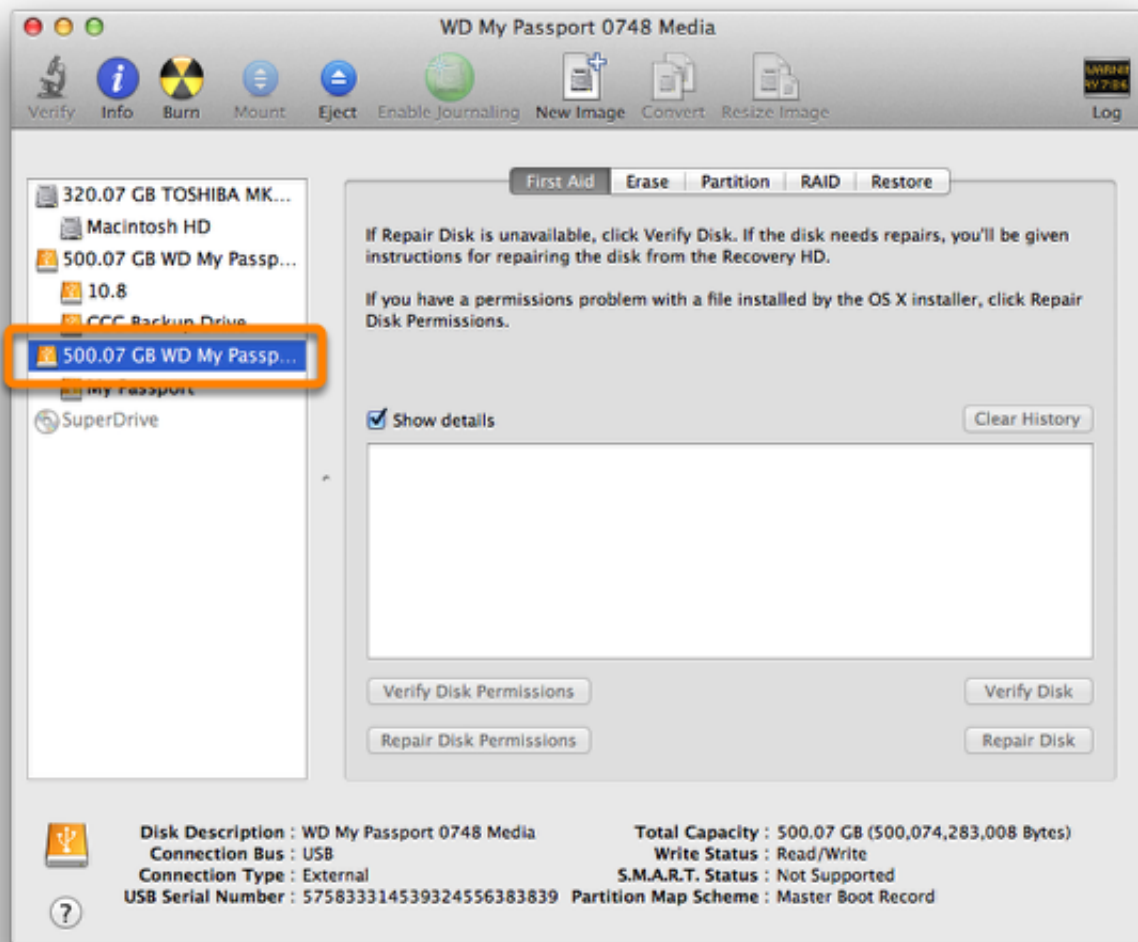
Instructions for Yosemite

Watch a video of this tutorial on YouTube <<https://www.youtube.com/watch?v=WZ1sstRdWjk>>

Select the destination disk

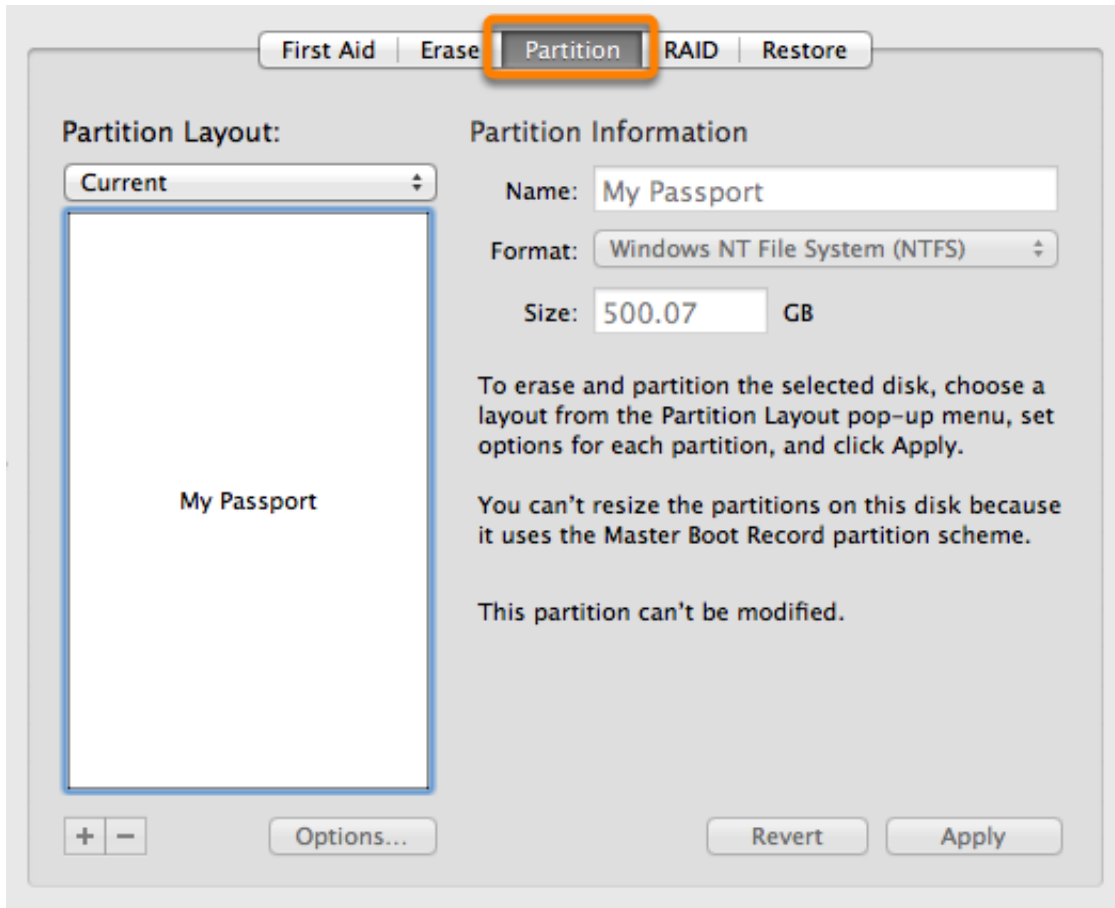
Click to select the disk that you would like to use as the destination for your CCC task. This disk should not be the same as your startup disk.

The name of a new disk will often include the storage capacity and manufacturer's name (e.g. 500.07 GB WD My Passp...). A startup disk will often include the manufacturer's serial number in the title (e.g. 320.07 GB TOSHIBA **MK3255GSXF** Media).

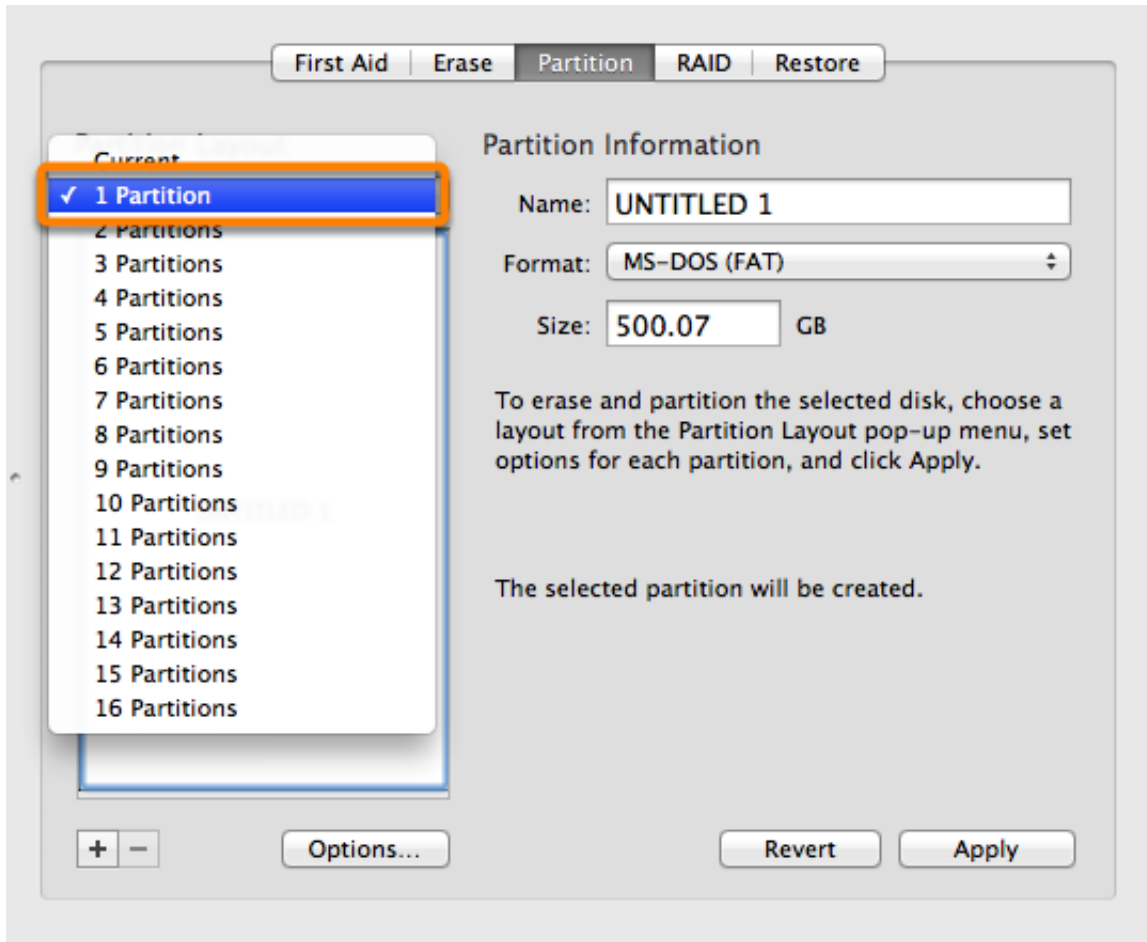


Partition the disk

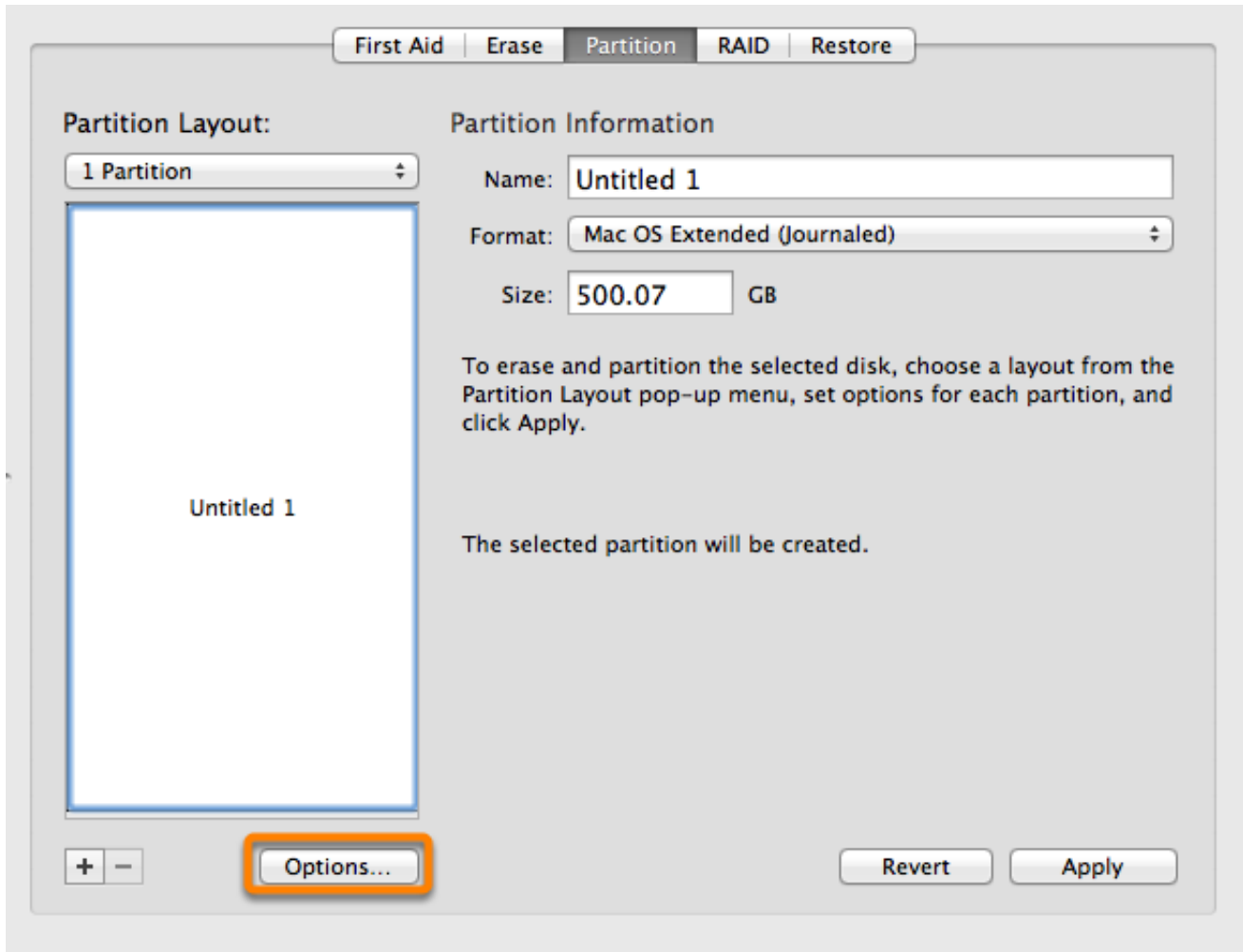
Click on the **Partition** tab.



Choose **1 Partition** from the Partition Layout popup menu (or more if desired).



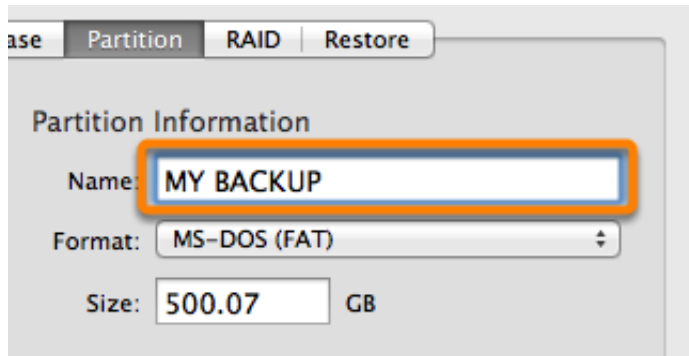
Click on **Options**.



Choose **GUID Partition Table**, then click the **OK**.

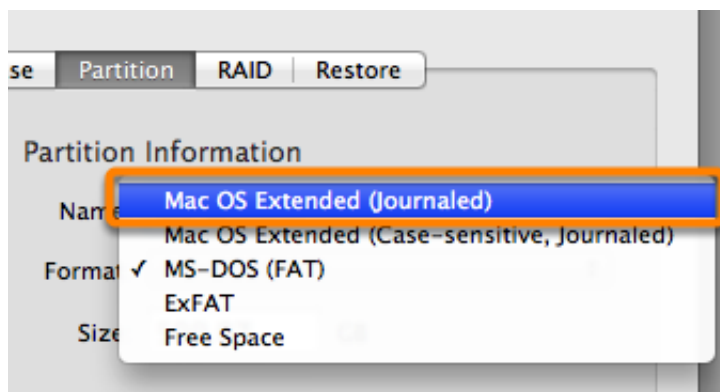


Name the Volume

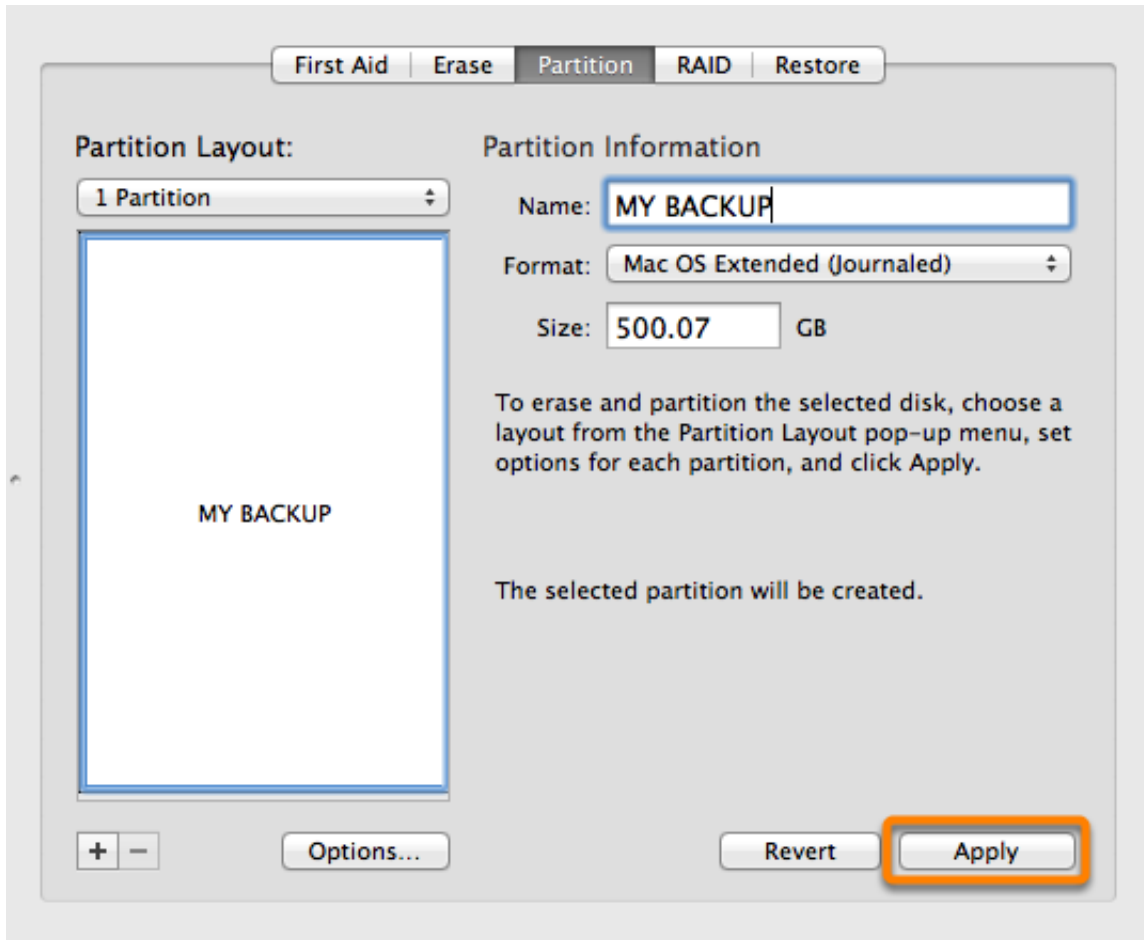


Format the Volume

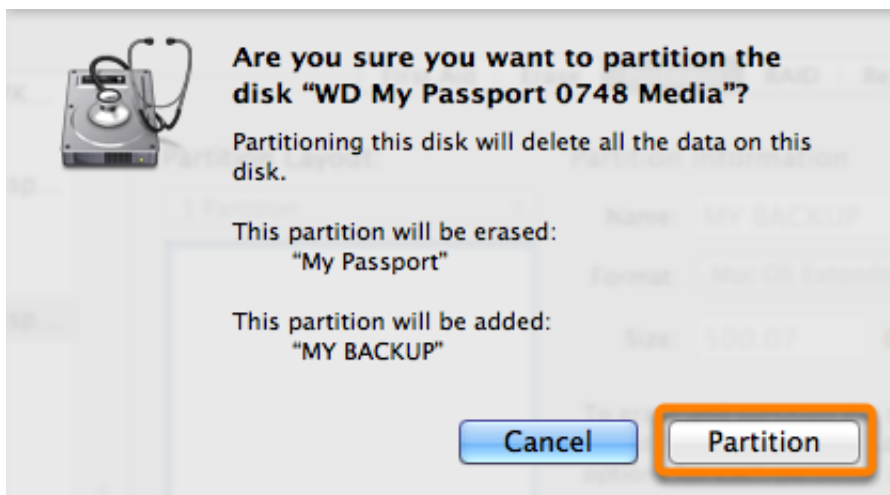
Select **Mac OS Extended (Journaled)** from the Partition Format popup menu.



Click **Apply**.



Ensure that you have selected the correct disk. This step will delete all data from the selected disk. Click **Partition**.



Now [skip ahead to the remainder of the instructions](#) that are not OS-specific.

Related Documentation

- "My disk is already formatted HFS+, why am I getting this warning?"
<<http://bombich.com/kb/cc5/my-disk-already-formatted-hfs-why-am-i-getting-warning>>
- Video: Creating a new/additional partition (OS X 10.10 and earlier)



<<https://www.youtube.com/watch?v=XQG6-Ojiv3s>>

- Support for third party filesystems (e.g. NTFS, FAT32) <<http://bombich.com/kb/ccc5/backing-up-tofrom-network-volumes-and-other-non-hfs-volumes>>

Best practices for updating 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](http://bombich.com/software/download_ccc.php?v=latest) <http://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 offer the thrill of 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 it's **impossible to downgrade to a previous OS**. Unless, that is, you have a complete, bootable backup of your Mac made before you upgrade.

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](http://bombich.com/kb/ccc5/best-practices-updating-your-macs-os#downgrade) <<http://bombich.com/kb/ccc5/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.

Make your bootable backup before upgrading

1. Get a backup disk. If you would like a recommendation, we offer some [here in CCC's documentation](http://bombich.com/kb/ccc5/how-set-up-your-first-backup) <<http://bombich.com/kb/ccc5/how-set-up-your-first-backup>>.
2. Prepare your backup volume for an installation of macOS <<http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x>>.
3. Download CCC <http://bombich.com/software/download_ccc> and fire it up.
4. Choose your startup disk in the Source selector.
5. Choose your backup volume in the Destination selector.
6. Click the Clone button.
7. Test that your backup drive is bootable <<http://bombich.com/kb/ccc5/how-verify-or-test-your->

backup>: Select the backup disk as the startup disk in the Startup Disk Preference Pane in the System Preferences application, then restart.

8. Choose **About This Mac** from the Apple menu to verify that your Mac booted from the backup disk.
9. Reset the startup disk selection in the System Preferences application to your production startup disk and restart.
10. **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.

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. 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.

If you have to downgrade, here's what you need to do

[Downgrading from macOS Catalina \(or Big Sur\) to macOS Mojave \(or an older OS\)](#)

<https://youtu.be/aBjk5ghQPFw>

[Downgrading from High Sierra \(or Mojave\) to Sierra using a CCC bootable backup](#)

<https://youtu.be/UMvSfDTaLWY?t=9m44s>

Keep in mind that when you open an Apple application on the newer OS (e.g. Mail, Contacts, Calendar, etc.), those applications will immediately and irreversibly upgrade the user data for those applications. You cannot simply reinstall Mojave (for example), then go about your day with the upgraded user data; the Mojave versions of those Apple applications can't use the upgraded data from Catalina. **If you need to downgrade to a previous OS, it is imperative that you have a complete, bootable backup of your Mac as it was prior to the upgrade.**

To effectively restore everything back to a previous version of the OS, do the following:

1. Temporarily disable your CCC backup tasks http://bombich.com/kb/ccc5/monitoring-backup-tasks-ccc-menubar-application#disable_tasks
2. Attach your CCC backup disk to your Mac.
3. Open the Startup Disk preference pane in the System Preferences application.
4. Choose your backup volume as the startup disk, then click on the Restart button.
5. Open Disk Utility
6. Unmount the original (upgraded) startup disk
7. Choose "Show all devices" from the View menu
8. Select the whole disk device that contains your original startup disk — the **parent** of the "Macintosh HD" volume.
9. Click the Erase button in Disk Utility's toolbar
10. If you're downgrading to an OS older than High Sierra or you're restoring to a Fusion device on High Sierra, use the **OS X Extended, Journaled** format. Otherwise, choose **APFS** as the format.
11. Open CCC



12. Select your backup volume from the source selector.
13. Select your original (now empty) OS volume from the destination selector.
14. Stick with the default settings — SafetyNet On.
15. Click the Clone button.

When the restore process has completed, reset your startup disk in the System Preferences application and restart your Mac. You'll be back to your previous OS in no time!

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. Calendar, AddressBook, Mail, Photos, etc.)** while using the newer OS will be [incompatible with an older OS](#) http://bombich.com/images/blog/newer_photos_library_not_backwards_compatible.png, so it is not possible to restore that information.

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

Downgrading without a bootable backup is not a simple task, and may not produce the result you're hoping for. There are some items that the older system applications can't read, e.g. Apple Mail, calendar – basically all of the Apple applications won't be able to use the upgraded data stores. If you're staring at a clean install of the older OS, your best option is to try restoring just your home folder. This is not a configuration that we can offer support for (the supported configuration requires having a pre-upgrade CCC bootable backup), but you can do the following in CCC to restore your home folder:

1. Downgrade your Mac's OS using a [bootable macOS Installer](https://support.apple.com/en-us/HT201372) <https://support.apple.com/en-us/HT201372>
2. Close all applications and all Finder windows
3. Open CCC and create a new task
4. Drag your home folder from the backup disk onto CCC's Source selector
5. Drag your home folder from the current startup disk to CCC's Destination selector
6. Click the **Advanced Settings** button
7. Under the Troubleshooting section, check the box next to **Don't preserve permissions** (this will avoid any ownership issues that would arise from your account having a different numeric ID on the old and new system)
8. Click the Clone button

If you have applications that you want to restore, we recommend restoring them via drag and drop in the Finder, or reinstall them from their installers.

Keep in mind that this is going to replace anything that you currently have in your home folder. If you have already restored items manually, this will undo that, and you may want to consider manually restoring files via drag and drop instead.

Additional Resources

- [Everything you need to know about Carbon Copy Cloner and APFS](http://bombich.com/kb/cc5/everything-you-need-know-about-carbon-copy-cloner-and-apfs) <http://bombich.com/kb/cc5/everything-you-need-know-about-carbon-copy-cloner-and-apfs>
- [Downgrading from macOS Catalina to macOS Mojave](https://youtu.be/aBjk5ghQPFw) <https://youtu.be/aBjk5ghQPFw>
- [Downgrading from High Sierra to Sierra using a CCC bootable backup](https://youtu.be/UMvSfDTaLwY?t=9m44s) <https://youtu.be/UMvSfDTaLwY?t=9m44s>
- [Downgrading an APFS-formatted Fusion volume](https://youtu.be/YeQ0N5izTlo) <https://youtu.be/YeQ0N5izTlo>
- [Preparing your backup volume for an installation of macOS](#)



<http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x>

- [Working with Disk Utility to prepare your CCC backup disk](https://youtu.be/n_arMTq3d58) <https://youtu.be/n_arMTq3d58>
- [Testing your CCC backup](http://bombich.com/kb/ccc5/how-verify-or-test-your-backup) <<http://bombich.com/kb/ccc5/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://www.youtube.com/watch?v=SADf7xp97nE>>

Attach the backup disk to your computer

See the [Choosing a backup drive](http://bombich.com/kb/ccc5/choosing-backup-drive) <<http://bombich.com/kb/ccc5/choosing-backup-drive>> section for additional advice on this subject.

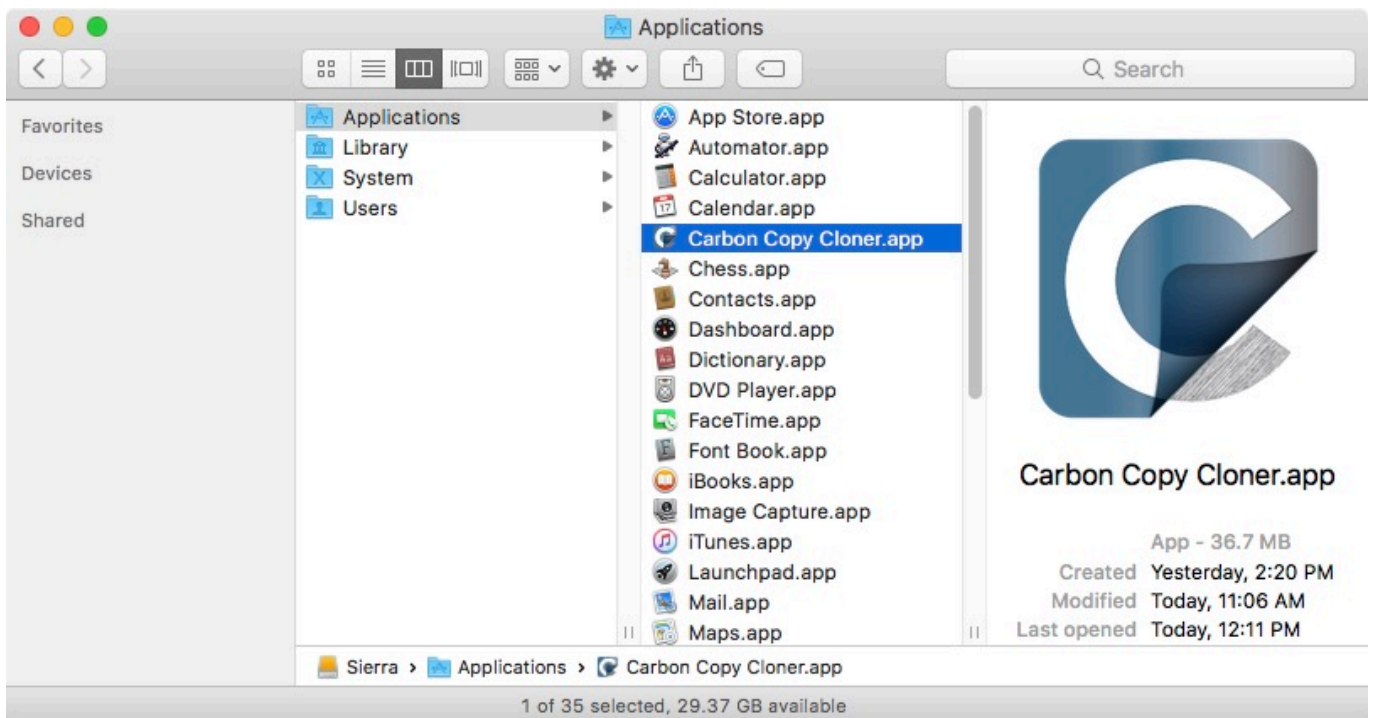
Format the disk

Before you can use a new disk for a backup of macOS, you must first initialize it with the correct format using Disk Utility.

See the [Preparing your backup disk for a backup of macOS](http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x) <<http://bombich.com/kb/ccc5/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://www.youtube.com/watch?v=3AUXkwaVVFQ) <<https://www.youtube.com/watch?v=3AUXkwaVVFQ>>

Open Carbon Copy Cloner

Applications > Carbon Copy Cloner

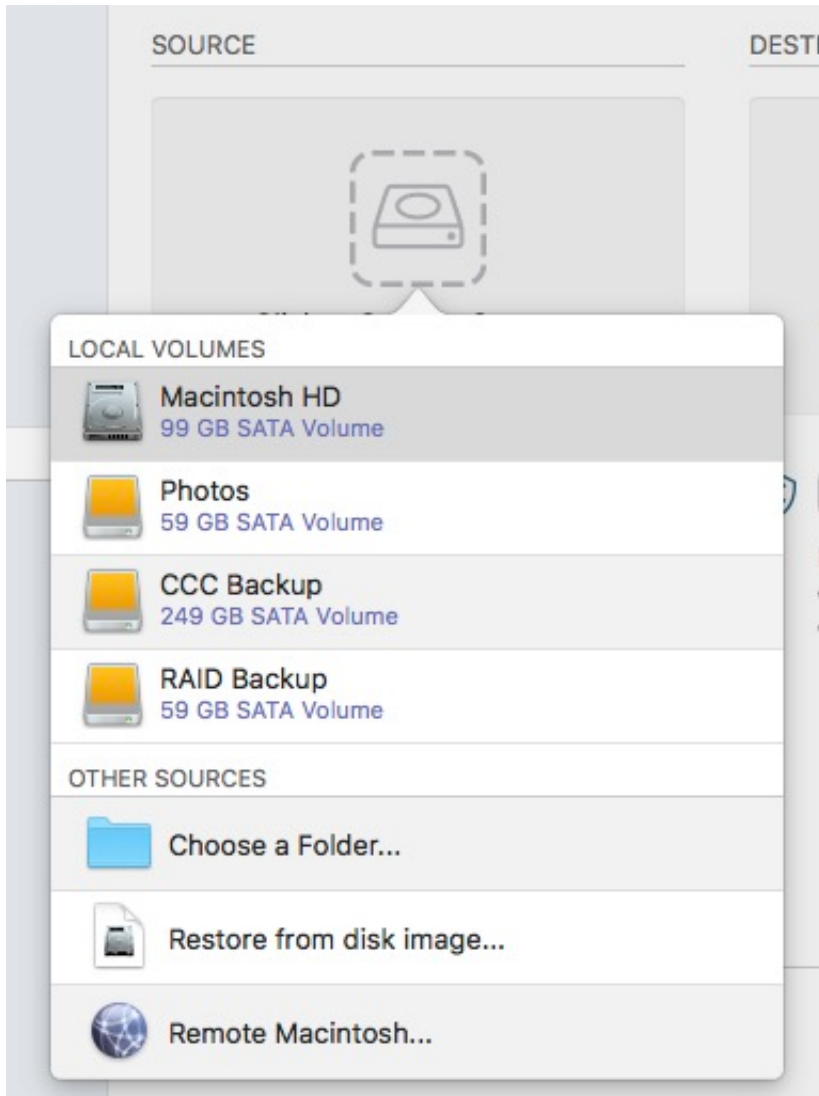


When you open CCC for the first time, you'll be guided through your first task setup. If you prefer to not be guided, click the **Tips** button in CCC's toolbar.

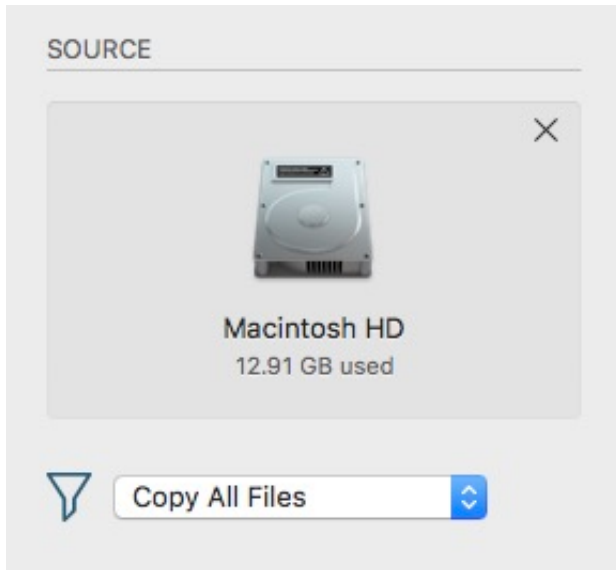
Select the Source

Click on the dotted 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"?](http://bombich.com/kb/ccc5/frequently-asked-questions-about-ccc-and-macos-catalina#separate_tasksCollapse)"

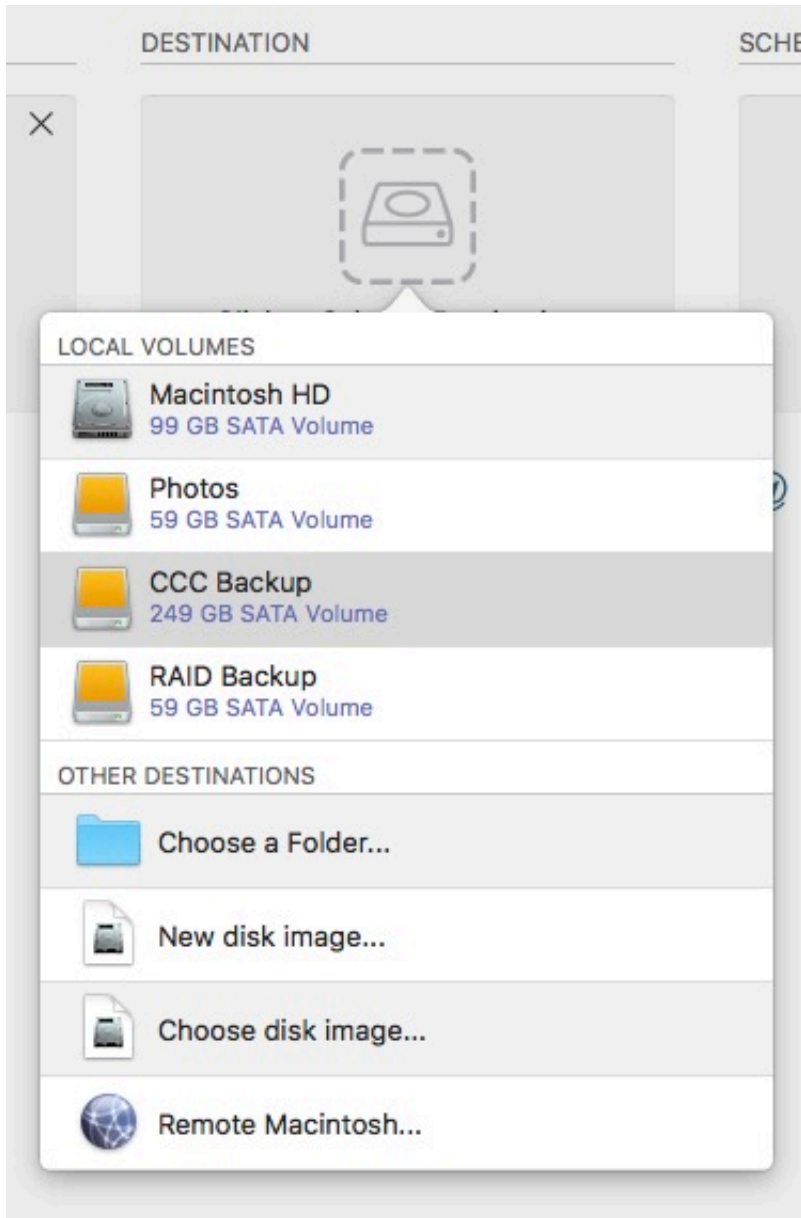


Select your startup disk from the menu of available volumes for the source.



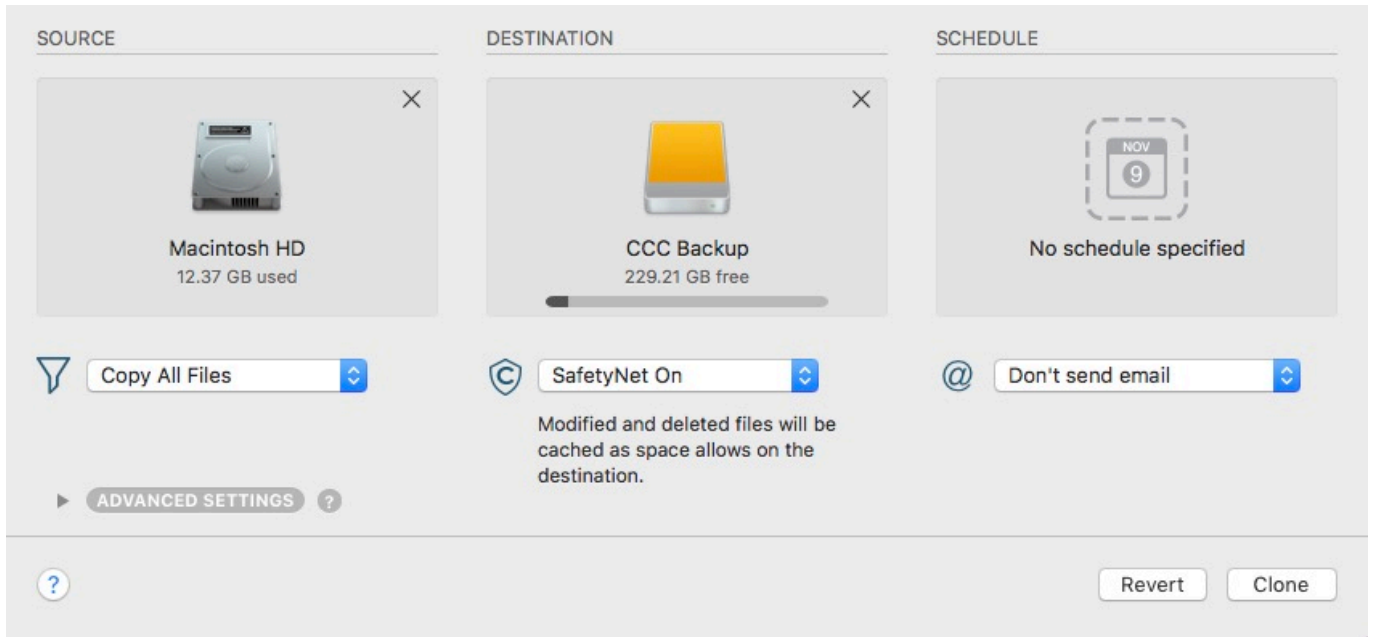
Select the Destination

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



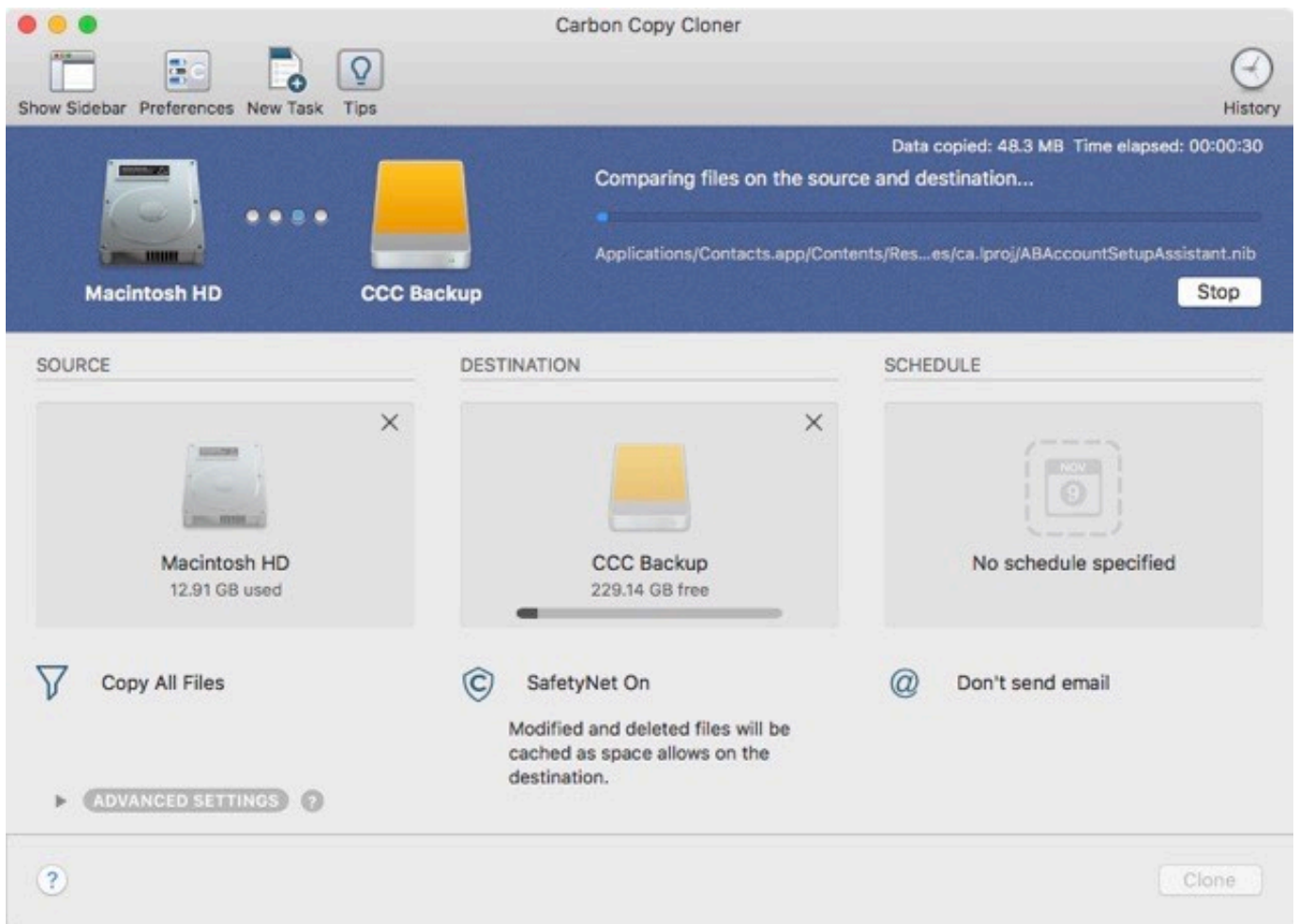
Begin the Clone

Click **Clone**. The first time you run a backup task, CCC will prompt you to authenticate so it can install its privileged helper tool. This helper tool is required to perform privileged tasks, e.g. to copy system files.



The screenshot shows the Carbon Copy Cloner setup interface. It is divided into three main sections: SOURCE, DESTINATION, and SCHEDULE. The SOURCE section shows 'Macintosh HD' with 12.37 GB used. The DESTINATION section shows 'CCC Backup' with 229.21 GB free. The SCHEDULE section shows 'No schedule specified'. Below these sections are three dropdown menus: 'Copy All Files', 'SafetyNet On', and '@ Don't send email'. A note under 'SafetyNet On' states: 'Modified and deleted files will be cached as space allows on the destination.' At the bottom, there is a 'Revert' button and a 'Clone' button.

Congratulations - your first clone is in progress!



The screenshot shows the Carbon Copy Cloner application window during a cloning process. The title bar reads 'Carbon Copy Cloner'. The top menu bar includes 'Show Sidebar', 'Preferences', 'New Task', and 'Tips'. The main area shows a progress bar and the text 'Comparing files on the source and destination...'. Below this, it shows 'Macintosh HD' and 'CCC Backup' with a 'Stop' button. The bottom section shows the same setup as the previous screenshot, but with a 'Clone' button instead of 'Revert' and 'Clone'. The progress bar shows 'Data copied: 48.3 MB' and 'Time elapsed: 00:00:30'. The file path 'Applications/Contacts.app/Contents/Res...es/ca.lproj/ABAccountSetupAssistant.nib' is visible.

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 Clone button again or configure your backup task to [run automatically on a scheduled basis <http://bombich.com/kb/ccc5/how-set-up-scheduled-backup>](http://bombich.com/kb/ccc5/how-set-up-scheduled-backup).

Related Documentation

- [Cloning macOS System volumes with Apple Software Restore <http://bombich.com/kb/ccc5/cloning-macos-system-volumes-apple-software-restore>](http://bombich.com/kb/ccc5/cloning-macos-system-volumes-apple-software-restore)
- [How to verify or test your backup <http://bombich.com/kb/ccc5/how-verify-or-test-your-backup>](http://bombich.com/kb/ccc5/how-verify-or-test-your-backup)
- [Sample Usage Scenarios <http://bombich.com/kb/tags/sample-usage-scenarios>](http://bombich.com/kb/tags/sample-usage-scenarios)
- [How do I get help? <http://bombich.com/kb/ccc5/how-do-i-get-help>](http://bombich.com/kb/ccc5/how-do-i-get-help)

How to verify or test a bootable backup

Attach the backup disk to your computer

Open the Startup Disk Preferences

System Preferences > Startup Disk

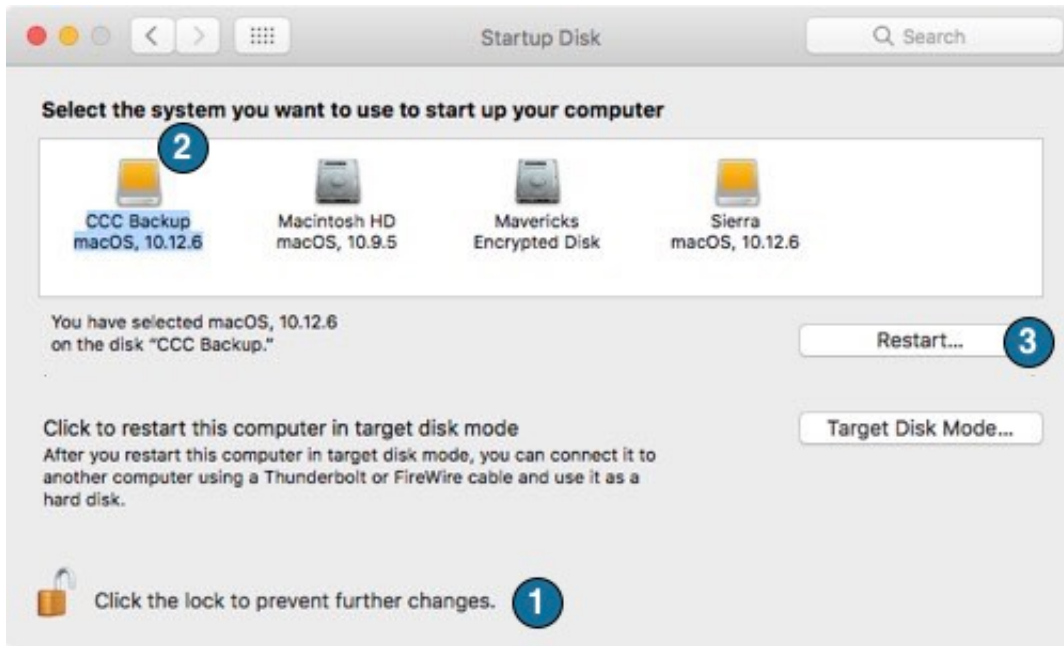


Select the backup volume

After clicking the lock in the lower-left corner, select the backup volume that you would like to verify. Click **Restart**.

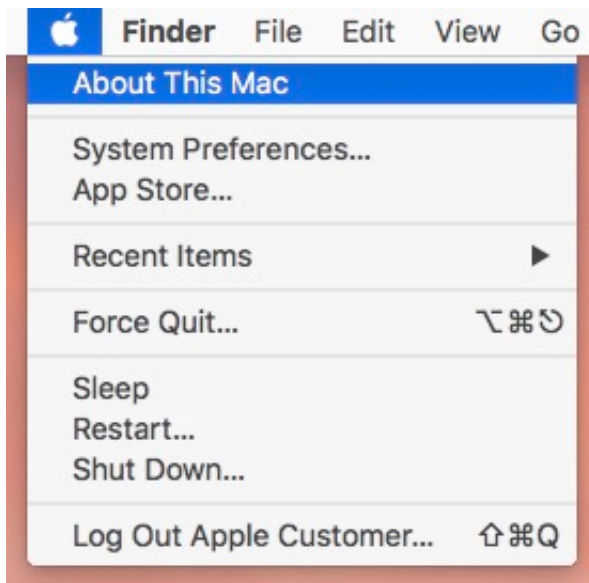
If you do not see your startup disk here, reboot your Mac while holding down the Option key (Intel Macs) or the Power button (Apple Silicon Macs) to choose the startup volume in the Startup Manager.

Some Big Sur startup volumes don't appear in the Startup Disk Preference Pane
<http://bombich.com/kb/cc5/macOS-big-sur-known-issues#startup_disk_pref_pane>



Verify the startup disk

When your Mac has finished restarting, choose **About this Mac...** from the **Apple** menu.



Verify that you are booted from the backup volume.



Test the Backup

Launch a few applications and verify that your data is intact.

Reset the Startup Disk

Reset your startup disk in the Startup Disk preference pane (as described earlier) to your original startup disk, then restart your computer.

Related Documentation

For a more in-depth verification of the integrity of your backup, see the [Advanced Settings](http://bombich.com/kb/ccc5/advanced-settings) <<http://bombich.com/kb/ccc5/advanced-settings>> article to learn more about the **Find and replace corrupted files** option.

- Some applications behave differently or ask for the serial number on the cloned volume. Did CCC miss something? <<http://bombich.com/kb/ccc5/some-applications-behave-differently-or-ask-serial-number-on-cloned-volume.-did-ccc-miss>>
- "The disk usage on the destination doesn't match the source — did CCC miss some files?" <<http://bombich.com/kb/ccc5/disk-usage-on-destination-doesnt-match-source.-did-ccc-miss-some-files>>
- Help! My clone won't boot! <<http://bombich.com/kb/ccc5/help-my-clone-wont-boot>>

How to restore from your backup

Restoring individual items from your backup volume <https://youtu.be/n_7JgLKy_W0> can be done in the Finder via drag and drop – simply find that item on the backup disk, then drag it back to your startup disk. If you're restoring more than a handful of items to your startup disk, configure a [folder-to-folder](http://bombich.com/kb/ccc5/folder-folder-backups) <<http://bombich.com/kb/ccc5/folder-folder-backups>> task to restore specific folders from your backup disk to a specific folder on your startup disk.

If you're trying to restore system files, applications, or perhaps everything from your backup, proceed with the steps below to boot your Mac from the backup disk and then restore your backup disk to your Mac's internal hard drive.

Attach the Backup Disk to Your Macintosh

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

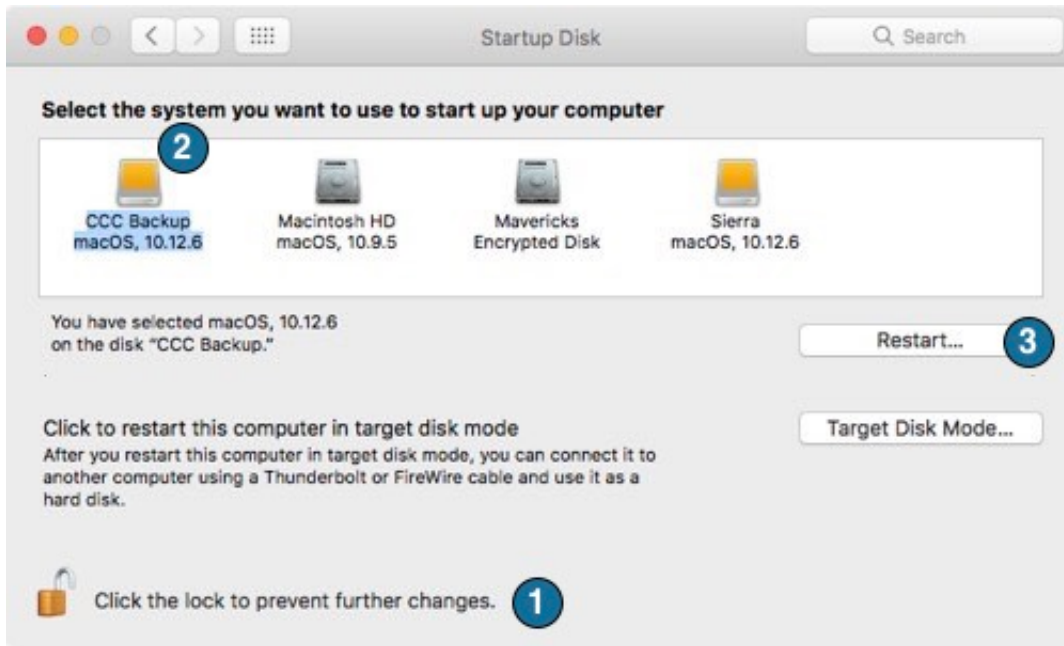
Open the Startup Disk Preference Pane

System Preferences > Startup Disk



Select the Backup Volume

Click the padlock icon at the bottom of the window to authenticate, then select the backup disk that you would like to use to restore. Click **Restart**. This will reboot the system from your backup and allow you to clone the backup onto your main hard drive.



If you are unable to use the Startup Disk Preference Pane...

If you cannot change the startup disk using the Startup Disk Preference Pane (e.g. you are unable to boot from your original hard drive), hold down the Option key (Intel Macs) or the Power button (Apple Silicon Macs) 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>](https://support.apple.com/en-us/HT204417). If you don't see your backup volume listed in the Startup Manager, see the [Help! My clone won't boot! <http://bombich.com/kb/ccc5/help-my-clone-wont-boot>](http://bombich.com/kb/ccc5/help-my-clone-wont-boot) section of CCC's documentation for additional troubleshooting suggestions.

Note: If you cannot boot your Mac from your backup disk, or if you are migrating data to a new Mac, then you can [use Migration Assistant to migrate data from your CCC backup disk <http://bombich.com/kb/ccc5/creating-and-restoring-data-only-backups#migrate>](http://bombich.com/kb/ccc5/creating-and-restoring-data-only-backups#migrate).

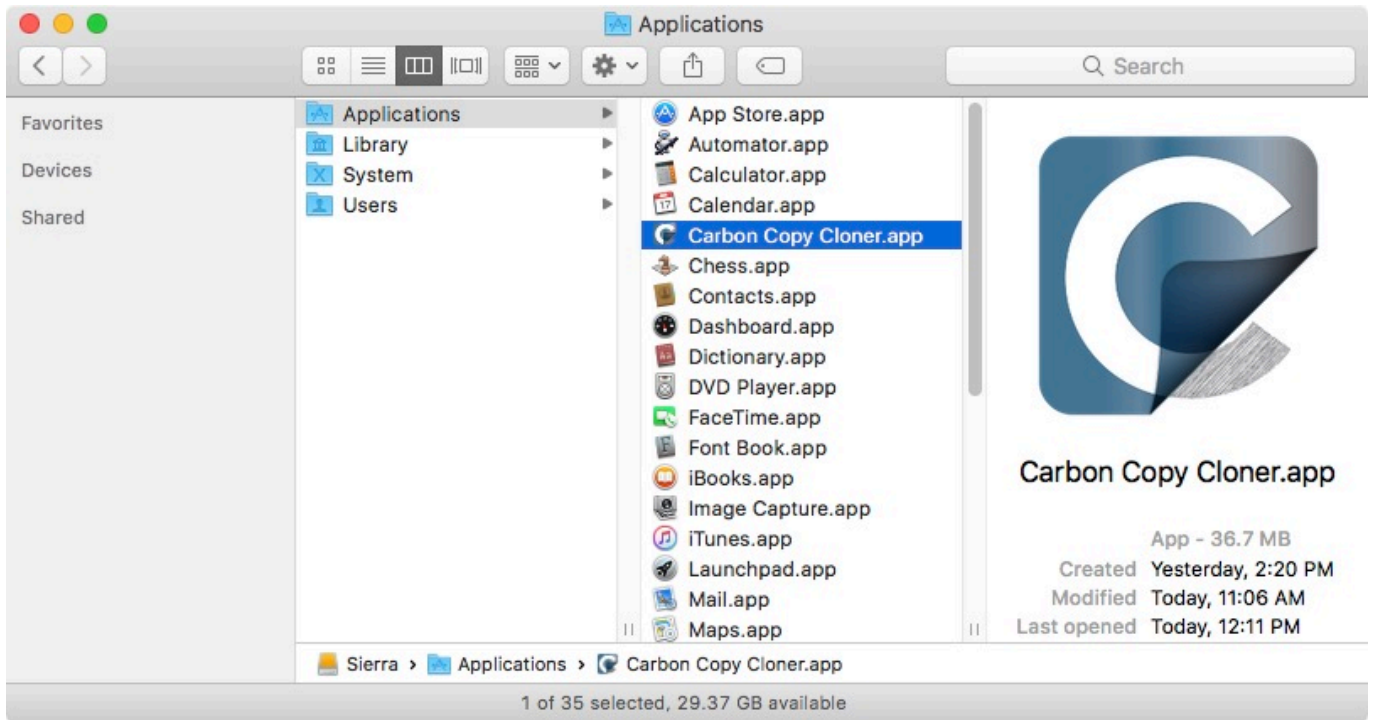
Prepare the disk that you're restoring to

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 OS X <http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x>](http://bombich.com/kb/ccc5/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 macOS High Sierra and later.

Open Carbon Copy Cloner

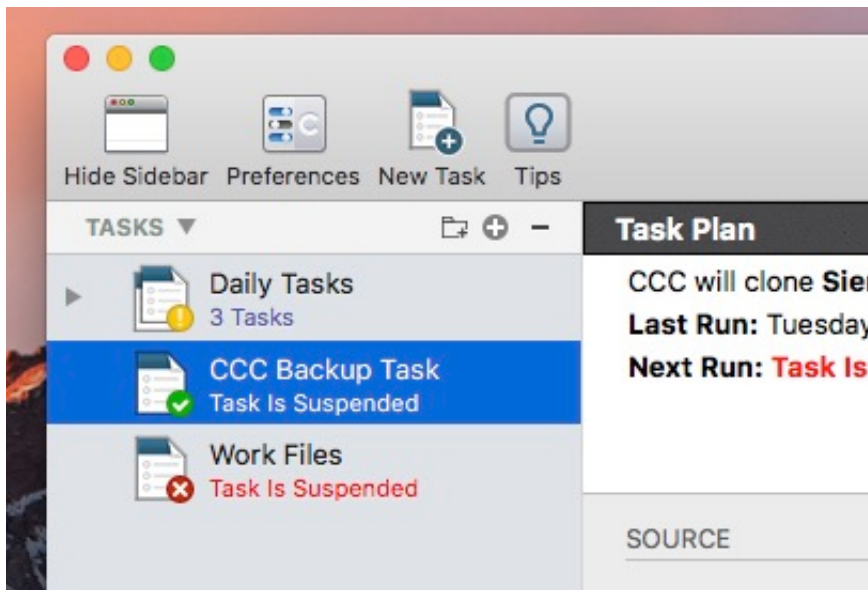
When your Mac has finished restarting, open Carbon Copy Cloner. **Applications > Carbon Copy Cloner**

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.

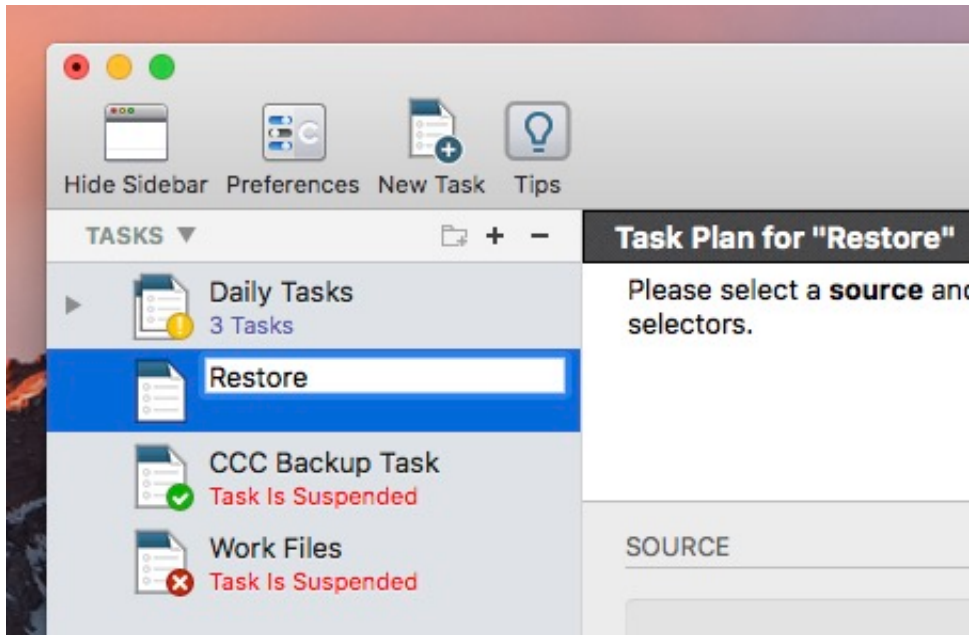


Create a New Task

Click + in the TASKS header. Click **Show Sidebar** if necessary.

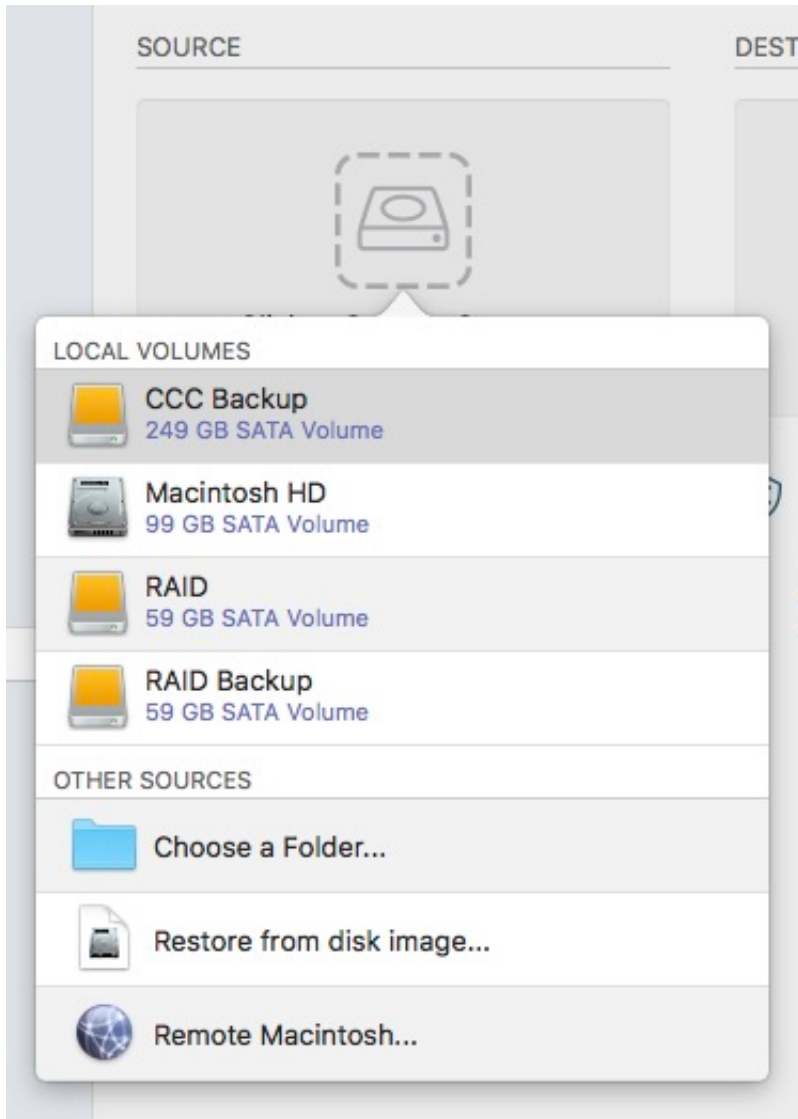


Name the new task.



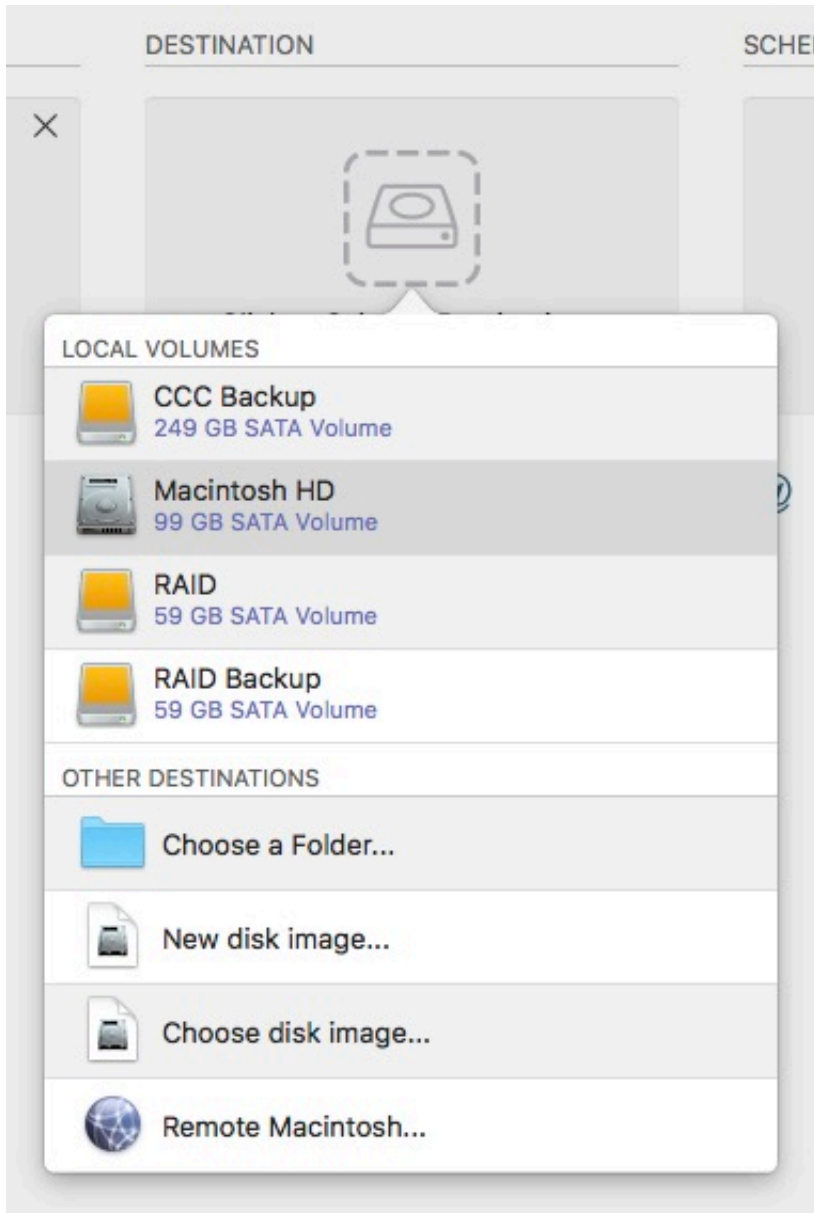
Select the Source

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



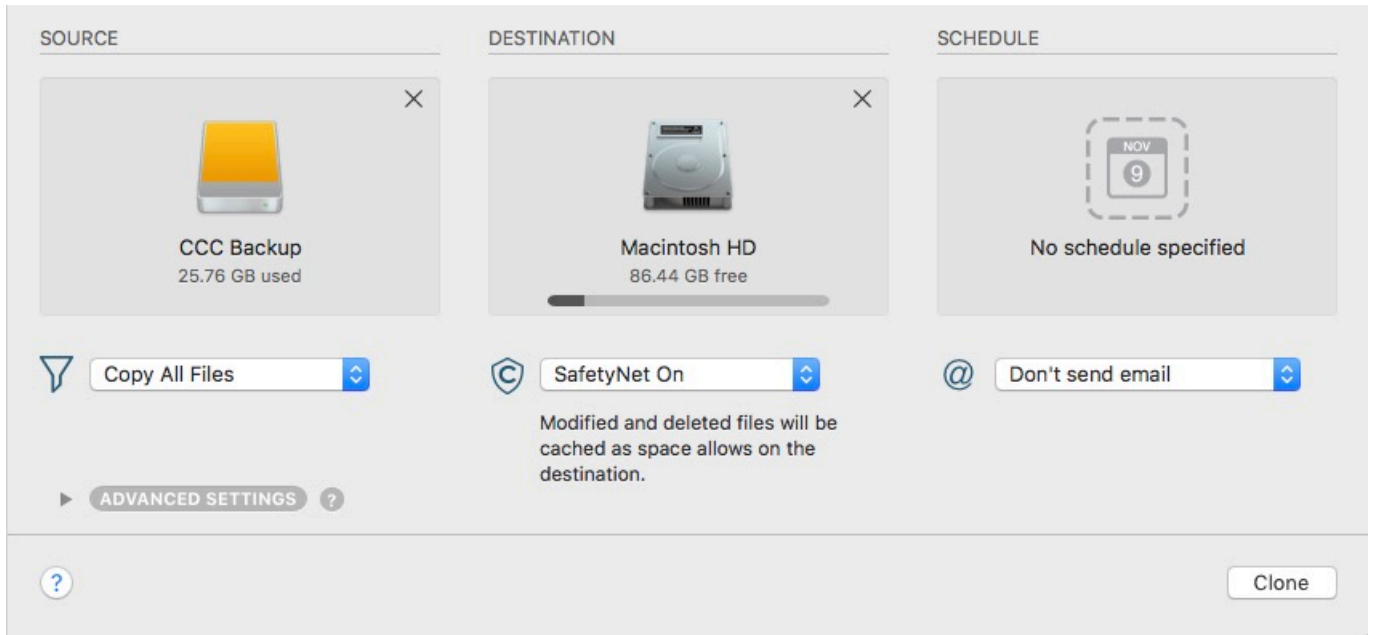
Select the Destination

Click on the **dotted box** under the Destination heading to view available destinations. Click to select the **volume** that you want to restore to.



Click Clone

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



Reset the Startup Disk

After the clone is finished, choose **Startup Disk** from CCC's **Utilities** menu, then reset the startup disk to your original startup disk and restart your computer.

Test the Restoration

Launch a few applications and verify that your data is intact.

Congratulations, you've just restored your data from a backup!

Related Documentation

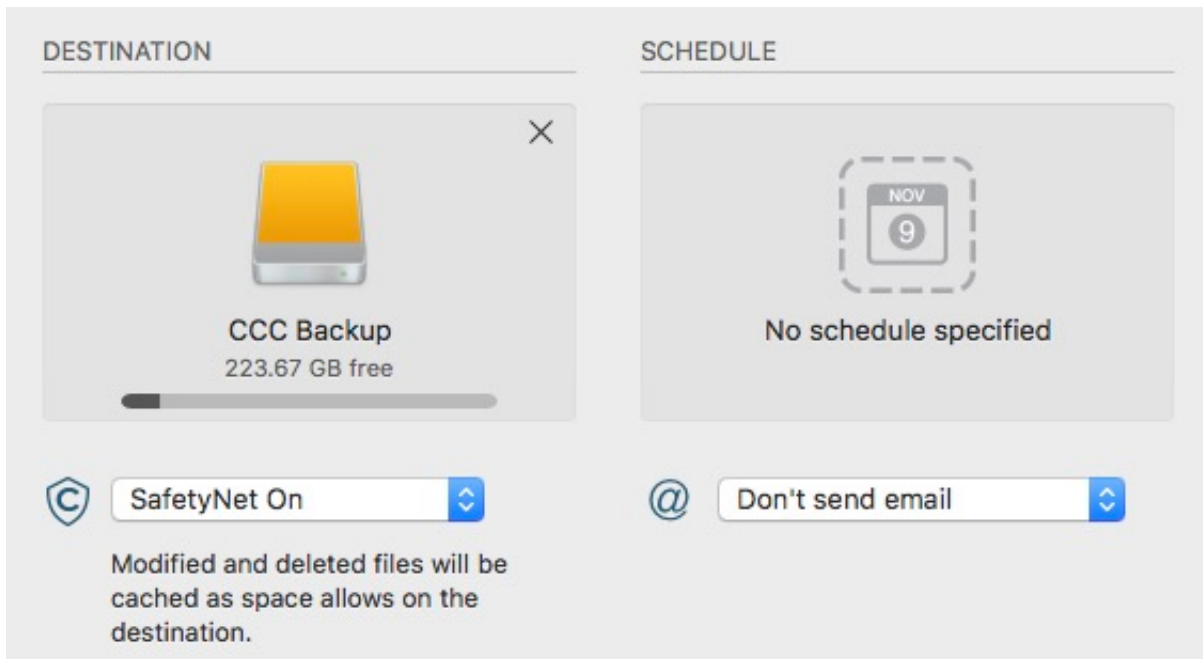
- [Help! My clone won't boot!](http://bombich.com/kb/ccc5/help-my-clone-wont-boot) <<http://bombich.com/kb/ccc5/help-my-clone-wont-boot>>
- [Video: How to restore individual files and folders from your CCC backup](https://youtu.be/n_7JgLY_W0) <https://youtu.be/n_7JgLY_W0>
- [Restoring non-system files](http://bombich.com/kb/ccc5/restoring-non-system-files) <<http://bombich.com/kb/ccc5/restoring-non-system-files>>
- [Restoring from a disk image](http://bombich.com/kb/ccc5/restoring-from-disk-image) <<http://bombich.com/kb/ccc5/restoring-from-disk-image>>
- ["I have a full-volume backup in a folder or a disk image, but I don't have a bootable backup. How can I restore everything?"](http://bombich.com/kb/ccc5/i-have-full-volume-backup-in-folder-or-disk-image-i-dont-have-bootable-backup.-how-can-i) <<http://bombich.com/kb/ccc5/i-have-full-volume-backup-in-folder-or-disk-image-i-dont-have-bootable-backup.-how-can-i>>

How to set up a scheduled backup

Watch a video of this tutorial on YouTube <<https://www.youtube.com/watch?v=IHijbbTiV4>>

Configure the Task

Configure CCC as if you were going to run a backup task immediately, selecting your **Source** and **Destination**. Click the dotted box below the **Schedule** heading to view the scheduling options.



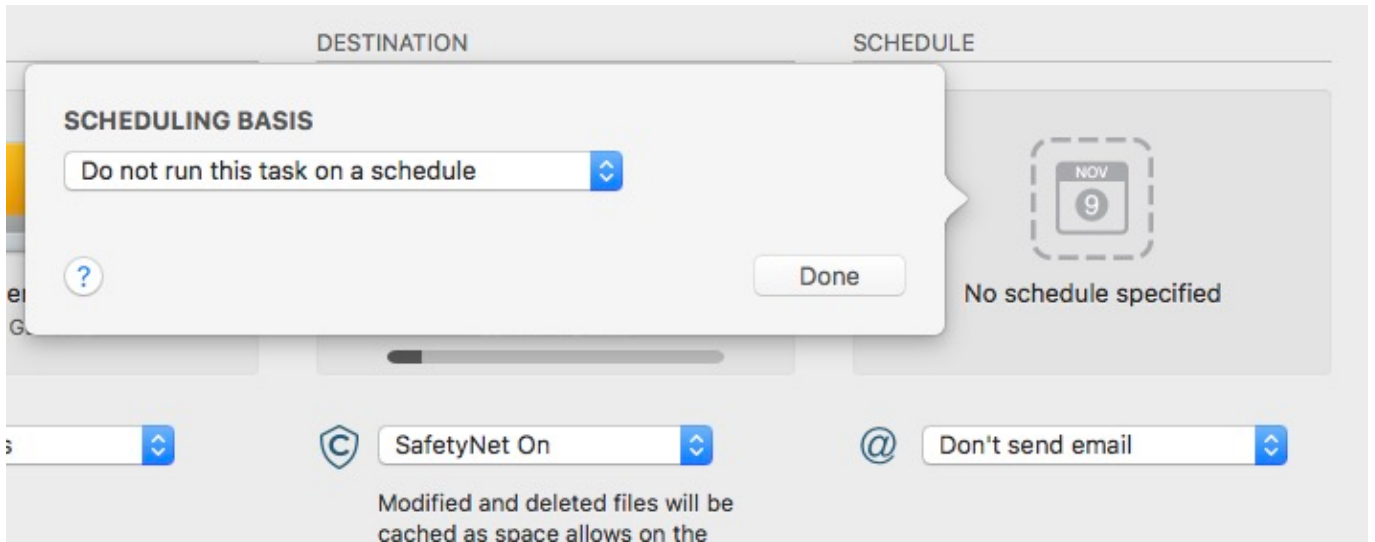
The screenshot shows the configuration window for a backup task. It is divided into two main sections: DESTINATION and SCHEDULE.

DESTINATION: Shows a selected destination named "CCC Backup" with 223.67 GB free space. Below this, there is a "SafetyNet On" toggle switch and a note: "Modified and deleted files will be cached as space allows on the destination."

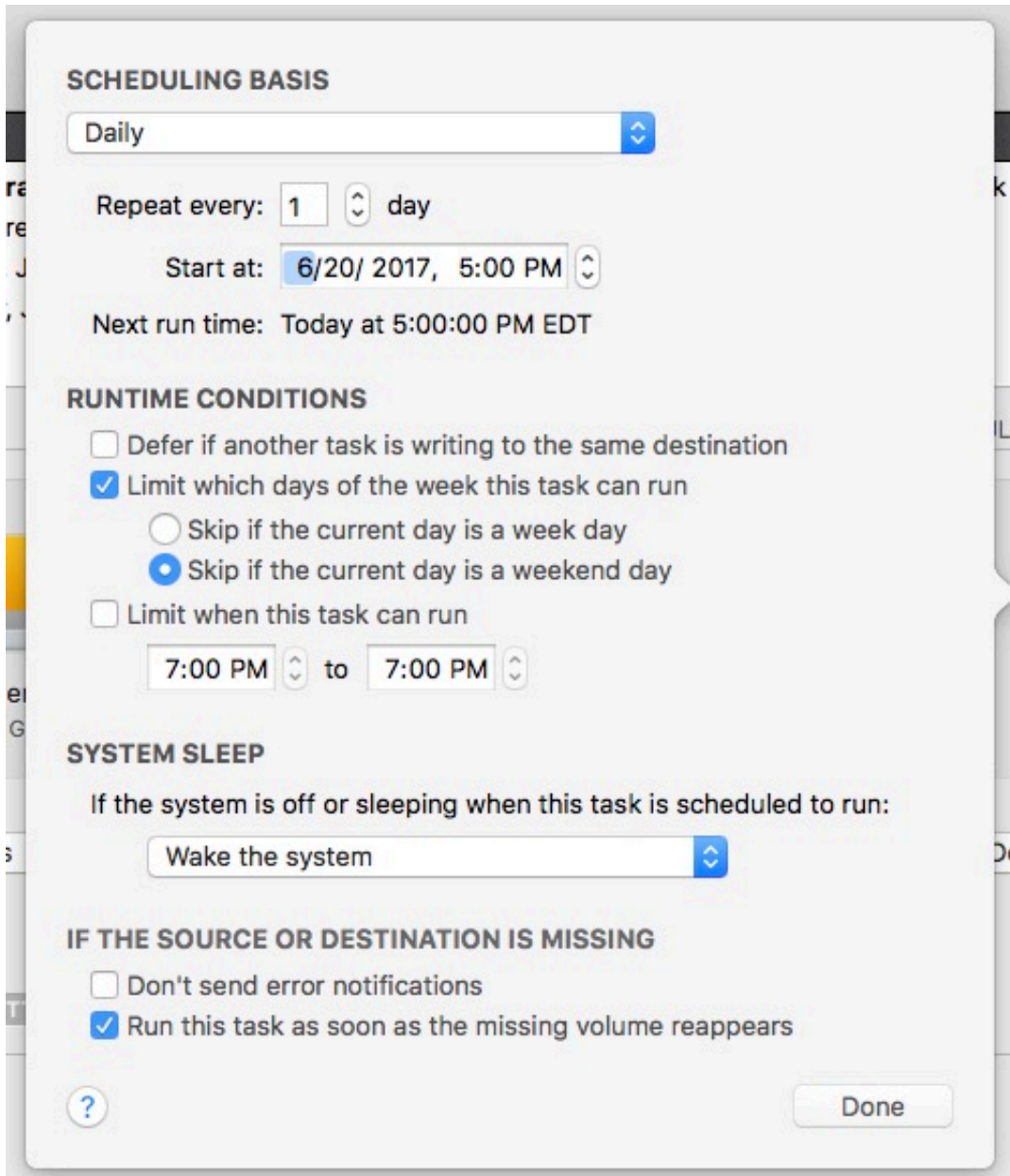
SCHEDULE: Shows a calendar icon with "NOV 9" and the text "No schedule specified". Below this, there is an "@ Don't send email" toggle switch.

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**.



SCHEDULING BASIS

Daily

Repeat every: 1 day

Start at: 6/20/ 2017, 5:00 PM

Next run time: Today at 5:00:00 PM EDT

RUNTIME CONDITIONS

Defer if another task is writing to the same destination

Limit which days of the week this task can run

Skip if the current day is a week day

Skip if the current day is a weekend day

Limit when this task can run

7:00 PM to 7:00 PM

SYSTEM SLEEP

If the system is off or sleeping when this task is scheduled to run:

Wake the system

IF THE SOURCE OR DESTINATION IS MISSING

Don't send error notifications

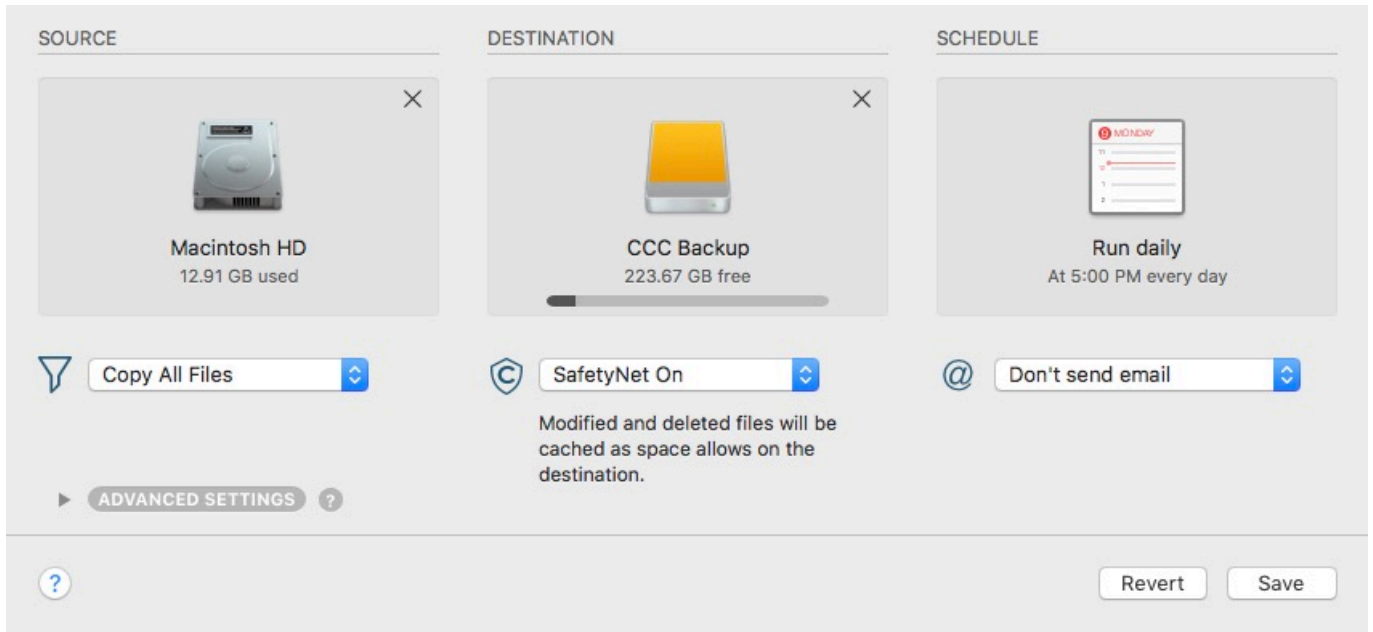
Run this task as soon as the missing volume reappears

?

Done

Save the Task

Click **Save**.



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

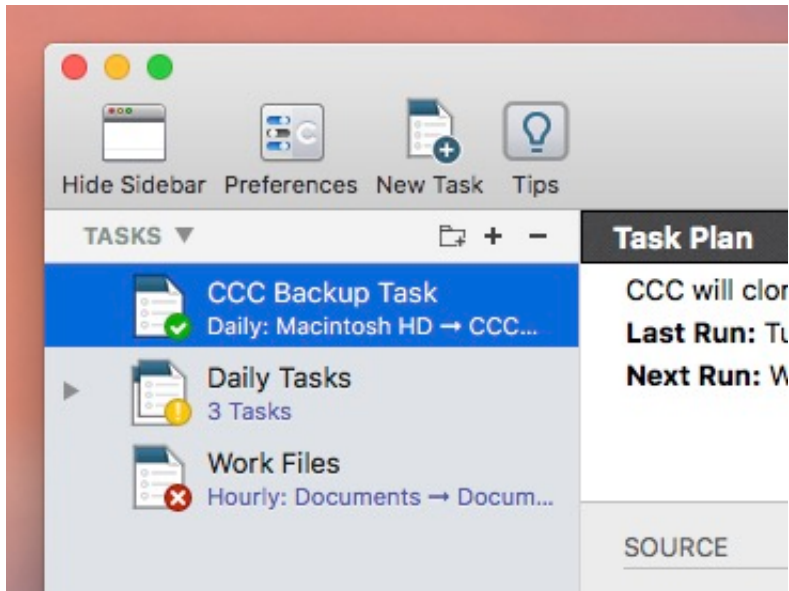
Related Documentation

- [How to modify a scheduled backup <http://bombich.com/kb/cc5/how-modify-scheduled-backup>](http://bombich.com/kb/cc5/how-modify-scheduled-backup)
- [Configuring Scheduled Task Runtime Conditions <http://bombich.com/kb/cc5/configuring-scheduled-task-runtime-conditions>](http://bombich.com/kb/cc5/configuring-scheduled-task-runtime-conditions)

How to modify a scheduled backup

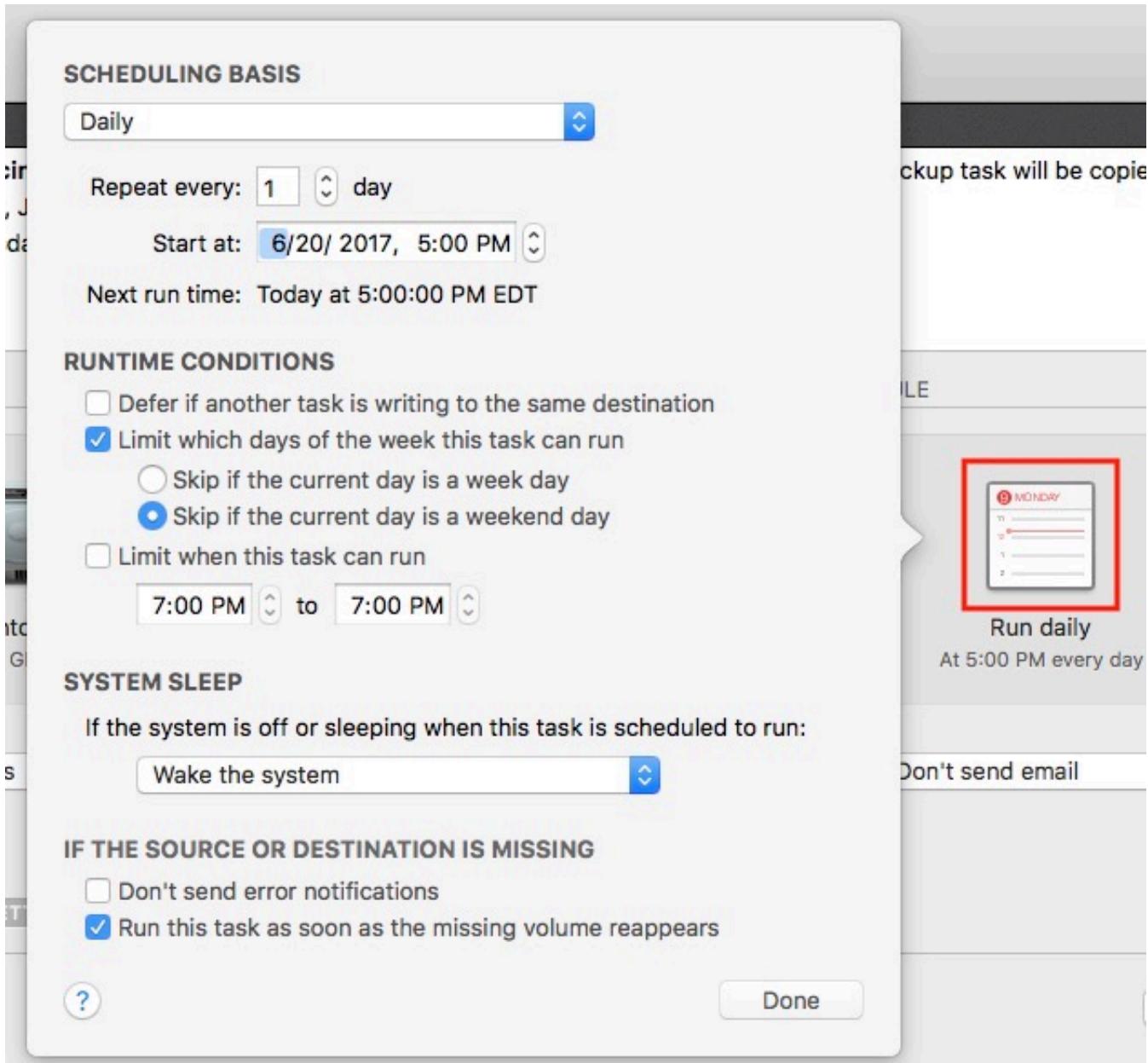
Select the Task

Select the **Task** to be modified. If necessary click **Show Sidebar** to reveal scheduled tasks.

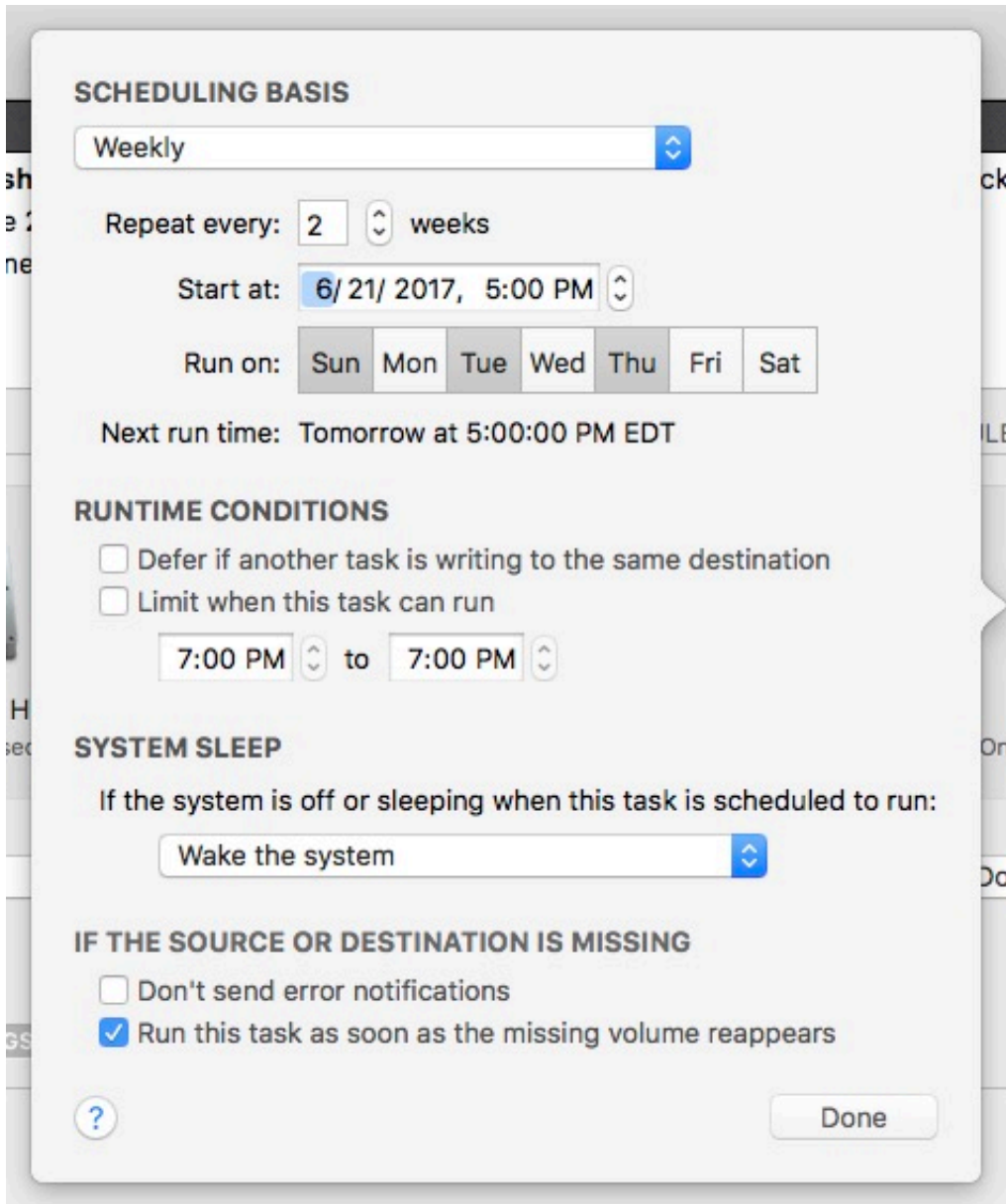


Modify the Schedule

Click the **Schedule Icon**.



Modify the schedule. Click **Done**.



SCHEDULING BASIS

Weekly

Repeat every: 2 weeks

Start at: 6/21/2017, 5:00 PM

Run on: Sun Mon Tue Wed Thu Fri Sat

Next run time: Tomorrow at 5:00:00 PM EDT

RUNTIME CONDITIONS

Defer if another task is writing to the same destination

Limit when this task can run

7:00 PM to 7:00 PM

SYSTEM SLEEP

If the system is off or sleeping when this task is scheduled to run:

Wake the system

IF THE SOURCE OR DESTINATION IS MISSING

Don't send error notifications

Run this task as soon as the missing volume reappears

?


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.

DESTINATION




CCC Backup
223.67 GB free


SCHEDULE



Run weekly
On [Su, Tu, Th] every 2 weeks

 SafetyNet On

Modified and deleted files will be cached as space allows on the destination.

 Don't send email

Revert Save

Your backup will now run according to the new schedule!

Monitoring backup tasks with the CCC menubar application

The Carbon Copy Cloner menubar application

CCC's menubar application gives you quick access to your tasks so that you can quickly determine their status, see which tasks are running, and start, stop, or defer a particular task.



No tasks are running



One or more tasks are running



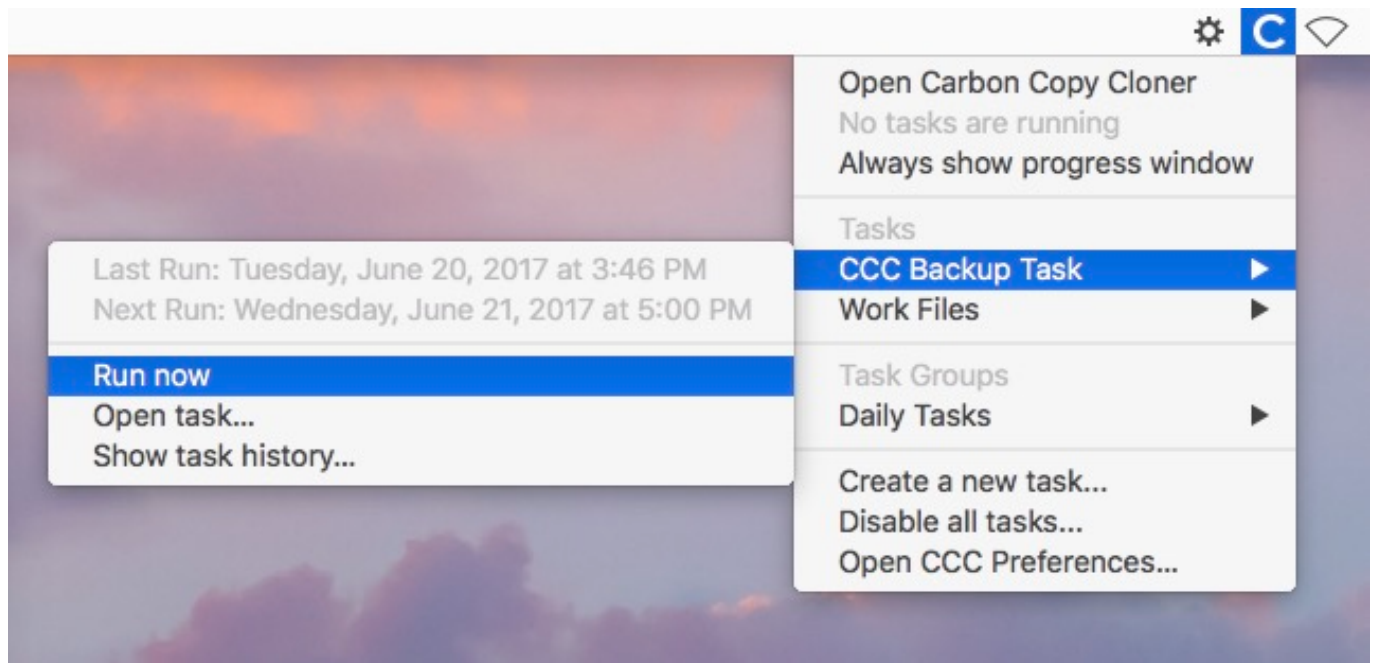
A task requires your attention



All tasks are suspended

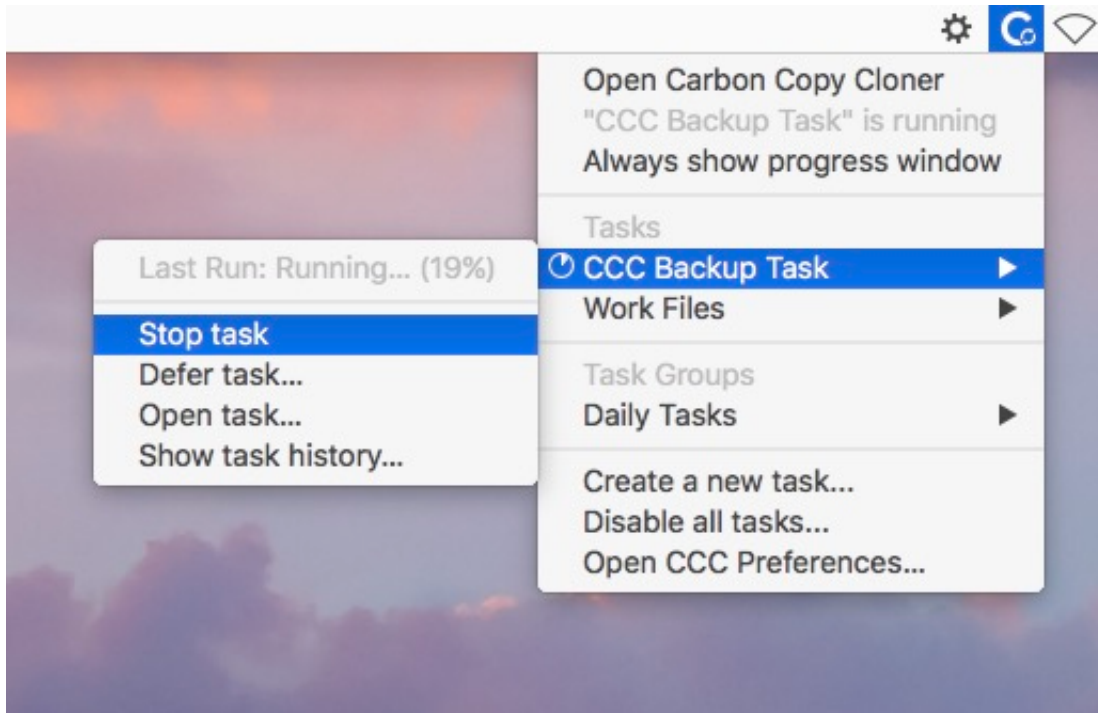
Starting a task

If you would like to run one of your tasks immediately, click on the Carbon Copy Cloner menubar application, then select **Run now** from that task's submenu.



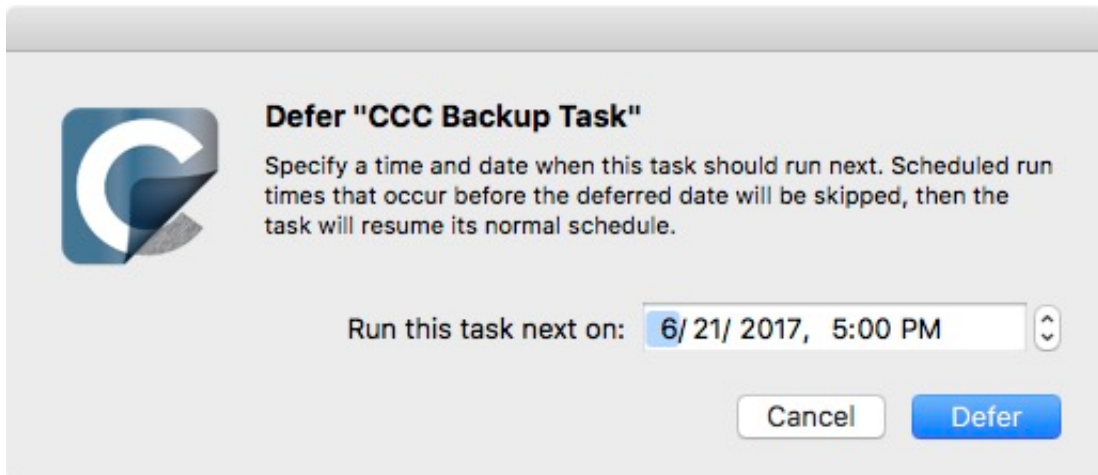
Stopping a task

Occasionally, you may find that one of your scheduled tasks is running at an inconvenient time. Working late? Getting ready to dash off to the airport? Click on the Carbon Copy Cloner menubar application, then select **Stop Task** from the task submenu to stop that task immediately.



Deferring a task

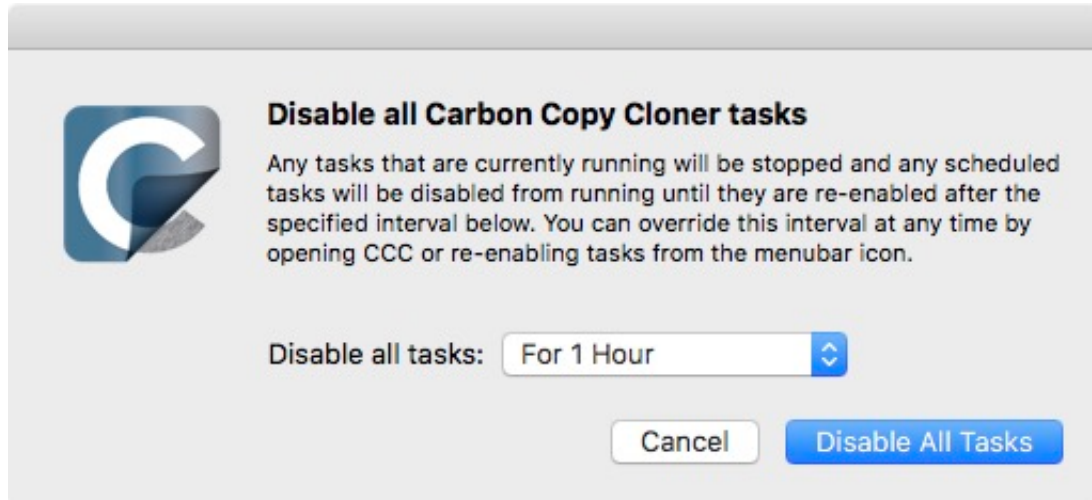
If you want to stop a regularly-scheduled task that is currently running, and also prevent it from running in the near future, you can choose "Defer task" from the Carbon Copy Cloner menubar application. For example, suppose you have taken your laptop with you on vacation, but decided it was safest to leave your backup disk at home. To avoid the daily or hourly indications that your backup volume is unavailable, defer the task until a time that you know your destination disk will be available.



Suspending tasks

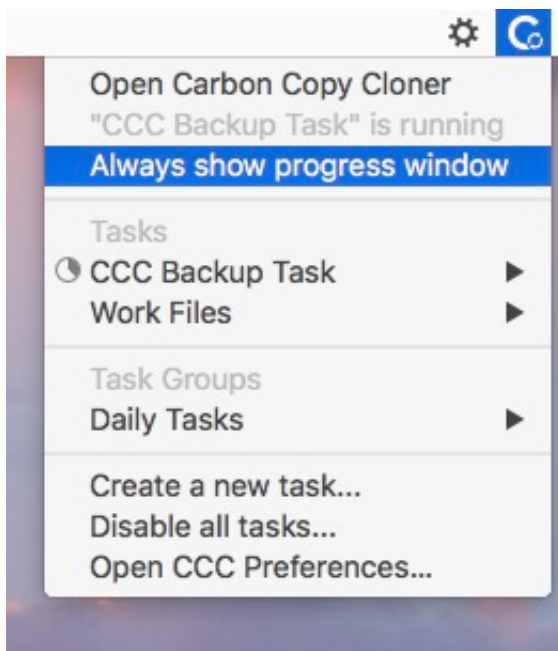
If you would like to suspend all tasks, choose **Suspend all tasks...** from the Carbon Copy Cloner menubar application menu. CCC will offer a list of choices ranging from one hour to one week, and also an option to suspend tasks indefinitely. To re-enable tasks, choose **Re-enable all tasks** from the Carbon Copy Cloner menubar application, or simply open CCC and choose to re-enable tasks when prompted.

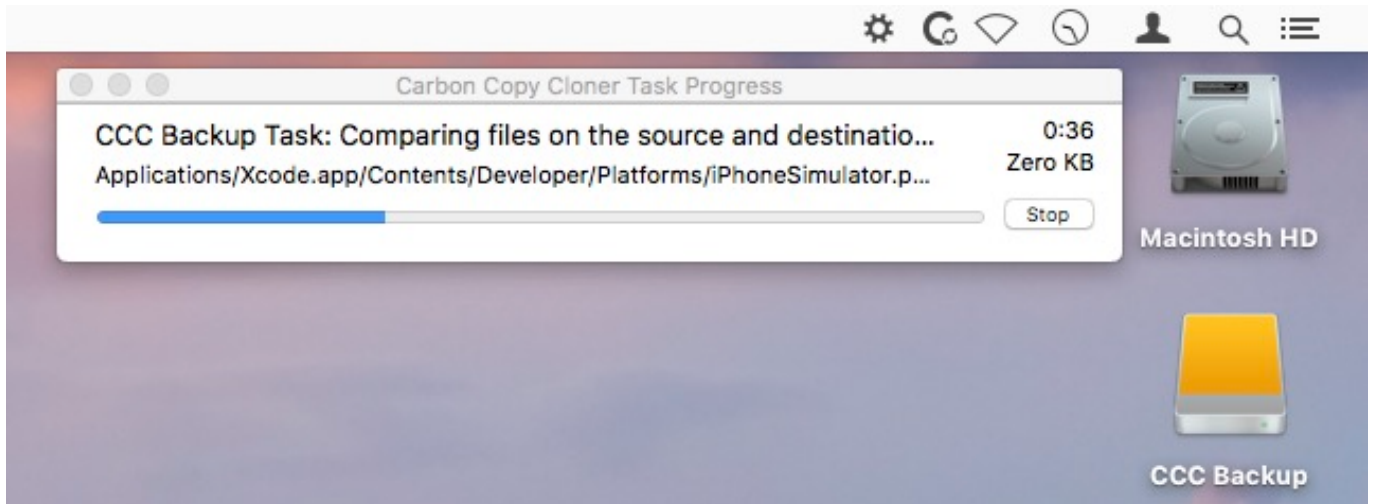
Note: If you would like to **disable** an individual task, choose **Open task...** from the task's submenu. In CCC, right-click on the task you would like to disable and choose the option to disable the task. Note that disabled tasks do not show up in the CCC menubar application list of tasks. Also note 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.



Viewing task progress indication

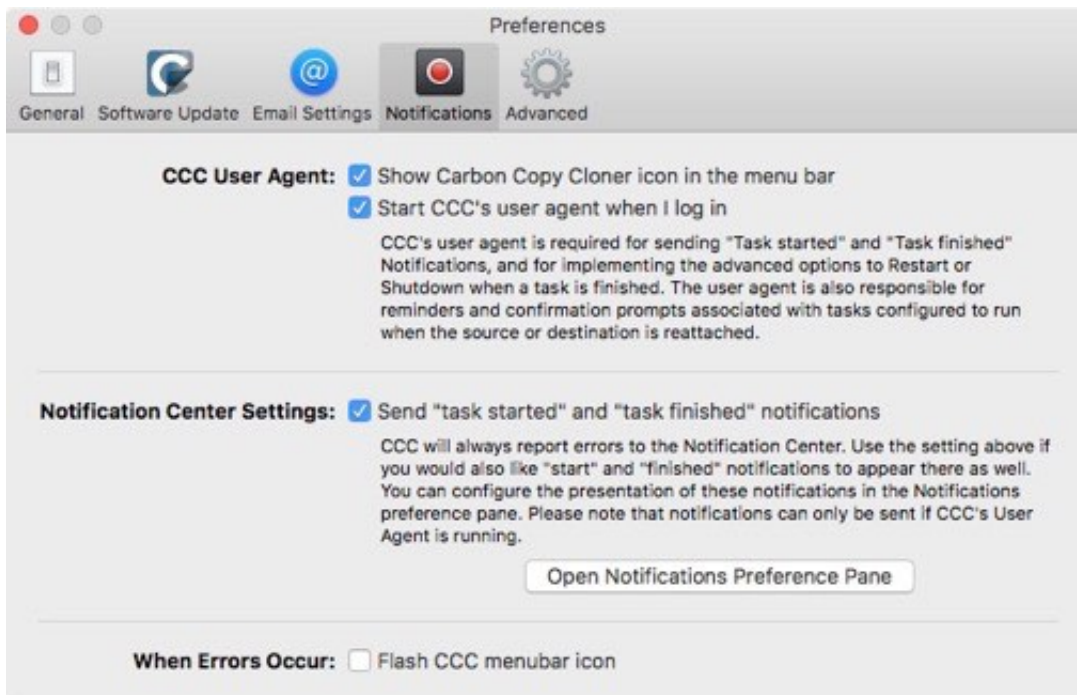
The CCC menubar application offers a miniature task progress window. This window will display detailed progress indication for every running task, and will automatically hide itself when no tasks are running. This window is not displayed by default, choose **Always show progress window** to reveal the window.



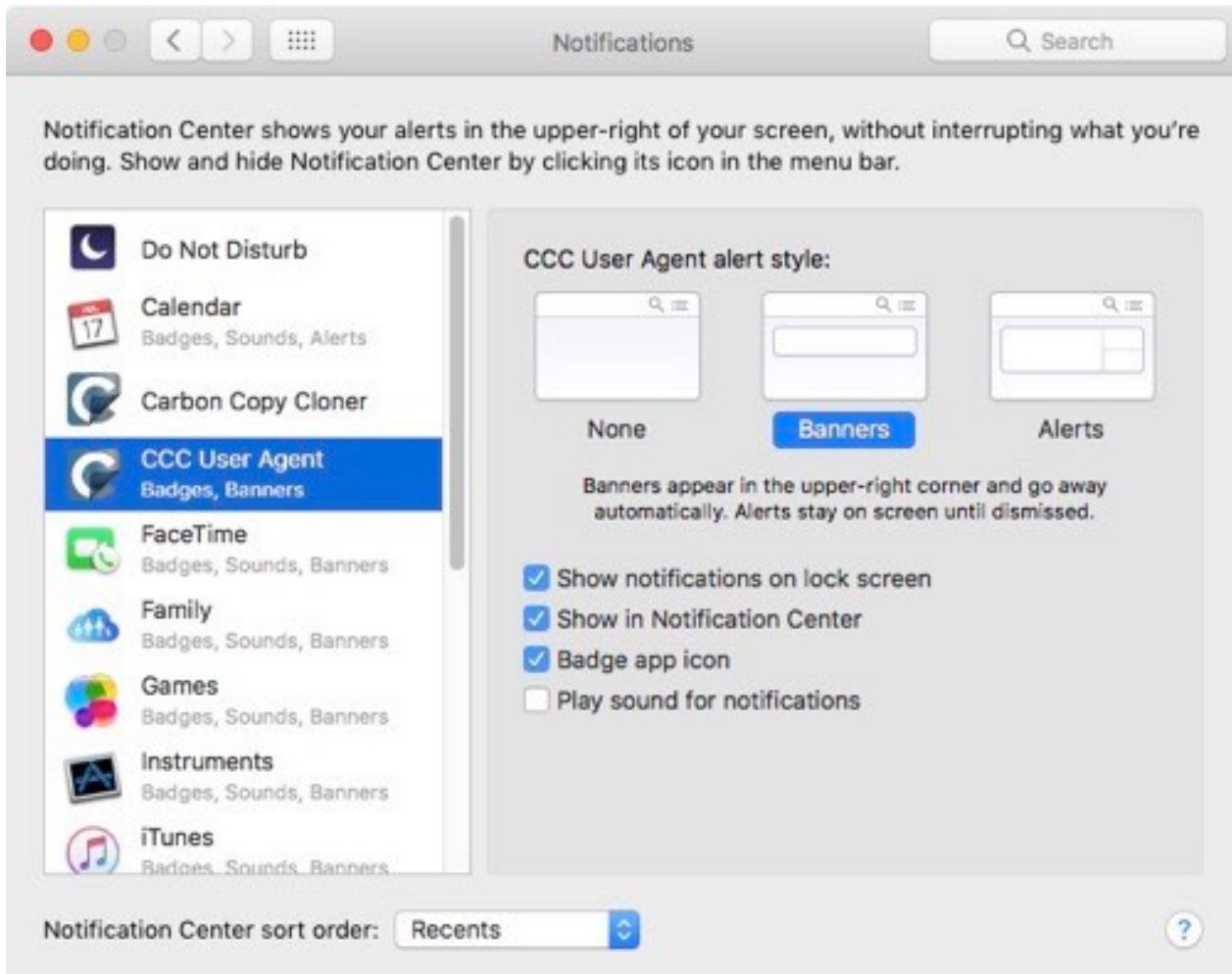


Notification Center

Carbon Copy Cloner sends notifications to macOS's Notification Center when a backup task starts and finishes, and when a task reports an error. These notifications will appear under an application named **CCC User Agent** in Notification Center. The Notifications panel of CCC's preferences windows offers an option to disable task started and task finished notifications, as well as an option to flash the CCC menubar icon when errors are encountered.



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



In older versions of CCC, a scheduled task would present a dialog box if the source or destination was missing, or if errors had occurred. Where can I find that setting in CCC 5?

CCC 5 sends these notifications to Notification Center, so they are subject to the display preferences specified in the Notification Center preference pane. By default, notifications are presented as banners, and these are automatically dismissed after a few seconds. You can configure the **CCC User Agent** notifications to be presented as Alerts instead if you want them to stay on screen until you dismiss them.

Removing CCC User Agent from the Notification Center

If you would like to remove CCC User Agent (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.

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

The CCC menubar application is named "CCC User Agent", and is bundled inside of the CCC application file. The user agent places the CCC icon in the menubar, but it also provides other proxy-like functionality for CCC's background helper tool. The following features are provided by the CCC user agent:



- **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 user agent as a login item. You can change the CCC user agent login item setting in the Notifications section of CCC's Preferences window at any time.

Related Documentation

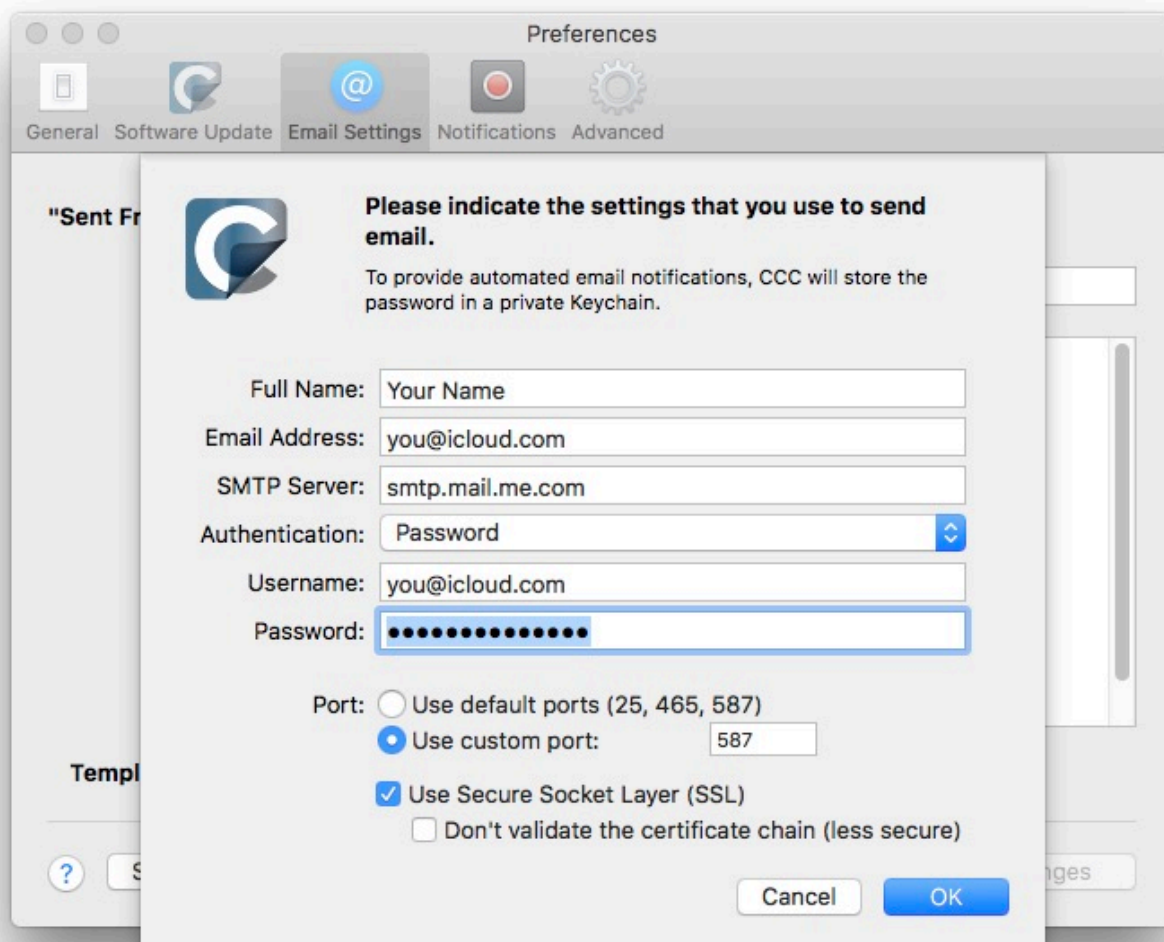
- [Configuring CCC's menubar application preferences](#)
- [How to find out when a backup last ran: CCC Task History <http://bombich.com/kb/ccc5/how-find-out-when-backup-last-ran-ccc-task-history>](http://bombich.com/kb/ccc5/how-find-out-when-backup-last-ran-ccc-task-history)

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. Choose **Preferences** from the Carbon Copy Cloner menu (or click the **Preferences** button in the toolbar).
2. Click the **Email Settings** button in the toolbar of the Preferences 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](http://bombich.com/software/get_help) <http://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.

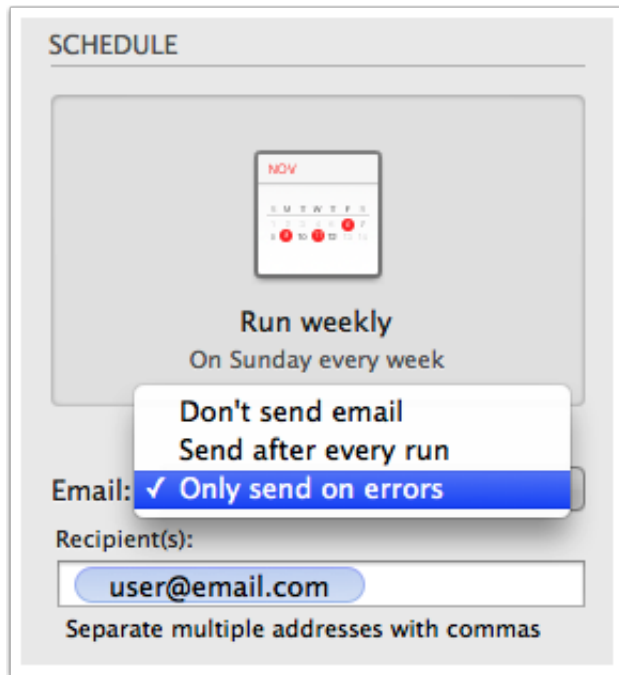
Select a notification level

Close the Preferences window, then select the task to which you would like to add email notifications. 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 addresses 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 File 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.

Solution: 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) <<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) <<https://support.apple.com/kb/HT6186>>

Solution: 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) <<https://login.yahoo.com/account/personalinfo>>.
2. Click on the **Generate app password** link at the bottom of the page.
3. Click **Select your app** and choose **Other App**. Type in CCC or Carbon Copy Cloner 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.

Solution: Create an App Password for Gmail

Visit your App Passwords page to generate an application-specific password for CCC:

1. Visit your [App passwords page](https://security.google.com/settings/security/apppasswords) <<https://security.google.com/settings/security/apppasswords>>.
2. Click **Select app** and choose **Other (custom name)**. Type in CCC or Carbon Copy Cloner.
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)
<<https://support.google.com/accounts/answer/185833>>

"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. Rather than spend several days implementing support for Google's proprietary authentication mechanism, I have chosen to spend my precious development time improving other functionality within CCC; functionality that's core to protecting your data.

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) <<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) <<http://www.google.com/settings/security/lesssecureapps>> that Google disabled

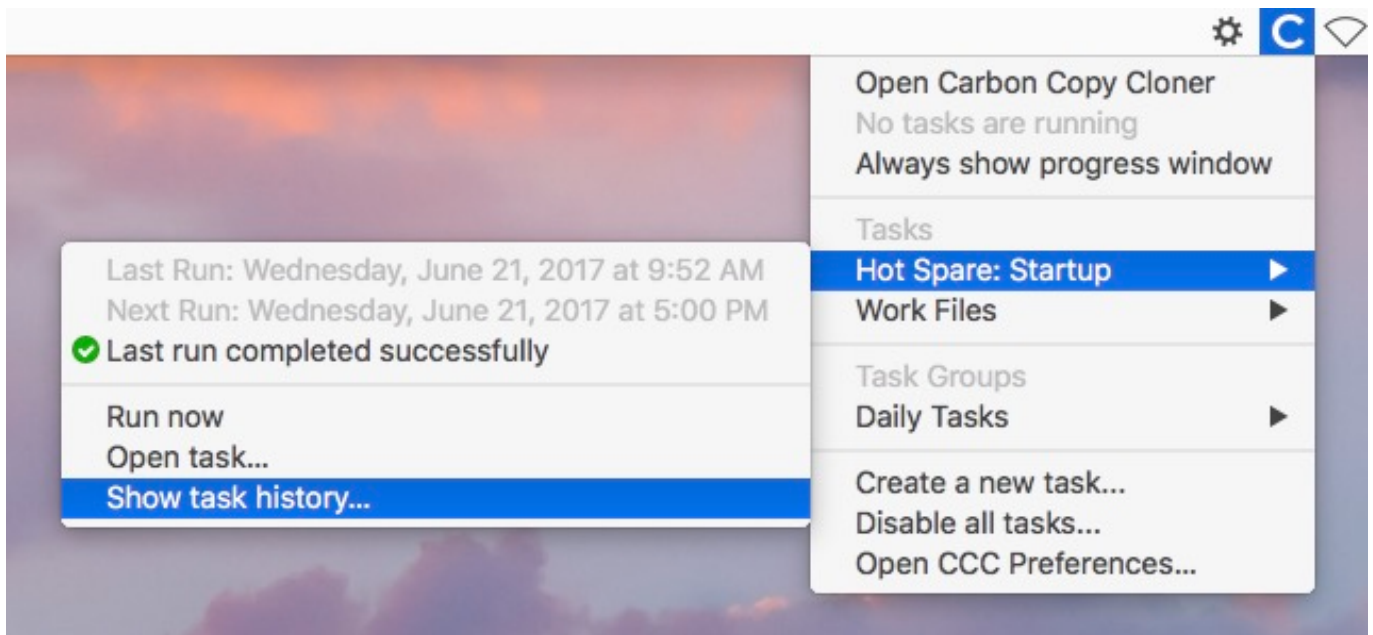
Alternatively, you could just specify a non-Google email account in the Email Settings section of CCC's Preferences window.

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 to find out when a backup last ran: CCC Task History

To find out when a backup task last ran, click on the Carbon Copy Cloner icon in your menubar, then move the mouse over the submenu of the task you would like to inspect. The submenu for each task will indicate when the task last ran, the status of that last run, and when the task is scheduled to run next (if applicable). Select **Show task history...** to open CCC and view more detail about the previous times that that task has run.



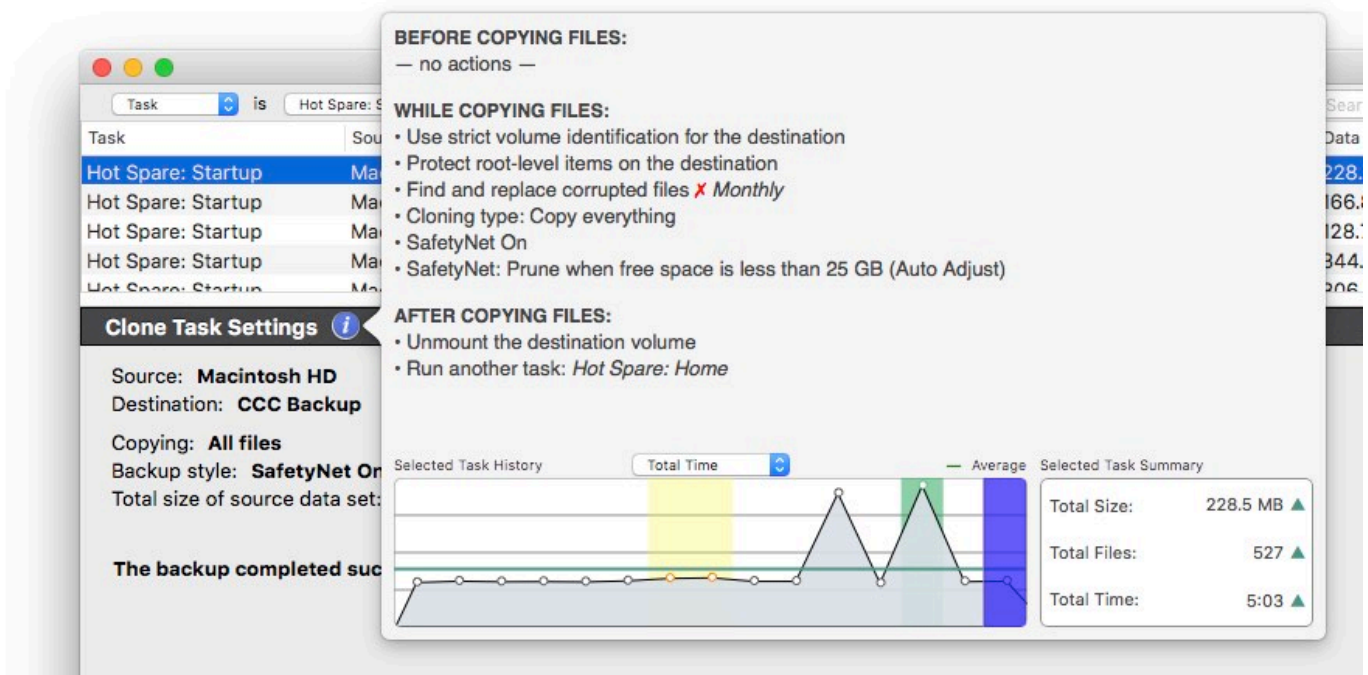
Each time CCC performs a backup task, the results and statistics of that task are recorded and displayed in CCC's Task History window. To view task history, click on the History button in the toolbar, or choose **History** from the Window menu. Within the Task History window, your task events can be filtered and sorted by task name, source, destination, or start time. CCC will show up to 1000 task history events. Each event will indicate when the task started and ended, how much data was copied, and the overall status of the task. The color of the status indicator is defined as follows:

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

If errors occurred, CCC will indicate a list of the affected files. CCC does not record a list of every file that is copied.

Trends

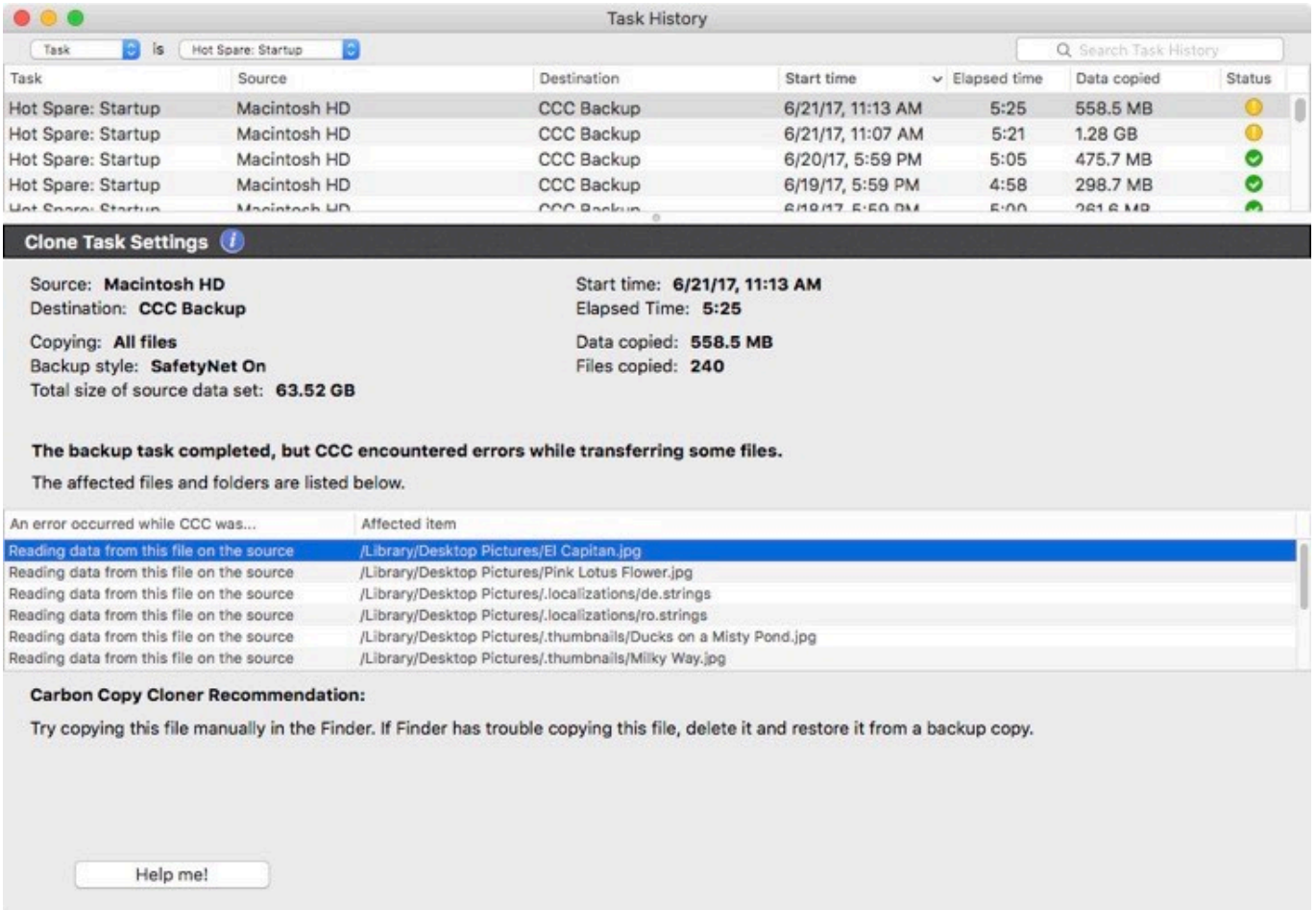
When a task event is selected in the Task History window, you can click on the Info icon in the bottom pane to reveal a popover containing task settings and statistics. A chart will plot those statistics for that task over time. You can use the arrow keys on your keyboard to navigate in time through the task events. Any changes in your task's settings will be highlighted in yellow.



The currently-selected task will be represented in the chart with a dark blue background. Events that end with an error will have a red background, events that end with some errors but otherwise succeed will have a yellow background. Events that used the Backup Health Check (Find and replace corrupted files) will have a green background. You can use the up and down arrow keys to scroll through your task events while watching the trend chart to see changes to your task configuration over time.

Error Reporting

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 the 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.



Task	Source	Destination	Start time	Elapsed time	Data copied	Status
Hot Spare: Startup	Macintosh HD	CCC Backup	6/21/17, 11:13 AM	5:25	558.5 MB	⚠
Hot Spare: Startup	Macintosh HD	CCC Backup	6/21/17, 11:07 AM	5:21	1.28 GB	⚠
Hot Spare: Startup	Macintosh HD	CCC Backup	6/20/17, 5:59 PM	5:05	475.7 MB	✅
Hot Spare: Startup	Macintosh HD	CCC Backup	6/19/17, 5:59 PM	4:58	298.7 MB	✅
Hot Spare: Startup	Macintosh HD	CCC Backup	6/18/17, 5:59 PM	5:00	281.8 MB	✅

Clone Task Settings

Source: **Macintosh HD** Start time: **6/21/17, 11:13 AM**
Destination: **CCC Backup** Elapsed Time: **5:25**
Copying: **All files** Data copied: **558.5 MB**
Backup style: **SafetyNet On** Files copied: **240**
Total size of source data set: **63.52 GB**

The backup task completed, but CCC encountered errors while transferring some files.
The affected files and folders are listed below.

An error occurred while CCC was...	Affected item
Reading data from this file on the source	/Library/Desktop Pictures/EI Capitan.jpg
Reading data from this file on the source	/Library/Desktop Pictures/Pink Lotus Flower.jpg
Reading data from this file on the source	/Library/Desktop Pictures/.localizations/de.strings
Reading data from this file on the source	/Library/Desktop Pictures/.localizations/ro.strings
Reading data from this file on the source	/Library/Desktop Pictures/thumbnails/Ducks on a Misty Pond.jpg
Reading data from this file on the source	/Library/Desktop Pictures/.thumbnails/Milky Way.jpg

Carbon Copy Cloner Recommendation:
Try copying this file manually in the Finder. If Finder has trouble copying this file, delete it and restore it from a backup copy.

Help me!

You can resize the task history window to see more events at once. You can also drag the divider at the bottom of the events list to make more room for error messages.

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 File 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. 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?" <<http://bombich.com/kb/ccc5/where-can-i-find-cccs-log-file>>

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

To remove a task event from the history table, right-click on the event and choose **Remove** from the contextual menu to remove the record of that event. 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. 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 File menu.

Protecting data that is already on your destination volume: The Carbon Copy Cloner SafetyNet

As the name implies, SafetyNet is a **safety mechanism** that works to avoid accidental loss of data on the destination.

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?](http://bombich.com/kb/cc5/frequently-asked-questions-about-ccc-and-macos-catalina#safetynet)

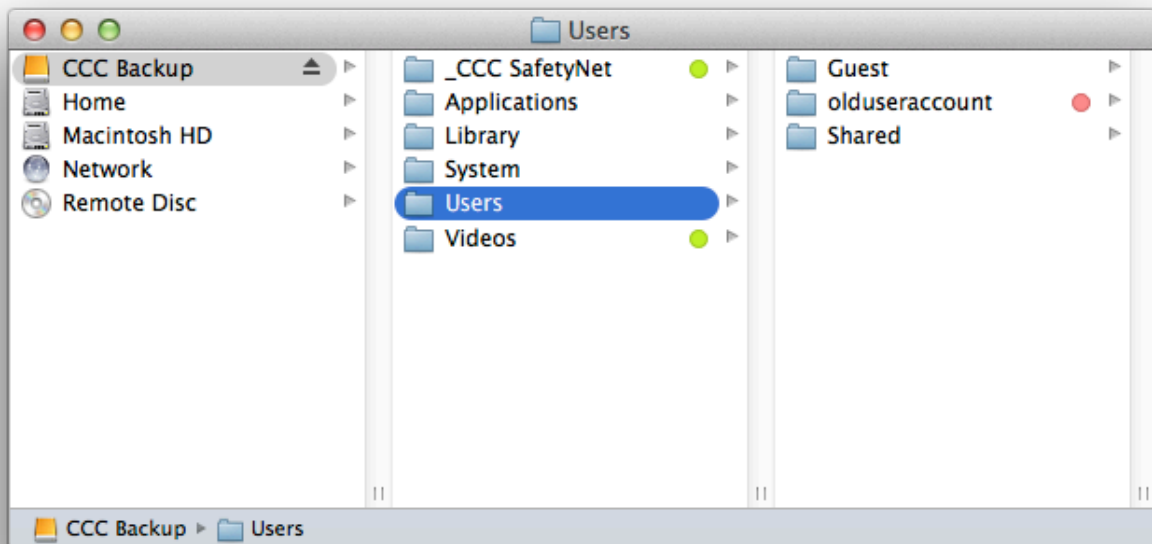
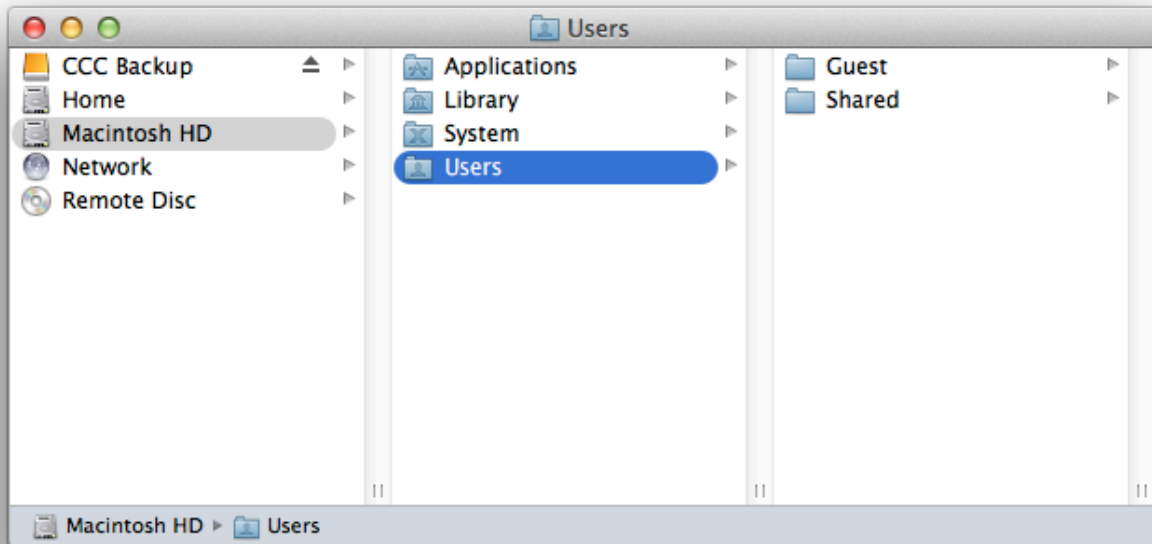
<<http://bombich.com/kb/cc5/frequently-asked-questions-about-ccc-and-macos-catalina#safetynet>>

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 idea of what that means, consider the following two Finder windows:



The first window shows the contents of the startup disk, with the usual Applications, Library, System, and Users folders. 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 "Videos". 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 Users folder, however, is not unique to the destination — that folder is present on both the source and destination. As a result, the "olduseraccount" folder that is inside the Users 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 **Videos** on a volume named **CCC Backup**. When you choose the **CCC Backup** volume as the destination for your task and leave SafetyNet enabled, CCC will leave that **Videos** 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 **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 (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, and you have no need for retaining older versions of modified files or files deleted from the destination since a previous backup task, you can disable CCC's SafetyNet with the large switch icon underneath the destination selector. 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 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.

"An error occurred while replacing an item on the destination"

When you use the **Don't delete anything** SafetyNet setting, CCC won't be able to replace items that have a different type on the destination. For example, if you replace a folder with an alias, CCC won't be able to copy the alias file; instead, you'll get an error. You can manually remove the offending item from the destination, or choose one of the other SafetyNet settings so that CCC may do the replacement.

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 partitions to APFS containers. These actions can be done non-destructively, that is, 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

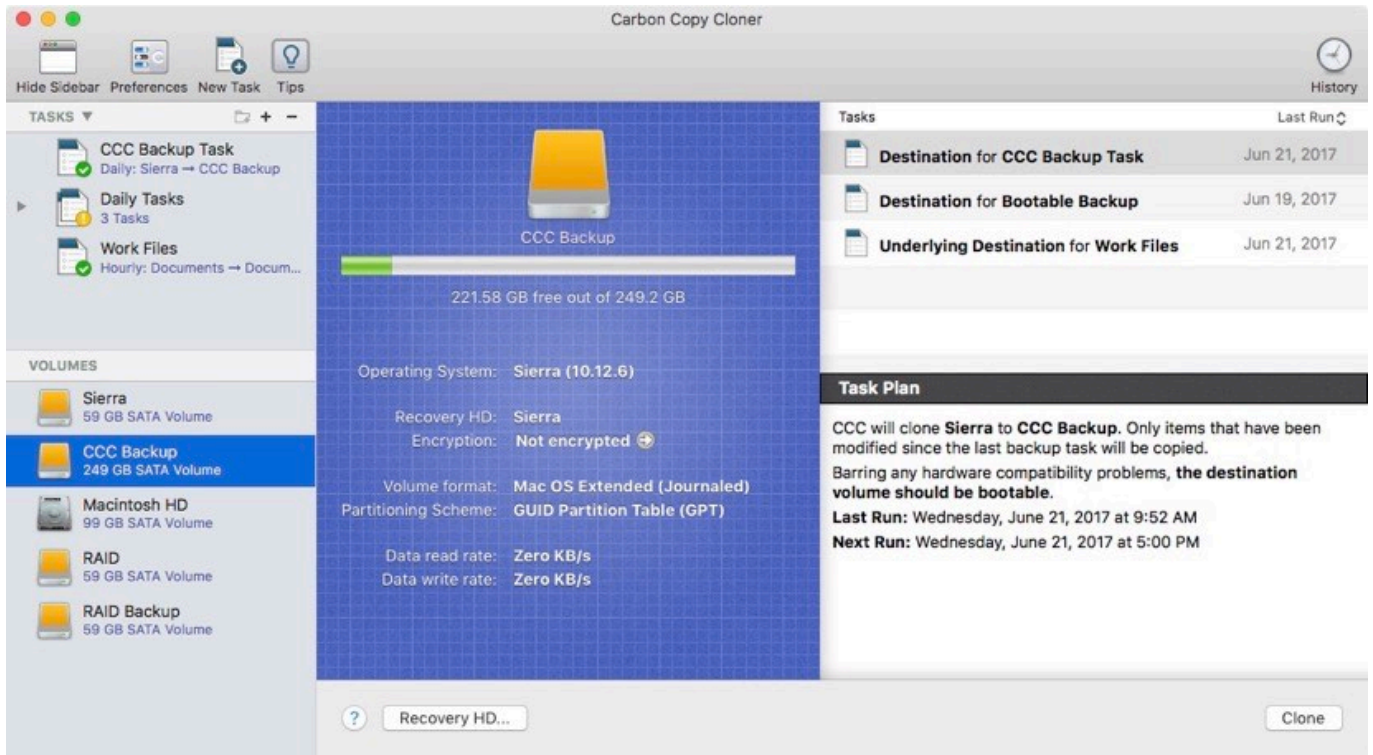
We strongly recommend that you find the means to dedicate a volume to the task of backing up your irreplaceable data. If you have data on your backup volume that exists nowhere else, it is not backed up! Whenever you target a volume for use with Carbon Copy Cloner, there is a risk that some files will 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 Carbon Copy Cloner SafetyNet <http://bombich.com/kb/ccc5/frequently-asked-questions-about-carbon-copy-cloner-safetynet>](http://bombich.com/kb/ccc5/frequently-asked-questions-about-carbon-copy-cloner-safetynet)
- [Leveraging Snapshots on APFS Volumes <http://bombich.com/kb/ccc5/leveraging-snapshots-on-apfs-volumes>](http://bombich.com/kb/ccc5/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, 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. Simply click the Clone button to run a selected task, or double-click the task to edit the task.



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 information about the Recovery HD associated with the volume, as applicable. CCC displays a level indicator above the disk usage figure. When disk usage exceeds 70% of the volume capacity, the level indicator will turn yellow to indicate that you may want to consider "cleaning house". If the disk usage exceeds 90% of the volume capacity, the level indicator will turn red. Especially on a volume that contains an installation of macOS, we recommend that you try to maintain at least 10% of the volume as free space. General performance of macOS begins to decline when the startup disk is very full.

APFS volume usage indicator

When you select an APFS-formatted volume in CCC's sidebar, the volume usage indicator may show several different colors. Green, yellow and red have the same meaning as described above. A lighter shade of each of those colors indicates the percentage of disk usage that is consumed by snapshots (and this is only applicable when snapshots are present on the selected volume). Light gray indicates free space. Dark gray indicates disk usage that is consumed by other APFS volumes that reside in the same APFS container (the same as "Other Volumes" noted in Disk Utility).

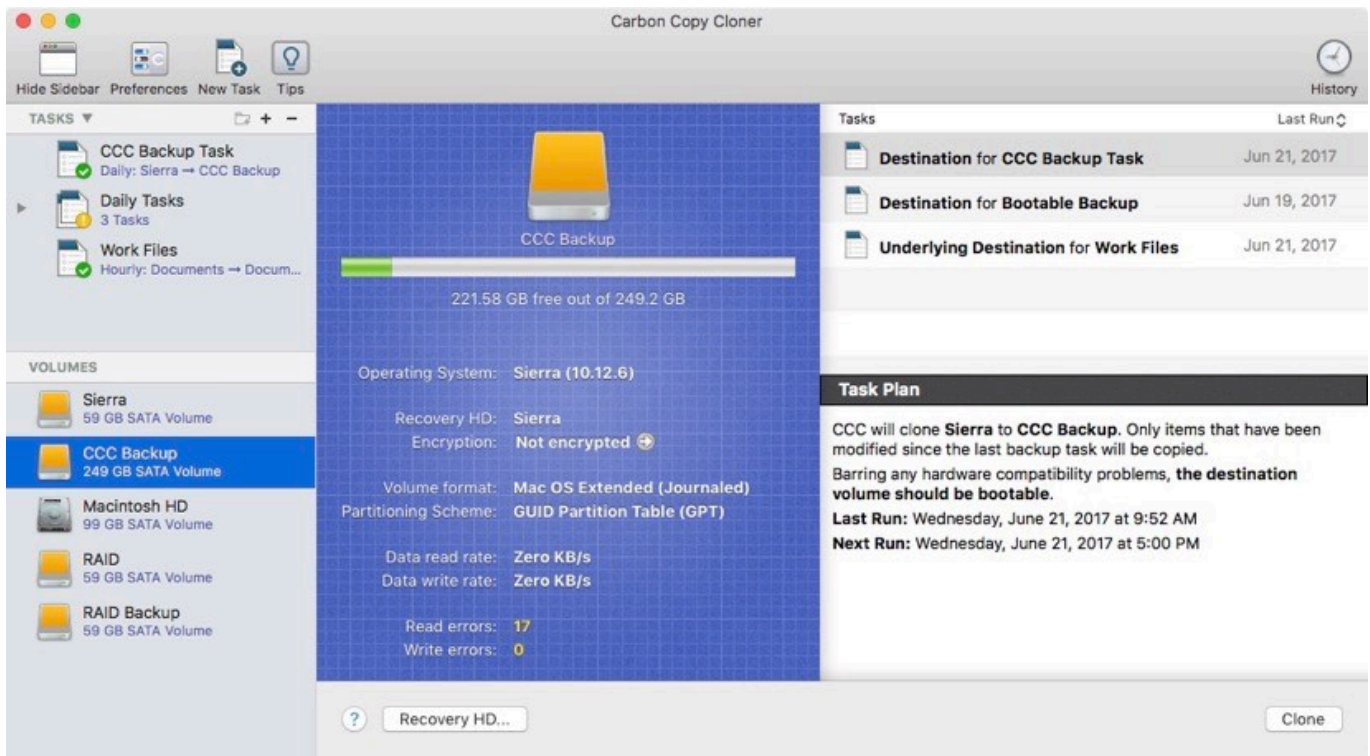
Drive Statistics

The Disk Center will update disk activity statistics on a one-second interval. 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 seek activity occurring on your source and destination volumes. This seeking greatly reduces the overall throughput compared to the theoretical throughput of your disks.

If your backup task seems particularly slow, stop the task and see what the baseline disk activity is. If there is a considerable amount of activity, use the Activity Monitor application to determine which applications are using excessive Disk resources.

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 <http://bombich.com/kb/ccc5/leveraging-snapshots-on-apfs-volumes>](http://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 <http://bombich.com/kb/ccc5/identifying-and-troubleshooting-hardware-related-problems>](http://bombich.com/kb/ccc5/identifying-and-troubleshooting-hardware-related-problems)
- [Troubleshooting "Media errors" <http://bombich.com/kb/ccc5/identifying-and-troubleshooting-hardware-related-problems#io_errors>](http://bombich.com/kb/ccc5/identifying-and-troubleshooting-hardware-related-problems#io_errors)
- [Cloning Apple's Recovery HD partition <http://bombich.com/kb/ccc5/cloning-apples-recovery-hd-partition>](http://bombich.com/kb/ccc5/cloning-apples-recovery-hd-partition)
- [Working with FileVault Encryption <http://bombich.com/kb/ccc5/working-filevault-encryption>](http://bombich.com/kb/ccc5/working-filevault-encryption)

Cloning Apple's Recovery HD partition

Watch a video of this tutorial on YouTube <https://www.youtube.com/watch?v=6q9xeU_jtx8>

The macOS Installer creates a hidden volume on your startup disk named "Recovery HD". The primary purpose of the Recovery HD volume is to offer a method to reinstall macOS. When performing a backup of a macOS volume, Carbon Copy Cloner automatically archives the Recovery HD volume that is associated with the source volume. This archive can later be restored to another Recovery HD volume. CCC's Disk Center also offers the ability to create a new Recovery HD volume on volumes formatted with Apple's legacy filesystem, HFS+ <<http://bombich.com/kb/ccc5/glossary-terms#h>>.

CCC automatically manages the special "helper" volumes on APFS-formatted destinations

CCC will automatically create and update the Preboot and Recovery helper volumes on an APFS-formatted destination volume. The Recovery HD cloning tasks described below are not applicable to APFS-formatted destinations, CCC takes care of all of this for you without requiring any additional steps. Note that these volumes are not visible in Disk Utility.

Why can't I see the Recovery volume in the Startup Manager?

The Startup Manager doesn't show APFS Recovery volumes, Apple decided to not reveal those in that interface. Instead, you press Command+R (Intel Macs) or hold down the Power button (Apple Silicon Macs) on startup to boot into Recovery mode.

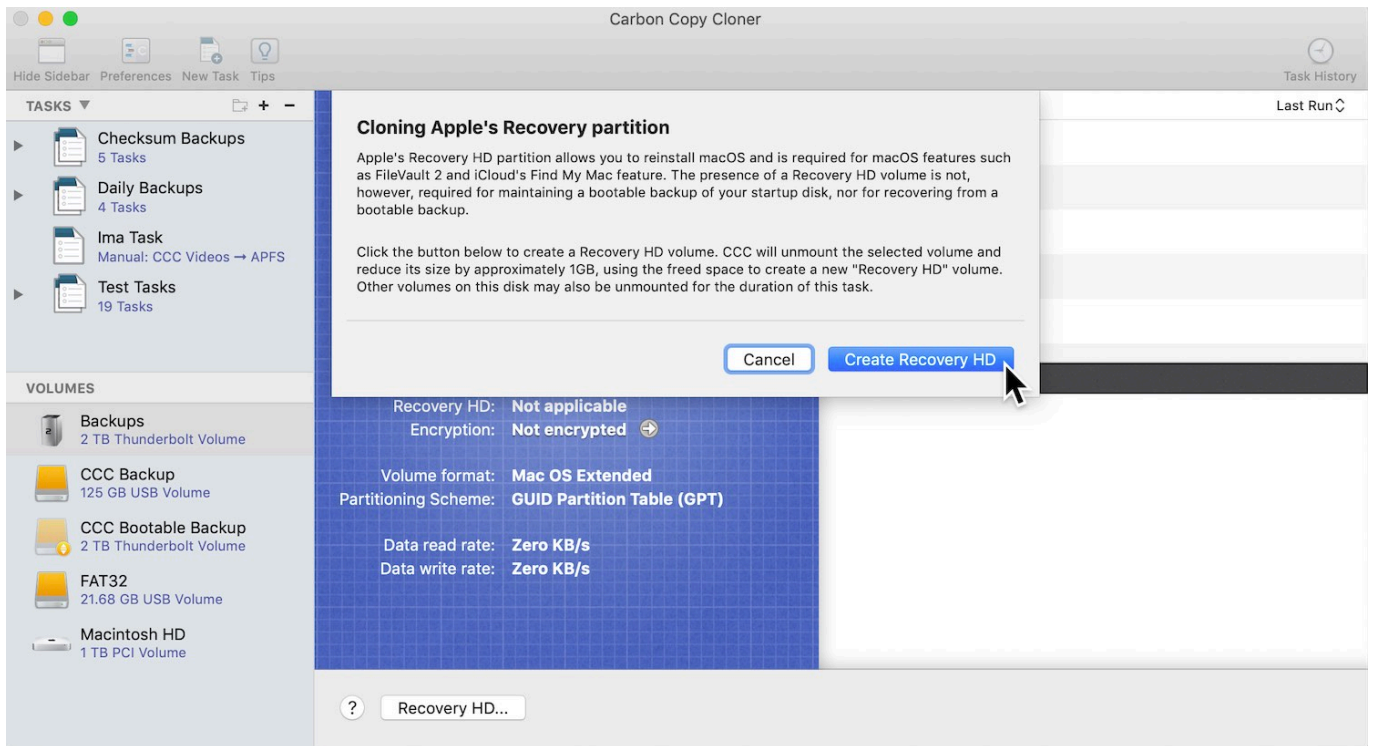
Please note that you would not normally boot into Recovery mode on the backup disk. If you want to restore from the backup, you'd [boot from the backup](http://bombich.com/kb/ccc5/how-restore-from-your-backup) <<http://bombich.com/kb/ccc5/how-restore-from-your-backup>>, not a Recovery volume.

How do I create a Recovery HD volume on my backup disk?

Note: macOS restricts access to Recovery volumes. You must log in as an admin user to create or modify a recovery volume in CCC.

With these simple steps:

1. Use CCC to clone your startup disk (or other source volume that contains an installation of macOS) to your backup volume
2. Select your backup volume in the **Volumes** section of CCC's sidebar (click the **Show Sidebar** button in CCC's toolbar if you do not see CCC's sidebar)
3. Click the **Recovery HD...** button at the bottom of the window
4. Click the **Create Recovery HD** button



Creating a new Recovery HD volume

Note: Drobo devices do not support dynamic volume resizing ([reference <http://www.drobo.com/support/updates/firmware/Release_Notes_Firmware_B800i_Elite_2.0.4.pdf>](http://www.drobo.com/support/updates/firmware/Release_Notes_Firmware_B800i_Elite_2.0.4.pdf)), and therefore cannot accept a Recovery HD volume. Do NOT attempt to create a Recovery HD volume on a Drobo device.

Note: You cannot create a Recovery volume on Fusion or RAID volumes. Creation of recovery volumes on these devices must be done prior to the creation of these "virtual" volumes. See [this CCC Kbase article <http://bombich.com/kb/cc5/frequently-asked-questions-about-cloning-apples-recovery-hd-partition#fusion>](http://bombich.com/kb/cc5/frequently-asked-questions-about-cloning-apples-recovery-hd-partition#fusion) for additional details.

The Recovery HD volume is approximately 650MB, so to create a new Recovery HD volume, you must choose a volume on your disk that has at least 1GB of free space available. This documentation will refer to the chosen disk as the "donor" disk. No data will be harmed on the donor disk, it will simply be resized so some space can be allocated for the new Recovery HD volume. When you click the button to create a new Recovery HD volume, CCC will do the following:

1. Unmount the donor disk
2. Perform the equivalent of Disk Utility's "Verify disk" tool
3. Resize the donor volume to (size of the donor volume) - 1GB
4. Create a new volume named Recovery HD using the 1GB of borrowed space
5. Clone a suitable Recovery HD volume from an archive of the Recovery HD volume or another disk (such as the startup disk) onto the newly-created Recovery HD volume
6. Remount the donor volume

When the task has completed, the Recovery HD volume will not be mounted on your Desktop, nor will it appear in Disk Utility (it's a very special, very hidden volume!). You can verify the functionality of this Recovery HD volume by holding down the Option key on startup, then selecting the Recovery HD volume as the startup disk.

Note: When performing Recovery HD cloning tasks on a laptop, be sure to keep the Mac plugged into an AC power supply for the duration of the task.

Recloning an existing Recovery HD volume

If you choose a volume that already has an associated Recovery HD volume, CCC will indicate that you may "Clone Recovery HD". Recloning the Recovery HD volume may be helpful if the Recovery HD volume is invalid, or its partition type is invalid (and it appears on your Desktop).

Removing an existing Recovery HD volume

In some cases you may have reason to remove a Recovery volume from your backup disk. To remove the Recovery HD volume:

1. Select your backup volume in the **Volumes** section of CCC's sidebar (click the **Show Sidebar** button in CCC's toolbar if you do not see CCC's sidebar)
2. Click the **Recovery HD...** button at the bottom of the window
3. Hold down the Option key (⌘) and click the **Remove Recovery HD** button [VoiceOver users: Use QuickNav to locate the **Remove Recovery HD...** button to the left of the Cancel button]

CCC will remove the Recovery HD volume and give the space back to the donor volume. While this is a non-destructive task for the donor volume, we recommend that you back up any data on this volume before making partitioning changes to it.

Related Documentation

- [Frequently Asked Questions about cloning Apple's "Recovery HD" partition](http://bombich.com/kb/ccc5/frequently-asked-questions-about-cloning-apples-recovery-hd-partition) <<http://bombich.com/kb/ccc5/frequently-asked-questions-about-cloning-apples-recovery-hd-partition>>
- [The Disk Center](http://bombich.com/kb/ccc5/disk-center) <<http://bombich.com/kb/ccc5/disk-center>>
- [Working with FileVault Encryption](http://bombich.com/kb/ccc5/working-filevault-encryption) <<http://bombich.com/kb/ccc5/working-filevault-encryption>>

Leveraging Snapshots on APFS Volumes

Watch a video of this tutorial on YouTube <<https://youtu.be/buM2HzDJKU4>>

What is a snapshot?

Snapshots are a new feature of Apple's APFS filesystem, and they're available on macOS High Sierra and later. 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 on macOS High Sierra and later.

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 bootable backup on an external disk will get you back to work immediately.

	Snapshots	Bootable Backup	Backup to Remote Macintosh
Accidental file deletion			
Malware/ransomware			
Bad OS update			
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 SSD 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.

APFS and snapshots on rotational HDD devices

CCC will only automatically enable snapshot support on an APFS volume backed by a Solid State Device, and only when CCC can determine that the device is a Solid State Device — that assessment is often not possible on external devices. If you are encountering poor performance on an APFS-formatted HDD device, we recommend that you disable snapshot support on that volume and delete any snapshots that are on that volume. We also recommend that you [consider purchasing an SSD for making bootable backups of your startup disk](http://bombich.com/kb/ccc5/choosing-backup-drive) <<http://bombich.com/kb/ccc5/choosing-backup-drive>>

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](#). 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 have snapshots disabled for the source volume (see more on how to do that below), CCC will automatically remove the temporary source snapshot at the end of the backup task.

macOS Catalina and later: CCC won't create snapshots on the source System volume in an [APFS volume group](#) <<http://bombich.com/kb/ccc5/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.

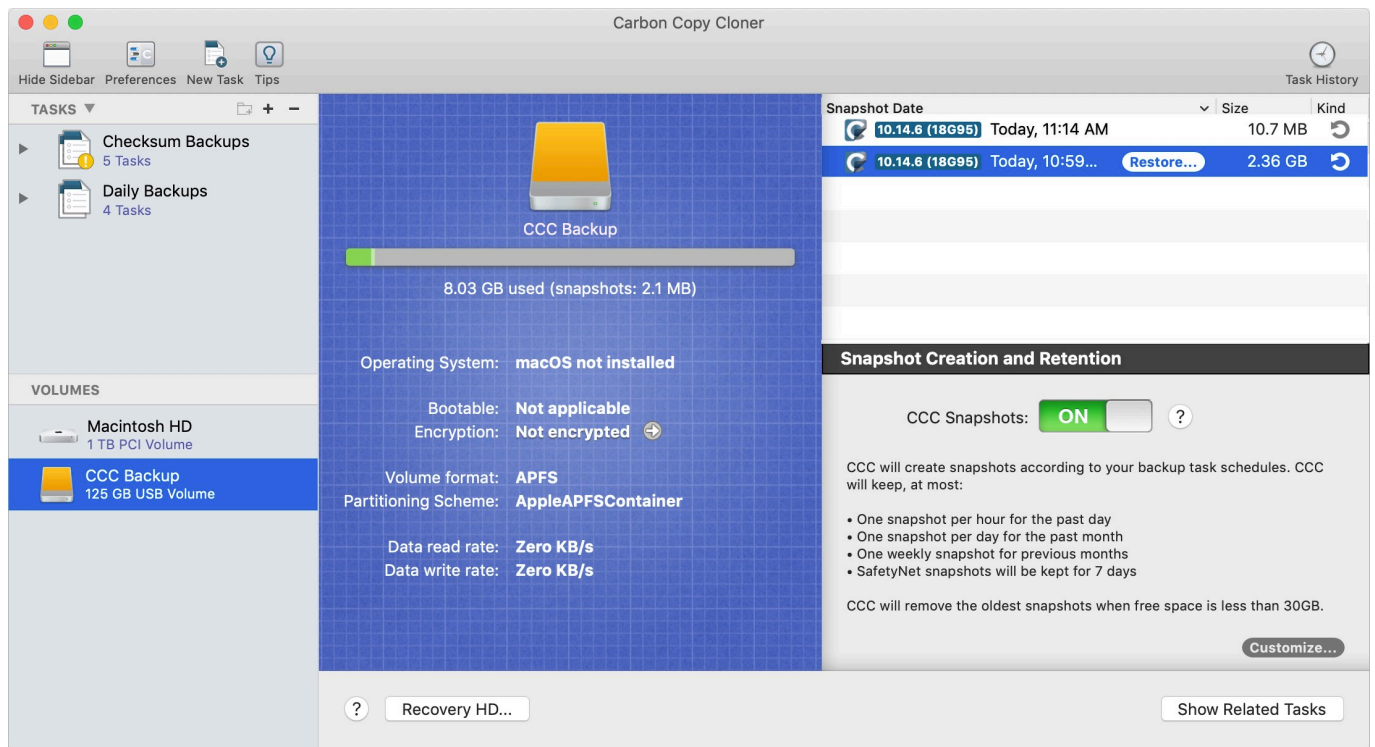
Snapshots on the destination

If you have CCC's SafetyNet feature enabled, CCC will create a [SafetyNet Snapshot](#) <http://bombich.com/kb/ccc5/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 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 Preferences 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 — 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, but any snapshot may be deleted if doing so is required 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

Volume groups <<http://bombich.com/kb/ccc5/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](http://bombich.com/kb/ccc5/how-find-out-when-backup-last-ran-ccc-task-history) <<http://bombich.com/kb/ccc5/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 <http://bombich.com/software/get_help>](http://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, most cloning 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](http://bom.bich.com/kb/ccc5/i-want-back-up-multiple-macs-or-source-volumes-same-hard-drive#apfs_add_volume_startup_disk) <http://bom.bich.com/kb/ccc5/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.

Snapshot Date	Size	Kind
 10.13.4 3/21/18, 9:22 PM	8.9 MB	
 10.13.2 3/21/18, 9:16 PM	19 MB	
 10.13.2 3/21/18, 2:29	20 KB	
 10.13.2 3/21/18, 2:28	12 KB	
 10.13.2 3/21/18, 1:28	33 KB	
 10.13.2 3/21/18, 1:26	33 KB	
 10.13.2 3/21/18, 10:05 AM	12 KB	

1 Snapshot: 20 KB
Browse in Finder
 Delete
 Task Event Details

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.

Restoring from a snapshot

CCC offers two methods to restore from a snapshot. The simplest method is to start from CCC's Disk Center:

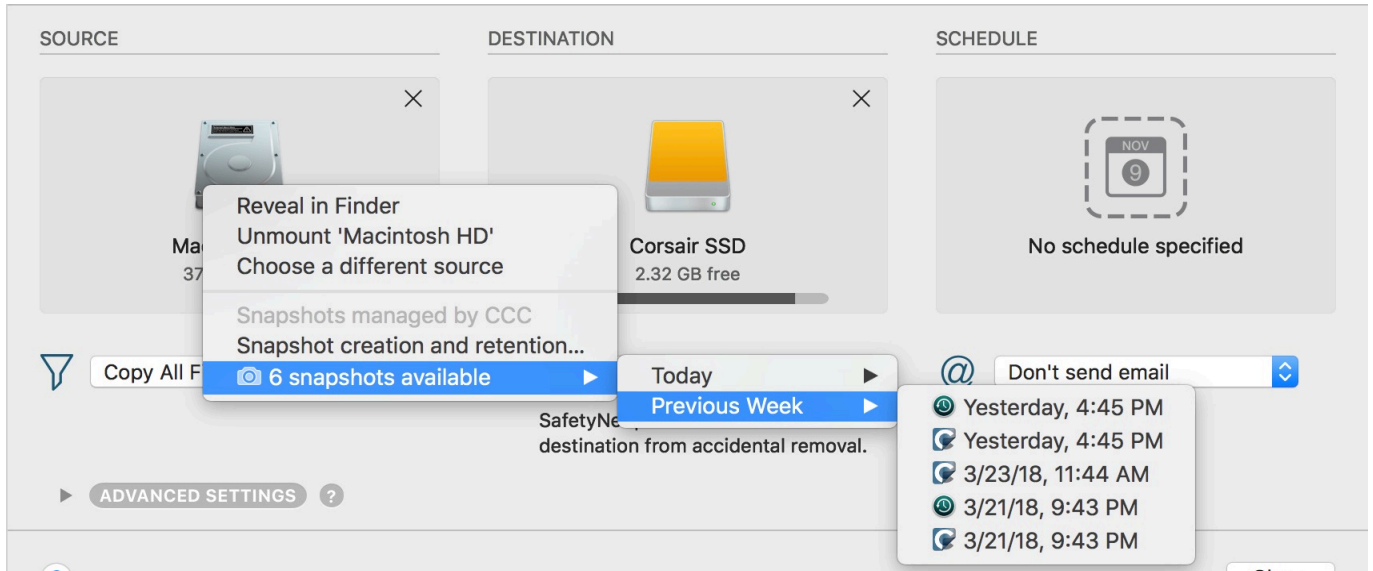
1. Click on a volume in CCC's sidebar to view a list of snapshots available on that volume
2. Select an individual snapshot
3. Click on the **Restore...** button

CCC will create a new Restore task, mount the snapshot and select it as the source for the backup task. If the selected snapshot was a SafetyNet snapshot, CCC will select the original destination volume as the destination. If the selected snapshot was a Backup snapshot created by CCC, CCC will select the original source volume as the destination. If the selected snapshot was not created by CCC, click on the Destination selector to choose a destination for the restore task. You may also

choose to [limit the restore task to a specific set of files and folders](http://bombich.com/kb/ccc5/excluding-files-and-folders-from-backup-task) <<http://bombich.com/kb/ccc5/excluding-files-and-folders-from-backup-task>>.

You can also select a snapshot when configuring a restore task manually:

1. Create a new task
2. Select the volume containing the snapshot as the source
3. Click on the source selector and select a specific snapshot from the contextual menu



Restoring system files to your startup disk (High Sierra and Mojave only)

macOS does not allow you to modify the operating system while you are booted from it. If you would like to restore your OS from an earlier snapshot, [boot your Mac from your CCC backup volume](http://bombich.com/kb/ccc5/how-restore-from-your-backup) <<http://bombich.com/kb/ccc5/how-restore-from-your-backup>>, then you can proceed to restore from a snapshot.

Restoring an APFS volume group from a pair of snapshots (macOS Catalina only)

This procedure is not available on macOS Big Sur - Apple does not accommodate the restoring of macOS Big Sur from a snapshot..

Apple introduced the concept of [volume groups](http://bombich.com/kb/ccc5/working-apfs-volume-groups) <<http://bombich.com/kb/ccc5/working-apfs-volume-groups>> in macOS Catalina. A volume group consists of a pair of volumes; one volume contains the operating system files, the other contains your data. CCC will retain a single snapshot of each OS version on your destination's System volume, and will retain snapshots of your Data volume according to your snapshot retention policy for the destination. When listing snapshots, CCC indicates the OS version and build number that was current when the snapshot was created.

To restore an APFS volume group from snapshots, you will perform two separate restore tasks. First, select a snapshot on your backup disk's Data volume, click the "Restore" button, then proceed to restore that snapshot to an APFS-formatted destination. Second, select a snapshot on your backup disk's System volume, click the "Restore" button, then proceed to restore that snapshot to the same APFS-formatted destination. CCC will automatically create a volume group on the destination and handle the logistics of restoring each snapshot to the correct volume on the destination.

- You may restore System and Data snapshots that are associated with different OS versions, but we don't yet know the implications of mixing these. When possible, restore System and Data snapshots with matching OS versions.
- CCC can identify whether the source snapshot is a System or Data volume snapshot, and will handle the logistics of restoring each to the correct volume on the destination. You don't have to take any special steps to direct the snapshots to the right location, simply select the volume that you want to restore to.

Restoring files to your destination from a SafetyNet Snapshot

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 Clone 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 resources:

- [How to restore from your backup <http://bombich.com/kb/ccc5/how-restore-from-your-backup>](http://bombich.com/kb/ccc5/how-restore-from-your-backup)
- [Excluding files and folders from a backup task <http://bombich.com/kb/ccc5/excluding-files-and-folders-from-backup-task>](http://bombich.com/kb/ccc5/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?" <http://bombich.com/kb/ccc5/cc-reported-destination-full.-what-can-i-do-avoid#destination_is_tight_on_space>](http://bombich.com/kb/ccc5/cc-reported-destination-full.-what-can-i-do-avoid#destination_is_tight_on_space)



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 Carbon Copy Cloner
-  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 Preferences application
2. Open the Time Machine Preference Pane
3. Click on the **Options...** button at the bottom of the window
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.

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://www.youtube.com/watch?v=4wqAC4YXiaY>>



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?](#)
- [Where did the _CCC SafetyNet folder go?](#)
- [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?](#)
- [I just enabled encryption on my APFS-formatted volume. Why am I now getting errors that CCC can't create snapshots?](#)

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?

Prior to CCC 5.1, CCC would create a "_CCC SafetyNet" folder at the root of the destination volume if the SafetyNet feature was enabled. As CCC updates the destination, any files that don't exist on the source or that were getting replaced by an updated version would be moved into that SafetyNet folder. With snapshot support in CCC 5.1 and later, that folder is no longer used as part of the SafetyNet mechanism when snapshots are enabled on the destination. 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, select the SafetyNet Snapshot, right-click on that snapshot and choose **Browse In 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 in CCC 5.1. 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 <http://bombich.com/kb/ccc5/legacy-safetynet-folder-not-used-when-snapshots-are-enabled-on-destination>](http://bombich.com/kb/ccc5/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 <http://bombich.com/kb/ccc5/folder-folder-backups>](http://bombich.com/kb/ccc5/folder-folder-backups) on that same source volume. What gets copied in that case isn't important (in fact the folders can be 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.

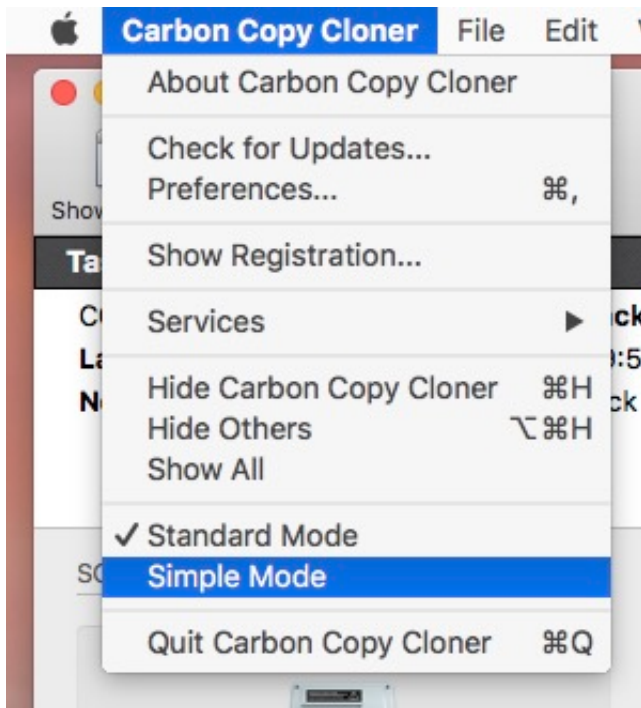
1. Create two new folders somewhere on the source volume, named "source" and "destination"
2. Open CCC and click the **New Task** button in the toolbar
3. Drag the source folder onto CCC's Source selector
4. Drag the destination folder onto CCC's Destination selector
5. Turn off the SafetyNet feature
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.

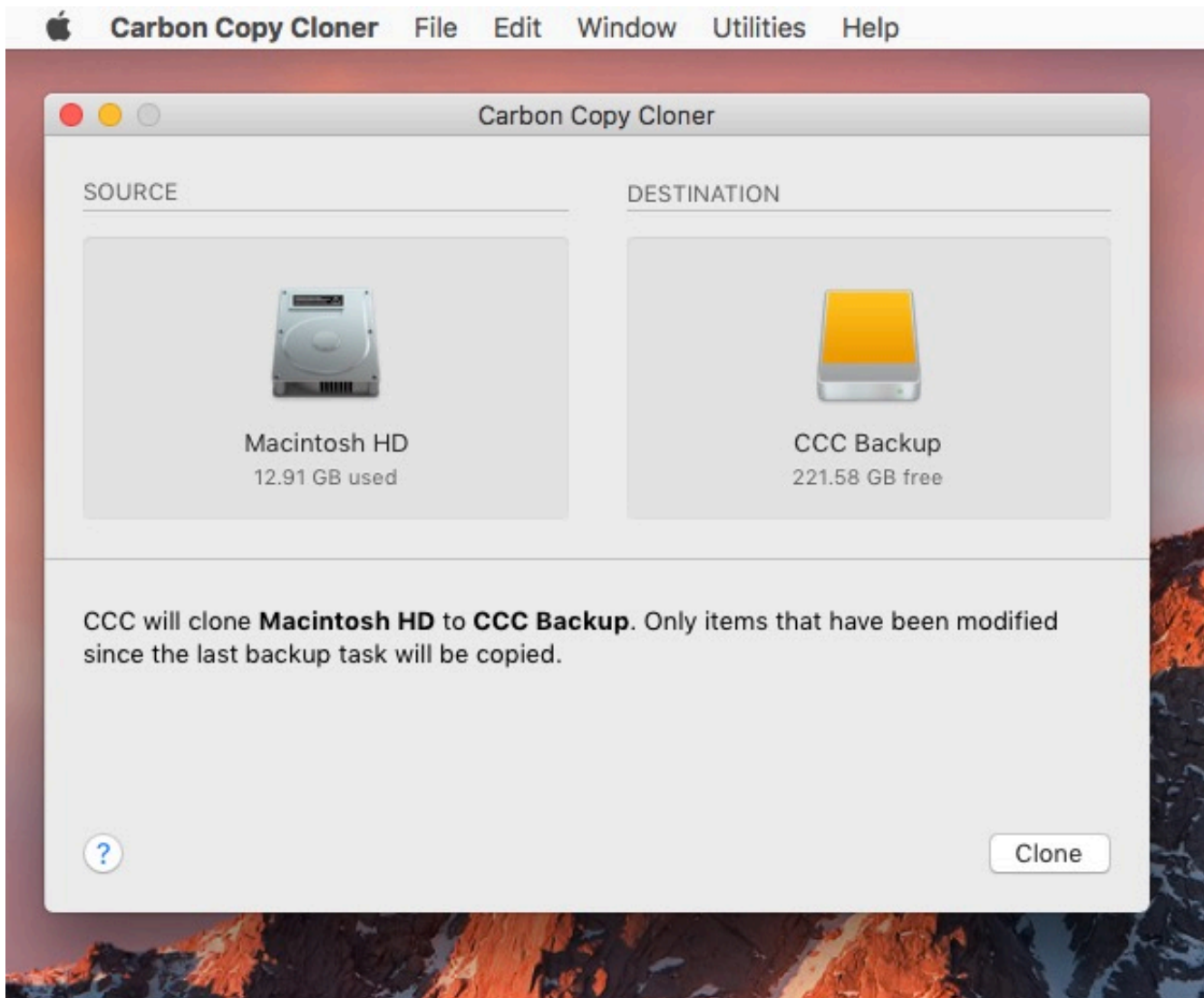
Simple Mode

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, Clone button. For users that desire a basic ad hoc clone 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 Clone button



Related Documentation

- [Preparing your backup disk for a backup of OS X <http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x>](http://bombich.com/kb/ccc5/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?

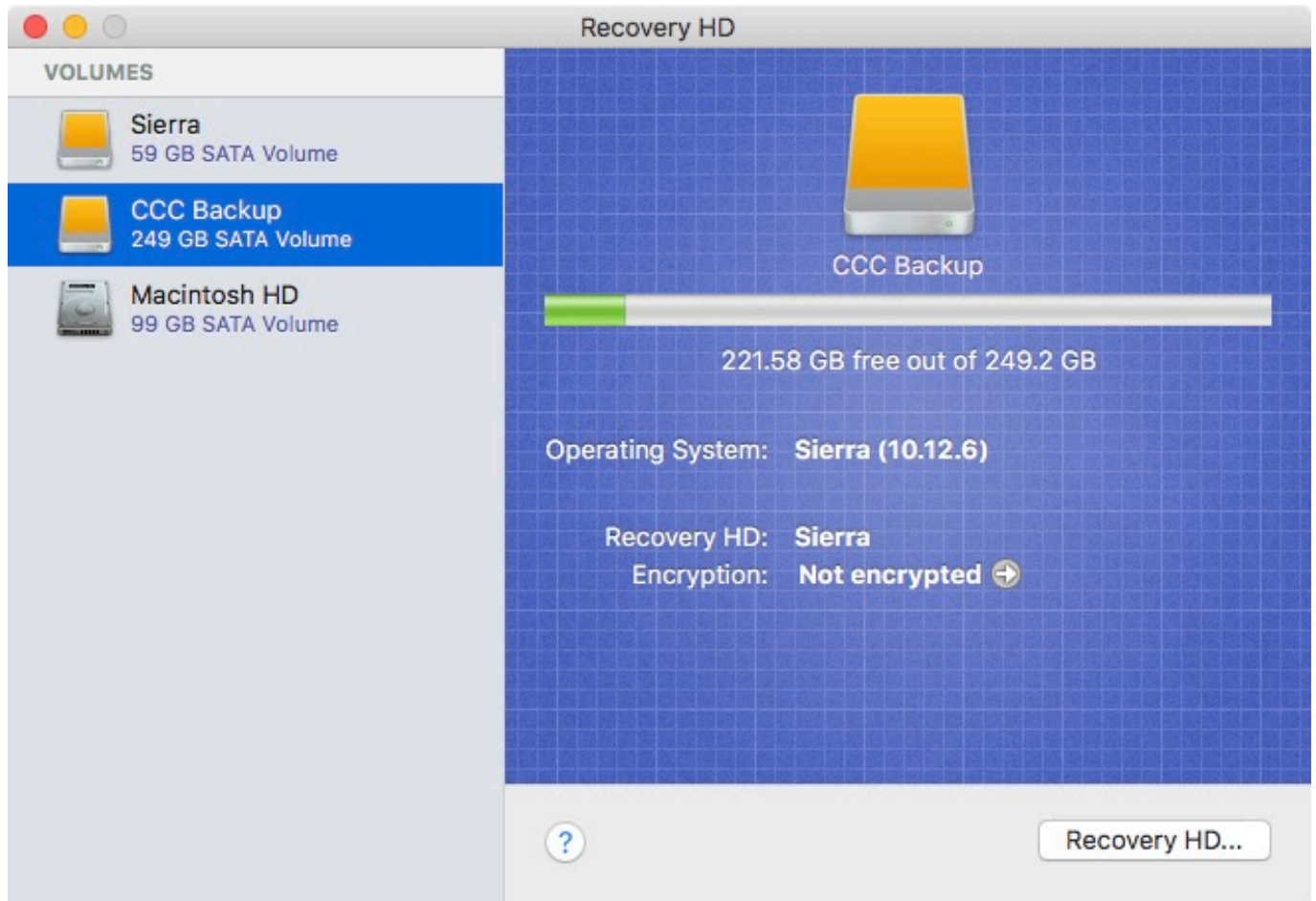
Simple mode aims to simplify **basic** cloning tasks. For additional options, choose **Standard Mode** from the Carbon Copy Cloner menu to switch back to standard mode.

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).

Cloning Apple's Recovery HD volume

Note: This procedure and window is not applicable nor available on Macs running macOS Catalina or later.

While the background of this procedure tends to be the opposite of simple, we felt that this functionality should be made available in Simple Mode. After you have cloned an OS to your backup volume, you can choose **Recovery HD** from CCC's Window menu to reveal a separate window listing locally-attached volumes.



To create a Recovery HD on your backup volume, click on the backup volume in the table on the left, then click on the **Recovery HD...** button at the bottom of the window.

- [Cloning Apple's Recovery HD partition <http://bombich.com/kb/ccc5/cloning-apples-recovery-hd-partition>](http://bombich.com/kb/ccc5/cloning-apples-recovery-hd-partition)
- [Frequently Asked Questions about cloning Apple's "Recovery HD" partition <http://bombich.com/kb/ccc5/frequently-asked-questions-about-cloning-apples-recovery-hd-partition>](http://bombich.com/kb/ccc5/frequently-asked-questions-about-cloning-apples-recovery-hd-partition)

Notes for VoiceOver users

CCC's main window is divided into three main sections. At the top is a toolbar, and beneath that there is a split pane divided vertically. The view on the left is called the sidebar, the view on the right holds the task configuration view. When you open CCC for the first time, the sidebar is hidden. The sidebar is automatically revealed when you add a new task.

The sidebar is split horizontally. The top half contains a table of backup tasks, the bottom half lists locally-attached volumes on your Mac. When you select a task in the task list, the details of that task are presented in the right pane of the window. Likewise, if you select a volume from the list in the bottom of the sidebar, the details of that volume are presented in the right pane. CCC requires that you save any changes you have made to a task before selecting another task or a volume, so if you switch away from a task that is currently being edited, you will be prompted to save unsaved changes, revert the task to its on-disk state, or cancel the event that would have changed the task selection.

Navigation challenges and solutions

The "Automatically interact when using tab key" setting in VoiceOver Utility > Navigation can make navigation to CCC's task configuration view quite challenging. If you prefer to leave this setting enabled, we recommend that you hide CCC's sidebar to avoid navigation challenges. You can use CCC's View menu to select tasks and volumes (in other words, the contents of the View menu completely replaces the need for the sidebar).

Quick Nav

The Tab key will effectively move your cursor to each control in CCC. With Quick Nav enabled (to enable it, simultaneously press the left and right arrow keys), you can also navigate through non-control user interface elements, such as labels, scroll views and split view dividers. Largely this is quite intuitive, however there is one place where the order of elements as interpreted by the window is not very intuitive. This is only applicable when the sidebar is revealed -- if the sidebar is hidden, focus goes to the source selector, and the following is irrelevant.

Upon launch, CCC places focus on the tasks table. The task configuration view lies to the right of the tasks table, so you would think that you could use the right arrow key to move focus to the task configuration view. However, the tasks configuration view is ordered in front of the tasks table, so you must use the **left** arrow key to get from the tasks table to the task configuration view. Alternatively, use the Tab key.

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 three primary controls: Source, Destination, Clone button. For users that desire a basic ad hoc clone from one volume to another, this simplified interface is the perfect solution.

Granting Full Disk Access to CCC and its helper tool

macOS Mojave (and newer) imposes new privacy restrictions that disallow, by default, access to certain application data (e.g. Mail, Messages, Safari, Photos). Restrictions have been imposed previously for data associated with applications such as Calendar and AddressBook, but unlike these previous limitations, macOS Mojave imposes these limitations on privileged applications (like CCC's file copier) as well. macOS Catalina applies these privacy changes even more broadly, preventing applications from accessing any external hard drives and network volumes.

To further complicate the matter, 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 complete a long list of steps to 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.



Grant Full Disk Access to CCC

To back up your Application Data (e.g. Mail, Calendars, Messages), grant CCC and its helper access to that data.

1. [Click here to open Security & Privacy](#)
2. Click the lock icon to allow changes
3. Drag the fish icon below into the Full Disk Access table
4. Choose "Later" when asked whether to quit CCC


Drag this icon in step 3

Don't prompt me again ?

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. To begin, click the button to open the Security & Privacy Preference Pane in the System Preferences application. CCC will take you directly to the Privacy tab and select the Full Disk Access category. Next, click the padlock icon in the lower-left corner of the Privacy window to allow changes. 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 Preferences window at that point, and if you're prompted to quit CCC now or later, you can choose the "Later" option.

CCC's Cloning Coach will issue a warning if CCC's helper tool lacks access to some of your data

If you select your startup disk as the source to a backup task and you have not yet granted full disk access to CCC's privileged helper tool, CCC's Cloning Coach will raise this to your attention when you save or run that task. When you click on the "Grant Access..." button offered by the Cloning Coach, CCC will present the Install Assistant, indicated by the screenshot above.

Likewise, if you proceed with a backup task without granting full disk access to CCC's privileged helper tool and CCC is prevented from backing something up, the error will be raised to your attention in CCC's Task History window, along with the "Grant Access..." button.

"I added Carbon Copy Cloner to the Full Disk Access category but I still get errors"

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, it is CCC's privileged helper tool ("com.bombich.ccchelper") that needs Full Disk Access, not the main application. After adding 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? <http://bombich.com/kb/ccc5/what-cccs-privileged-helper-tool>](http://bombich.com/kb/ccc5/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 Security & Privacy Preference Pane in the System Preferences application
2. Click on the Privacy tab
3. 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

ESET Cyber Security may interfere with the Privacy Preference Pane

We have received several reports that ESET software will prevent modifications to the settings in the Privacy tab of the Security & Privacy Preference Pane. If you are unable to add items to the Full Disk Access category and you have ESET installed, temporarily uninstall ESET before attempting to grant CCC and its helper tool full disk access. After you have granted CCC full disk access, you can then reinstall ESET.

My Mac is booted from an HFS+ formatted volume, and I can't make any changes to the Full Disk Access list

macOS will not allow modifications to the Privacy database if the current startup disk is formatted as HFS+. If you did not grant CCC Full Disk Access before making a backup to an HFS+ formatted volume, you will be unable to grant CCC Full Disk Access while booted from that volume. As a result, CCC will be unable to restore large portions of your user data. You can do the following to resolve this conundrum:

1. [Use Disk Utility to erase the destination volume as APFS <http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x>](http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x)
2. [Download macOS Mojave <https://itunes.apple.com/us/app/macOS-mojave/id1398502828?mt=12>](https://itunes.apple.com/us/app/macOS-mojave/id1398502828?mt=12) and install macOS onto the destination volume
3. Use Migration Assistant to migrate data from your HFS+ formatted backup to the fresh installation of Mojave

When you have completed the migration, open CCC and configure a task to back up the new startup disk to the original backup disk. This time, grant CCC Full Disk Access before proceeding so you can avoid the reinstall+Migration Assistant procedure in the future. To proactively grant CCC and its helper tool full disk access, choose "Grant CCC Full Disk Access..." from the Carbon Copy Cloner menu.

Cloning macOS System volumes with Apple Software Restore

This functionality is not currently available for Apple Silicon Macs: [Apple Software Restore is not compatible with the storage in Apple Silicon Macs <http://bombich.com/kb/ccc5/macOS-big-sur-known-issues#asr_broken_arm>](http://bombich.com/kb/ccc5/macOS-big-sur-known-issues#asr_broken_arm)

Starting in macOS Big Sur (11.0), the system resides on a cryptographically sealed "[Signed System Volume](https://developer.apple.com/news/?id=3xpv8r2m)" <<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 cannot use its own file copier to *establish* an initial bootable backup of your Mac's startup disk. When you configure a CCC backup task to make a clone of a Big Sur startup volume, CCC will use Apple's APFS replicator (named "ASR") to create the initial clone. For subsequent backups, CCC will use its own file copier and will copy just the differences from your Mac's Data volume.

What to expect as you configure your first backup task

When you select an APFS volume group (e.g. your macOS Big Sur startup disk) as the source to a task, and a destination that is not an already-established Big Sur volume, CCC 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 the backup task, because the volume will have to be erased to establish a bootable backup.

Erase the destination

When you select this option, CCC will configure the task to use Apple's APFS replicator to clone 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).

Add a volume

If the selected destination is an APFS-formatted volume, and if the volume's container has enough capacity to accommodate a complete backup of the source volume, CCC will offer an option to add a volume to the destination APFS container. When you choose this option, your selected destination is not erased, nor affected at all by the backup task. Instead, CCC will add a new volume on the destination and use the new volume as the dedicated backup for the source.

Data Only backup

If you cannot or do not want to make a bootable backup of the selected source, and you also do not want to erase the selected destination, you can select the **Data Only** option. When you select this option, CCC will select the Data volume of your selected source as the source to your task, and will not erase the selected destination. This option is convenient if you have an existing encrypted backup volume that you would like to continue to use without erasing or decrypting it. Data-only backups will not be bootable, however [you can use these backups as a source to Migration Assistant <http://bombich.com/kb/ccc5/creating-and-restoring-data-only-backups#migrate>](http://bombich.com/kb/ccc5/creating-and-restoring-data-only-backups#migrate), e.g. to migrate data to a fresh installation of macOS.

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 backup?

If your Mac is running Big Sur, yes. As of macOS Big Sur, we're required to use Apple's APFS replicator to *establish* a bootable clone 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 backup volume. You must dedicate a volume to your bootable backup. Once your bootable backup is established, CCC will use its own file copier to update the destination Data volume in subsequent backup tasks.

Can I use my backup disk for other purposes as well?

Yes. We recommend that you add an APFS volume to the destination APFS container and use that new volume for either your dedicated CCC backup, or for your other content. As long as the CCC backup 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 backup 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 your CCC backup.

Can I exclude some content from the initial backup?

If your Mac is running Big Sur, then it is not possible to exclude content and produce a bootable backup. If you must exclude content from the initial backup, then we recommend that you [proceed with a data-only backup](http://bombich.com/kb/ccc5/creating-and-restoring-data-only-backups#create) <<http://bombich.com/kb/ccc5/creating-and-restoring-data-only-backups#create>>. If you would like to make that backup bootable afterwards, then you can [install macOS onto the backup volume](http://bombich.com/kb/ccc5/creating-and-restoring-data-only-backups#install_macos) <http://bombich.com/kb/ccc5/creating-and-restoring-data-only-backups#install_macos>.

Related documentation

- [Adding a volume or partition to the destination](http://bombich.com/kb/ccc5/frequently-asked-questions-about-ccc-and-macos-catalina#dedicated_volume) <http://bombich.com/kb/ccc5/frequently-asked-questions-about-ccc-and-macos-catalina#dedicated_volume>

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 back up to 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 clone to 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 cloned volume. To enable FileVault on the destination, you can boot from the backup volume and enable FileVault in the Security & Privacy Preference Pane.

Related documentation

- [Troubleshooting APFS Replication <http://bombich.com/kb/ccc5/troubleshooting-apfs-replication>](http://bombich.com/kb/ccc5/troubleshooting-apfs-replication)
- [Working with FileVault Encryption <http://bombich.com/kb/ccc5/working-filevault-encryption>](http://bombich.com/kb/ccc5/working-filevault-encryption)



Creating and restoring data volume backups

A data-only backup is a complete backup of all of your data, settings, and applications

In some cases CCC will create a data-only backup of a macOS startup disk. If you're unfamiliar with the APFS Volume Group concept that Apple introduced in macOS Catalina, you can learn more about it here:

[Working with APFS Volume Groups <http://bombich.com/kb/ccc5/working-apfs-volume-groups>](http://bombich.com/kb/ccc5/working-apfs-volume-groups)

For a data-only backup, CCC copies the entire Data volume within that APFS volume group. The System volume, which contains only about 15GB of read-only system files that are installed by the macOS Installer, will not be copied. A data-only backup is not bootable, however the backup can be made bootable by installing macOS onto it, or you can use the data-only backup as a source to Migration Assistant.

Creating a data-only backup

In some cases CCC will configure your task for a data-only backup automatically. You can perform the following steps to manually configure a data-only backup.

1. If you would ultimately like to make the backup bootable, [erase your destination volume as APFS in Disk Utility <http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x#high_sierra>](http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x#high_sierra)
2. Click the **Show Sidebar** button in CCC's toolbar
3. Drag the **Macintosh HD - Data** volume from CCC's sidebar onto the Source selector
4. Click on the Destination selector and choose your destination

Installing macOS onto a data-only backup

If your data-only backup resides on a non-encrypted APFS volume, you can install macOS onto the backup disk to make it bootable.

Intel-based Macs

1. Download and open the macOS Installer: [[Catalina <https://itunes.apple.com/us/app/macos-catalina/id1466841314?ls=1&mt=12>](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>](https://itunes.apple.com/us/app/macos-big-sur/id1526878132)]
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

Apple Silicon Macs

1. Shut down your Mac, then power it on while holding down the Power button until the startup options are loaded
2. Click on the Options button, then click the Continue button
3. When Recovery has loaded, click on the WiFi option and join a WiFi network if your Mac is not



connected to a wired network

4. Choose the option to Reinstall macOS Big Sur
5. Proceed to install macOS onto your backup disk

Migrating data from a CCC backup using Migration Assistant

You can use Migration Assistant to migrate data from your CCC backup to a clean installation of macOS. For example, if your startup disk is corrupted or had to be replaced, you could 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>](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 <http://bombich.com/kb/cc5/preparing-your-backup-disk-backup-os-x#high_sierra>](http://bombich.com/kb/cc5/preparing-your-backup-disk-backup-os-x#high_sierra))
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

Sample Usage Scenarios

I want to clone my entire hard drive to a new hard drive or a new machine

There are many different reasons to make an exact clone of your hard drive. Suppose your laptop is damaged and you must send it in for repair. In the meantime, you not only have to borrow another computer for the duration of the repair, you also don't have your data, applications and work environment exactly as they were on your machine. This lack of organization can be very frustrating and inhibit your productivity. When you get your machine back from repair, you have to deal with locating any modified documents on your loaner computer and copying them to your original computer. Also, Apple recommends that you backup your data before sending in a machine for repairs because they are not responsible for lost data.

In this situation, it would be ideal to simply copy off the entire contents of your hard drive to an external hard drive — to create a "bootable clone" of your production machine. You can then boot a loaner machine from this bootable clone and work from it as if working from your original machine (see the related documentation below for common questions related to running another Mac from your backup).

When you need a complete, simple backup of your entire hard drive:

1. Open Carbon Copy Cloner
2. Choose the volume that you want to clone from the Source selector
3. Choose a [properly-formatted volume <http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x>](http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x) from the Destination menu
4. Click the Clone button

If you want to update your cloned volume in the future, simply run the same task (or schedule it so it runs automatically) and CCC will update the backup volume with only the items that have changed since your last backup.

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 cloning your old Mac onto your new Mac won't work. Due to this limitation, 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. Once you have migrated your user accounts and applications using Setup Assistant or Migration Assistant, you can continue to use Carbon Copy Cloner 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 "_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.

Apple Kbase #HT2186: Use the Mac operating system that came with your Mac, or a compatible newer version <<https://support.apple.com/kb/HT201686>>

Apple Kbase #HT204350: Move your content to a new Mac [Mavericks and later] <<https://support.apple.com/kb/HT204350>>

Apple Kbase #HT3322: How to use Migration Assistant to transfer files from another Mac [Lion and Mountain Lion] <<https://support.apple.com/kb/ht3322>>

Related Documentation

- Can I back up one computer and use the clone to restore another computer? <<http://bombich.com/kb/cc5/can-i-back-up-one-computer-and-use-clone-restore-another-computer>>

I want to back up my data to a Time Capsule, NAS, or other network volume

Time Capsule and other network storage appliances are becoming 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. Indeed, this storage is well suited for the sharing of media files, but there are some logistical and practical hurdles to backing up large amounts of data to these devices. For example, we do not recommend backing up macOS system files to a NAS; there are simply too many logistical and reliability concerns with this configuration. Below we explain how to back up your data to a network volume, then we describe some of the limitations and performance expectations of this solution.

Note on bootability: If you require a bootable backup **or if you ever need to restore system files**, you must use an [external hard drive enclosure <http://bombich.com/kb/ccc5/choosing-backup-drive>](http://bombich.com/kb/ccc5/choosing-backup-drive) attached directly to your Mac to create a bootable backup.

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 your home folder to a NAS volume with CCC:

1. Choose **Choose a folder** from the Source selector.
2. Select your home folder as the source (shortcut: press Command+Shift+H to navigate to your home folder)
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. Click the **Clone** button to run the task immediately, or schedule the task to run later.

Restoring from a data backup on a NAS or network share

Restoring your data from data-only backup to a network share can be done with the following steps:

1. Close all applications and all Finder windows
2. Open CCC and create a new task
3. Drag your home folder from the network share onto CCC's Source selector
4. Drag your home folder from the current startup disk to CCC's Destination selector
5. Click the **Advanced Settings** button
6. Under the Troubleshooting section, check the box next to **Don't preserve permissions** (this will avoid any ownership issues that would arise from your account having a different numeric ID on the old and new system)
7. Click the Clone button
8. When the task completes, reboot the computer

Performance expectations when using a network volume

"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 involves several of them. If you're finding that your network backups are slow, consider our [network backup troubleshooting suggestions <http://bombich.com/kb/ccc5/troubleshooting-slow-performance-when-copying-files-or-from-network-volume>](http://bombich.com/kb/ccc5/troubleshooting-slow-performance-when-copying-files-or-from-network-volume).

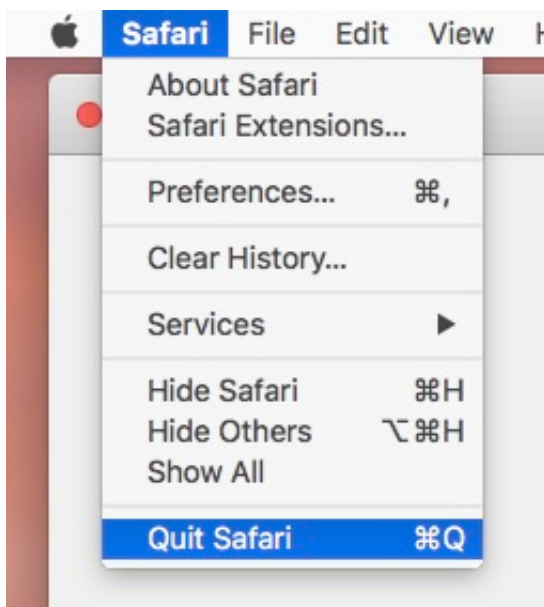
Restoring an item from a hidden folder

*This article is primarily written for users running **macOS Yosemite or El Capitan**. If you are running macOS Sierra or later, simply press Command+Shift+Period (⌘ Shift ↑ .) to toggle the Finder's display of hidden items, then you can easily navigate to the hidden items in the Finder and restore those items via drag and drop.*

Usually it's easiest to restore a single item from your backup by simply dragging it from the backup volume to your original source volume. Sometimes, though, it's not that easy. Suppose, for example, that you have inadvertently deleted all of your Safari bookmarks. The Safari Bookmarks file is stored in a hidden folder within your home directory, and the fact that this folder, and the folder on the backup volume are both hidden makes accessing that file in the Finder quite difficult. The steps below demonstrate how to restore this item from your Carbon Copy Cloner backup volume.

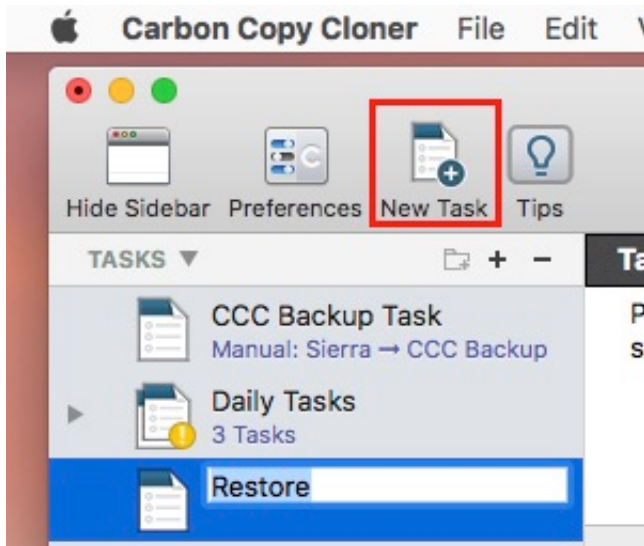
Quit Safari

Before you restore any files that are referenced by a particular application, you should quit that application first.



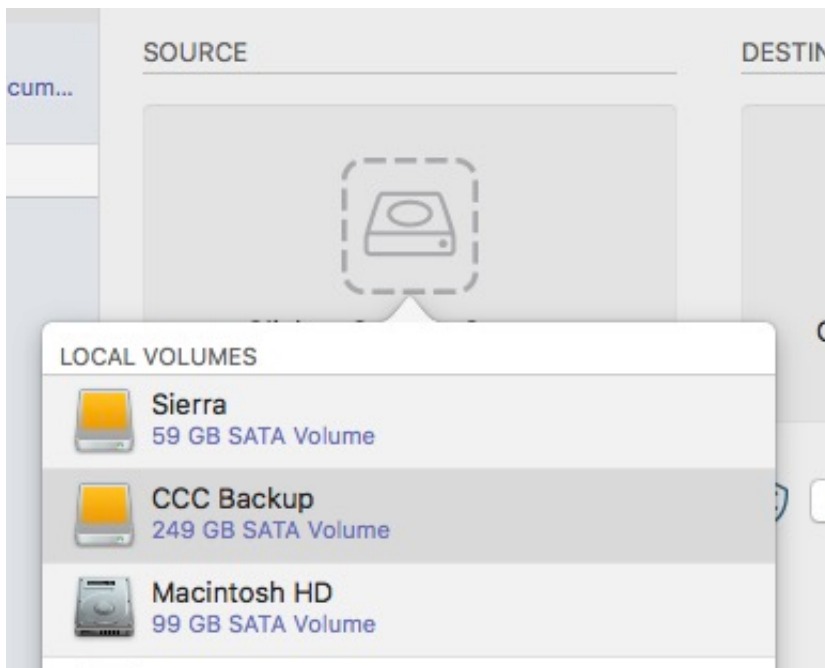
Open CCC and create a new task

Rather than making changes to your usual backup task, click the "+" button to create a new task. You can delete the task when you're done.



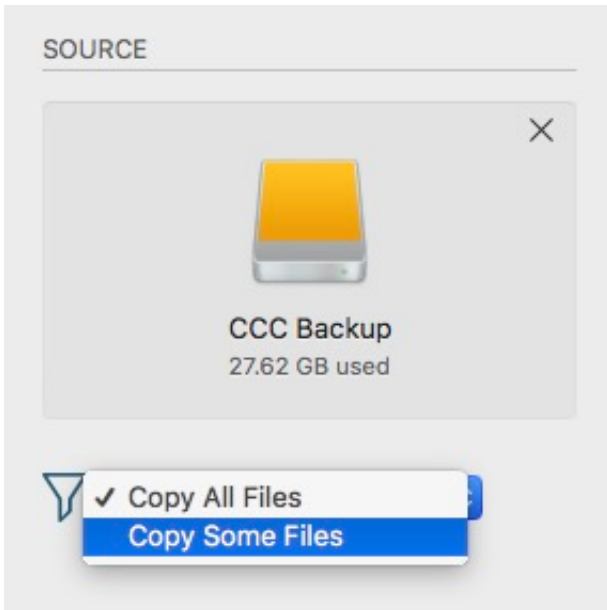
Select your backup volume as the source

Click on the Source selector and choose your backup volume as the source.



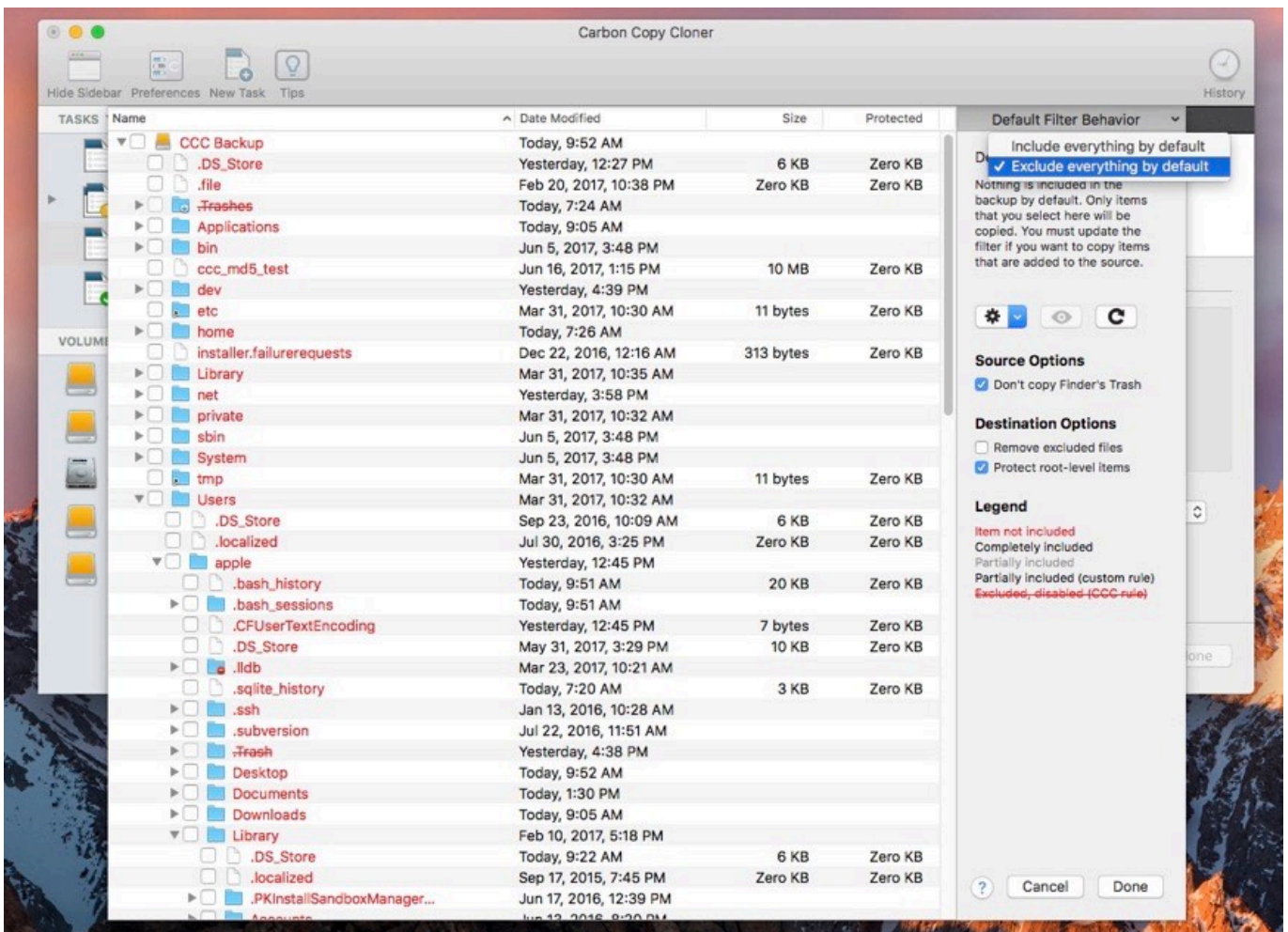
Choose "Some Files..." from the Clone popup menu

We don't want to restore everything, so choose the "Some Files..." option in the Clone popup menu.



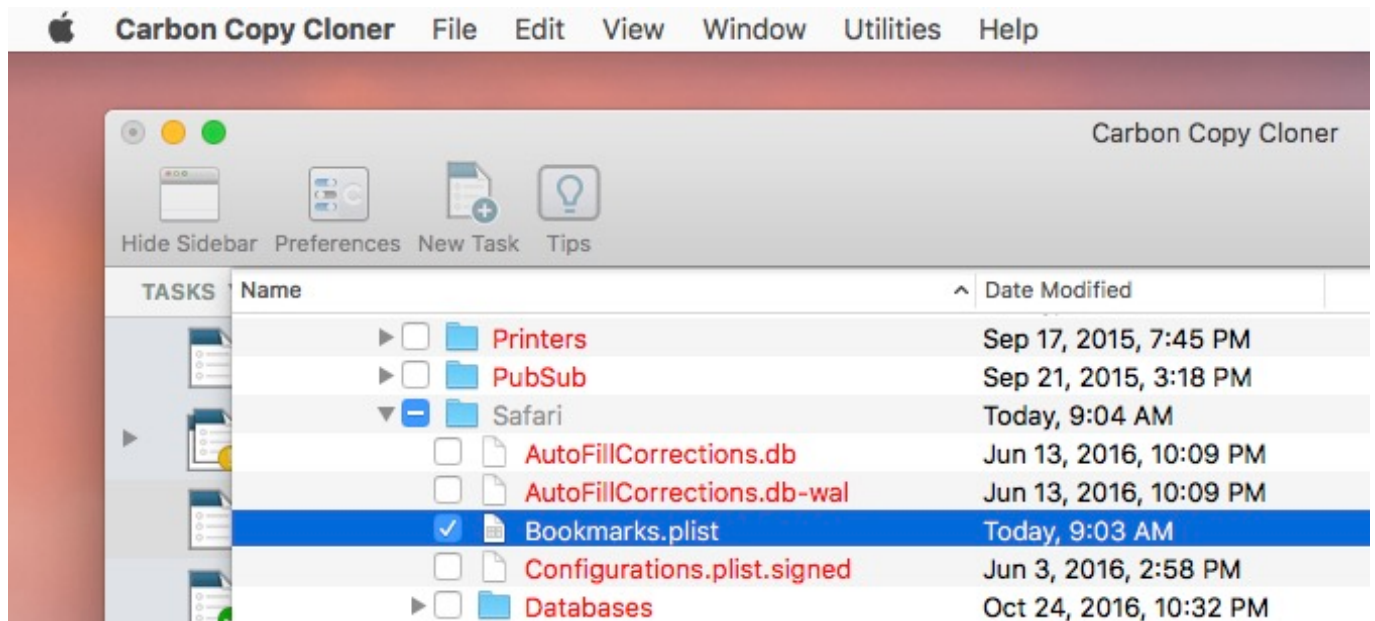
Exclude everything by default

We're only restoring a single item, so change the task filter's default behavior to "Exclude everything by default".



Navigate to the desired folder and select the item you would like to restore

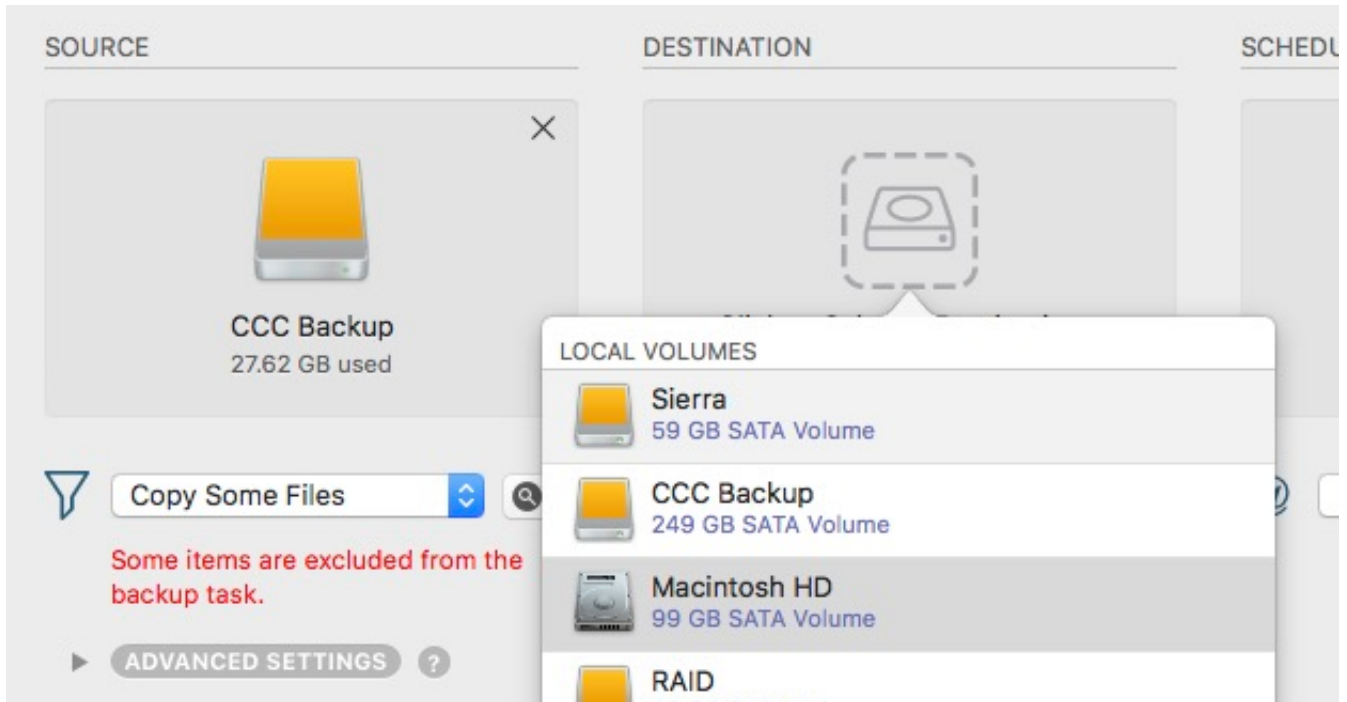
Start opening disclosure triangles next to the folders that you would like to descend into until you reach the item you want to restore. In this case, the path is Users > apple > Library > Safari. The Library folder is hidden in the Finder, but CCC makes it visible here so you can restore items from it.



Check the box next to the item you want to restore. **Bookmarks.plist** is the file we're trying to restore in this case.

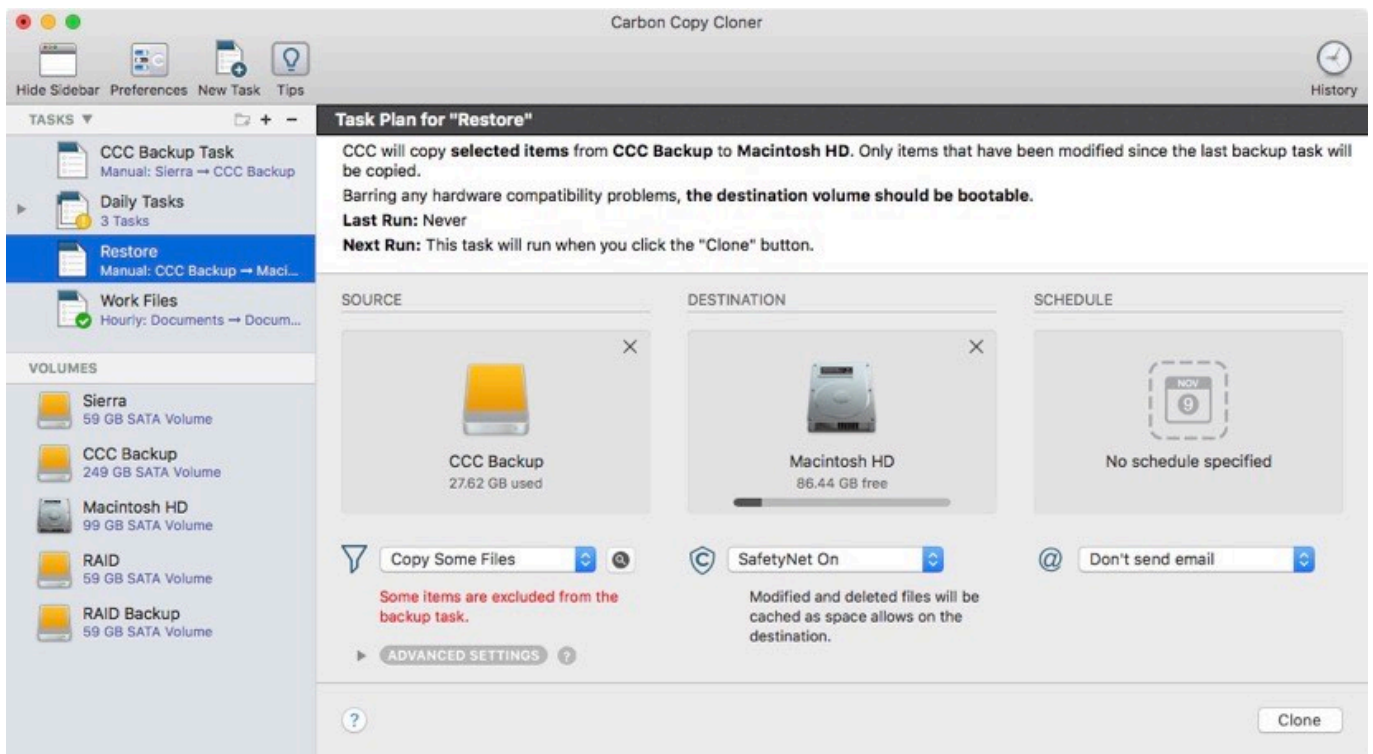
Select the volume to restore to as the destination

In this case, we want to restore the item back to the startup disk, so choose **Macintosh HD** from the destination selector. When you select your startup disk as the destination, CCC will produce a stern warning about restoring files to the startup disk. To prevent accidentally restoring system files to an active startup disk, CCC will explicitly exclude system files from this restore task. In this case, we can ignore the dialog because we already excluded everything except for the single file.



Click the Clone button

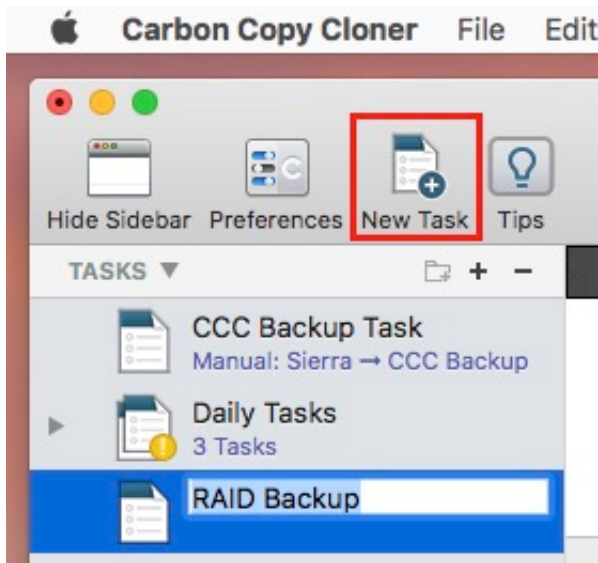
This restore task will go really quickly, and when it's done you can open Safari to verify that your bookmarks have been restored.



Cloning one external hard drive to another external hard drive

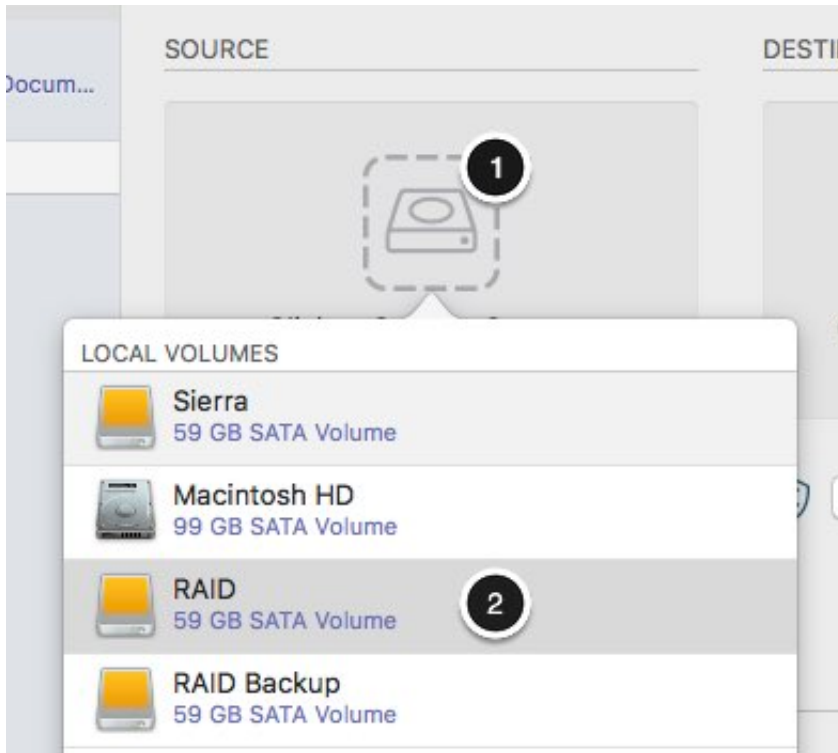
Create a new task

Click on the **New Task** button in the toolbar to create a new task, then type in a name for the new task.



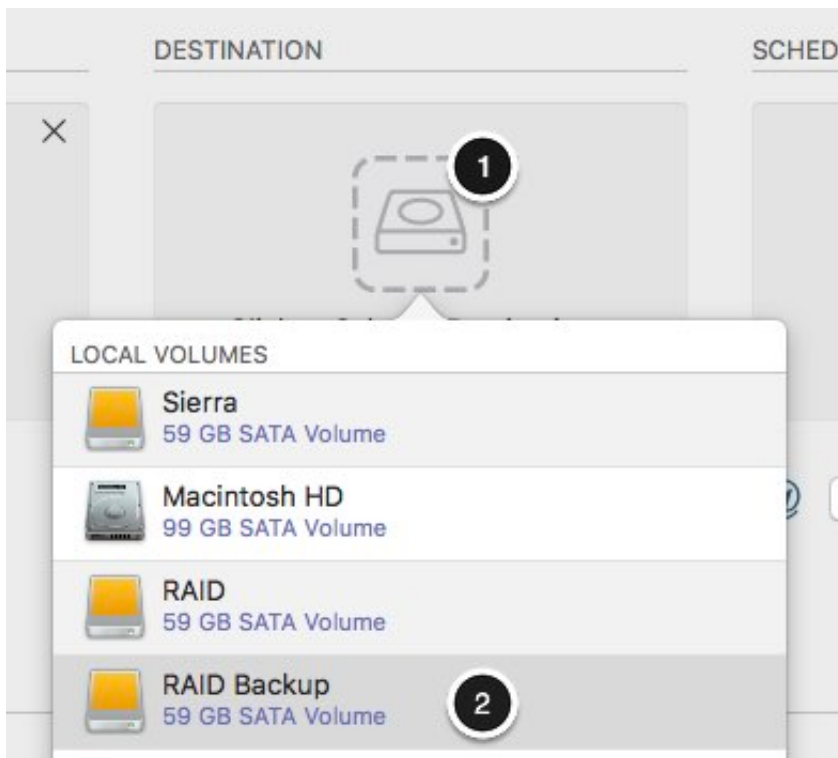
Select a source volume

Click on the Source selector button, then choose the volume that you want to copy files from.



Select a destination volume

Click on the Destination selector button, then choose the volume that you want to copy files to.



Click the Clone button

Click the Clone button to copy files right away, or click the Scheduler selector to configure the task to

run on a regular basis.

Related Documentation

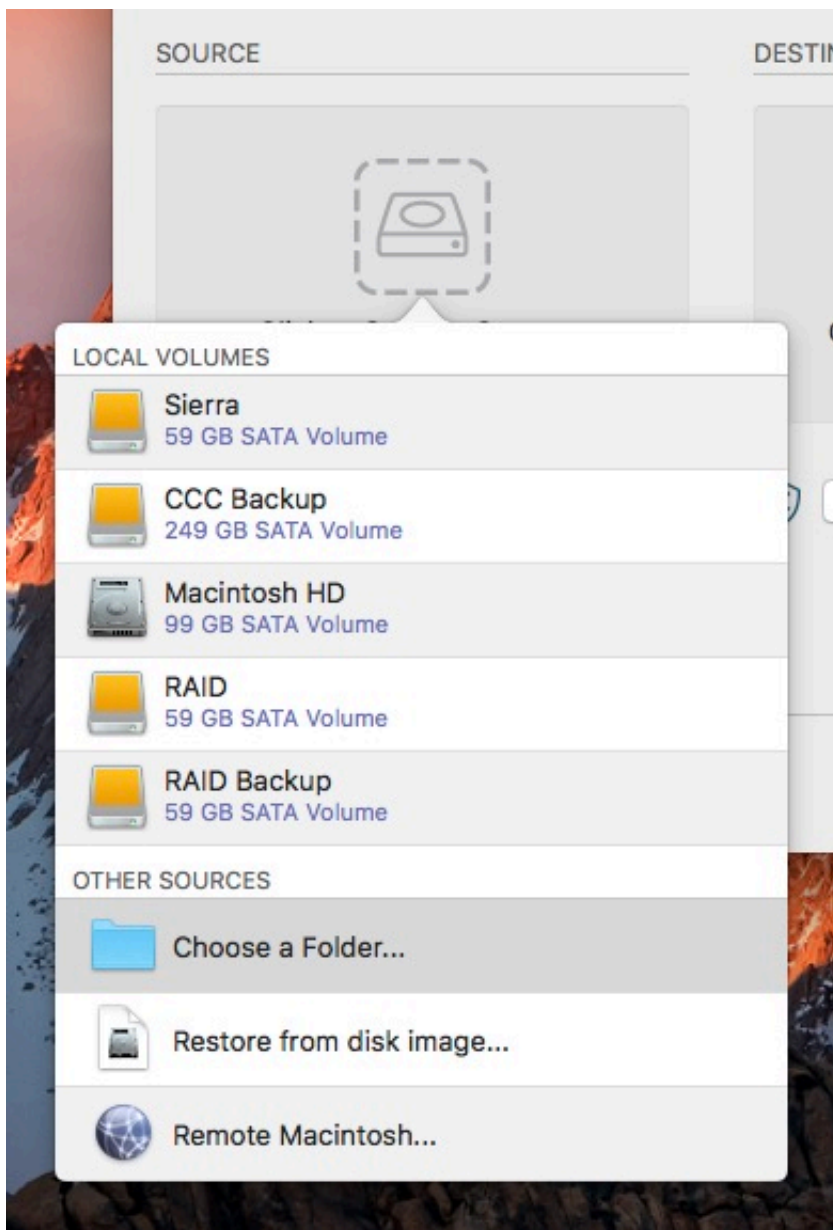
- [How to set up a scheduled backup <http://bombich.com/kb/cccl5/how-set-up-scheduled-backup>](http://bombich.com/kb/cccl5/how-set-up-scheduled-backup)

Folder-to-Folder Backups

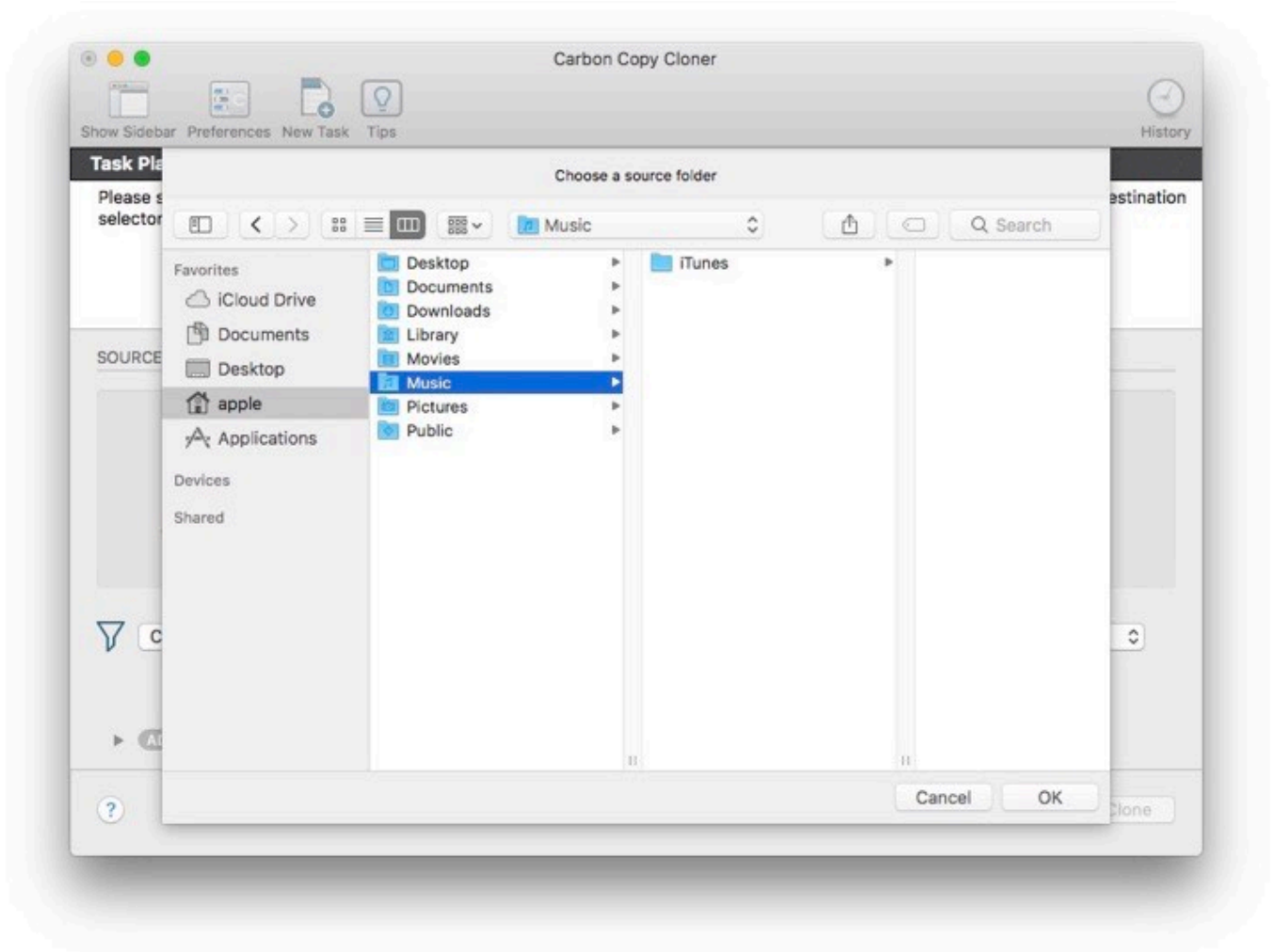
When you select a volume as the source and destination, CCC copies the entire contents of that volume (minus anything you exclude) to the destination volume, preserving the full hierarchy of folders on the source. If you don't want to preserve that hierarchy, you can back up a specific folder from the 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

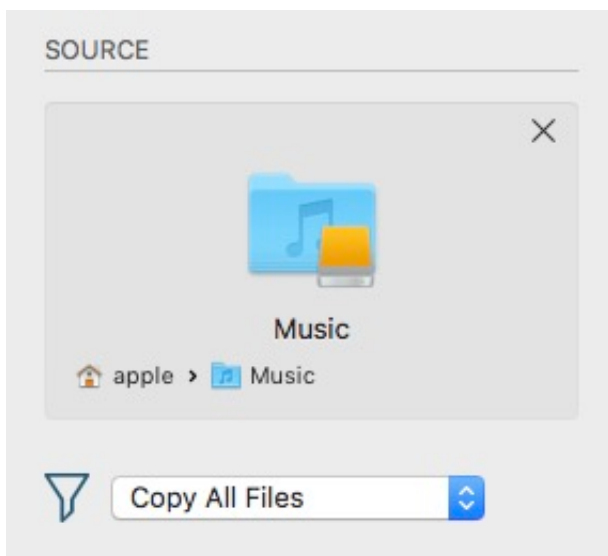
From the Source selector, select **Choose a Folder...**



Select your source folder and click **OK**.

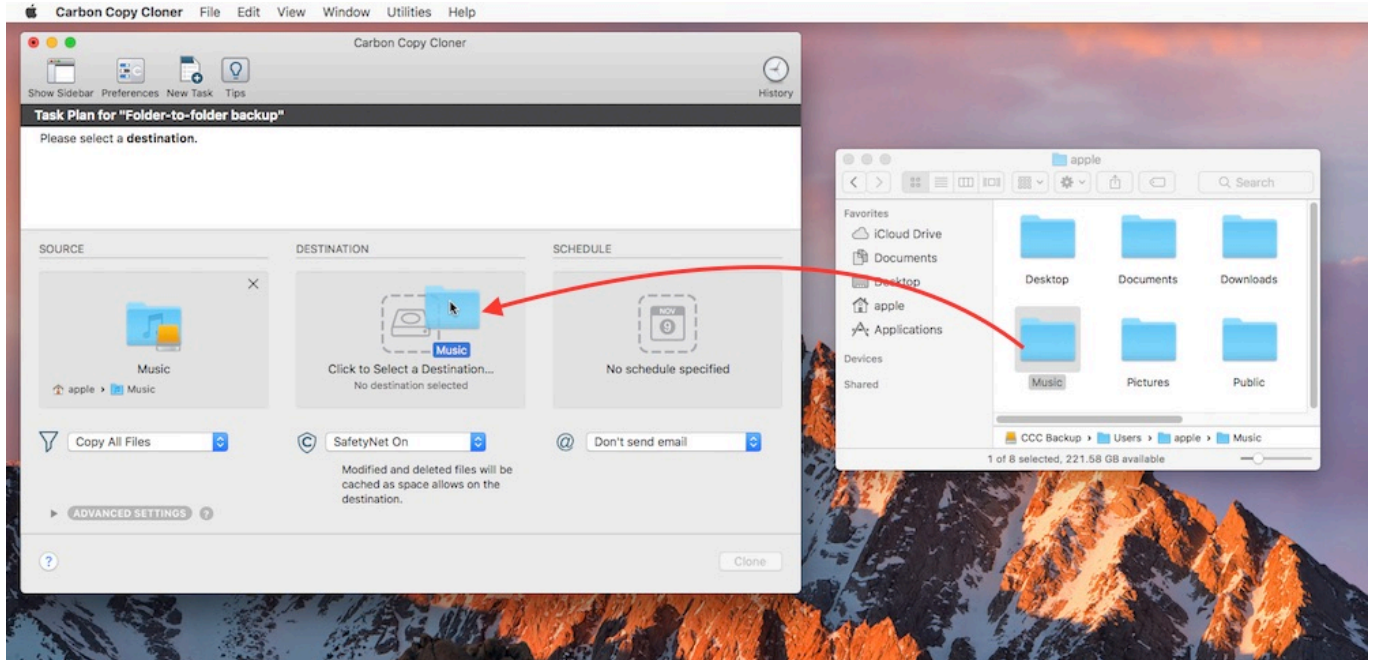


When correctly selected, the Source selector should display a folder icon and a path to the folder beneath it. Note that this path may be truncated but if you mouse over it, individual items will be expanded. You may choose to **Copy All Files**, the default, or define a task filter by choosing **Copy Some Files** from the Filter popup menu.

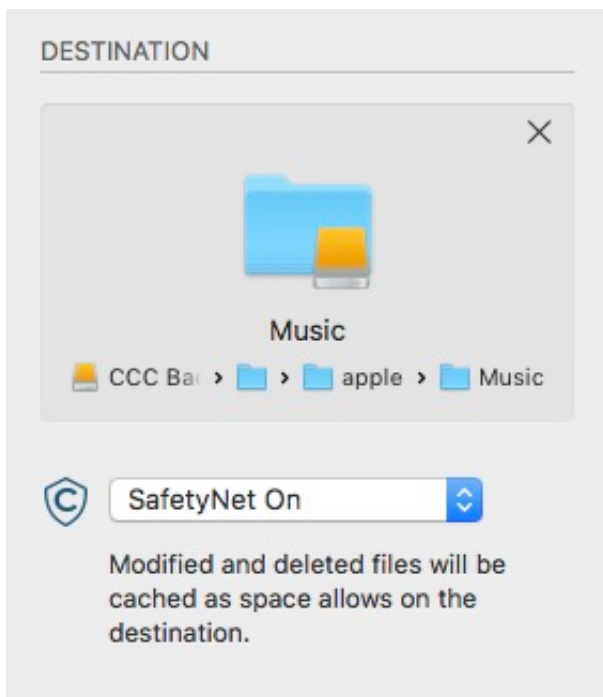


Choose your destination

The steps used to select the source need to be repeated for the 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.

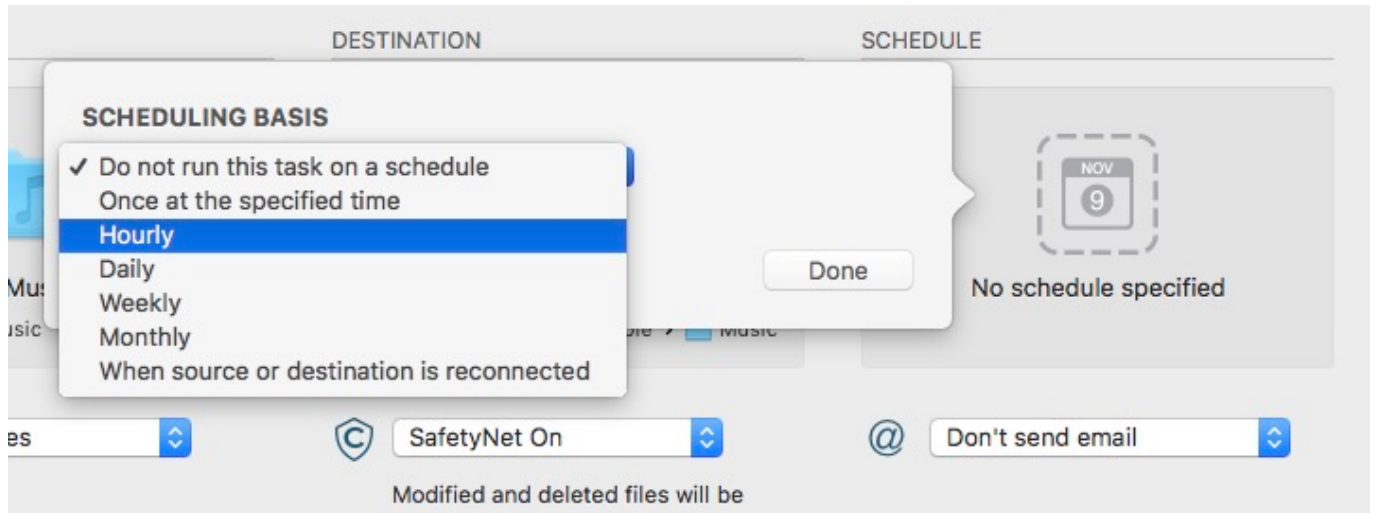


Once you have selected the destination folder, the Destination box should have a folder icon in it with the path displayed beneath it. You may choose to leave SafetyNet on or turn it off. To learn more about SafetyNet, please see [Protecting data that is already on your destination volume: The Carbon Copy Cloner SafetyNet <http://bombich.com/kb/ccl5/protecting-data-already-on-your-destination-volume-carbon-copy-cloner-safetynet>](http://bombich.com/kb/ccl5/protecting-data-already-on-your-destination-volume-carbon-copy-cloner-safetynet).



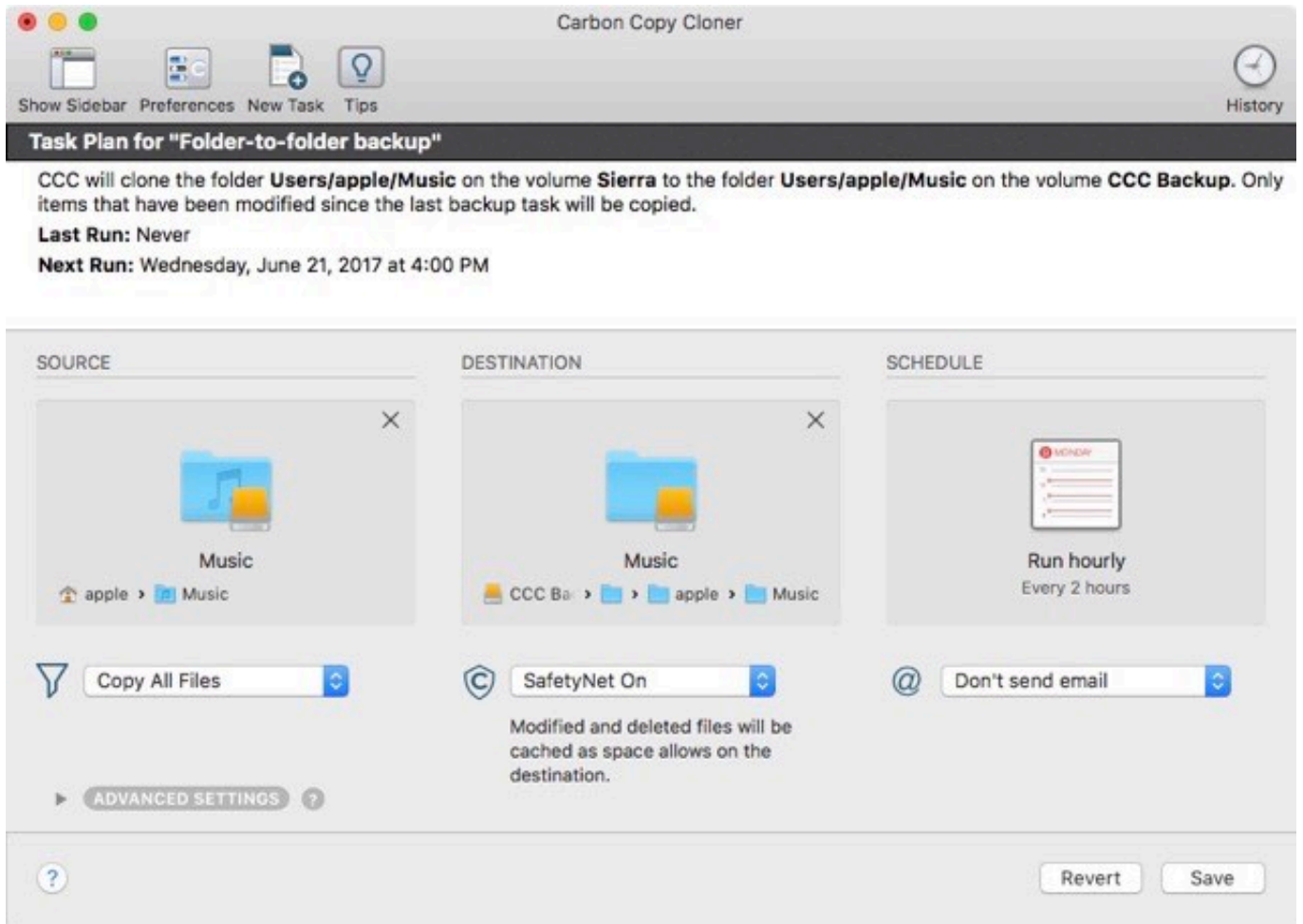
Schedule the backup

Click in the Schedule box and design a backup schedule that meets your needs. Click **Done** when you have finished.



Save and clone

Once you have your source, destination and schedule complete, click on Save in the bottom right-hand corner. This will save the task and you can find it in the tasks area on the left sidebar. If you don't see the sidebar, click on **Show Sidebar** in the CCC window header. You may click the **Clone** button to run the backup manually, or let it run on a schedule.



Carbon Copy Cloner

Show Sidebar Preferences New Task Tips History

Task Plan for "Folder-to-folder backup"

CCC will clone the folder **Users/apple/Music** on the volume **Sierra** to the folder **Users/apple/Music** on the volume **CCC Backup**. Only items that have been modified since the last backup task will be copied.

Last Run: Never

Next Run: Wednesday, June 21, 2017 at 4:00 PM

SOURCE **DESTINATION** **SCHEDULE**

SOURCE: Music
apple > Music

DESTINATION: Music
CCC Ba > > apple > Music

SCHEDULE: Run hourly
Every 2 hours

Copy All Files SafetyNet On Don't send email

Modified and deleted files will be cached as space allows on the destination.

ADVANCED SETTINGS

Revert Save

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 5 offers an [option to back up the Finder's Trash](#) <<http://bombich.com/kb/ccc5/excluding-files-and-folders-from-backup-task#trash>> in the Task Filter window. Choose **Copy Some Files** from the popup menu underneath the Source selector to reveal CCC's Task Filter window.

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:

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 [boot from your backup volume to recover the item](#) <<http://bombich.com/kb/ccc5/how-restore-from-your-backup>>, because once booted from the backup volume, that item **will** appear in the Trash.

You can also recover an item from a user home folder Trash folder on the backup volume using the procedure described here: [Restoring an item from a hidden folder](#) <<http://bombich.com/kb/ccc5/restoring-item-from-hidden-folder>>. The hidden Trash folder is located at `/Users/{yourname}/.Trash`.



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 **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 chose "Copy some files" and 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 <http://bombich.com/kb/ccc5/folder-folder-backups>](http://bombich.com/kb/ccc5/folder-folder-backups)



Troubleshooting

macOS Big Sur Known Issues

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 volumes cloned by CCC (whether CCC used ASR or its own file copier). Some Big Sur cloned volumes do not appear in the Startup Disk Preference Pane, despite being perfectly bootable.

We have reported this issue to Apple (FB8889774) and we are currently awaiting a response.

Workaround: To boot from the cloned volume, restart your Mac while holding down the Option key, then select the cloned 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 cloned 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)" <<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 clone just the System volume. As a result, every time an OS update is applied to the source, we would have to erase the whole destination volume (including any existing snapshots on that volume <<http://bombich.com/kb/coc5/leveraging-snapshots-on-apfs-volumes>>) just to update the system on the destination.

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.

We made a feature request to Apple in September 2019 (FB7328230) to allow ASR to clone just the System volume. Apple's APFS team acknowledged the request in June 2020 and clarified the requirements, and now we're waiting on the implementation.

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. **If you would like to update the OS on the backup volume, you can boot your Mac from the backup and apply any updates via the Software Update preference pane in the System Preferences application.** This is not something that we anticipate you would need to do frequently, nor even proactively. You could apply updates before attempting to restore from the backup, for example, if that need ever arises.

Apple Software Restore doesn't yet support the storage in Apple Silicon Macs

In the current shipping version of macOS Big Sur (11.2.3), Apple's ASR utility cannot replicate the startup disk in an M1-based Mac. Attempting to do so results in an error:

'Apple System Restore Tool': Source volume format not yet supported in this version of macOS

Apple is aware of the problem and is working towards resolving it for a future update to macOS. CCC 5.1.23+ will automatically perform Data Volume backups on M1 Macs and avoid any attempts to copy a System volume on those Macs — that's a complete backup of your data, applications, and

system settings. If you would like to make your Apple Silicon Mac backup bootable, you can [install Big Sur onto the CCC Data Volume backup](#) <http://bombich.com/kb/ccc5/creating-and-restoring-data-only-backups#install_macos>. Please keep in mind, however, that [your CCC backup does not have to be bootable for you to be able to restore data from it](#) <<http://bombich.com/kb/ccc5/creating-and-restoring-data-only-backups#migrate>>.

When Apple posts an update to macOS that resolves the ASR problem, we'll post an update to CCC that adds back support for copying the System volume on these Macs.

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 creates 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 ".Volumelcon.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/.Volumelcon.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 .Volumelcon.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 on M1 Macs, leads to kernel panics

We have received several reports from M1 Mac users of kernel panics that occur while copying files to an SMB-mounted NAS volume. The kernel panic reports have confirmed that the SMB filesystem client (implemented via the smbfs.kext kernel extension) was stalled, which led to a ["watchdog" panic](#). These panic reports are automatically submitted to Apple, so we can presume that Apple is aware of the problem and working on a solution.

Workaround: Users have reported that using AFP rather than SMB consistently works around the panic (in cases where using AFP is an option):

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. Open CCC and select the applicable backup task
5. Drag the currently-mounted NAS volume (or folder or disk image on that volume) onto CCC's source or destination selector (whichever is applicable for your particular task)

macOS Catalina Known Issues

Apple introduced a bug in 10.15.5 that prevents the creation of firmlinks

The `chflags` system call no longer works correctly on 10.15.5 with regard to setting the special "firmlink" flag that establishes links between the System and Data volume group members. If you're establishing a new backup of macOS 10.15.5 or later, CCC 5.1.17 (and earlier) will be unable to create a correctly-functioning APFS volume group. Many folders on the destination volume will appear empty, and the volume will not be bootable.

Solution: Update to macOS 10.15.6 and CCC 5.1.20. See [this blog post for more details <http://bombich.com/blog/2020/05/27/bug-in-macos-10.15.5-impacts-bootable-backups-weve-got-you-covered>](http://bombich.com/blog/2020/05/27/bug-in-macos-10.15.5-impacts-bootable-backups-weve-got-you-covered).

We have reported this issue to Apple (FB7706647) and we are currently awaiting a response. Update: Apple resolved this issue in macOS 10.15.6. Apple made this "bug" a permanent change, however, in macOS Big Sur.

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>](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).

We recommend using NAS devices for secondary backups. **For primary backups, we recommend that you procure a USB or Thunderbolt hard drive and create a bootable backup on that locally-attached disk.** Local, bootable backups are much simpler and more reliable, and a lot easier to restore from should your Mac's startup disk fail. The logistics of restoring the operating system from a disk image on a network volume are pretty complicated if you don't have a functional startup disk. Providing that functional startup disk is the primary appeal of the CCC backup solution.

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](http://bombich.com/kb/ccc5/choosing-backup-drive#recommendations) <<http://bombich.com/kb/ccc5/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](http://bombich.com/kb/ccc5/help-my-clone-wont-boot#install_macos) <http://bombich.com/kb/ccc5/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](http://bombich.com/kb/ccc5/choosing-backup-drive#recommendations) <<http://bombich.com/kb/ccc5/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 <http://bombich.com/kb/ccc5/choosing-backup-drive#not_recommended> 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 non-bootable 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 we are currently awaiting a response.

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 <http://bombich.com/kb/ccc5/why-cant-i-eject-destination-volume-after-backup-task-has-completed>](http://bombich.com/kb/ccc5/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.

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](http://bombich.com/kb/ccc5/frequently-asked-questions-about-ccc-and-macos-catalina#conversion_encrypted) <http://bombich.com/kb/ccc5/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?](http://bombich.com/kb/ccc5/frequently-asked-questions-about-ccc-and-macos-catalina#conversion_encrypted) <http://bombich.com/kb/ccc5/frequently-asked-questions-about-ccc-and-macos-catalina#conversion_encrypted>
- [Working with FileVault Encryption](http://bombich.com/kb/ccc5/working-filevault-encryption) <<http://bombich.com/kb/ccc5/working-filevault-encryption>>
- [Frequently Asked Questions about encrypting the backup volume](http://bombich.com/kb/ccc5/frequently-asked-questions-about-encrypting-backup-volume) <<http://bombich.com/kb/ccc5/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?](http://bombich.com/kb/ccc5/working-filevault-encryption#highest_security) <http://bombich.com/kb/ccc5/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.

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 ".Volumelcon.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/.Volumelcon.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 .Volumelcon.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.

Resolved Issues

On login, macOS fails to unlock and mount the Data volume of an encrypted APFS volume group

If you have an installation of macOS Catalina on a separate volume (e.g. a backup disk) and FileVault is enabled on that volume, the prompt to unlock the volume only unlocks the System volume. If the Data volume is not unlocked and mounted, the volume does not work correctly and the bulk of your data will appear to be missing.

Workaround: You must manually mount the Data volume in CCC (or Disk Utility) to get access to

your data on the backup: Right-click the Data volume in CCC's sidebar and choose **Mount**.

We have reported this issue to Apple (FB6786776) and we are currently awaiting a response.

Update: This issue appears to be resolved in Catalina Beta 7.

The APFS filesystem causes a kernel panic when remounting the System volume in an encrypted APFS volume group

If you unmount and then remount the System volume (or sometimes when you then unmount the System volume again) in an encrypted APFS volume group, the system will kernel panic. CCC will only need to mount or unmount the System volume of the backup disk during a backup task if changes have been made to the source System volume (e.g. after applying a software update). If a kernel panic occurs, simply re-run the backup task after the system reboots to complete the backup.

Partial mitigation: Disabling Spotlight on the destination appears to reduce the incidents of kernel panics. 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.

Update: This issue appears to be resolved in Catalina Beta 9.

System Preferences cannot enable FileVault on external volumes

This is an emerging issue as of Catalina Beta 6. When attempting to enable FileVault on an external volume (whether it is a backup or an installation placed there by the Installer), the FileVault preference pane claims:

FileVault Failed [sic]

This operation is restricted by your settings in System Preferences > Security & Privacy > Privacy > Files and Folders.

The meaning of this dialog is ambiguous, and you can't actually make configuration changes in the "Files and Folders" category. In fact, the problem is not that you have misconfigured something in "Files and Folders", rather some component of the Security Preference Pane, or a service that it relies upon to enable FileVault **lacks** access to external volumes (i.e. "Full Disk Access"). The identity of that service is not made clear by this dialog.

We have reported this issue to Apple (FB7083306) and we are currently awaiting a response.

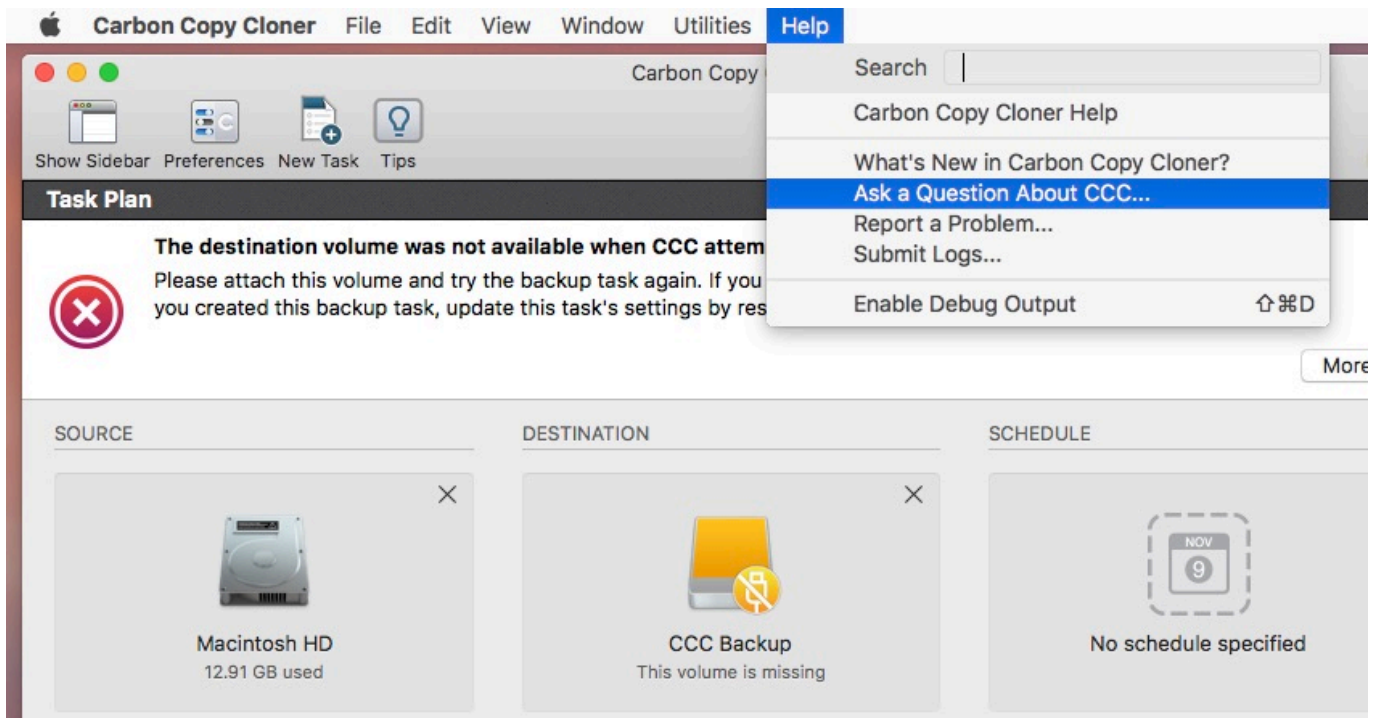
Update: This issue appears to be resolved in Catalina Beta 7.

How do I get help?

The best way to receive help is by requesting it from within the Carbon Copy Cloner 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 Carbon Copy Cloner'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.

Carbon Copy Cloner 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. Donec finibus egestas sagittis. Etiam id nisi turpis. Donec eu consequat justo. Vestibulum eget egestas elit, et ornare augue. Duis dapibus consectetur tortor eu fringilla. Proin tellus leo, elementum ac odio ac, ultrices mattis sem. In ut sapien porta neque hendrerit lobortis ac commodo massa. In iaculis rutrum aliquet. Nulla facilisi. Integer et nisi aliquam, fringilla erat in, rhoncus libero. Nulla ac aliquam enim, laoreet aliquam odio. Ut lobortis diam id ornare venenatis. Aliquam ut erat et libero efficitur viverra.

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...

Help! My clone won't boot!

We're happy to [help you troubleshoot](http://bombich.com/software/get_help) <http://bombich.com/software/get_help> your bootability problems. Before you ask for help, please try the troubleshooting steps below. If you're having trouble with the steps or have run out of options, please let us know how far you got, or how far your Mac gets into the boot process.

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](http://bombich.com/kb/ccc5/creating-and-restoring-data-volume-backups#migrate) <<http://bombich.com/kb/ccc5/creating-and-restoring-data-volume-backups#migrate>> — **do not attempt to restore an older Mac's backup onto a new Mac.**

Related Documentation

- [Can I back up one computer and use the clone to restore another computer?](http://bombich.com/kb/ccc5/can-i-back-up-one-computer-and-use-clone-restore-another-computer) <<http://bombich.com/kb/ccc5/can-i-back-up-one-computer-and-use-clone-restore-another-computer>>
- [Apple Kbase #HT2186: Don't install older versions of Mac OS than what comes with your computer](https://support.apple.com/kb/HT2186) <<https://support.apple.com/kb/HT2186>>
- [Apple Kbase #HT204350: Move your content to a new Mac](https://support.apple.com/en-us/HT204350) <<https://support.apple.com/en-us/HT204350>>

macOS 11, "Big Sur" bootability troubleshooting

Starting in macOS Big Sur, the system now resides on a "[Signed System Volume](https://developer.apple.com/news/?id=3xpv8r2m)" <<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 make a backup of a Big Sur startup disk with CCC 5.1.23 or later, CCC will automatically use Apple's proprietary APFS replication utility (ASR) to make an 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. If that does not produce a bootable device, then the device is not suitable for functioning as a bootable device on your Mac.

Related Documentation

- [Some Big Sur startup volumes don't appear in the Startup Disk Preference Pane](http://bombich.com/kb/ccc5/help-my-clone-wont-boot#ssv) <<http://bombich.com/kb/ccc5/help-my-clone-wont-boot#ssv>>
- [Cloning macOS System volumes with Apple Software Restore](http://bombich.com/kb/ccc5/cloning-macos-system-volumes-apple-software-restore) <<http://bombich.com/kb/ccc5/cloning-macos-system-volumes-apple-software-restore>>
- [Installing macOS onto a CCC backup](http://bombich.com/kb/ccc5/creating-and-restoring-data-only-backups#install_macos) <http://bombich.com/kb/ccc5/creating-and-restoring-data-only-backups#install_macos>

Sometimes the Mac's firmware cannot detect your backup device

When you boot your Mac while holding down the Option key, the [Mac Startup Manager](https://support.apple.com/en-gb/HT202796#startupmanager) <<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](http://bombich.com/kb/ccc5/frequently-asked-questions-about-ccc-and-macos-catalina#encrypted_non_bootable) <http://bombich.com/kb/ccc5/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) <<https://support.apple.com/en-us/HT201316>>. Some people have found that cloning 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) <<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) <<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 <http://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 <http://bombich.com/kb/ccc5/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 CCC 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>](https://support.apple.com/en-us/HT204455)

T2-based Macs can't boot from encrypted HFS+ volumes

Our testing has confirmed that Macs with Apple's T2 controller chip cannot boot from an encrypted, "Mac OS Extended"-formatted, external volume. Booting from an external volume works fine in general, but if your external disk is formatted using Apple's legacy HFS+, "Mac OS Extended" format, enabling FileVault on that volume will render it non-bootable, producing an error message like this on startup:

A software update is required to use this startup disk. You can update now or select another startup disk.

Spoiler alert: The "Update" option does not work. This may be a bug in the firmware of the T2 Macs, or it may be a limitation that Apple does not intend to address. In either case, if you want to encrypt your external, bootable backup of a T2-based Mac, we recommend formatting that backup volume as APFS.

Make the Startup Manager load additional drivers

Some third-party external devices use [Option ROM firmware <https://en.wikipedia.org/wiki/Option_ROM>](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. [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, 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.
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:

USB 2 Micro B



USB 3 Micro B



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:

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](http://bombich.com/kb/coc5/creating-and-restoring-data-only-backups#install_macos) <http://bombich.com/kb/coc5/creating-and-restoring-data-only-backups#install_macos>. If that fails to make the disk bootable, then it definitely isn't going to happen. **Please report these enclosures to us** <http://bombich.com/software/get_help> so we can assemble a list of troublesome enclosures.

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 <<http://bombich.com/kb/coc5/preparing-your-backup-disk-backup-os-x>>, then reclone your startup disk to the destination.
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 commands:

```
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](#).

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](#) <<http://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](#) <<http://bombich.com/kb/ccc5/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](#) <<http://bombich.com/kb/ccc5/choosing-backup-drive#recommendations>>
- [Migrating data from a CCC backup using Migration Assistant](#) <<http://bombich.com/kb/ccc5/creating-and-restoring-data-only-backups#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://www.cindori.org/trim-enabler-and-yosemite/) to modify macOS Storage drivers.

- **As of macOS Catalina, 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 cloned volume while your Mac is booted in [Recovery mode](https://support.apple.com/en-us/HT204904) <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 cloned volume while booted in [Recovery mode](https://support.apple.com/en-us/HT204904) <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](http://bombich.com/kb/ccc5/automated-maintenance-ccc-safetynet-folder) <http://bombich.com/kb/ccc5/automated-maintenance-ccc-safetynet-folder>
- [Snapshots and space concerns; Deleting snapshots](http://bombich.com/kb/ccc5/leveraging-snapshots-on-apfs-volumes#space) <http://bombich.com/kb/ccc5/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. We have found a few conditions that will prevent you from making a startup disk selection:

APFS is not a supported, bootable format on older OSes

If you boot from an older backup, e.g. macOS Sierra, APFS-formatted volumes may mount in the Finder, but you may have trouble selecting them as a startup disk. APFS was a beta filesystem on Sierra; the components required for making an APFS volume bootable were not yet baked.

Likewise, support for APFS-formatted Fusion volumes was not added until macOS Mojave. If you boot from a High Sierra backup volume, you'll notice that your APFS-formatted, Mojave-containing Fusion volume is mounted read-only, and you will be unable to set that volume as the startup disk.

The solution in both cases is to use the Startup Manager (boot your Mac while holding down the Option key) to select an alternate boot disk. Once you have booted your Mac from the newer OS, you will be able to reset the startup disk selection.

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. Multiple, bootable volumes within a single APFS container is a supported configuration, but you can only make the second volume bootable if you boot from some other startup disk for the duration of the cloning procedure. Likewise, you will be unable to change the startup disk selection to the second volume while booted from the first volume. The solution is the same as above — use the Startup Manager (boot your Mac while holding down the Option key) to temporarily change the startup disk selection, then set the startup disk explicitly to the new startup volume.

Catalina users: 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

The bless utility cannot bless some Firewire-attached devices

We have received a handful of reports from macOS Mojave users that attempting to select a Firewire-attached volume as the startup disk yields this same "unable to bless" error. In the cases where USB was an alternative option, selecting the device as the startup disk works fine when connecting the same device to the Mac via USB.

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](http://bombich.com/kb/ccc5/frequently-asked-questions-about-ccc-and-macos-catalina#encrypted_non_bootable) <http://bombich.com/kb/ccc5/frequently-asked-questions-about-ccc-and-macos-catalina#encrypted_non_bootable>.
- 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 excellent success with is the WD MyPassport SSD.
- [Hands Off!](http://bombich.com/kb/discussions/no-boot-from-firewire800-disc) and possibly [Little Snitch](http://bombich.com/kb/discussions/no-boot-from-firewire800-disc) may prevent a cloned volume from booting <<http://bombich.com/kb/discussions/no-boot-from-firewire800-disc>>
- [Some Macs have trouble booting from USB 3.0 enclosures](http://bombich.com/kb/discussions/no-boot-from-firewire800-disc)
- [Reports indicate that](https://discussions.apple.com/thread/4243814) <<https://discussions.apple.com/thread/4243814>>, contrary to its published documentation, the [NewerTech Voyager Dock](http://www.newertech.com/products/voyagerq.php) <<http://www.newertech.com/products/voyagerq.php>> enclosure is **not** bootable via Firewire.
- 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) <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/>](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 63 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.
- 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.
- One user reported very inconsistent bootability of the "ICY BOX IB-AC6032-U3" SATA-to-USB adapter cable. In general we discourage the use of "adapter"-type devices, and instead recommend that you invest in a genuine, high-quality USB or Thunderbolt enclosure for your production backup devices.

Compatibility issues specific to the Samsung T5 Portable SSD

Update for macOS Catalina users : We have seen good results with these enclosures on macOS Catalina. Our internal testing has been 100% successful and we have received several reports that corroborate our results. The comments below are specific to macOS Mojave and High Sierra.

Some users have reported that the Samsung T5 Portable SSD cannot function at all as a bootable

device on the T2-based MacBook Pro 2018. Efforts even to install macOS Mojave onto this device fail to produce a bootable volume. This is a popular enclosure that we've seen great success with, and so far these reports are limited to the 2018 MacBook Pro.

The Samsung T5 Portable SSD (and also the Transcend StoreJet SSD) also introduces an exceptional delay during startup (on any Mac, not just T2 Macs), whether you're attempting to boot from that device or your Mac's internal hard drive. This appears to be a compatibility problem between the Mac's firmware and this particular SSD **when the SSD is formatted as APFS and when the SSD has an installation of macOS** (whether placed there via cloning or via the Installer). To avoid this delay, and only if your Mac is running macOS Mojave or an *earlier* OS, we recommend formatting these SSDs as HFS+ until the compatibility problem is resolved:

1. Open Disk Utility
2. Choose **Show all devices** from the View menu
3. Select the top-level "parent" device of the Samsung T5 SSD in Disk Utility's sidebar
4. Click the Erase button in the toolbar
5. Set the format to **Mac OS Extended, Journaled**, set the Scheme to **GUID Partition Map**, and give the new volume a name
6. Click the Erase button
7. Open CCC and re-select the new volume as the destination, then run the backup task

Note: If you have a T2 Mac, please bear in mind that [T2 Macs cannot boot from an encrypted HFS+ formatted device](#). The Samsung T-series devices will not be a suitable backup device for your T2-based Mac if you require that the backup disk is encrypted.

Another note: HFS+ is not a suitable format for a **production** startup disk. It's fine to format your Mojave **backup** disk as HFS+, but if you're using your Samsung T5 as a production startup device, you won't be able to apply system updates to that volume as long as it is formatted as HFS+.

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.

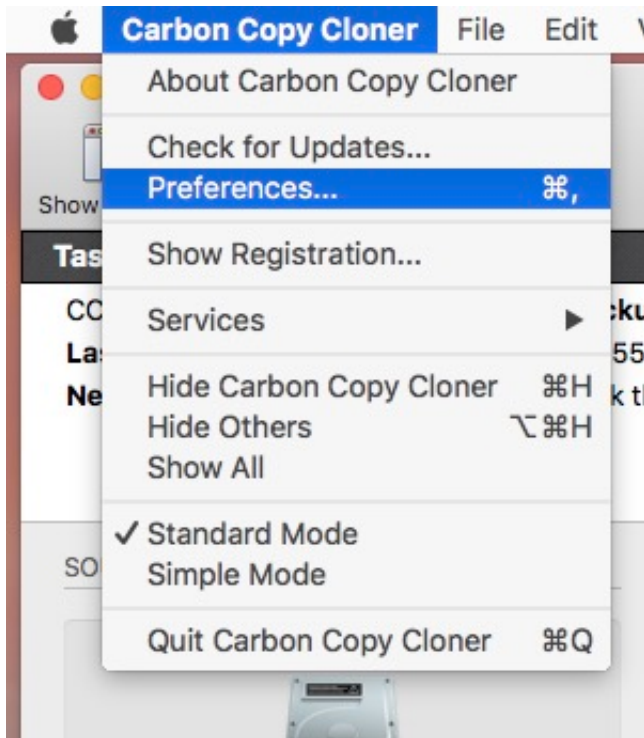
Related Documentation

- [Can I back up one computer and use the clone to restore another computer?](http://bombich.com/kb/ccc5/can-i-back-up-one-computer-and-use-clone-restore-another-computer) <<http://bombich.com/kb/ccc5/can-i-back-up-one-computer-and-use-clone-restore-another-computer>>
- [A closer look at how CCC determines the "bootability" of a destination volume](http://bombich.com/kb/ccc5/closer-look-how-ccc-determines-bootability-destination-volume) <<http://bombich.com/kb/ccc5/closer-look-how-ccc-determines-bootability-destination-volume>>
- [Apple Kbase: About the screens you see when your Mac starts up](https://support.apple.com/en-us/HT204156) <<https://support.apple.com/en-us/HT204156>>



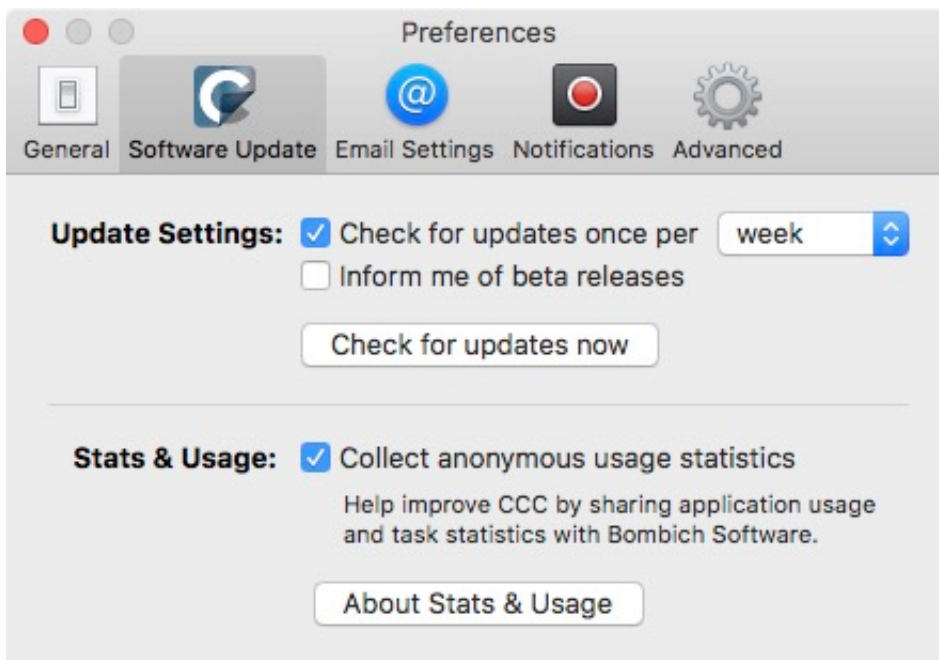
Keeping CCC up to date

Open Preferences



Select **Preferences** from the **Carbon Copy Cloner** menu

Select Software Update



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.

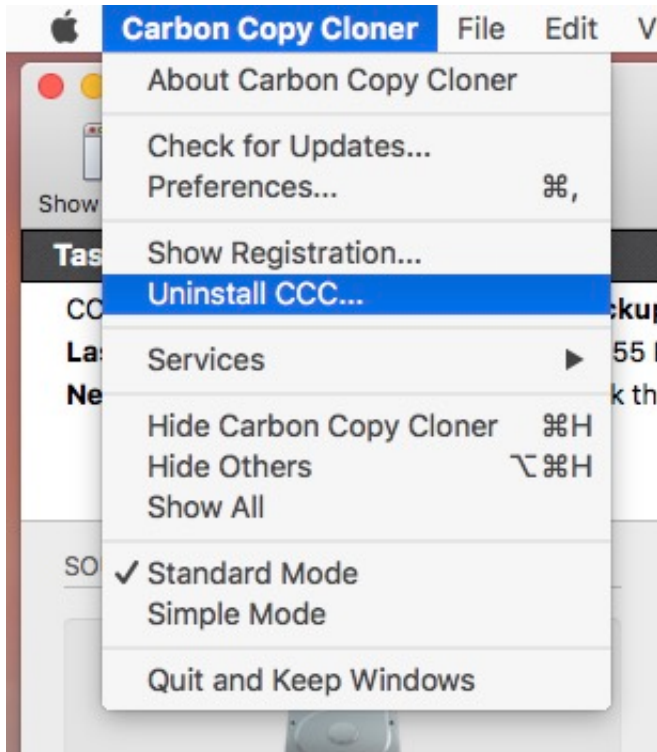
Do not use third-party update mechanisms

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.

Uninstalling CCC

Uninstalling from within Carbon Copy Cloner

To Uninstall Carbon Copy Cloner, 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 Carbon Copy Cloner 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 <http://bombich.com/kb/cccl5/leveraging-snapshots-on-apfs-volumes#space>](http://bombich.com/kb/cccl5/leveraging-snapshots-on-apfs-volumes#space)

Manually removing files associated with Carbon Copy Cloner

If you deleted the Carbon Copy Cloner 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.useragent
- /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 User Agent and the com.bombich.ccchelper privileged helper tool

When you install and use Carbon Copy Cloner, 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 User Agent is running.

The CCC User Agent 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 User Agent 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 (Carbon Copy Cloner menu > Preferences > Notifications)
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? <http://bombich.com/kb/ccc5/what-cccs-privileged-helper-tool>](http://bombich.com/kb/ccc5/what-cccs-privileged-helper-tool)

Antivirus software may interfere with a backup

Some antivirus applications may prevent Carbon Copy Cloner 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. Check the **Don't update newer files on the destination** option in the Troubleshooting box
3. 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 <http://bombich.com/software/get_help>](http://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

- [Sync problems and ACL issues <http://bombich.com/kb/discussions/sync-problems-and-acl>](http://bombich.com/kb/discussions/sync-problems-and-acl)

issues>

- Subsequent backups are slow <<http://bombich.com/kb/discussions/subsequent-backups-both-full-and-incremental-slow.>>
- Source Disk becomes full when cloning <<http://bombich.com/kb/discussions/source-disk-becomes-full-when-cloning>>
- System hangs during scheduled backup task <<http://bombich.com/kb/discussions/having-finished-backup-task-launches-if-connecting-specific-firewire-disk-waking-up>> (Sophos)
- Problem with CCC and F-Secure 2011 virus scanner <<http://bombich.com/kb/discussions/problem-ccc-and-f-secure-2011-virusscanner>>
- McAfee changes modification date of files on the destination <<http://bombich.com/kb/discussions/unchanged-files-being-archived>>
- Backup task is slower than it should be <<http://bombich.com/kb/discussions/change-in-time-backup>> (VirusBarrier)
- Slow performance during backup <<http://bombich.com/kb/discussions/slow-incremental-clone>> (F-Secure)
- Symantec Internet Security may cause kernel panics during a backup task <<http://bombich.com/kb/discussions/ccc-causes-my-os-x-lion-10.7.4-panic>>
- 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 make a cloned system volume bootable.
- 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/) <<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.

Antivirus Software concerns regarding the BaseSystem.dmg file

There is a file named "BaseSystem.dmg" on the Recovery volume associated with your Mac's startup disk. That disk image file contains the lightweight recovery operating system that is used when your Mac is booted in Recovery mode. At the beginning of every backup task that backs up a startup volume, CCC mounts the recovery volume and creates an archive of the data on that volume. Copying the "BaseSystem.dmg" file is part of that procedure. CCC stores an archive of the recovery volume at /Library/Application Support/com.bombich.ccc/Recovery on the startup disk so that the archive can be included in the backup of that volume.

We have received some reports of users seeing a dialog window (presented by antivirus software) reporting that "the BaseSystem.dmg disk image is being opened", perhaps with a suggestion that the disk image contains a virus or malware. This dialog appears and disappears very quickly, and some users are understandably concerned about the presence and erratic behavior of that dialog. Lacking any credible information from the AV software, users naturally turn to the Internet, and unfortunately are greeted with terrible advice and misinformation. **The BaseSystem.dmg file is not a virus. You should not attempt to delete parts of the operating system.**

Users that have attempted to delete that file are prompted for admin credentials, and the deletion attempt still fails. Contrary to what AV software purveyors may claim, the prompt for admin credentials is not coming from a virus, it's coming from macOS because you're trying to delete system files. The attempt to delete system files subsequently fails thanks to macOS's System Integrity Protection. This is not an attempt to get your admin credentials, it's normal macOS system processes working to protect the operating system. **The BaseSystem.dmg file is not a virus. You should not attempt to delete parts of the operating system.**

If you're seeing a dialog related to the BaseSystem.dmg file and it occurs at the beginning of a CCC backup task, this is a false positive from your antivirus software. Please contact your antivirus application vendor and ask them to fix that. Making a backup of the BaseSystem.dmg file is not something that should be brought to your attention.

Related Documentation

- [CCC automatically manages the special "helper" volumes on APFS-formatted destinations <http://bombich.com/kb/ccc5/cloning-apples-recovery-hd-partition#apfs>](http://bombich.com/kb/ccc5/cloning-apples-recovery-hd-partition#apfs)
- [Apple Kbase HT201314: About macOS Recovery <https://support.apple.com/en-us/HT201314>](https://support.apple.com/en-us/HT201314)

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.

Before concluding that CCC is recopying **every** file, open your most recent completed task in CCC's Task History window and compare the **Total size of source data set** and **Data copied** values. 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. If the amount of data copied is just a fraction of the total data set, then the amount of data being copied is probably normal.

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 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 Troubleshooting box.
3. Save and run your task.

Related Documentation

- [Antivirus software may interfere with a backup <http://bombich.com/kb/ccc5/antivirus-software-may-interfere-backup>](http://bombich.com/kb/ccc5/antivirus-software-may-interfere-backup)
- [Advanced Settings <http://bombich.com/kb/ccc5/advanced-settings>](http://bombich.com/kb/ccc5/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>](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/cc" -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>](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 many Iomega and Western Digital 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" Iomega hard drives to your computer.

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)

[<https://support.wdc.com/knowledgebase/answer.aspx?ID=18502>](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

With an advanced setting, you can [configure CCC to unmount the destination](http://bombich.com/kb/ccc5/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

If applications still open from the destination volume, you can use this [Reset LaunchServices Register](http://bombich.com/software/files/tools/Reset_LaunchServices_Register.app.zip) application to reset the LaunchServices database, then restart your Mac.

Launchpad ignores settings created while booted from another volume

If you have assembled a custom arrangement of your application icons in the Launchpad application, you will discover that that arrangement is lost when booted from your backup volume. When you see this happen, you would naturally think, "Why didn't CCC copy the Launchpad settings?" In fact, though, CCC is faithfully copying the Launchpad settings. Here we'll show you how you can verify that, and also why the settings don't work while booted from your backup volume.

Verifying the fidelity of the backup copy of your Launchpad settings

The LaunchPad preferences database is stored in your home folder at this location:

```
/Users/yourname/Library/Application Support/Dock/{long number}.db
```

You can calculate a checksum of this file on the source and destination volumes (immediately after running a backup task) to verify that it matches, e.g. in the Terminal application:

```
[bombich:~] md5 ~/Library/Application\ Support/Dock/*.db
MD5 (/Users/bombich/Library/Application
Support/Dock/861852F1-B632-455A-8632-78BC7137A959.db) =
1988498deef00393db335a7015995413
```

```
[bombich:~] md5 /Volumes/Home\ Backup/Users/bombich/Library/Application\ Support/Dock/*.db
MD5 (/Volumes/Backup/Users/bombich/Library/Application
Support/Dock/861852F1-B632-455A-8632-78BC7137A959.db) =
1988498deef00393db335a7015995413
```

Why don't the settings work while booted from another volume?

If you boot from the backup volume, you may notice an additional database file in that folder (it will be removed every time your backup runs, though). That's the new settings file that Launchpad creates because it's ignoring the settings file from your original volume.

If you examine the contents of that database file†, you'd see references to each application that resides in Launchpad. It's these references to your applications that are not "portable". Rather than referencing the application based on its relative path to your startup disk, the references are complex, proprietary "bookmark" data. These bookmark data have references to several defining attributes of the application files, such as path, name, volume unique identifier, and inode number. This allows you to move these applications around on your startup disk without breaking things inside of Launchpad. Unfortunately, though, the bookmark data is completely meaningless when you're booted from a physically different volume, because those attributes within the bookmark are **volume specific**. It is not possible to alter the contents of this database such that the references will point to the cloned volume.

†: Paste this in Terminal to get a "dump" of the database:

```
sqlite3 ~/Library/Application\ Support/Dock/*.db
```


"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, Carbon Copy Cloner 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:

- 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 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) <<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. Select **Selected files...** from the Clone popup menu (underneath the Source selector), 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 <http://bombich.com/kb/ccc5/backing-up-tofrom-network-volumes-and-other-non-hfs-volumes#nas_EINVAL>](http://bombich.com/kb/ccc5/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.



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. If you're running Yosemite or later, that performance could 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.

Eject the network volume in the Finder

Our first recommendation is to **eject your network shares in the Finder**, then run your task again. 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 browseable in the Finder.

Disable support for extended attributes

If a performance issue persists despite trying the steps above, you can try dropping the extended attributes from the source. While it is our preference to preserve extended attributes, Apple considers extended attributes to be "disposable" because some filesystems cannot support them.

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 Troubleshooting Options

box.

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. To try AFP instead of SMB:

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. Open CCC and select the applicable backup task
5. Drag the currently-mounted NAS volume (or folder or disk image on that volume) onto CCC's source or destination selector (whichever is applicable for your particular 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](http://bombich.com/kb/ccc5/performing-actions-before-and-after-backup-task#chain_tasks) <http://bombich.com/kb/ccc5/performing-actions-before-and-after-backup-task#chain_tasks>, or [place your tasks into a task group](http://bombich.com/kb/ccc5/task-organization) <<http://bombich.com/kb/ccc5/task-organization>> so that they will be run sequentially instead.

Consider backing up to a disk image on the NAS device rather than directly to it

Network file sharing is a surprisingly CPU-intensive task. While network appliances are well suited to the task of serving media to multiple workstations, the overhead of individual filesystem transactions makes them less suited to the task of backing up millions of files. Media files, in comparison, are generally large and the required data rate for streaming media is relatively low. Consider a 1-hour, 1GB HD movie file. Streaming 1GB over the course of an hour requires only 0.27MB/s. That's an easy task, even over a weak wireless network. But if you want to back up 100GB of data in an hour, and that 100GB is made up of a million smaller files, then a network appliance may not be up to that task.

The actual bandwidth that you achieve in your backup task will be based on the number of files you're copying, the file size distribution, and the number and size of extended attributes in the source data set. Copying large files (e.g. media files) to a network volume will achieve the maximum potential bandwidth, while copying lots of small files will take quite a bit longer due to network filesystem overhead. If the data that you're backing up consists primarily of large files, e.g. music, photos, video — backing up directly to a network appliance will be fine. **If you're backing up system files or applications, or many files that are smaller than a few MB, we recommend that you back up to a disk image on your network appliance** <<http://bombich.com/kb/ccc5/i-want-back-up-my-whole-mac-time-capsule-nas-or-other-network-volume>> **to improve performance and to maintain important filesystem metadata.**



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 User Agent: ~/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 <http://bombich.com/software/get_help>](http://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.

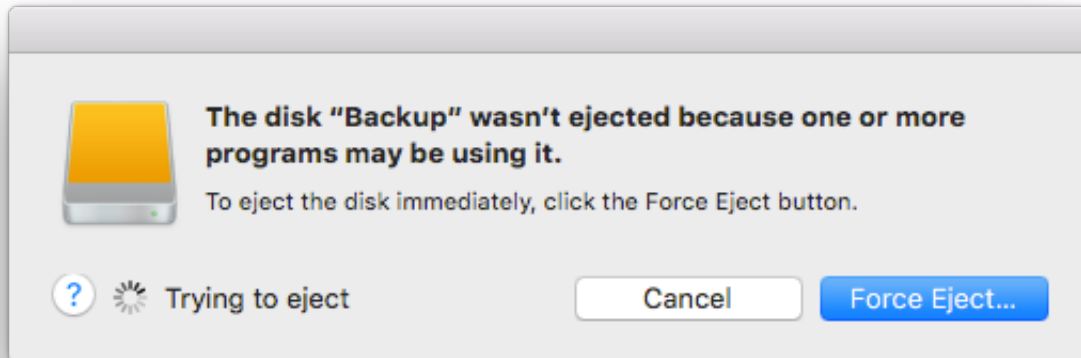
Where can I find a list of every file that CCC has copied?

CCC does not retain that information for each backup task. If you're concerned that CCC is copying too many or too few files, please [contact us for assistance <http://bombich.com/software/get_help>](http://bombich.com/software/get_help).

Related documentation

- [Using the ccc Command Line Tool to Start, Stop, and Monitor CCC Backup Tasks <http://bombich.com/kb/ccc5/using-ccc-command-line-tool-start-stop-and-monitor-ccc-backup-tasks>](http://bombich.com/kb/ccc5/using-ccc-command-line-tool-start-stop-and-monitor-ccc-backup-tasks)
- [Why is CCC recopying every file during each backup? <http://bombich.com/kb/ccc5/why-ccc-recopying-every-file-during-each-backup>](http://bombich.com/kb/ccc5/why-ccc-recopying-every-file-during-each-backup)
- [How do I get help? <http://bombich.com/kb/ccc5/how-do-i-get-help>](http://bombich.com/kb/ccc5/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 gracefully. If your backup task isn't 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 probably caused by macOS's "kextcache" utility — that utility rebuilds a cache file on the destination that is required for startup. That process 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 wait for kextcache to finish, 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 **After Copying Files** box, choose the option to [unmount the destination volume <http://bombich.com/kb/cc5/performing-actions-before-and-after-backup-task#dest_postactions>](http://bombich.com/kb/cc5/performing-actions-before-and-after-backup-task#dest_postactions) after the backup task completes.
4. Save and run your backup task.

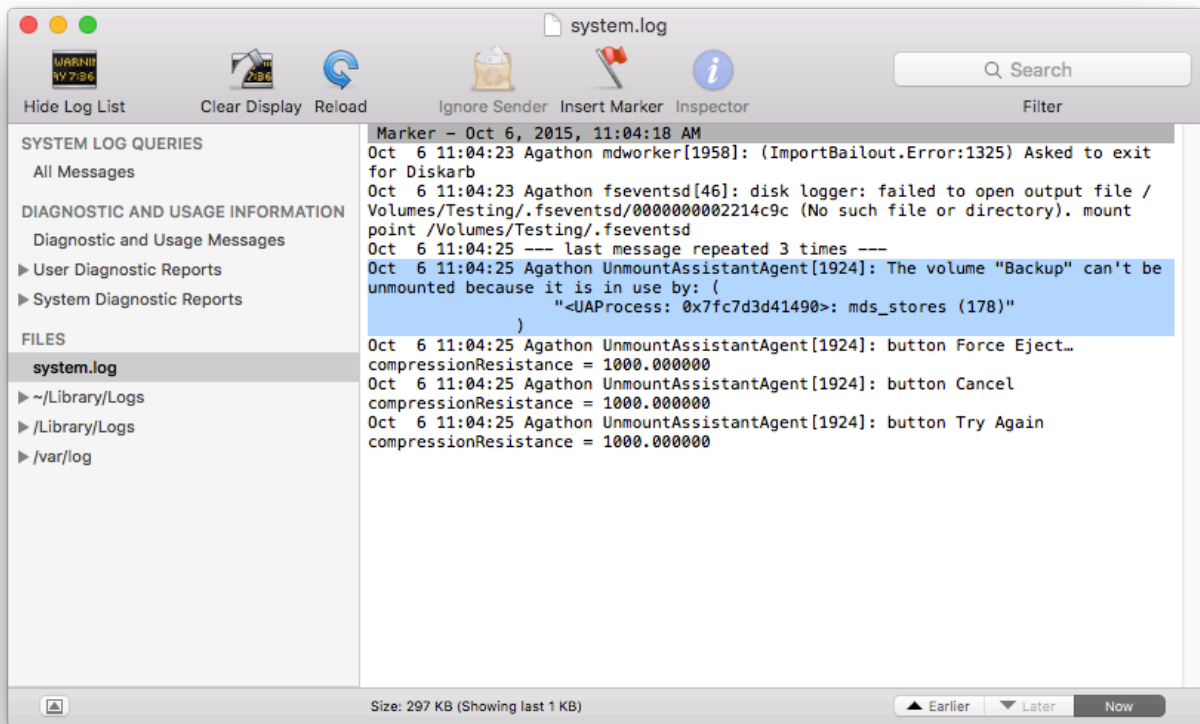
If the disk cannot be unmounted several minutes after the backup task has completed, or if CCC is also unable to eject the destination, use the Console application to track down the culprit.

Sierra and later OSes:

1. Open the Console application (in /Applications/Utilities)
2. Type or paste **UnmountAssistantAgent** into the Search field in the toolbar

El Capitan and earlier OSes

1. Open the Console application (in /Applications/Utilities)
2. Click on **system.log** in the sidebar
3. Go to the **Edit** Menu > **Find** > **Find...** (or press Command+F) to search for messages from the **UnmountAssistantAgent** application. Avoid using the Search field in the toolbar for this search, because that will hide important context.



In the example above, we can see that an application named **mds_stores** is preventing the Backup volume from being ejected. **mds_stores** and **mdworker** are Spotlight helper applications, so the issue here is that Spotlight is preventing the destination from being ejected. We have received numerous reports showing the same culprit since El Capitan was introduced. To resolve the conflict caused by Spotlight, you can disable Spotlight on the destination volume:

1. Open the Spotlight preference pane
2. Click on the Privacy tab
3. Drag the backup volume into the Privacy table

Disabling Spotlight in this manner only affects the destination volume, and it's reversible — you can remove your destination volume from that list should you decide that you want to re-enable indexing.

Other 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

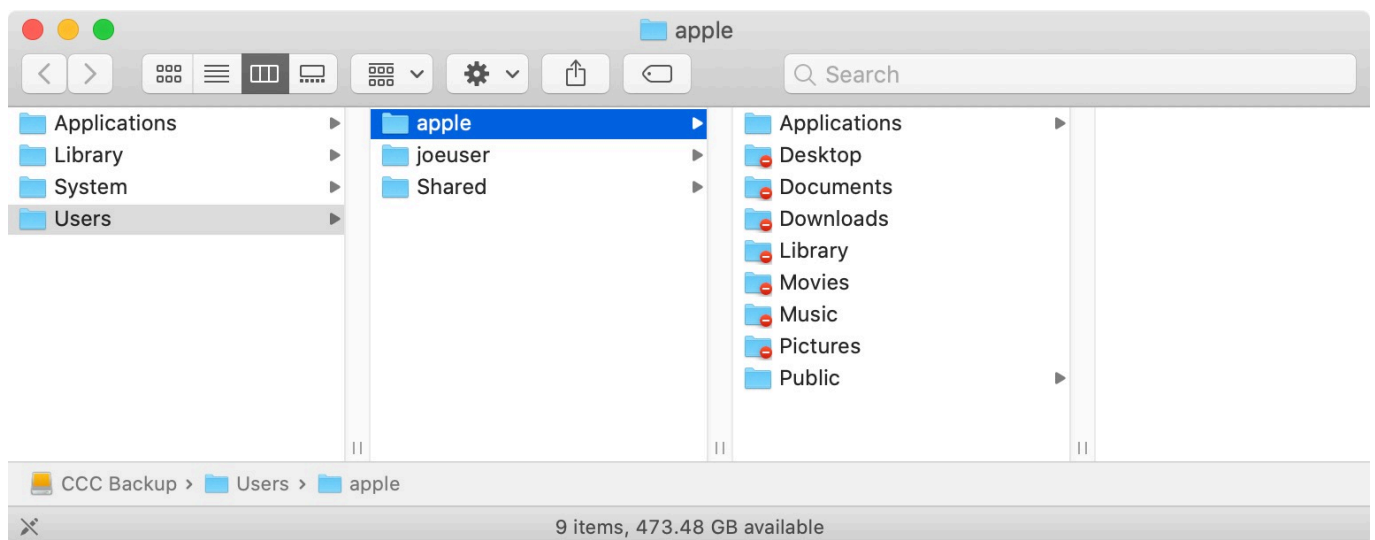
Remove any duplicate keychain entries in the Keychain Access application

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.

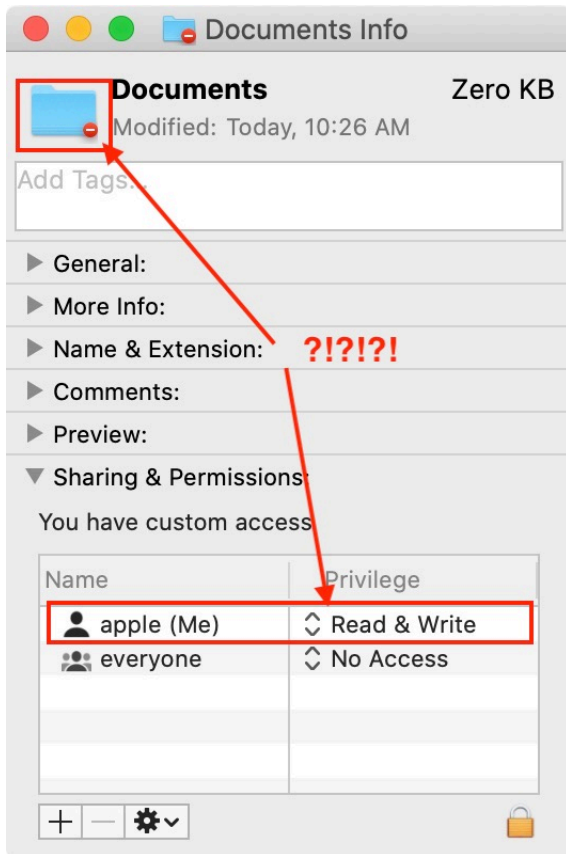
Why does Finder prevent me from viewing the home folder on my backup when it's attached to another Mac?

Update November 2020: Apple has resolved this Finder bug in macOS Big Sur.

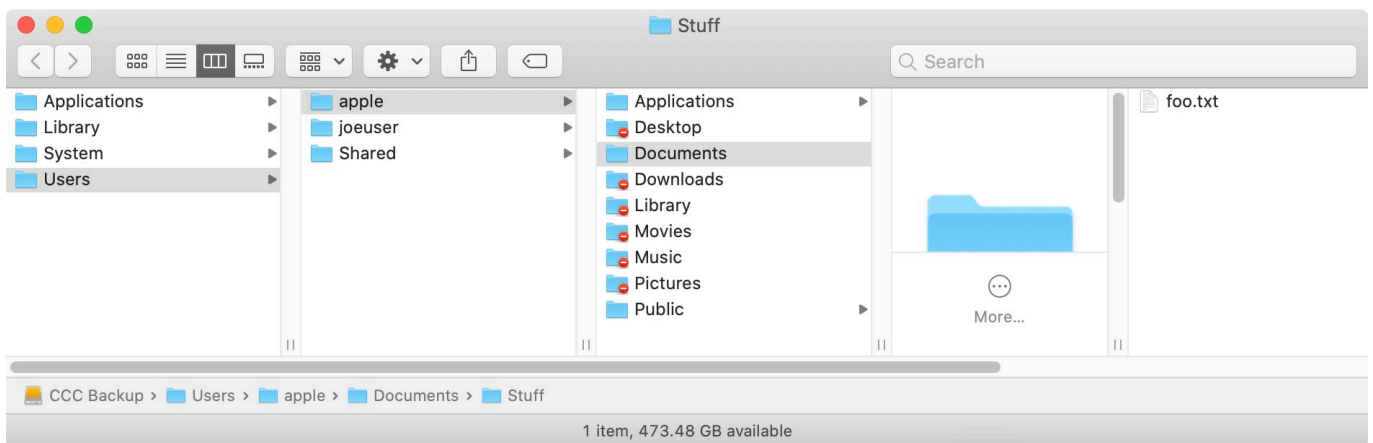
We are currently tracking a Finder bug in which the Finder incorrectly determines your access to some folders. The issue occurs when an "access control list" is applied to a folder and when ownership is disabled on the backup volume. Ownership is disabled by default when you attach your backup volume 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**
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. Drag the affected folders (or your entire home folder) from the backup volume onto our [Finder bug permissions workaround script](http://bombich.com/software/files/tools/finder_perms_bug.zip) <http://bombich.com/software/files/tools/finder_perms_bug.zip>†. 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.

† **Catalina users:** Gatekeeper throws a wrench into this workaround. [Download this script instead](http://bombich.com/software/files/tools/finder_perms_bug.scp) <http://bombich.com/software/files/tools/finder_perms_bug.scp> and run the script from within the Script Editor application.

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. 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) <<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) <<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 (you may not find all of these components, remove as many as you find):

Library/Extensions/SATSMARTDriver.kext

Library/Extensions/SATSMARTLib.plugin

Library/Extensions/SATSMARTDriver.kext

Library/Extensions/SATSMARTLib.plugin



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. If you have already tried these steps and the problem recurred, [see the next section for additional advice](#).

1. Restart your Mac
2. Rule out general hardware problems <<http://bombich.com/kb/ccc5/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 <http://bombich.com/kb/ccc5/some-third-party-storage-drivers-may-cause-hardware-misbehavior>](http://bombich.com/kb/ccc5/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, reset the destination selection, then try running the task again

† 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 use CCC's file copier to make a backup of your Mac's Data volume.

1. Create and maintain a data-only backup

A data-only 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 Catalina should that ever be required. Creation of the backup alone is sufficient to protect your data, however this will not produce a bootable backup, nor will it address any problems with the source. See [Creating a data-only backup <http://bombich.com/kb/ccc5/creating-and-restoring-data-only-backups#create>](http://bombich.com/kb/ccc5/creating-and-restoring-data-only-backups#create) for details on how to configure a data-only backup.

2. Install macOS onto your data-only backup to produce a bootable backup



Installing macOS onto your data-only backup will produce a complete, bootable backup of your system. If corruption on the startup disk eventually leads to a failure of that volume, then you would be able to boot your Mac from the backup and continue working from the backup, and you could also do a complete restore to the internal disk (e.g. after erasing or replacing it). See [Installing macOS onto a data-only backup <http://bombich.com/kb/ccc5/creating-and-restoring-data-only-backups#install_macos>](http://bombich.com/kb/ccc5/creating-and-restoring-data-only-backups#install_macos) for detailed instructions on installing macOS onto your data-only backup.

3. Erase the source and restore from the backup

Disk Utility typically cannot fix filesystem damage on APFS-formatted volumes; in most cases, the only way to resolve APFS filesystem corruption is to erase the affected volume and restore it from a backup. Especially if filesystem corruption on your source volume is causing misbehavior of the system, you can boot your Mac from the backup volume, erase the internal disk and restore the backup. See [How to restore from your backup <http://bombich.com/kb/ccc5/how-restore-from-your-backup>](http://bombich.com/kb/ccc5/how-restore-from-your-backup) for details instructions for restoring your backup.

Related documentation

- [Creating and restoring data-only backups <http://bombich.com/kb/ccc5/creating-and-restoring-data-only-backups>](http://bombich.com/kb/ccc5/creating-and-restoring-data-only-backups)
- [How to restore from your backup <http://bombich.com/kb/ccc5/how-restore-from-your-backup>](http://bombich.com/kb/ccc5/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 make a data-only backup, then address the hardware concern that led to the read/write errors, then restore your data from the backup.



Related documentation

- [Creating and restoring data-only backups <http://bombich.com/kb/ccc5/creating-and-restoring-data-only-backups>](http://bombich.com/kb/ccc5/creating-and-restoring-data-only-backups)
- [Identifying and Troubleshooting Hardware-Related Problems <http://bombich.com/kb/ccc5/identifying-and-troubleshooting-hardware-related-problems>](http://bombich.com/kb/ccc5/identifying-and-troubleshooting-hardware-related-problems)
- [Disk error statistics <http://bombich.com/kb/ccc5/disk-center#errors>](http://bombich.com/kb/ccc5/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 overly-optimistic advice:

Use Disk Utility to repair any filesystem problems, then try the backup task again. Note that you will need to boot from your backup volume or the Apple Recovery HD volume if repairs are required on your startup disk's filesystem. If this error persists and Disk Utility is unable to detect or repair the problems, you may have to reformat the affected volume to address the problems.

In both of these cases, 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](http://bombich.com/kb/cc5/excluding-files-and-folders-from-backup-task) [<http://bombich.com/kb/cc5/excluding-files-and-folders-from-backup-task>](http://bombich.com/kb/cc5/excluding-files-and-folders-from-backup-task) to avoid the errors that its content would cause.



Identifying and Troubleshooting Hardware-Related Problems

Sometimes hardware components die slow and annoyingly inconsistent deaths. At one moment, it appears that you can copy data to the disk and use it ordinarily. In the next moment, you're getting seemingly random errors, stalls, crashes, the destination volume "disappearing" in the middle of a backup task, Finder lockups and other unruly behavior.

When hardware fails in this way, it's nearly impossible for the OS or CCC to pop up a dialog that says "Hey, it's time to replace XYZ!" Instead, you have to dig a little deeper, rule out components, try replacements, etc. to isolate the faulty component.

Many times that hardware problems occur, CCC will get meaningful errors from the macOS kernel 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 backup task was aborted because the [source or destination] volume's mountpoint changed."

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 backup 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.

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. Filesystem problems are commonplace, and easy to rule out. If you discover filesystem problems on your startup disk, boot from your CCC backup volume or boot into [Recovery Mode](https://support.apple.com/en-us/HT201314) <<https://support.apple.com/en-us/HT201314>> to run Disk Utility so you can repair the problems.
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. 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.

4. Replace the cable that you're using to connect the external hard drive enclosure to your Mac (if applicable).
5. Try connecting the external hard drive enclosure to your Mac via a different interface (if applicable)
6. Try the same hard drive in a different external hard drive enclosure (we offer [some recommendations here <http://bombich.com/kb/ccc5/choosing-backup-drive#recommendations>](http://bombich.com/kb/ccc5/choosing-backup-drive#recommendations)).
7. Reformat the hard drive in Disk Utility. If the affected disk is not an SSD, click the **Security Options** button in the Erase tab and drag the slider to the right to specify the option to write a single pass of zeroes. Writing zeroes to every sector will effectively detect and spare out any additional failing sectors that have yet to be discovered.
8. 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. If a firmware update is available for your enclosure, try applying that as well to see if a problem with the enclosure has been resolved recently through a software update.

Related

- [Uninstalling Seagate diagnostic utilities alleviates hangs <http://bombich.com/kb/discussions/cant-restore-image>](http://bombich.com/kb/discussions/cant-restore-image)
- 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. **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 the affected disk is not an SSD, click the **Security Options** button in the Erase tab and drag the slider to the right to specify the option to write a single pass of zeroes. Writing zeroes to every sector will effectively detect and spare out any additional failing sectors that have yet to be discovered. If the affected disk is your startup disk, boot from your CCC bootable backup volume to perform this procedure (after you have allowed CCC to complete a backup).

† 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, or see [this section of CCC's documentation for guidance on restoring a hidden item using CCC <http://bombich.com/kb/cc5/restoring-item-from-hidden-folder>](http://bombich.com/kb/cc5/restoring-item-from-hidden-folder).

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 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?

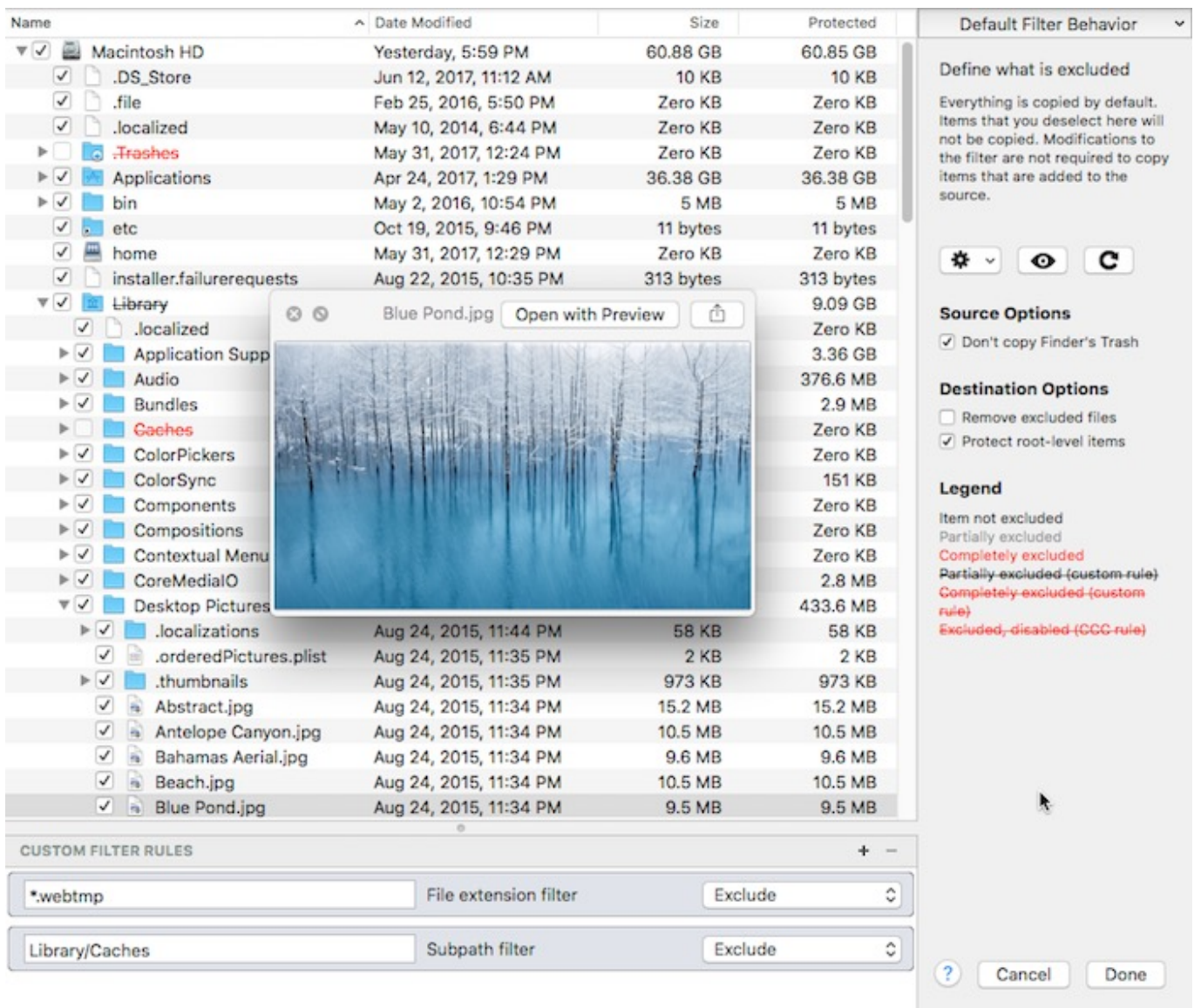
More often than not, you're completely out of luck. You may be able to revive a hard drive for small amounts of time by letting the drive cool down (somewhere cool and dry, not cold) and then powering it up attached to a service workstation (i.e. don't attempt to boot from it, you may not have enough time).



Advanced Topics

Excluding files and folders from a backup 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. Choose **Copy Some Files** from the popup menu underneath the Source selector, or click on the Task Filter button () to open the Task Filters panel.



Name	Date Modified	Size	Protected
Macintosh HD	Yesterday, 5:59 PM	60.88 GB	60.85 GB
.DS_Store	Jun 12, 2017, 11:12 AM	10 KB	10 KB
.file	Feb 25, 2016, 5:50 PM	Zero KB	Zero KB
.localized	May 10, 2014, 6:44 PM	Zero KB	Zero KB
.Trashes	May 31, 2017, 12:24 PM	Zero KB	Zero KB
Applications	Apr 24, 2017, 1:29 PM	36.38 GB	36.38 GB
bin	May 2, 2016, 10:54 PM	5 MB	5 MB
etc	Oct 19, 2015, 9:46 PM	11 bytes	11 bytes
home	May 31, 2017, 12:29 PM	Zero KB	Zero KB
installer.failurerequests	Aug 22, 2015, 10:35 PM	313 bytes	313 bytes
Library		9.09 GB	
.localized		Zero KB	
Application Supp		3.36 GB	
Audio		376.6 MB	
Bundles		2.9 MB	
Caches		Zero KB	
ColorPickers		Zero KB	
ColorSync		151 KB	
Components		Zero KB	
Compositions		Zero KB	
Contextual Menu		Zero KB	
CoreMediaIO		2.8 MB	
Desktop Pictures		433.6 MB	
.localizations	Aug 24, 2015, 11:44 PM	58 KB	58 KB
.orderedPictures.plist	Aug 24, 2015, 11:35 PM	2 KB	2 KB
.thumbnails	Aug 24, 2015, 11:35 PM	973 KB	973 KB
Abstract.jpg	Aug 24, 2015, 11:34 PM	15.2 MB	15.2 MB
Antelope Canyon.jpg	Aug 24, 2015, 11:34 PM	10.5 MB	10.5 MB
Bahamas Aerial.jpg	Aug 24, 2015, 11:34 PM	9.6 MB	9.6 MB
Beach.jpg	Aug 24, 2015, 11:34 PM	10.5 MB	10.5 MB
Blue Pond.jpg	Aug 24, 2015, 11:34 PM	9.5 MB	9.5 MB

Default Filter Behavior

Define what is excluded

Everything is copied by default. Items that you deselect here will not be copied. Modifications to the filter are not required to copy items that are added to the source.

Source Options

- Don't copy Finder's Trash

Destination Options

- Remove excluded files
- Protect root-level items

Legend

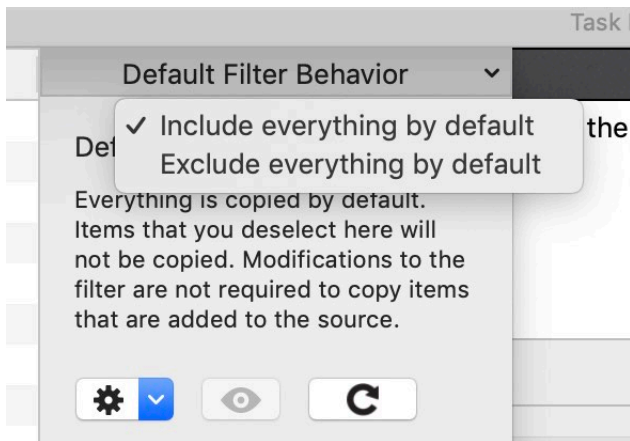
- Item not excluded
- Partially excluded
- Completely excluded
- Partially-excluded-(custom-rule)
- Completely-excluded-(custom-rule)
- Excluded,-disabled-(CCC-rule)

CUSTOM FILTER RULES

- *.*webtmp File extension filter Exclude
- Library/Caches Subpath filter Exclude

Default Filter Behavior

The CCC task filter offers two paradigms for defining the task filter. The task filter can either include everything by default or the filter can exclude everything by default. 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:



Include everything by default: Define what is excluded

CCC's default behavior is to include everything by default. In this mode you define what is excluded from the backup 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 back up everything because you don't have to revisit the task filter to indicate that new items should be included in the backup 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 backup task, that item will automatically be included in the backup task.

Exclude everything by default: Define what is included

In this mode, everything is excluded by default, and you define what is **included** in the backup 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 backed up. This mode is helpful in cases where you only want to back up a handful of items on a volume whose subfolders frequently change.

Calculating disk usage and Protected Size

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 and the protected size of the folder (i.e. how much data is included in the backup task). You can also click on the **Refresh Disk Usage** button (⌂) 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 **Refresh Disk Usage** 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 back up your Trash, [open the Task Filter window](#), then uncheck the **Don't copy Finder's Trash** box to remove the exclusion. See [this section of CCC's documentation](#) <<http://bombich.com/kb/cc5/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 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. In fact, excluding an item from the backup task implicitly protects that item on the destination. If you have items on the destination that are now excluded from a backup 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.

This 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.

Please carefully consider the scope of effect that this option will have when using the **Exclude everything by default** filter behavior.

The **Protect root level items** setting is described in more detail in the [Advanced Settings article](http://bombich.com/kb/ccc5/advanced-settings#protect) <<http://bombich.com/kb/ccc5/advanced-settings#protect>>.

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. Choose **Show custom filters** from the gear menu 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 `/`. 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.

Bracket characters, "[" and "]"

When specifying a custom rule that includes bracket characters, those characters must be "escaped", e.g. `\[foo\]`. Note that when using escaped bracket characters, the result of the custom filter rule will not be expressed in the folder listing. This will be resolved in a future version of CCC.

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.

Special considerations for the 'Exclude everything by default' filter behavior and custom rules

Normally the 'Exclude everything by default' filter behavior will ignore any folders on the source that are not explicitly included by your task filter. That 'ignore' behavior imparts explicit protection on those items as well — if those items are present on the destination, CCC will leave them alone. When you add a custom filter to your task, however, CCC must perform a complete scan of the source to find items that match your custom rules. As it does that, CCC must collect a list of all folders on the source. At the end of the scan, many of these folders may be empty. To avoid creating these empty folders on the destination, CCC removes all empty folders from its "list of items to consider". That has the side effect, however, of removing any protection that would be afforded to implicitly excluded folders. Therefore, if you configure a filter to exclude everything by default and add a custom rule to that filter, you should expect CCC to remove any folder on the destination that has no items matching your custom rules. You can avoid that behavior by choosing the 'Don't Delete anything' SafetyNet setting.

Including folders and their content with the 'Exclude everything by default' 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

Carbon Copy Cloner 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 <http://bombich.com/kb/ccc5/some-files-and-folders-are-automatically-excluded-from-backup-task>](http://bombich.com/kb/ccc5/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 Carbon Copy Cloner SafetyNet <http://bombich.com/kb/ccc5/frequently-asked-questions-about-carbon-copy-cloner-safetynet#restore_archives>](http://bombich.com/kb/ccc5/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. On macOS Catalina and later, CCC will also exclude system files if you select a destination volume that is in the same APFS container as the current startup disk. 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 <http://bombich.com/kb/ccc5/folder-folder-backups>](http://bombich.com/kb/ccc5/folder-folder-backups) options in the Source and Destination selectors. With great power comes great responsibility — take care to avoid overwriting your system files.

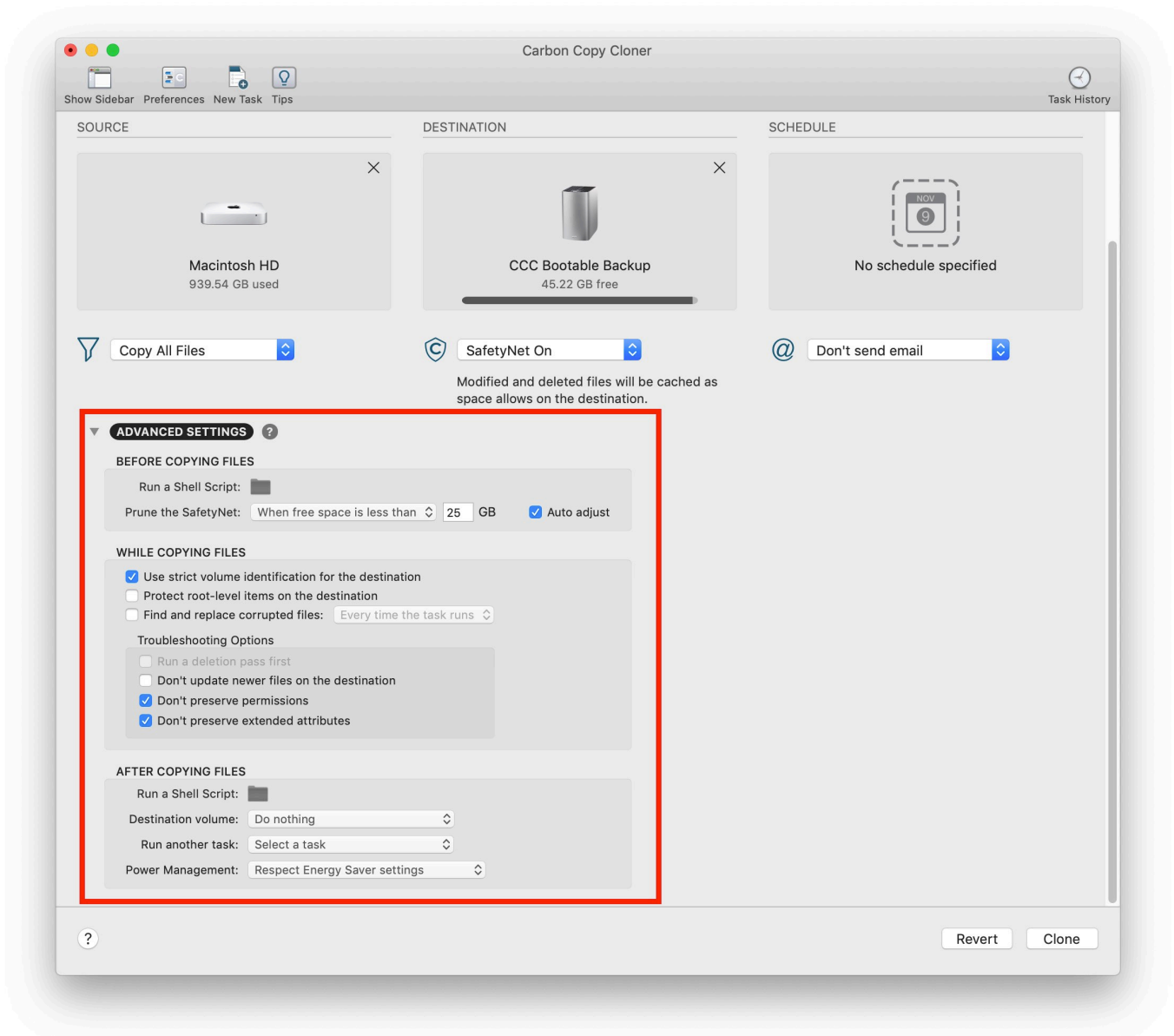
Related documentation

- [Restoring macOS System files from a bootable backup <http://bombich.com/kb/ccc5/how-restore-from-your-backup>](http://bombich.com/kb/ccc5/how-restore-from-your-backup)
- [Folder-to-Folder Backups <http://bombich.com/kb/ccc5/folder-folder-backups>](http://bombich.com/kb/ccc5/folder-folder-backups)
- [Restoring an item from a hidden folder <http://bombich.com/kb/ccc5/restoring-item-from-hidden-folder>](http://bombich.com/kb/ccc5/restoring-item-from-hidden-folder)
- [Some files and folders are automatically excluded from a backup task <http://bombich.com/kb/ccc5/some-files-and-folders-are-automatically-excluded-from-backup-task>](http://bombich.com/kb/ccc5/some-files-and-folders-are-automatically-excluded-from-backup-task)
- [Backing up and restoring Finder's Trash <http://bombich.com/kb/ccc5/backing-up-and-restoring-finders-trash>](http://bombich.com/kb/ccc5/backing-up-and-restoring-finders-trash)

Advanced Settings

CCC's Advanced Settings are helpful in specific situations, but are not generally required for routine use. Some of these settings involve more risk, so please use them with caution, and don't hesitate to ask questions via the **Ask a question about CCC...** menu item in CCC's Help menu if the explanations below are insufficient for your particular scenario.

To access the advanced settings, click on the **Advanced Settings** button below CCC's Source selector.



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 backup 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.

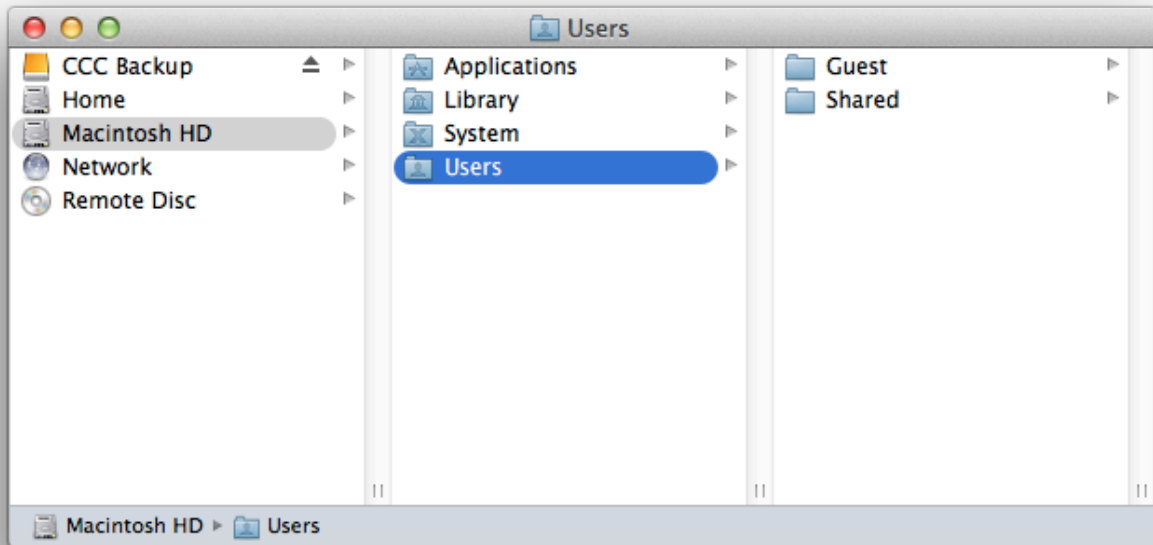
This option is automatically disabled when the destination volume does not have a UUID. Network volumes and some third-party filesystems, for example, do not have volume UUIDs. This option is also disabled if the originally-selected destination device is not attached.

Note: This setting is only applicable to the **destination** volume. CCC **always** uses the name and UUID to positively identify the source volume.

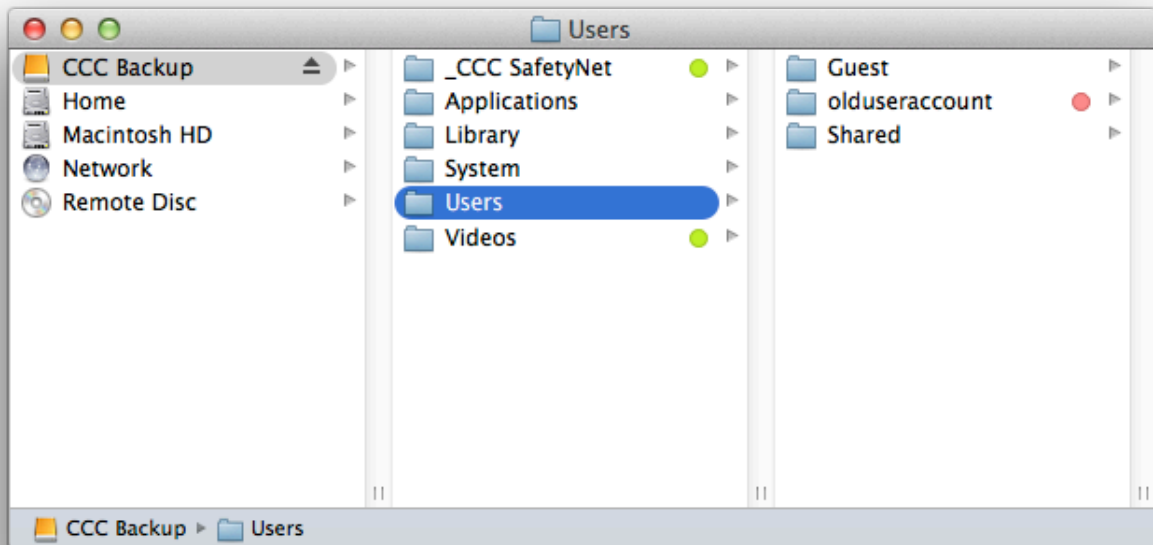
Note: If your rotating destination volumes are encrypted, CCC will only be able to unlock and mount the **original** encrypted volume selected as the destination for your backup task. CCC must have a unique identifier of the destination volume in order to unlock that volume, and CCC will only retain 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 **Videos** folder will **not** be moved to the **_CCC SafetyNet** folder because it is unique to the root level of the destination. The **Users** 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 **olduseraccount** 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.

Find and replace corrupted files, "Backup Health Check"

CCC normally uses file size and modification date to determine whether a file should be copied. With this option, CCC will calculate an MD5 checksum of every file on the source and every corresponding file on the destination. If the checksums differ, CCC will recopy the file. 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.

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.

Frequent use of the checksum calculation option is unnecessary and may be a burden upon your productivity, so CCC offers weekly and monthly options to limit how frequently the checksumming occurs.

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.

Using the "Find and replace corrupted files" option to verify your backup

CCC's checksum option verifies the integrity of the files on your destination volume **before** files are copied, it is not a verification of files that have just been written. In general, the checksum of a file immediately after it is written to disk is of questionable value. Most disks have a write cache, and file data goes to the cache before it is written to actual media. If you write a file and then immediately ask to read it back, as much as x amount of data (where x = the size of the cache) is going to come from the volatile cache. If *any* of the file's data comes from the write cache, then the checksum doesn't reflect the status of the data on the permanent media, and that really defeats the purpose of checksumming the file in the first place.



If you want to verify the integrity of the files on your destination immediately after copying files, a subsequent backup with CCC's **Find and replace corrupted files** option is the best way to do that. You can even automate this process by creating a second task that uses this option, then select the second task in the "Run another backup task" popup menu in the **After task runs** section of advanced settings.

Troubleshooting Options

Run a deletion pass first

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.

Related Documentation

- [CCC reported that the destination is full. What can I do to avoid this?](http://bombich.com/kb/ccc5/ccc-reported-destination-full.-what-can-i-do-avoid)
- [Troubleshooting slow performance when copying files to or from a network volume](http://bombich.com/kb/ccc5/troubleshooting-slow-performance-when-copying-files-or-from-network-volume)



- Performing actions Before and After the backup task
<<http://bombich.com/kb/cc5/performing-actions-before-and-after-backup-task>>



Performance Suggestions

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.

Reduce the number of files considered for backup

CCC analyzes all of the files that are included in your backup set for consideration to be copied. If you have a particularly high number of files on your source volume, you may want to put some thought into how your files are organized. 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 ask it to using Advanced Settings), 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 or RAM enumerating through those files for changes.

Related Documentation

- [Excluding files and folders from a backup task <http://bombich.com/kb/ccc5/excluding-files-and-folders-from-backup-task>](http://bombich.com/kb/ccc5/excluding-files-and-folders-from-backup-task)
- [Folder-to-Folder Backups <http://bombich.com/kb/ccc5/folder-folder-backups>](http://bombich.com/kb/ccc5/folder-folder-backups)

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. Especially as Apple's new APFS filesystem becomes harder to avoid, [we recommend using SSDs for any volume that has an installation of macOS <http://bombich.com/kb/ccc5/choosing-backup-drive#recommendations>](http://bombich.com/kb/ccc5/choosing-backup-drive#recommendations), including your backups.

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.

Additionally, 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 and hardware type

It's important to choose the right filesystem for the hardware that you have and the data that you're backing up. If you have an older, rotational HDD, it's generally better to [format that device using the "Mac OS Extended, Journaled" \(HFS+\) format <http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x>](http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x) if you're backing up macOS High Sierra (or older), or if you're making a data-only backup. APFS is the new, modern standard, but [its performance on rotational devices is inferior to HFS+ <http://bombich.com/blog/2019/09/12/analysis-apfs-enumeration-performance-on-rotational-hard-drives>](http://bombich.com/blog/2019/09/12/analysis-apfs-enumeration-performance-on-rotational-hard-drives). If you're making a backup of macOS Catalina, APFS is required. If you find the performance of your backups to be too slow, [we recommend using an SSD for your backups <http://bombich.com/kb/ccc5/choosing-backup-drive#recommendations>](http://bombich.com/kb/ccc5/choosing-backup-drive#recommendations).

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, drag the icon of the destination volume into the "Privacy" tab of Spotlight Preference Pane in the System Preferences application. If you do want the backup volume indexed, drag its icon out of the "Privacy" tab after the cloning and indexing will start immediately.

Find and replace corrupted files

CCC offers an advanced option to ["Find and replace corrupted files"](http://bombich.com/kb/ccl5/advanced-settings#checksum) <<http://bombich.com/kb/ccl5/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, and scheduling such tasks to run when you are not typically using your Mac.

Target Disk Mode is slow

In fact it's unbelievably slow. If you attach an SSD-bearing Mac in Target Disk Mode to another Mac via a USB-C cable (so both at 10Gb/s connections), you might expect to get incredible speed (e.g. >500MB/s). You will be sorely disappointed by speeds of less than 20MB/s; slower than USB 2.0. For better performance, we recommend that you avoid Target Disk Mode. Boot the target Mac from the volume you're trying to restore instead. Not only will you get better performance, but you also have the assurance that the Mac can boot from the OS that you're restoring to it.

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](http://bombich.com/kb/ccl5/antivirus-software-may-interfere-backup) <<http://bombich.com/kb/ccl5/antivirus-software-may-interfere-backup>> is a common culprit, but we have also seen problems caused by other watcher applications, such as memed 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.
- Daisy chaining Firewire devices is usually OK, though some enclosures can stall the entire Firewire bus when given too much bandwidth. If you see this behavior, try switching the order of devices in the chain, or attach your backup disk directly to a Firewire port 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.

- 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 <http://bombich.com/kb/ccc5/excluding-files-and-folders-from-backup-task>](http://bombich.com/kb/ccc5/excluding-files-and-folders-from-backup-task) to avoid the performance problem.

Use the Console application to view the contents of the system log. If you're still having trouble identifying a performance problem, [we're here to help <http://bombich.com/software/get_help>](http://bombich.com/software/get_help).

Related Documentation

- [Slow performance of network appliances can be mitigated by backing up to a disk image <http://bombich.com/kb/ccc5/slow-performance-network-appliances-can-be-mitigated-backing-up-disk-image>](http://bombich.com/kb/ccc5/slow-performance-network-appliances-can-be-mitigated-backing-up-disk-image)
- [Troubleshooting slow performance when copying files to or from a network volume <http://bombich.com/kb/ccc5/troubleshooting-slow-performance-when-copying-files-or-from-network-volume>](http://bombich.com/kb/ccc5/troubleshooting-slow-performance-when-copying-files-or-from-network-volume)



Working with FileVault Encryption

CCC is fully qualified for use with FileVault-protected volumes (HFS+ and APFS). CCC offers some advice around enabling encryption in the Disk Center.

Enabling encryption on a volume that contains (or will contain) an installation of macOS

If your goal is to create a bootable, encrypted backup, use the following procedure:

1. Follow CCC's documentation to [properly format the destination volume](http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x) [<http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x>](http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x). Do **not** format the volume as encrypted. Choose APFS if your Mac is a T2 Mac [<http://bombich.com/kb/ccc5/help-my-clone-wont-boot#t2_encrypted_hfs>](http://bombich.com/kb/ccc5/help-my-clone-wont-boot#t2_encrypted_hfs) (e.g. iMac Pro, 2018 MacBook Pro; [see the full list here](https://support.apple.com/en-us/HT208862) [<https://support.apple.com/en-us/HT208862>](https://support.apple.com/en-us/HT208862)).
2. Use CCC to [back up your startup disk](http://bombich.com/kb/ccc5/how-set-up-your-first-backup) [<http://bombich.com/kb/ccc5/how-set-up-your-first-backup>](http://bombich.com/kb/ccc5/how-set-up-your-first-backup) to the unencrypted destination volume.
3. If you're running an OS **older** than Mojave, select the destination volume in CCC's sidebar, then click the **Recovery HD** button to [create a Recovery HD](http://bombich.com/kb/ccc5/cloning-apples-recovery-hd-partition) [<http://bombich.com/kb/ccc5/cloning-apples-recovery-hd-partition>](http://bombich.com/kb/ccc5/cloning-apples-recovery-hd-partition) volume. Note: You must be logged in to an administrator account to perform this step. This step is unnecessary if your destination is an APFS-formatted volume.
4. Hold down the Option key (Intel Macs) or the Power button (Apple Silicon Macs) while restarting your Mac and choose the backup volume as the startup disk.
5. Enable FileVault encryption in the **Security & Privacy** preference pane of the System Preferences application.
6. [Configure CCC for regular backups](http://bombich.com/kb/ccc5/how-set-up-scheduled-backup) [<http://bombich.com/kb/ccc5/how-set-up-scheduled-backup>](http://bombich.com/kb/ccc5/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

Additionally, **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 `diskutil apfs list` (or `diskutil cs list` if the applicable volume is HFS+ formatted) 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?

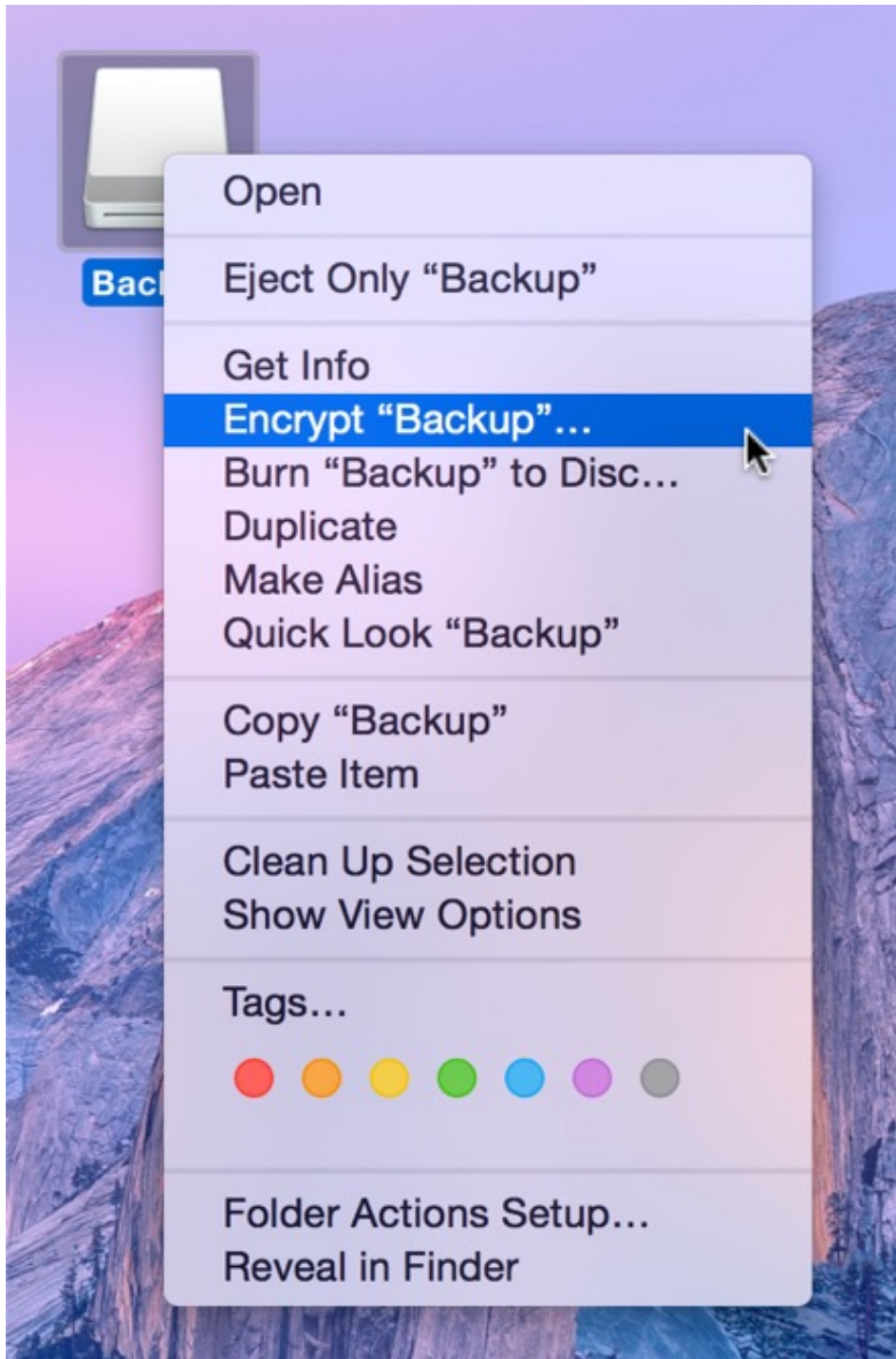
Enabling FileVault on the destination means that the volume starts out unencrypted, and then over the course of several hours the data is encrypted in place. If the encryption conversion process completes successfully, then for most intents and purposes, no trace of the unencrypted data will be left 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 <http://bombich.com/kb/ccc5/excluding-files-and-folders-from-backup-task>](http://bombich.com/kb/ccc5/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 users: When prompted to erase the destination, [proceed with a Data-only backup <http://bombich.com/kb/ccc5/creating-and-restoring-data-only-backups#create>](http://bombich.com/kb/ccc5/creating-and-restoring-data-only-backups#create) instead. You will not be able to exclude content from a Full Volume Clone. After the initial backup has completed, proceed to [install Big Sur onto the destination <http://bombich.com/kb/ccc5/creating-and-restoring-data-only-backups#install_macos>](http://bombich.com/kb/ccc5/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.

Enabling encryption on a volume that will not contain an installation of macOS

If your backup volume won't be a bootable backup of macOS, simply right-click on that volume in the Finder and choose the option to encrypt the volume. If your Mac is running macOS High Sierra or later, please note that [macOS will convert an HFS+ formatted volume to APFS <http://bombich.com/blog/2017/09/29/think-twice-before-encrypting-your-hfs-volumes-on-high-sierra>](http://bombich.com/blog/2017/09/29/think-twice-before-encrypting-your-hfs-volumes-on-high-sierra) when you enable encryption in this manner.



Related Documentation

- Frequently Asked Questions about encrypting the backup volume <<http://bombich.com/kb/ccc5/frequently-asked-questions-about-encrypting-backup-volume>>
- The Disk Center <<http://bombich.com/kb/ccc5/disk-center>>
- [Apple Kbase] Learn more about FileVault <<https://support.apple.com/kb/HT4790>>
- T2-based Macs can't boot from encrypted HFS+ volumes <http://bombich.com/kb/ccc5/help-my-clone-wont-boot#t2_encrypted_hfs>

Some files and folders are automatically excluded from a backup task

Carbon Copy Cloner 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
- .Volumelcon.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](#) <http://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
- /.fsevents
- /.hotfiles.btree
- /private/var/db/systemstats
- [/private/var/folders/*/*C](#)
- [/private/var/folders/*/*T](#)

These items are Apple-proprietary data stores that get regenerated when absent. Attempting to copy these data stores without unmounting the source and destination is not only futile, it will likely corrupt them (and their respective apps will reject them and recreate them).

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 cloned 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`

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. Choose **Copy Some Files** from the popup menu underneath the Source selector
2. Click the Inspector button adjacent to that same popup menu to reveal the Task Filter window
3. Uncheck the box next to **Don't copy the Finder's Trash**
4. 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 cloned 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.*
- .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 the backup volume. 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
- /.cleverfiles
- /Library/Application Support/Comodo/AntiVirus/Quarantine
- /private/var/spool/qmaster
- \$Recycle.Bin
- Library/Preferences/ByHost/com.apple.loginwindow*
- [.dropbox.cache <https://www.dropbox.com/help/desktop-web/cache-folder>](https://www.dropbox.com/help/desktop-web/cache-folder)
- [/private/var/db/atpstatdb*](#)
- [.@_thumb](#)
- [/.com.prosofteng.DrivePulse.ignore](#)
- [com.apple.photolibraryd/tmpoutboundsharing](#)

CCC SafetyNet folders

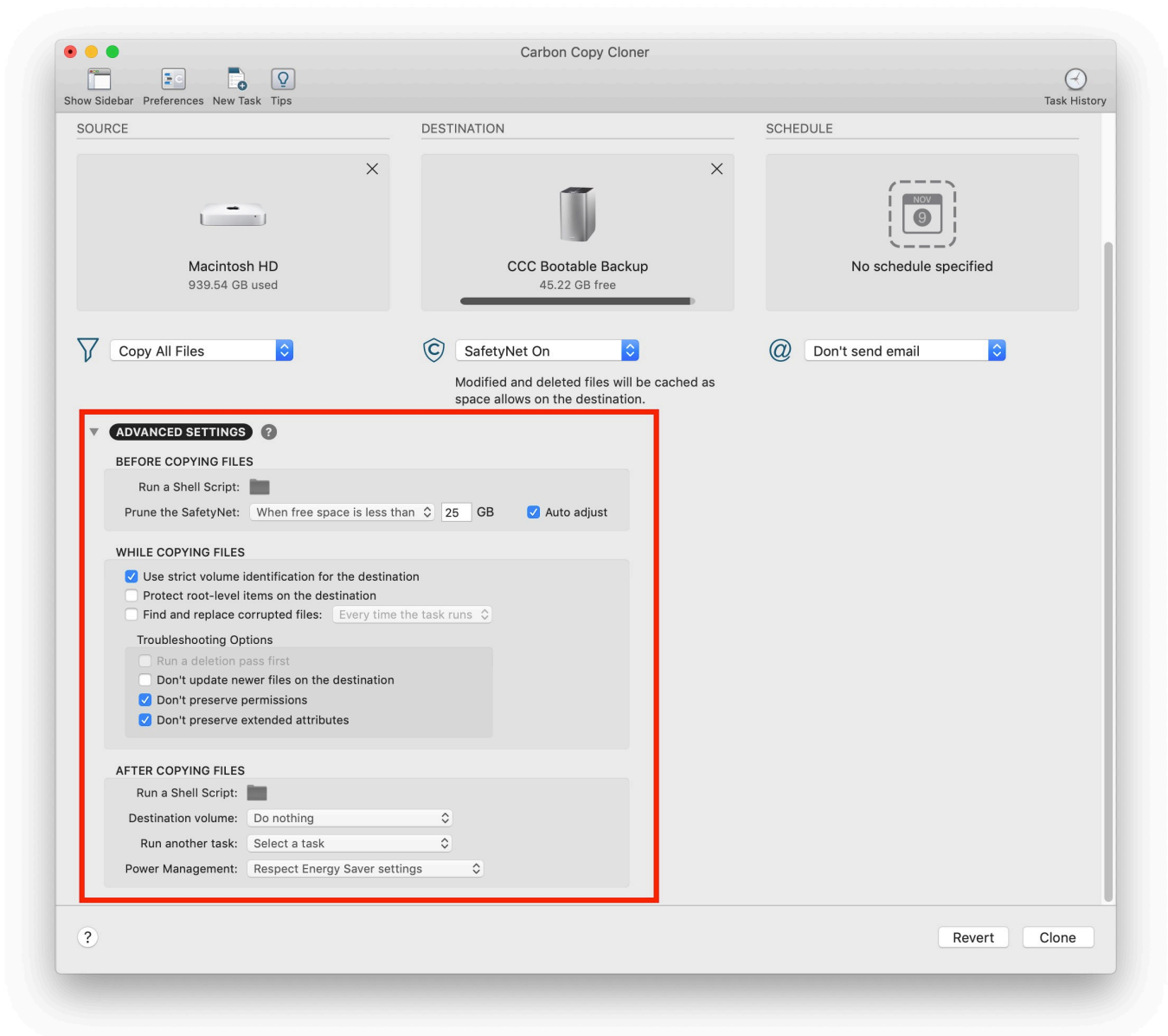
When CCC's SafetyNet feature is enabled, CCC creates a `_CCC SafetyNet` folder at the root of the selected destination volume or folder. When CCC encounters an item on the destination that does not exist on the source, or an item that will be replaced with an updated item from the source, that item gets 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 or set the destination as the startup disk, 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 post clone tasks, click the **Advanced Settings** button below CCC's Source selector.



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 pre clone 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](http://bombich.com/kb/coc5/automated-maintenance-coc-safetynet-folder) <<http://bombich.com/kb/coc5/automated-maintenance-coc-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.

CCC will not forcefully unmount the destination volume. 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 an error, though it will make a note of it in the Task History window.

Yosemite users have an option to set the destination volume as the startup disk. Starting in El Capitan, however, Apple's System Integrity Protection prevents third-party applications from changing the startup disk setting. We do not recommend disabling System Integrity Protection to make this feature work, rather we recommend that you use the Startup Disk Preference Pane to change the startup disk selection.

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 preference 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. 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.

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](#) <http://bombich.com/kb/ccc5/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 post clone shell scripts may be the solution for you. Pre clone 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 Preferences 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 <http://bombich.com/software/get_help>](http://bombich.com/software/get_help) rather than attempt to address the issue with a preflight shell script.

Post-clone 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 post clone 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 post-clone scripts, underlying volume path for a disk
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 post clone 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). On macOS Catalina and later, 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/Clone - Data"`.

Third parameter

- Pre clone script: The underlying mountpoint for the volume that holds the destination disk image, if applicable.
- Post clone script: The exit status of the file copying phase of the backup task.

Fourth parameter

The path to the destination disk image, if applicable.

If your pre clone 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 pre clone 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 Preferences 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 post clone 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.

AppleScripts are not supported

You cannot specify an AppleScript as a pre or post clone 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 post clone 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.

Security implications of pre and post clone 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 post clone 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 post clone 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 <http://bombich.com/software/files/tools/parallels_pause.sh.zip>](http://bombich.com/software/files/tools/parallels_pause.sh.zip)

This is a pre clone 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 post clone 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 <http://bombich.com/software/files/tools/parallels_start.sh.zip>](http://bombich.com/software/files/tools/parallels_start.sh.zip)

This post clone script will resume any Parallels VM containers that were suspended by the parallels_pause.sh pre clone script. Note: This script relies on command-line tools offered only in Parallels Desktop for Mac Pro or Business Edition.

[play_sound.sh <http://bombich.com/software/files/tools/play_sound.sh.zip>](http://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](http://bombich.com/software/files/tools/eject_source_and_destination.sh.zip)

[<http://bombich.com/software/files/tools/eject_source_and_destination.sh.zip>](http://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 post clone 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 macOS's desire to automatically regenerate various cache files. This delay can be adjusted if necessary by editing the script.

[pm_on_success.sh](http://bombich.com/software/files/tools/pm_on_success.sh.zip) <http://bombich.com/software/files/tools/pm_on_success.sh.zip>

This post clone 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](#)

<http://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](http://bombich.com/software/files/tools/post_to_slack.sh.zip) <http://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) <<https://slack.com>> channel.

[ifttt_maker.sh](http://bombich.com/software/files/tools/ifttt_maker.sh.zip) <http://bombich.com/software/files/tools/ifttt_maker.sh.zip>

This postflight script will post an [IFTTT Maker Event](https://ifttt.com/maker_webhooks) <https://ifttt.com/maker_webhooks> of the status of your backup task.

Restoring non-system files

Watch a video of this tutorial on YouTube <https://www.youtube.com/watch?v=n_7jgLKy_W0>

Because CCC backups are non-proprietary copies of your original volume, you can navigate the contents of your CCC backup volume in the Finder and find your files exactly where you would find them on the original source volume. If you need to restore a single file, **you can copy it directly from your backup volume in the Finder**. CCC *is not required* to gain access to your data. If you have a larger restore need, though, CCC is ready to help make the restore process as easy as it was to back up in the first place.

Restoring non-system files

The restore process is virtually identical to the backup process. The notable differences are that you will probably be restoring a smaller subset of files than what you backed up, and that you may want to indicate that files newer on the original volume shouldn't be overwritten by potentially older versions on your backup.

1. Launch CCC and create a new task
2. Select **Choose a folder...** from the Source selector and select a folder on your backup volume as the source
3. Select **Choose a folder...** from the Destination selector and choose a folder on your original source volume as the destination
4. Click the Clone button

Note: If you choose your startup disk as the destination volume directly (rather than choosing a folder on that volume), CCC will impose a protective filter on system files and folders. It wouldn't be a good idea to overwrite or delete system files on the OS that you're booted from, so this isn't something that CCC will allow. If you need to restore system items or items in the Applications folder, we recommend that you [boot from the backup volume before attempting to restore](http://bombich.com/kb/ccc5/how-restore-from-your-backup) <<http://bombich.com/kb/ccc5/how-restore-from-your-backup>>.



Backing up to a disk image

Disk images are not bootable backups. To create a bootable backup, you must back up to a hard drive that is attached directly to your Mac. We recommend that you only use a disk image if you are backing up to a network volume connected to via ethernet, and we recommend using locally-attached storage for your primary backups.

A disk image is a single file residing on your hard drive 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. We recommend using disk images sparingly. If you're backing up to a network volume and your Mac and the NAS device are connected to the network via ethernet, then a disk image may be a good fit. In most cases, however, disk images are not a great choice for your backup strategy.

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.

Read/write "sparseimage" disk images

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. **Use of this older disk image format is only recommended when backing up to non-AFP network volumes on an OS older than macOS Sierra.** 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. We recommend this disk image format for most scenarios.

Running out of space on a sparseimage or sparsebundle 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](#)

[<http://bombich.com/software/files/tools/Compact_Sparse_Image.app.zip>](http://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.

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](#) [<http://bombich.com/kb/ccc5/automated-maintenance-ccc-safetynet-folder>](http://bombich.com/kb/ccc5/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](#) [<http://bombich.com/kb/ccc5/protecting-data-already-on-your-destination-volume-carbon-copy-cloner-safetynet>](http://bombich.com/kb/ccc5/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](#) [<http://bombich.com/kb/ccc5/leveraging-snapshots-on-apfs-volumes>](http://bombich.com/kb/ccc5/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.

Sparsebundle disk images are not supported on some filesystems

If your Mac is running an OS older than macOS Sierra, CCC will refuse to save or mount a sparse bundle disk image if the underlying filesystem that the disk image file resides upon does not support the F_FULLFSYNC file control. Most filesystems support this file control, but the SMB file sharing protocol does not. Most people that encounter issues with creating a sparsebundle disk image on a network volume are encountering issues because the network volume is mounted via SMB.

Starting in Mavericks, Apple's preferred file sharing service is SMB. As a result, if you attempt to connect to a network volume, Finder will use SMB to establish that connection unless you explicitly specify AFP as the protocol to use. In this configuration, a sparse bundle disk image will not work, and CCC will issue an error. To avoid this error, connect to the network volume explicitly using AFP:

1. Eject the network volume if it is currently mounted
2. Choose **Connect to server** from the Finder's Go menu
3. Type in "afp://yourserver.local" (changing the hostname, of course), then click the Connect button and mount the network volume
4. Go back to CCC and choose **Choose disk image...** from the Destination selector, then select the sparsebundle disk image on your network volume

Why can't I use a sparsebundle disk image on a filesystem that does not support the F_FULLFSYNC file control?

When your computer writes a file out to the hard drive, the data usually goes to a "write buffer" — a small portion of RAM that is installed on the circuit board of the hard drive. By accumulating smaller write operations onto this RAM chip, the hard drive can increase overall write performance by writing large blocks of cached data to the physical media all at once. While this write buffer improves performance, it also carries a risk. If the power fails or the disk's connection to the computer is suddenly broken between the time that data was written to the buffer and when the buffer is flushed to the disk, your filesystem will have an inconsistency. Filesystem journaling typically mitigates this risk, however it doesn't offer enough protection for Apple's sparsebundle disk image type.

In Mac OS 10.5, Apple implemented the F_FULLFSYNC file control for network servers and clients. The F_FULLFSYNC file control is a command that is sent to the hard drive after some (or all) write operations that tells the disk to immediately flush its cache to permanent storage. To provide better protection for data on sparsebundle disk images, Apple disabled support on Mac OS 10.6 for using sparsebundle disk images that reside on filesystems that do not support the F_FULLFSYNC file control. Apple relaxed this requirement in macOS 10.12 (Sierra).

You are likely to encounter this error condition if your sparse bundle disk image is hosted on a pre-Mac OS 10.5 Macintosh or various Network Attached Storage (NAS) devices (especially SMB). When you encounter this error, copy the sparsebundle disk image to another network volume, or ask CCC to create a new sparseimage disk image file (sparseimage disk images are not the same as sparsebundle disk images).

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 other 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 <http://bombich.com/kb/cccl5/restoring-from-disk-image>](http://bombich.com/kb/cccl5/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. Launch 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, choose **Some files...** from the Clone menu (below the Source selector) and deselect any item that you do not wish to restore.
5. Click the Clone button.

Restoring system files to your startup disk

If you want to restore system files to your startup disk, you must start up your Macintosh from an installation of macOS on another hard drive, such as a bootable backup created by CCC. Once you have booted your Mac from another volume, follow the steps from the previous section.

Restoring system files to your startup disk when you don't have a bootable backup

If you do not have an installation of macOS on another hard drive, you can boot your Mac from your macOS Recovery volume and use Disk Utility to restore the entire disk image:

High Sierra and Mojave

Note: The destination volume format must match the format of the disk image that you're restoring from. This limitation is specific to Disk Utility – if you're [restoring from a disk image using CCC](#), CCC can restore an APFS disk image to an HFS+ volume, and you can restore an HFS+ disk image to an APFS volume. Use Disk Utility as a last resort.

1. Hold down Command+R while you restart your computer.
2. Choose **Disk Utility** in the Utilities application.
3. Choose **Show All Devices** from the View menu.
4. Click on the device you want to restore **to** in the sidebar (see [this article for specific formatting instructions <http://bombich.com/kb/cc5/preparing-your-backup-disk-backup-os-x>](http://bombich.com/kb/cc5/preparing-your-backup-disk-backup-os-x)).
5. Click the **Erase** button in the toolbar and proceed to erase the device using the GUID Partition Map partitioning scheme, and the format that matches your source disk image.
6. Reselect the volume that you would like to restore to. If you are restoring to an APFS volume,



choose the parent APFS container.

7. Choose **Open Disk Image...** from the File menu and select the disk image file that you would like to restore from.
8. Choose **Restore...** from the Edit menu.
9. Select the mounted disk image volume that you would like to restore. If you are restoring to an APFS volume, choose the container that is the parent of the disk image volume you are trying to restore.
10. Click the **Restore** button.

El Capitan and Sierra

1. Hold down Command+R while you restart your computer
2. Choose **Disk Utility** in the Utilities application
3. Click on the volume you want to restore **to** in the sidebar
4. Choose **Restore...** from the Edit menu
5. Click on the **Image...** button and locate the disk image that you would like to restore
6. Click the **Restore** button

Yosemite

1. Hold down Command+R while you restart your computer
2. Choose "Disk Utility" in the Utilities application
3. From the File menu, choose **Open Disk Image...** and locate the disk image that you would like to restore
4. In the list in the pane on the left, click on the mounted disk image's volume
5. Click on the **Restore** tab on the right side of the window
6. Drag the mounted disk image to the Source field. If the Source field does not accept the dragged volume, right-click on the disk image's mounted volume and choose **Set as source** from the contextual menu.
7. Drag the hard drive that you would like to restore to into the **Destination** field
8. Check the box to erase the destination (if present), then click on the Restore button.
9. Restart your Mac from your newly restored volume, then [use CCC to restore the Recovery HD volume <http://bombich.com/kb/ccc5/cloning-apples-recovery-hd-partition>](http://bombich.com/kb/ccc5/cloning-apples-recovery-hd-partition) from the archive on your startup disk.

Using Migration Assistant to migrate data from a disk image

If you have a clean installation of macOS and simply 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, it will not accept a disk image that has only user data.

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.

Migration Assistant and Yosemite, El Capitan

On Yosemite and El Capitan, Migration Assistant will ask that you close all applications, and it will then log you out before presenting migration options. This poses a problem for migrating data from a disk image because the disk image will be unmounted when you are logged out, and Migration Assistant doesn't offer any interface to choose a disk image. To work around this problem, you can use our [Mount disk image for Migration Assistant](http://bombich.com/software/files/tools/Mount_disk_image_for_Migration_Assistant.app.zip) [<http://bombich.com/software/files/tools/Mount_disk_image_for_Migration_Assistant.app.zip>](http://bombich.com/software/files/tools/Mount_disk_image_for_Migration_Assistant.app.zip) application. Simply drag the disk image containing your full system backup onto the application and it will guide you through a fairly simple procedure that will make the disk image available to Migration Assistant after a short delay.

Preliminary tests indicate that this workaround is not required on Sierra and later OSes.

I have a full-volume backup in a folder or a disk image, but I don't have a bootable backup. How can I restore everything?

CCC makes bootable backups specifically to avoid this kind of situation. When you have a bootable backup, you simply boot from that, then restore everything to a replacement disk or the original disk. One step, minimal time, couldn't be easier. Occasionally people get into this sticky situation though -- I have a backup of everything in a disk image or in a folder on the backup volume, there's a clean installation of macOS on my replacement disk, now how do I get everything back to the way that it was before?

The first thing that you need to do is **make a boot volume that is not the volume you want to restore to**. Once you have done that, you can boot from that volume and then do a complete restore of your backup to the replacement disk. There are several options for how and where you create this other bootable volume. For example, you could install macOS onto a thumb drive, or you could use CCC to clone your clean installation of macOS to a thumb drive. You could also create a new partition on your replacement disk and clone the fresh installation of macOS to that. The steps below attempt to make very few assumptions about the resources you'll have in this scenario: a) You have a fresh installation of macOS on a hard drive and b) you have your backup in a folder or disk image on some other disk. Given those assumptions, here is how we recommend that you proceed.

Create a new partition on your replacement disk

1. Open the Disk Utility application and click on the disk icon that represents your internal hard drive. Don't click on the **Macintosh HD** icon, click on the one above that.
2. Click on the Partition tab.
3. Click on the + button.
4. Set the size of the new partition to 20GB and name it something like **Rescue**.
5. Click the **Apply** button.

This video <<https://www.youtube.com/watch?v=XQG6-Ojiv3s>> describes the same procedure (albeit in a slightly different context).

Clone your fresh installation of macOS to the Rescue volume

1. Open Carbon Copy Cloner and create a new task.
2. Choose your current startup disk as the source.
3. Choose the Rescue volume as the destination.
4. If you aren't working from a fresh installation of macOS, choose **Some files...** from the Clone popup menu and take a moment to exclude third-party applications from the list of items to be copied, as well as any large items in your home folder (e.g. /Users/yourname/Music).
5. Click the Clone button.

Boot from the Rescue volume and restore your data to the replacement disk

1. Open the Startup Disk Preference Pane, set the Rescue volume as the startup disk, then click on the Restart button.
2. Once restarted from the Rescue volume, attach the backup volume to your Mac and open the Carbon Copy Cloner application.
3. If your data is backed up in a folder, choose **Choose a folder...** from the Source selector and select that folder as the source. Otherwise, choose **Restore from a disk image...** and locate your backup disk image.
4. Choose your **Macintosh HD** volume as the destination.
5. Verify that CCC's SafetyNet feature is enabled.
6. Click the Clone button.

Reboot from your restored volume and clean up

1. Open the Startup Disk Preference Pane, set the restored volume as the startup disk, then click on the Restart button.
2. Open the Disk Utility application and click on the disk icon that represents your internal hard drive.
3. Click on the Partition tab.
4. Click on the Rescue volume, then click on the - button to delete that volume.
5. Click the Apply button.

Finally, make a new backup to the root of a locally-attached hard drive so you'll have a bootable backup from here forward.

Using Carbon Copy Cloner to back up to/from another Macintosh on your network

Carbon Copy Cloner 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.

Note on bootability: This feature is not intended to create bootable backups of the source Macintosh. See [this section below](#) for additional details.

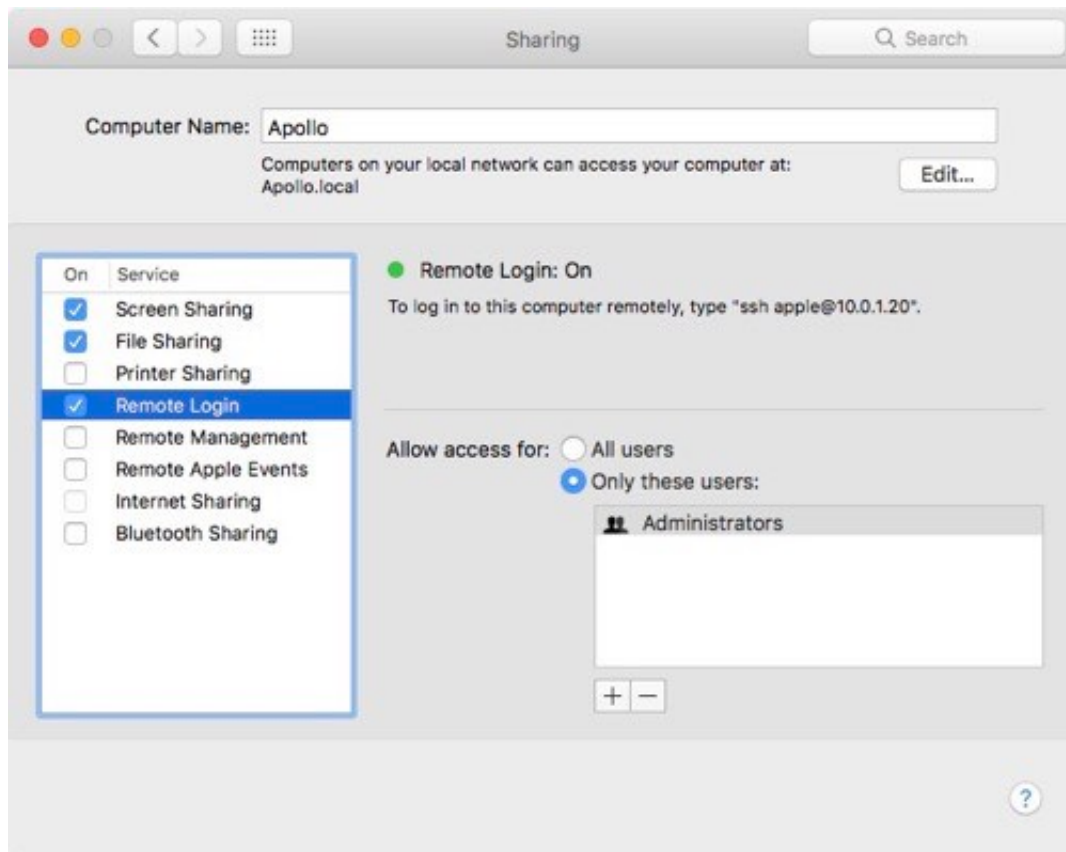
Before setting up CCC to back up to a remote Macintosh, you must:

1. Confirm that the remote Macintosh is running a supported OS (OS X 10.7 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

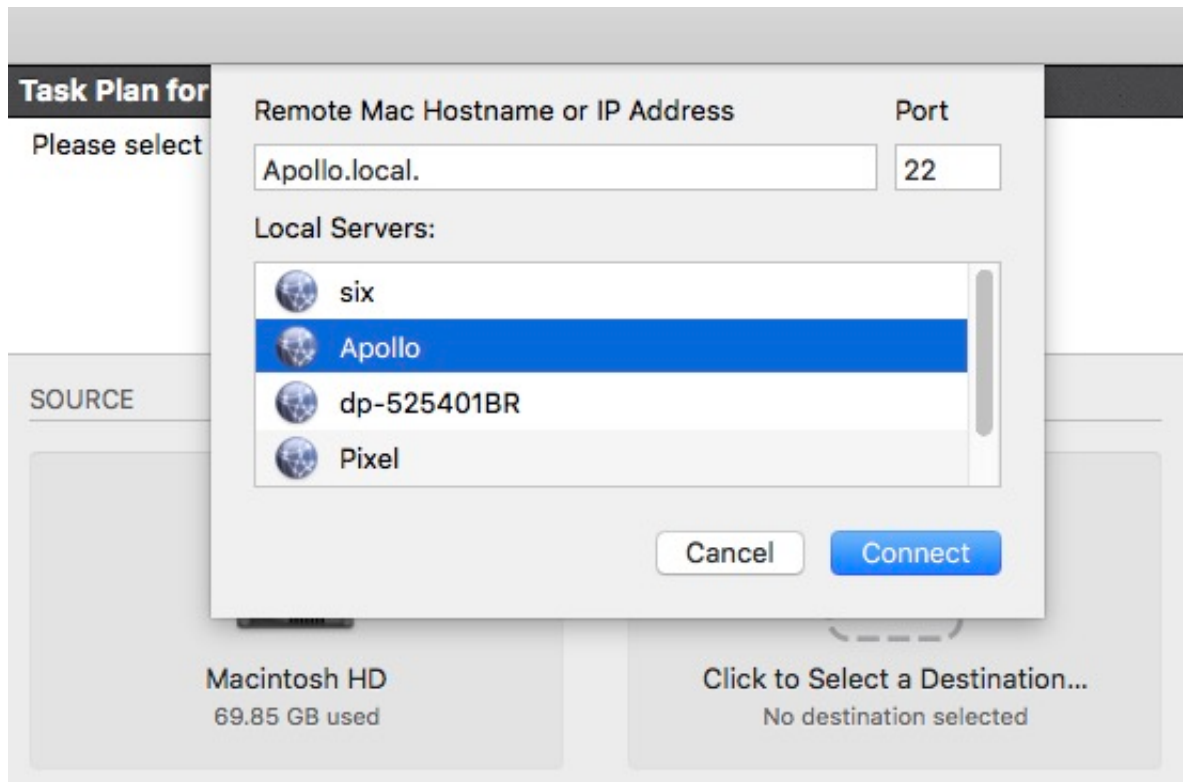
To enable Remote Login on your remote Macintosh:

1. Log in to that machine as an admin user.
2. Open the **System Preferences** application.
3. Open the **Sharing** Preference Pane.
4. Check the box next to **Remote Login**.
5. Be sure to allow access to **All users**, or explicitly add the **Administrators** group to the list of restricted users and groups.
6. Make a note of your remote Mac's hostname. The hostname is indicated underneath the Computer Name text field. In the screenshot below, "Apollo.local" is the hostname of the remote Macintosh.



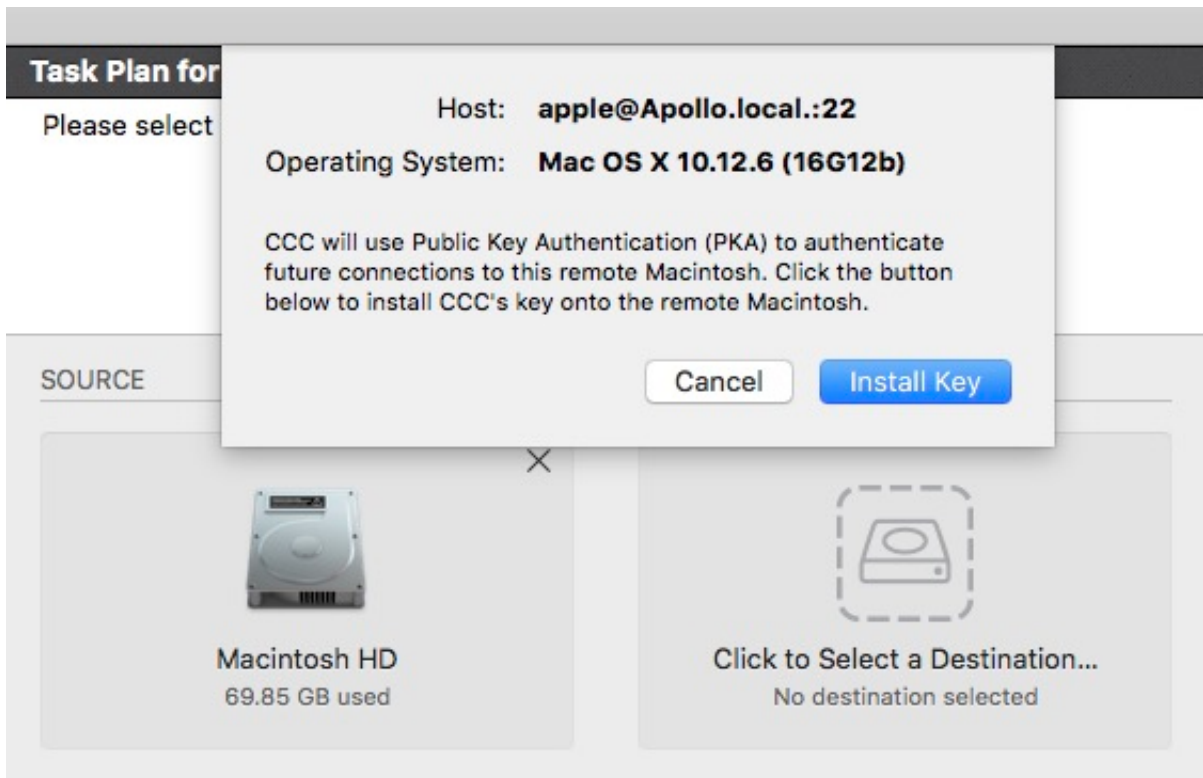
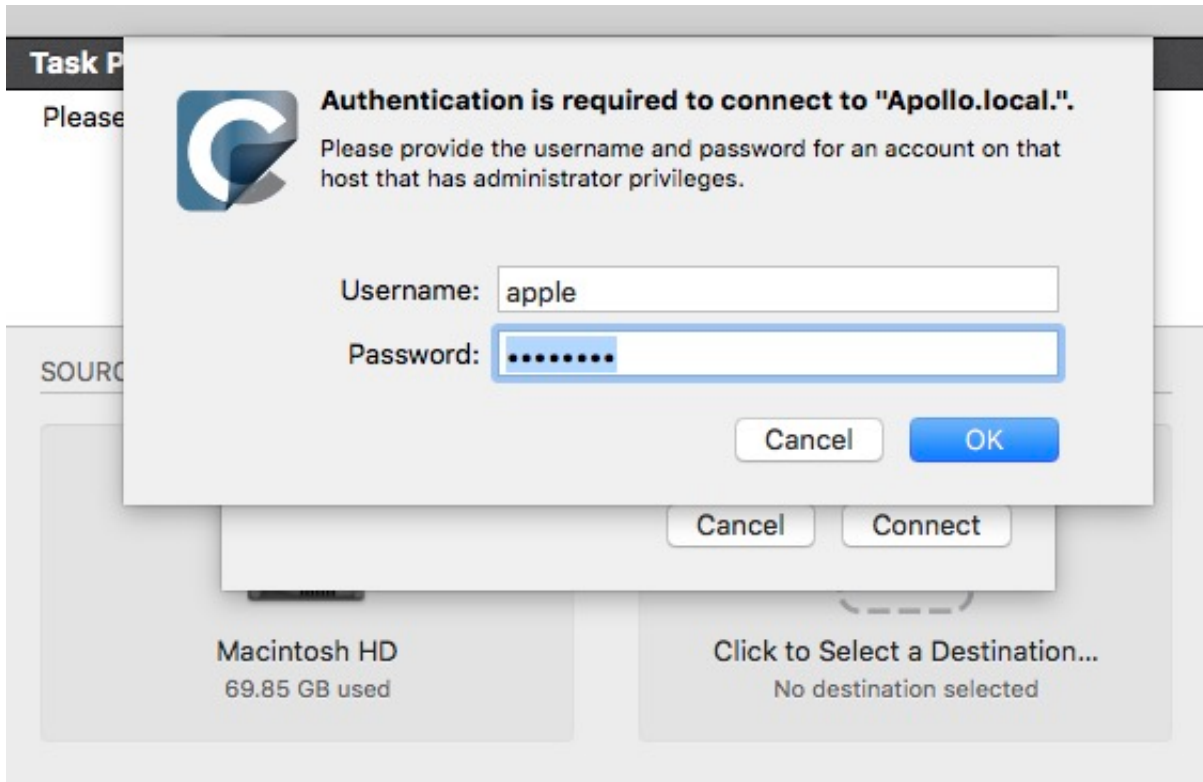
Configuring a Remote Macintosh source or destination

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.

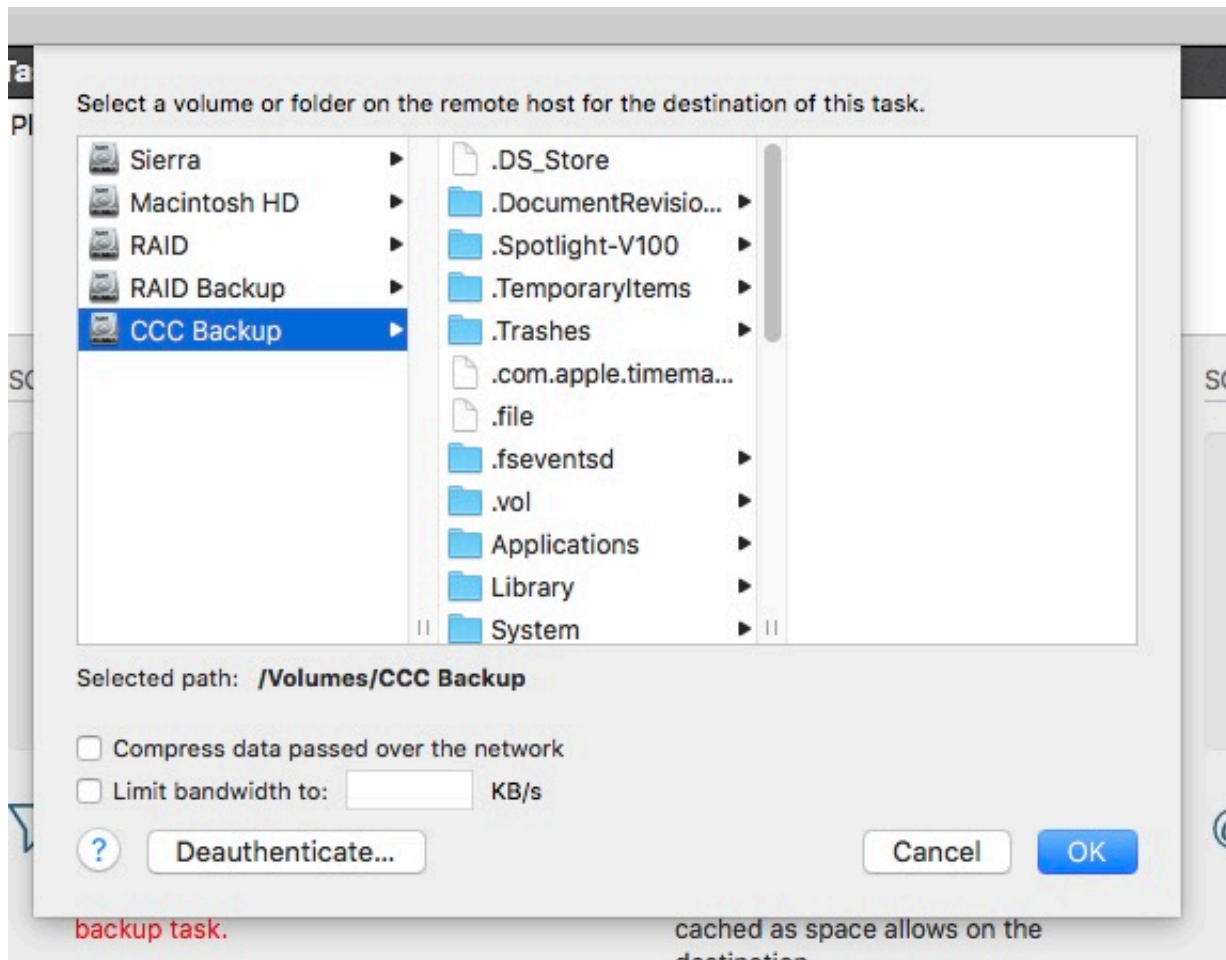


Once CCC has established a connection to the remote Mac, you will be prompted to install a Mac-specific Public Key Authentication (PKA) key pair onto the remote Mac. You must provide the username and password of an admin user on the remote Mac to permit this, and that admin user must have a non-blank 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 10.7 or later. Non-Macintosh systems are not supported with the **Remote Macintosh** feature.

Note for Yosemite, El Capitan, & Sierra users: If your source contains macOS Yosemite (or later) system files, the Remote Macintosh must be running macOS 10.9.5 or later. If the Remote Macintosh is not running 10.9.5 or later and you attempt to back up macOS Yosemite (or later) system files, the backup task will report numerous "Input/output" ("Media") errors. Filesystem changes introduced on Yosemite cannot be accommodated by older OSes. Apple added support for those filesystem changes in 10.9.5 to offer a modest amount of backwards compatibility.

Additional pointers for advanced users

Carbon Copy Cloner'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) <<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.

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 System Preferences and click on the User Accounts preference pane.
2. Click on the lock and authenticate.
3. Control+click on your account in the accounts table and choose "Advanced options".

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 <http://bombich.com/kb/coc5/restoring-from-backup-on-remote-macintosh>](http://bombich.com/kb/coc5/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.

Making bootable backups on remote Macs

If you are attempting to create a bootable backup of your Mac, you should attach the backup disk directly to your local Mac for an initial backup task. After verifying that the backup volume is bootable, you can then attach that disk to a remote Macintosh and proceed with regular backups. You should also repeat the local backup any time you apply major operating system upgrades so that any helper partitions on the backup disk can be updated accordingly.

Catalina users: Starting with macOS Catalina, *creating* bootable backups on a remote Macintosh is no longer practical — CCC can only perform the myriad of partitioning tasks that are required by Catalina on a locally-attached device. You can establish a bootable backup by attaching the destination disk directly to your Mac for the initial backup, but once that disk is attached to a remote Mac, CCC will only be able to maintain a backup of the Data volume. Copying system files to a remote Macintosh is not supported on systems running Catalina or later. If you select a Catalina startup disk as the source for a backup task and a remote Macintosh destination, CCC will automatically exclude system files from the backup task. When selecting a destination on the remote Mac for this sort of backup, choose the "Data" volume that is associated with your backup destination, e.g. "CCC Backup - Data" (**NOT** the volume named just "Data"; that is your remote Mac's startup disk Data volume!). If you would like to avoid the system file restriction and back up your whole source Data volume, you can drag that volume (e.g. "Macintosh HD - Data") from CCC's sidebar onto the Source selector.

Likewise, CCC will not allow the selection of a Catalina+ System volume on a remote Mac as the source for a backup task. Instead, choose the "Data" volume on the remote Mac to back up the user data portion of the startup disk. This backup will not be bootable, but it can be used as a source to the Migration Assistant application.

Snapshot support on remote Macs

Snapshot support is not available for volumes attached to a remote Macintosh.

Related Documentation

- [Restoring from a backup on a remote Macintosh <http://bombich.com/kb/coc5/restoring-from-backup-on-remote-macintosh>](http://bombich.com/kb/coc5/restoring-from-backup-on-remote-macintosh)
- [A caveat for backing up to a remote Macintosh that has no user logged in <http://bombich.com/kb/coc5/caveat-backing-up-remote-macintosh-has-no-user-logged-in>](http://bombich.com/kb/coc5/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 Carbon Copy Cloner to backup to another Macintosh on your network <http://bombich.com/kb/ccc5/using-carbon-copy-cloner-back-up-another-macintosh-on-your-network>](http://bombich.com/kb/ccc5/using-carbon-copy-cloner-back-up-another-macintosh-on-your-network)

Restoring from a backup on a remote Macintosh

macOS Catalina (10.15) and later

Starting with macOS Catalina, *creating* bootable backups on a remote Macintosh is no longer practical — CCC can only perform the myriad of partitioning tasks that are required by Catalina on a locally-attached device. You can establish a bootable backup by attaching the destination disk directly to your Mac for the initial backup, but once that disk is attached to a remote Mac, CCC will only be able to maintain a backup of the Data volume. That volume will remain bootable, but depending on how far out of date the OS is on the backup, you may not want to restore the OS to a replacement disk. You can use Migration Assistant instead in those cases:

1. Hold down Option(⌥)-Command (⌘)-R to boot the Mac in Internet Recovery mode
2. Install macOS onto the replacement hard drive
3. When prompted, attach the backup disk to your Mac and use Migration Assistant to migrate data from the backup volume to the replacement startup disk

Related Documentation

- [Making bootable backups on remote Macs <http://bombich.com/kb/ccc5/using-carbon-copy-cloner-back-up-another-macintosh-on-your-network#bootable>](http://bombich.com/kb/ccc5/using-carbon-copy-cloner-back-up-another-macintosh-on-your-network#bootable)

macOS Yosemite, El Capitan, Sierra, High Sierra, Mojave (10.10 through 10.14)

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
7. Click the **Clone** button

Related Documentation

- [Using Carbon Copy Cloner to back up to/from another Macintosh on your network <http://bombich.com/kb/ccc5/using-carbon-copy-cloner-back-up-another-macintosh-on-your-network>](http://bombich.com/kb/ccc5/using-carbon-copy-cloner-back-up-another-macintosh-on-your-network)



Task Organization

Adding a task

Tasks can be added in several different ways. To create a new task with default settings, click the **+** icon in the Tasks table header, or choose **New Task** from CCC's File 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 File 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, click the **-** button in the Tasks table header, or select the task and choose **Delete Task...** from CCC's File 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 the triangle icon 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.

Task Groups

Click the Add Task Group (folder with a "+") icon 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 Clone 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.

Task list sort order vs. task group run order

Tasks listed within a group in the Tasks table will be sorted based on the Tasks table sort criteria. If you have chosen to sort the Tasks table manually, then you can order the tasks within the group in the Tasks table however you want. Don't confuse this with the run order for the tasks within the group. The task run order is defined in the **Upcoming Group and Task Events** table.

Scheduling task groups

Task groups can be scheduled in the same manner as individual tasks; simply click on the Scheduler 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 File menu. If you would like to export all of your tasks, choose **Export All Tasks...** from CCC's File menu.

I want to defragment my hard drive

A welcome side-effect of cloning one volume to another is that the files on the resulting volume are largely defragmented. While fragmentation is not as significant of an issue as it used to be (e.g. in the Mac OS 9 days), people that have begun to fill the last 10-15% of their boot volume may see some performance benefit from defragmentation. If you find yourself in this situation, this is also a really good time to consider migrating to a larger hard drive altogether, or to an SSD, which is not affected by fragmentation.

Defragmentation is a natural result of backing up your data to an empty backup volume. Simply [prepare your backup volume for use with Carbon Copy Cloner](http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x) <<http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x>>, then use CCC to clone your source volume to your destination volume.

"Clone, wipe, restore" — think twice before you wipe that original volume

It may be really tempting to do the following:

1. Clone your boot volume — the one with your lifetime of irreplaceable data — to another hard drive
2. Boot your Mac from that cloned volume
3. Use Disk Utility to wipe the original volume
4. Restore the cloned volume to the original volume

Very quickly you'll be booted back up from your boot volume and you'll have a backup to boot, right? In most cases, this would work out great for you, and you'd be fine. There are two really good reasons, however, to stop after the second step and take a breather:

1. As soon as you erase the original volume, you're down to one copy of your data — you have no backup. The restore task will stress both the source and destination disks with massive reads and writes. If either disk were on the verge of failure, this level of stress could push it over.
2. You really should take the time to verify your backup. I trust CCC with my data, but do I trust that I asked it to copy the right items? Did my destination disk turn out to be a lemon?

The Best Practice for defragmenting your hard drive

1. Establish a backup regimen to a primary backup volume. Test your backups regularly.
2. Quit open applications and use CCC to update your backup one last time.
3. Use CCC to clone your hard drive to some physical volume other than your primary backup.
4. Boot from the cloned volume.
5. Use Disk Utility to reformat your original volume.
6. Use CCC to restore your cloned volume back to the original volume.
7. Boot from the original volume.

Performance upon first boot from a cloned volume will always be slightly slower than normal as Spotlight reindexes your data. When the system has "settled down", you will be able to evaluate whether the defragmentation has offered any performance benefit.

Using the ccc Command Line Tool to Start, Stop, and Monitor CCC Backup Tasks

Carbon Copy Cloner 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. nia 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 top
of the Task History window.
    -c prints in CSV format
    -d prints dates in seconds since Midnight Jan 1, 1970 (rather than formatting the date)
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 date)
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 databases on OS X Server

Databases are proprietary file types that often cannot be backed up in the conventional manner. In CCC, you can leverage a preflight shell script to perform an "out of band" backup of various databases using database-specific tools. The CCC backup task will subsequently back up the database archive files, from which you could restore the database at a later time.

The following pre-clone shell script will dump the contents of any MySQL databases. In the event that your standard backup of the database doesn't open, you can later restore it from the dump.

```
#!/bin/sh
PATH="$PATH:/Applications/Server.app/Contents/ServerRoot/usr/bin"
PATH="$PATH:/Applications/Server.app/Contents/ServerRoot/usr/sbin"
PATH="$PATH:/Applications/Server.app/Contents/ServerRoot/usr/libexec"
export PATH

# Path to recovery directory (permissions should be 700 -- read-only root or admin)
recover="/etc/recover"
ts=`date "+%F"`

echo "Removing manual archives older than two weeks"
find $recover/ -mindepth 1 -mtime +14 -exec rm '{}' \;

# mysqldump the databases
dbs="some_database another_database mysql"
for db in $dbs; do
    echo "Dumping $db"
    mysqldump --user=root --password='s3kr!t' $db > $recover/${db}_${ts}.dump
    gzip $recover/${db}_${ts}.dump
done

# If you ever need to restore from a database dump, you would run:
# gunzip $recover/database_name_(timestamp).dump.gz
# mysql -u root -p database_name < $recover/database_name.dump
```

Backing up an Open Directory Master

Archiving an OD master database requires encryption, and providing the encryption password interactively can be challenging in an automated backup. The expect shell environment can be helpful for this task. The following pre-clone shell script will archive a macOS Server Open Directory master to a disk image for later restoration via the server administration application.

```
#!/usr/bin/expect -f

set date [timestamp -format "%Y-%m-%d"]
set archive_path "path/to/you/backup/dir"
set archive_password "password"
set archive_name "opendirectory_backup"
set timeout 120

spawn /usr/sbin/slapconfig -backupdb $archive_path/$archive_name-$date
```



```
expect "Enter archive password"  
send "$archive_password\r"  
expect eof
```

Related Documentation

- [Example pre and post clone shell scripts <http://bombich.com/kb/ccc5/performing-actions-before-and-after-backup-task#examples>](http://bombich.com/kb/ccc5/performing-actions-before-and-after-backup-task#examples)
- [Bender - Automated Backup of OS X Server Settings \[Third-party script\] <https://forgetcomputers.zendesk.com/hc/en-us/articles/201008710-Bender-Automated-Backup-of-OS-X-Server-Settings>](https://forgetcomputers.zendesk.com/hc/en-us/articles/201008710-Bender-Automated-Backup-of-OS-X-Server-Settings)

Backing up large files, mounted disk images, and Virtual Machine containers

Note: When backing up an APFS-formatted volume with CCC 5.1 or later, 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 post clone 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 post clone shell scripts <http://bombich.com/kb/ccc5/performing-actions-before-and-after-backup-task#examples>](http://bombich.com/kb/ccc5/performing-actions-before-and-after-backup-task#examples)
- [Creating a separate task to prevent VM container versions from bloating the SafetyNet <http://bombich.com/kb/ccc5/creating-separate-task-prevent-vm-container-versions-from-bloating-safetynet>](http://bombich.com/kb/ccc5/creating-separate-task-prevent-vm-container-versions-from-bloating-safetynet)
- [Leveraging Snapshots on APFS Volumes <http://bombich.com/kb/ccc5/leveraging-snapshots-on-apfs-volumes>](http://bombich.com/kb/ccc5/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 <http://bombich.com/kb/ccc5/leveraging-snapshots-on-apfs-volumes#srp>](http://bombich.com/kb/ccc5/leveraging-snapshots-on-apfs-volumes#srp) for more information on SafetyNet Snapshot retention.

Carbon Copy Cloner 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 in CCC's main window.

Task Plan

CCC will copy **Macintosh HD** to **CCC Backup**. Only items that have been modified since the last run. Barring any hardware compatibility problems, **the destination volume should be bootable**.

Last Run: Today at 9:20 AM

Next Run: This task will run when you click the "Clone" button.

The screenshot shows the CCC interface with two columns: SOURCE and DESTINATION. The SOURCE is 'Macintosh HD' (82.34 GB used) and the DESTINATION is 'CCC Backup' (3.1 TB free). Below the disks are two dropdown menus: 'Copy All Files' and 'SafetyNet On'. A note states: 'Modified and deleted files will be cached as space allows on the destination.' The 'ADVANCED SETTINGS' section is expanded, showing 'BEFORE COPYING FILES' with a 'Run a Shell Script' field and a 'Prune the SafetyNet' dropdown menu. The dropdown menu is open, showing options: 'When free space is less than' (selected), 'Archives that are older than', 'Archives that are larger than', and 'Never'. The 'When free space is less than' option is set to '25 GB' and has a checked 'Auto adjust' checkbox.

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 <<http://bombich.com/kb/cc5/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 restart the task.

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, then 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 specific folder for this purpose at the root level of your backup volume.

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.

Additional References

- [Apple Kbase HT201583: You can't empty the Trash or move a file to the Trash <https://support.apple.com/en-us/HT201583>](https://support.apple.com/en-us/HT201583)

Related Documentation

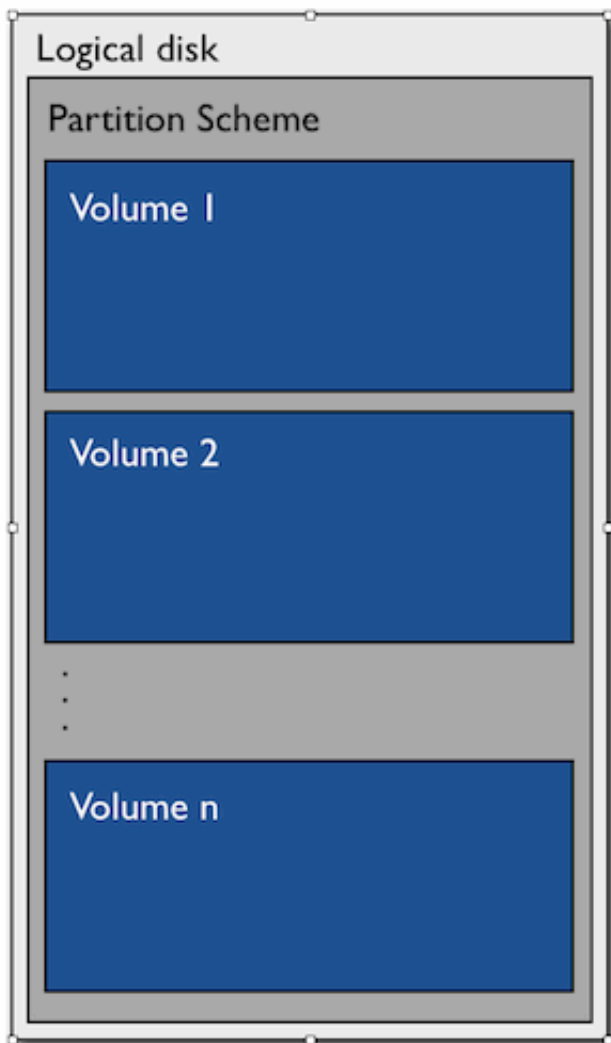
- [Frequently asked questions about the Carbon Copy Cloner SafetyNet <http://bombich.com/kb/cc5/frequently-asked-questions-about-carbon-copy-cloner-safetynet>](http://bombich.com/kb/cc5/frequently-asked-questions-about-carbon-copy-cloner-safetynet)

"My disk is already formatted APFS or HFS+, why am I getting this warning?"

If your disk is not partitioned using the scheme recommended and supported by Apple, CCC will indicate a warning when you start the backup task such as:

"You may have difficulty booting from this destination volume, the underlying disk is not partitioned with a partitioning scheme that Apple recommends for Intel Macs.", or when CCC attempts to convert the destination to APFS after installing macOS 10.15 Catalina, CCC may be unable to convert the volume from HFS+.

How your destination volume is formatted is not actually relevant to this warning. The problem is not a matter of how your destination **volume** is formatted, rather it is a matter of how the **disk** is partitioned. The following graphic explains the relationship between a disk and a volume:



Every disk has exactly one partition scheme. A disk can be partitioned as "Apple Partition Map"

(APM), "GUID Partition Table" (GPT), "Master Boot Record" (MBR), or the Fdisk partitioning scheme. PowerPC Macs could only boot from a disk that is partitioned with the APM partitioning scheme. Intel Macs can boot from a disk that is partitioned with either the APM or GPT partitioning scheme. Note, however, that Apple only supports booting an Intel Mac from a disk partitioned with the GPT partitioning scheme. **Because Apple no longer supports the APM partitioning scheme, CCC will warn you if your destination disk is not partitioned with the GPT partitioning scheme.** As the warning indicates, you **may** have difficulty booting from the destination volume, but it may work just fine. We expect that Intel Macs will eventually drop support for booting from APM-partitioned disks.

Apple's New APFS format can only reside on a "GUID Partition Table" (GPT) partition scheme so if your destination is not using GPT, CCC will be unable to convert an HFS+ volume to the volume to APFS as required by macOS 10.15 Catalina and the backup will fail with a warning about the partition scheme.

Here's what you need to do about the warning

If you haven't copied any data to the destination disk, then take the time to repartition your disk using the GPT partitioning scheme (see above) so you have a sanctioned, bootable backup volume.

If you cannot repartition the disk because you already have a considerable amount of data on the disk, and are using macOS 10.14 Mojave or earlier, proceed with the backup task, but [confirm whether it can actually boot your Mac <http://bombich.com/kb/cc5/how-verify-or-test-your-backup>](http://bombich.com/kb/cc5/how-verify-or-test-your-backup). If it can, you're all set and you shouldn't be bothered by the warning again. If you cannot, you will have to back up the other data on your destination disk and repartition the disk using the GPT partitioning scheme to get a bootable backup.

If you are running macOS 10.15 Catalina, or newer, the volume must be repartitioned.

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. 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. It is not possible to update an OS backup on a network volume.

Related Documentation

- [Learn about alternatives to backing up macOS to non-macOS-formatted volumes <http://bombich.com/kb/ccc5/i-want-back-up-multiple-macs-or-source-volumes-same-hard-drive#disk_image>](http://bombich.com/kb/ccc5/i-want-back-up-multiple-macs-or-source-volumes-same-hard-drive#disk_image)
- [Preparing your backup disk for a backup of macOS <http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x>](http://bombich.com/kb/ccc5/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 **Clone** 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 Gear 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](http://bombich.com/kb/ccc5/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.

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](http://bombich.com/kb/ccc5/cloning-coach-configuration-concerns#metadata_preservation) between the source and destination volumes. You can view the Cloning Coach's warnings by clicking on the yellow caution button in the Task Plan header. 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 File Stream 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 File Stream – 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>](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.wdc.com/knowledgebase/answer.aspx?ID=2686>](https://support.wdc.com/knowledgebase/answer.aspx?ID=2686). 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 <http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x>](http://bombich.com/kb/ccc5/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 Cloning 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). Choose **Connect to server** from the Finder's Go menu, then specify "smb://servername.local/volume" or "afp://servername.local/volume" to connect to the server using a different protocol. If you are unsure which protocol you are currently using, click on the mounted volume in the Finder, then choose **Get Info** from the Finder's **File** menu to find out.
- 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 cope poorly with files and folders with special characters

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 character (":") are unacceptable. When the file sharing service encounters files or folders with these disallowed characters, 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. To avoid these errors, you should either rename the offending files on the source, or connect to the NAS device using AFP rather than SMB (if applicable). Choose **Connect to server** from the Finder's Go menu, then specify "afp://servername.local/volume" to connect to the server using a different protocol.

Possible workaround: If you can modify the configuration of the SMB file sharing service on your NAS, then you may be able to prevent the service from "mangling" these file names. The applicable setting is [documented here](#) <<https://www.samba.org/samba/samba/docs/man/manpages/smb.conf.5.html#idp60809664>>.

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://community.synology.com/enu/forum/1/post/133965>> 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.

A closer look at how CCC determines the "bootability" of a destination volume

CCC determines whether your destination volume will be bootable and indicates any configuration concerns in the "Cloning Coach" window. If you see a yellow warning icon in the Task Plan header, you can click on that icon to see these concerns. CCC will also present these concerns to you the first time that you configure a backup task to any particular destination volume.

If CCC doesn't raise any configuration concerns, and the destination volume has an OS on it when the backup task is completed, and barring any hardware problems that might interfere, your backup volume should be bootable.

Configuration concerns that affect the bootability of the destination volume

CCC looks for the following configurations to determine if a destination volume will not be bootable:

- The destination volume cannot be a disk image — you cannot boot your Macintosh from a disk image.
- The files and folders required by macOS must be present on the source volume. These include: /Library, /System, /bin, /etc, /mach_kernel, /private, /sbin, /tmp, /usr, and /var.
- The files and folders that are required by macOS must not be excluded from the backup (applicable only if you have chosen to back up **Some files**).
- The hard drive on which the destination volume resides must be partitioned using the GUID Partition Table partitioning scheme.

Related documentation:

- [What makes a volume bootable? <http://bombich.com/kb/ccc5/what-makes-volume-bootable>](http://bombich.com/kb/ccc5/what-makes-volume-bootable)
- [Don't install older versions of macOS <http://bombich.com/kb/ccc5/i-want-clone-my-entire-hard-drive-new-hard-drive-or-new-machine#dont_install_older_os_versions>](http://bombich.com/kb/ccc5/i-want-clone-my-entire-hard-drive-new-hard-drive-or-new-machine#dont_install_older_os_versions)

"Some file metadata cannot be preserved"

CCC will note a concern if there is a compatibility mismatch between the source and destination filesystems. For example, if you are backing up files from an HFS+ volume to a network filesystem, some of the filesystem metadata cannot be preserved. In many cases this is acceptable and you can ignore the message. The types of metadata that can't be preserved in these cases are described in more detail below.

Access Control Lists

[Access Control Lists <https://en.wikipedia.org/wiki/Access_control_list>](https://en.wikipedia.org/wiki/Access_control_list) specify a granular list of the privileges that users and groups have for a particular file or folder (e.g., read, write, get information, delete, etc.). These advanced privilege settings generally apply only to user accounts that have been created on your Macintosh — for example, to prevent other users from deleting items from your

home directory. If you are backing up your own files to a locally-attached hard drive, or to a network file share on a trusted computer, the Access Control List filesystem metadata is relatively unimportant. If you are backing up to or from a network filesystem in a business or education setting, however, check with your tech support staff for additional advice on whether this metadata must be preserved.

Hard links

A [hard link](https://en.wikipedia.org/wiki/Hard_links) <https://en.wikipedia.org/wiki/Hard_links> makes a single file appear to be located in multiple places on your hard drive. If a single file had 20 hard links scattered across the disk, each hard link file would consume no additional space on the hard drive, and editing the content of any one of those files would immediately affect the content of every other hard link to that file.

When you back up the contents of a volume that contains hard links, ideally you want to preserve the hard links. If the destination filesystem doesn't support hard links, each hard linked file will be disassociated from the original file and will become a copy on the destination. This won't result in any loss of data, but your backup set will consume more space on the destination than on the source. Hard links are leveraged quite a bit on macOS by the operating system, though they are generally less common among user data.

Ownership

File ownership indicates which user account on your Mac has control of a file. The owner of a file can limit access to that file from other users on the same computer. If the destination doesn't support ownership, then the owner of each file copied to the destination will be set to the user that mounted the destination. If the destination volume is accessed elsewhere (e.g. mounted on another Mac or even by a different user on the same Mac), then any restrictions that you have placed on those files may not be honored. If you are backing up files and folders that are not all owned by the same user (e.g. you), you should consider backing up to a local, HFS+ formatted volume or to a disk image instead.

Some filesystems have file size limitations

Some filesystems have restrictions on how large a file can be. FAT32, for example, limits files to 4GB or less. CCC will proactively warn you of this limitation if you choose to back up a volume whose filesystem supports files larger than 4GB to a filesystem that does not support files larger than 4GB. CCC will then automatically exclude files larger than 4GB from the backup task. Files that were excluded will be reported at the end of the backup task.

If you require that files larger than 4GB are backed up, you must reformat the destination volume with a format that supports larger files.

Related documentation:

- [Preparing your backup disk for a backup of macOS](http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x) <<http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x>>

The destination already has an installation of macOS. Merging a different version of macOS into this destination may cause problems with that installation of macOS

This message appears if you choose the **Don't delete anything** SafetyNet setting. While that setting will protect any data that you have on the destination volume that is unique to that volume,

it does a disservice to the installation of macOS on your destination. This message will also appear if you use the **Don't update newer files on the destination** advanced troubleshooting setting.

Suppose, for example, that you have a complete backup of Mac OS 10.12.4 on your backup volume. When you apply the 10.12.5 update to your source volume, many system files are updated, some new files are added, and some files may be deleted. If you use CCC to update your backup volume, but you don't allow CCC to delete the items on the destination that the OS update had deleted from the source, then there will be a bunch of "cruft" left over on the backup volume. If you should ever need to boot your Mac from your backup volume, these cruft files could cause the OS to behave unexpectedly, and they may prevent it from booting altogether.

CCC can help you perform a clean upgrade or downgrade of macOS on the destination volume by moving items that should be deleted to the SafetyNet folder. Any files and folders that you keep only on the destination would also be moved to the SafetyNet folder. See the [Protecting data that is already on your destination volume <http://bombich.com/kb/ccc5/protecting-data-already-on-your-destination-volume-carbon-copy-cloner-safetynet>](http://bombich.com/kb/ccc5/protecting-data-already-on-your-destination-volume-carbon-copy-cloner-safetynet) section of the documentation for more details on these settings.

Some Macs may not boot from USB devices larger than 2TB

In the past we received several reports of bootability problems related to USB devices larger than 2TB. At that time, we performed a simple litmus test: create an "x"TB partition at the beginning of the disk (varying x from 0.5 to 2.5TB) and a second partition consuming the remainder of the disk, then install macOS onto both partitions. The results of those tests suggested that some Macs couldn't "see" the partition that lied past the 2TB mark on the disk. This limitation was specific to USB devices — none of these problems occurred if you were to place the same disk into a Thunderbolt enclosure.

At the time of those initial reports and testing, the results were consistent. We concluded that there was likely a 32-bit addressing limitation imposed by the USB drivers that are embedded in the Macs' firmware ("likely" — unfortunately none of this information is documented by Apple). More recently, however, we've been unable to consistently reproduce the same results. Apple may have addressed the problem with a firmware update. It's also possible that our initial conclusion was wrong, e.g. that the problem was due to a partition alignment error; an error specific to macOS El Capitan and apparently only USB devices (you'd see "disk2s2: alignment error" messages in the system log when the affected volume is mounted).

In any case, CCC's warning was issued out of an abundance of caution. Our current recommendation is to [partition the destination device using the same procedure as defined for all other destination devices <http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x>](http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x), and do the partitioning while booted from any other OS than El Capitan. In other words, don't proactively create a 2TB partition at the beginning of the disk. Once you have completed your first backup, though, we encourage you to [verify that your Mac will boot from the backup volume <http://bombich.com/kb/ccc5/how-verify-or-test-your-backup>](http://bombich.com/kb/ccc5/how-verify-or-test-your-backup). If your Mac is unable to boot from the backup volume, [please reach out to us <http://bombich.com/hc/requests/new>](http://bombich.com/hc/requests/new) so we can investigate your specific configuration further.

Help! My clone won't boot!

See [this section of CCC's documentation <http://bombich.com/kb/ccc5/help-my-clone-wont-boot>](http://bombich.com/kb/ccc5/help-my-clone-wont-boot) for troubleshooting advice if you're having trouble getting your backup volume to start your Mac.

Cloning Coach Configuration Concerns

CCC determines whether your destination volume will be bootable and indicates any configuration concerns in the "Cloning Coach" window. If you see a yellow warning icon in the Task Plan header, you can click on that icon to see these concerns. CCC will also present these concerns to you the first time that you configure a backup task to any particular destination volume.

If CCC doesn't raise any configuration concerns, and the destination volume has an OS on it when the backup task is completed, and barring any hardware problems that might interfere, your backup volume should be bootable.

Configuration concerns that affect the bootability of the destination volume

CCC looks for the following configurations to determine if a destination volume will not be bootable:

- The destination volume cannot be a disk image — you cannot boot your Macintosh from a disk image.
- The files and folders required by macOS must be present on the source volume. These include: /Library, /System, /bin, /etc, /mach_kernel, /private, /sbin, /tmp, /usr, and /var.
- The files and folders that are required by macOS must not be excluded from the backup (applicable only if you have chosen to back up "Selected files").
- The hard drive on which the destination volume resides must be partitioned using the GUID Partition Table partitioning scheme.
- CCC will issue a warning if the operating system that you're backing up (or restoring) is older than the OS that your model of Mac shipped with.
- CCC will issue a warning if the destination volume is larger than 2TB and the device is connected to your Mac via USB.

CCC does not maintain an exhaustive list of hardware:shipping OS pairs. CCC also cannot determine whether the destination will be bootable when the source or destination are remote Macintosh volumes.

Related documentation:

- [What makes a volume bootable? <http://bombich.com/kb/cccl/what-makes-volume-bootable>](http://bombich.com/kb/cccl/what-makes-volume-bootable)
- [Don't install older versions of macOS <http://bombich.com/kb/cccl/i-want-clone-my-entire-hard-drive-new-hard-drive-or-new-machine#dont_install_older_os_versions>](http://bombich.com/kb/cccl/i-want-clone-my-entire-hard-drive-new-hard-drive-or-new-machine#dont_install_older_os_versions)

Configuration concerns that affect the preservation of filesystem metadata

CCC will note a concern if there is a compatibility mismatch between the source and destination filesystems. For example, if you are backing up files from an HFS+ volume to a network filesystem, some of the filesystem metadata cannot be preserved. In many cases this is acceptable and you can ignore the message. Each of the possible concerns that CCC might raise are listed below. The "risk" associated with not preserving each type of metadata is explained plainly, so you can decide



whether the destination volume will suit your needs.

The destination doesn't support Access Control Lists

[Access Control Lists](https://en.wikipedia.org/wiki/Access_control_list) <https://en.wikipedia.org/wiki/Access_control_list> specify a granular list of the privileges that users and groups have for a particular file or folder (e.g., read, write, get information, delete, etc.). These advanced privilege settings generally apply only to user accounts that have been created on your Macintosh — for example, to prevent other users from deleting items from your home directory. If you are backing up your own files to a locally-attached hard drive, or to a network file share on a trusted computer, the Access Control List filesystem metadata is relatively unimportant. If you are backing up to or from a network filesystem in a business or education setting, however, check with your tech support staff for additional advice on whether this metadata must be preserved.

The destination doesn't support hard links

A [hard link](https://en.wikipedia.org/wiki/Hard_links) <https://en.wikipedia.org/wiki/Hard_links> makes a single file appear to be located in multiple places on your hard drive. If a single file had 20 hard links scattered across the disk, each hard link file would consume no additional space on the hard drive, and editing the content of any one of those files would immediately affect the content of every other hard link to that file.

When you back up the contents of a volume that contains hard links, ideally you want to preserve the hard links. If the destination filesystem doesn't support hard links, each hard linked file will be disassociated from the original file and will become a copy on the destination. This won't result in any loss of data, but your backup set will consume more space on the destination than on the source. Hard links are leveraged quite a bit on macOS by the operating system, though they are generally less common among user data.

The destination doesn't support ownership

File ownership indicates which user account on your Mac has control of a file. The owner of a file can limit access to that file from other users on the same computer. If the destination doesn't support ownership, then the owner of each file copied to the destination will be set to the user that mounted the destination. If the destination volume is accessed elsewhere (e.g. mounted on another Mac or even by a different user on the same Mac), then any restrictions that you have placed on those files may not be honored. If you are backing up files and folders that are not all owned by the same user (e.g. you), you should consider backing up to a local, HFS+ formatted volume or to a disk image instead.

Some filesystems have file size limitations

Some filesystems have restrictions on how large a file can be. FAT32, for example, limits files to 4GB or less. CCC will proactively warn you of this limitation if you choose to back up a volume whose filesystem supports files larger than 4GB to a filesystem that does not support files larger than 4GB. CCC will then automatically exclude files larger than 4GB from the backup task. Files that were excluded will be reported at the end of the backup task.

If you require that files larger than 4GB are backed up, you must reformat the destination volume with a format that supports larger files.

Related documentation:

- [Preparing your backup disk for a backup of macOS](http://bombich.com/kb/ccc4/preparing-your-backup-disk-backup-os-x) <<http://bombich.com/kb/ccc4/preparing-your-backup-disk-backup-os-x>>

The destination already has an installation of macOS. Merging a different version of macOS into this destination may cause problems with that installation of macOS

This message appears if you choose the "Don't delete anything" SafetyNet setting. While that setting will protect any data that you have on the destination volume that is unique to that volume, it does a disservice to the installation of macOS on your destination. This message will also appear if you use the "Don't update newer files on the destination" advanced troubleshooting setting.

Suppose, for example, that you have a complete backup of Mac OS 10.9.3 on your backup volume. When you apply the 10.9.4 update to your source volume, many system files are updated, some new files are added, and some files may be deleted. If you use CCC to update your backup volume, but you don't allow CCC to delete the items on the destination that the OS update had deleted from the source, then there will be a bunch of "cruft" left over on the backup volume. If you should ever need to boot your Mac from your backup volume, these cruft files could cause the OS to behave unexpectedly, and they may prevent it from booting altogether.

CCC can help you perform a clean upgrade or downgrade of macOS on the destination volume by moving items that should be deleted to the SafetyNet folder. Any files and folders that you keep only on the destination would also be moved to the SafetyNet folder. See the [Protecting data that is already on your destination volume <http://bombich.com/kb/ccc4/protecting-data-already-on-your-destination-volume-carbon-copy-cloner-safetynet>](http://bombich.com/kb/ccc4/protecting-data-already-on-your-destination-volume-carbon-copy-cloner-safetynet) section of the documentation for more details on these settings.

CCC warns that Macs cannot boot from USB devices larger than 2TB

In the past we received several reports of bootability problems related to USB devices larger than 2TB. At that time, we performed a simple litmus test: create an "x"TB partition at the beginning of the disk (varying x from 0.5 to 2.5TB) and a second partition consuming the remainder of the disk, then install macOS onto both partitions. The results of those tests suggested that some Macs couldn't "see" the partition that lied past the 2TB mark on the disk. This limitation was specific to USB devices — none of these problems occurred if you were to place the same disk into a Thunderbolt enclosure.

At the time of those initial reports and testing, the results were consistent. We concluded that there was likely a 32-bit addressing limitation imposed by the USB drivers that are embedded in the Macs' firmware ("likely" — unfortunately none of this information is documented by Apple). More recently, however, we've been unable to consistently reproduce the same results. Apple may have addressed the problem with a firmware update. It's also possible that our initial conclusion was wrong, e.g. that the problem was due to a partition alignment error; an error specific to macOS El Capitan and apparently only USB devices (you'd see "disk2s2: alignment error" messages in the system log when the affected volume is mounted).

In any case, CCC's warning was issued out of an abundance of caution. Our current recommendation is to [partition the destination device using the same procedure as defined for all other destination devices <http://bombich.com/kb/ccc4/preparing-your-backup-disk-backup-os-x>](http://bombich.com/kb/ccc4/preparing-your-backup-disk-backup-os-x), and do the partitioning while booted from any other OS than El Capitan. In other words, don't create a 2TB partition at the beginning of the disk. Once you have completed your first backup, though, we encourage you to [verify that your Mac will boot from the backup volume <http://bombich.com/kb/ccc4/how-verify-or-test-your-backup>](http://bombich.com/kb/ccc4/how-verify-or-test-your-backup). If your Mac is unable to boot from the backup volume, [please reach out to us <http://bombich.com/hc/requests/new>](http://bombich.com/hc/requests/new) so we can investigate your specific configuration further.

Help! My clone won't boot!

See [this section of CCC's documentation <http://bombich.com/kb/cccl/help-my-clone-wont-boot>](http://bombich.com/kb/cccl/help-my-clone-wont-boot) for troubleshooting advice if you're having trouble getting your backup volume to start your Mac.

Configuring Scheduled Task 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.

SCHEDULING BASIS

Daily

Repeat every: 1 day

Start at: 6/20/ 2017, 5:00 PM

Next run time: Today at 5:00:00 PM EDT

RUNTIME CONDITIONS

Defer if another task is writing to the same destination

Limit which days of the week this task can run

Skip if the current day is a week day

Skip if the current day is a weekend day

Limit when this task can run

7:00 PM to 7:00 PM

SYSTEM SLEEP

If the system is off or sleeping when this task is scheduled to run:

Wake the system

IF THE SOURCE OR DESTINATION IS MISSING

Don't send error notifications

Run this task as soon as the missing volume reappears

Done

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 wake your computer when your tasks are scheduled to run. You can change this setting in the **Runtime Conditions** section of the Scheduler popover. There are four options:

Wake the system

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.

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.

Run this task 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.

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.

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 <http://bombich.com/kb/cc5/frequently-asked-questions-about-scheduled-tasks>](http://bombich.com/kb/cc5/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 you 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.

Creating a separate task to prevent VM container versions from bloating the SafetyNet

If you frequently use virtual machine container files (e.g. with Parallels, VMWare, VirtualBox, etc.), you may find that CCC's SafetyNet folder tends to get very large, very quickly. Every time you open your virtual machine, the monolithic virtual machine container file is modified, and CCC will require that it gets backed up during the next backup task. If the SafetyNet is on, CCC will move the older version of the VM container file into the SafetyNet folder. If you run your backup tasks on a daily basis and use your virtual memory container file every day, these large VM container files will quickly consume all of the free space on your backup volume.

You can avoid archiving the older versions of these virtual machine container files by creating a separate backup task for the parent folder of the virtual machine container files. Here's how to set things up:

1. Create a new task and name it something like **Everything except Parallels**
2. Choose your startup disk from CCC's Source selector
3. Choose **Some files...** from the Clone popup menu (underneath the Source selector)
4. In the file list in the Task Filter window, navigate to the location where your Parallels VM is saved (e.g. Users > yourname > Documents > Parallels) and uncheck the box next to the folder that contains your virtual machine container. You could exclude the container file itself, but choosing the parent folder gives you more flexibility in renaming the VM container, should you want to (e.g. Windows XP > Windows 7).
5. Choose your backup volume from the Destination selector
6. SafetyNet should be **ON**
7. Configure the task to run Daily and **Save** the changes
8. Create a new task and name it something like **Parallels Backup**
9. Choose **Choose a folder...** from the Source selector and select your Parallels folder as the source (e.g. the same folder that you excluded previously). By selecting this folder directly, you're explicitly limiting this task's scope to this folder.
10. Choose **Choose a folder...** from the Destination selector and select the Parallels folder on your backup volume as the destination
11. Turn SafetyNet **OFF** for this task
12. Schedule this task, then save the changes

Additionally, you can configure the first task to run that second task as a postflight action in **Advanced Settings**.

Outgoing network connections made by CCC

If you're using an application firewall such as [Little Snitch <https://www.obdev.at>](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 you submit a ticket to our help desk (mew.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

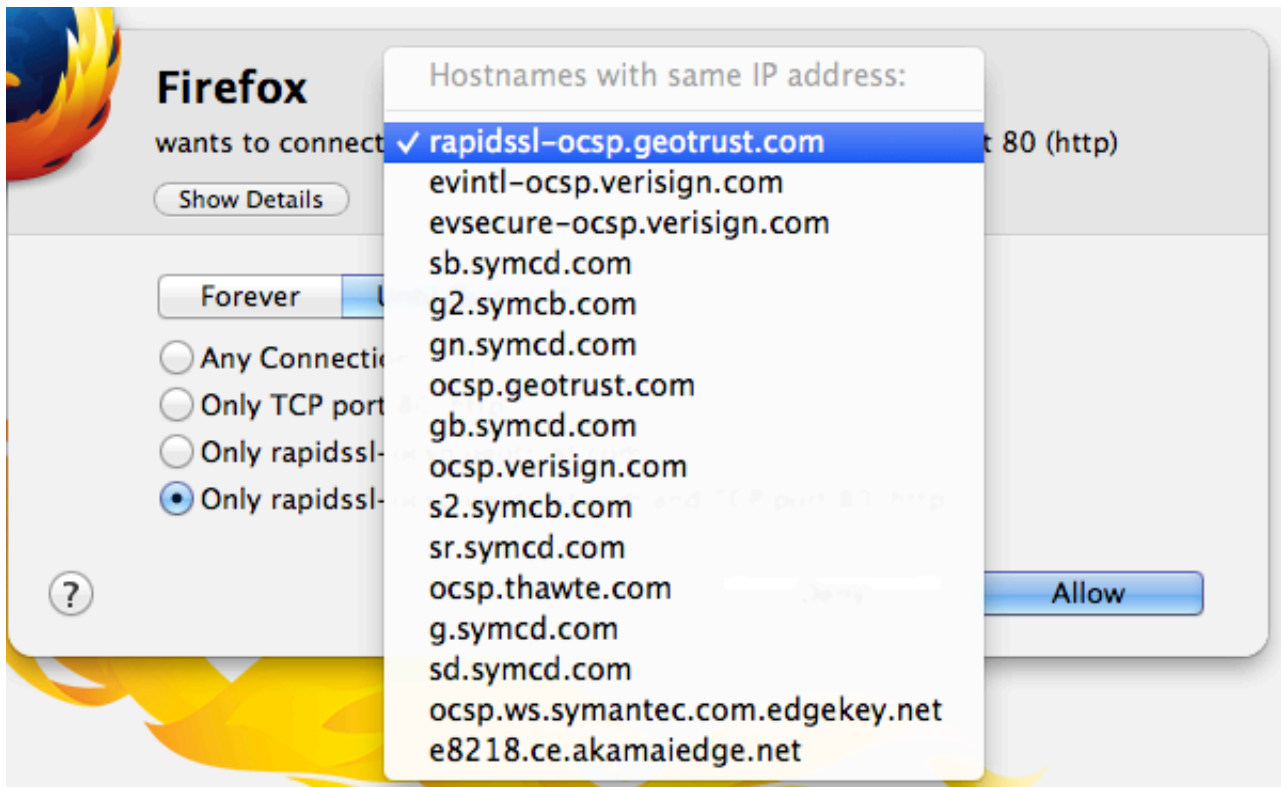
† These activities are enabled only upon your assent when you first launch CCC, and can be suppressed any time later via the Software Update section of CCC's Preferences window. No personal data, nor personally-identifiable data is **ever** sent to these services.

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>](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 yting.com are all domains associated with Google's servers. We aren't actually connecting to all 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). This forum post at the ObDev website describes a similar report of the same problem (unrelated to CCC): [Little Snitch showing wrong host name for IP](#) <<https://forums.obdev.at/viewtopic.php?f=1&t=8859>>.

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?

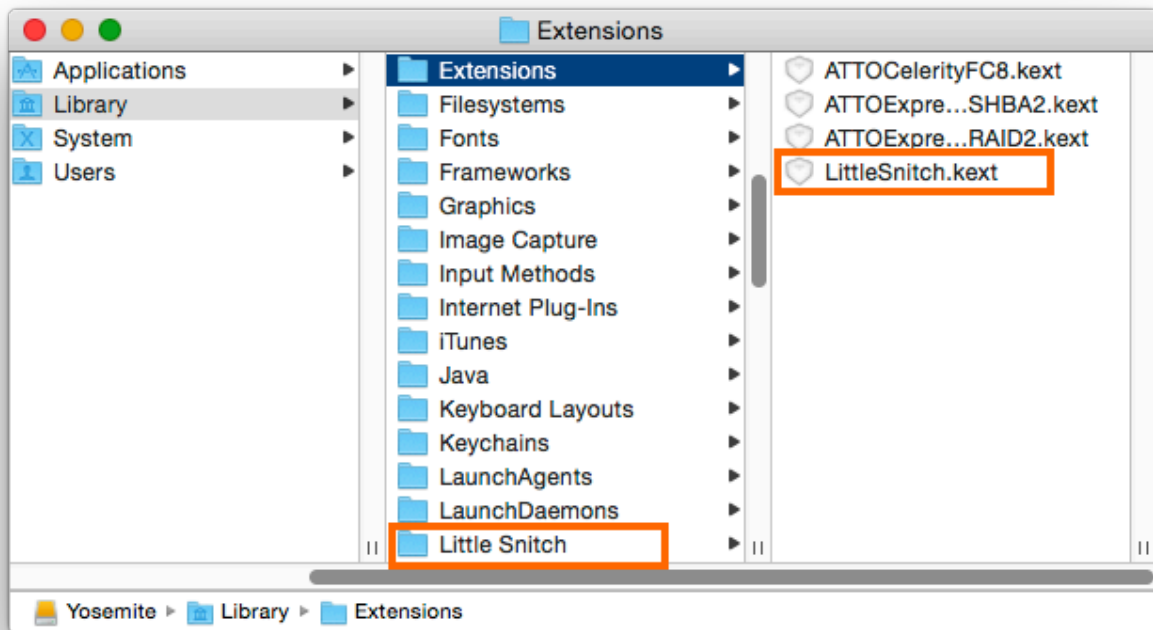
According to ObDev developers, it is crucial for Little Snitch to avoid unnoticed ruleset changes. Little Snitch therefore has numerous mechanisms to detect whether it is using the **exact** same ruleset file, as in, on the same volume and at the same physical address on that disk. This sort of mechanism 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](http://bombich.com/kb/ccc5/excluding-files-and-folders-from-backup-task) <<http://bombich.com/kb/ccc5/excluding-files-and-folders-from-backup-task>>.



CCC does not delete files from the destination that are excluded from the backup task <http://bombich.com/kb/ccc5/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.

Limitations of online-only placeholder files

Some cloud storage service providers offer services that allow you to sync a local folder to "the cloud", and optionally choose to store those 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's "Drive 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 you choose to have these services store your files only online, do so with the understanding that it's not possible to maintain a local backup of those files.

Online-only files can't be backed up

When you specify that a file stored by one of these storage services should reside only online, the local copy of your file is deleted from your Mac and replaced with a 0-byte placeholder file. If you attempt to open the placeholder file, the agent software for your storage service provider automatically downloads the data of the file to your Mac and the document opens. While this is a convenient feature that allows you to free up some space on your Mac, this feature removes files from your local storage, which means that CCC can't make a backup of these online-only files. Before using these online-only features, you should consider whether you are comfortable with not having a local backup of the files that you choose to store only in the cloud.

Placeholder files may be backed up, but may not function as placeholder files on the backup disk

As noted above, when you open a placeholder file in the Finder, the agent software downloads the original. Likewise, if you attempt to copy a placeholder file via the Finder from one volume to another, the agent software downloads the data to the source, then copies the original file (leaving the downloaded source file in place). **CCC backups do not behave like Finder copies.** And for good reason - if you have 1TB of online-only files on your 500GB SSD, you wouldn't want Dropbox or iCloud to download all of that data when CCC attempts to make a backup! Rather, CCC copies the placeholder files as they are, retaining all of the placeholder attributes of the source files. CCC makes a non-proprietary backup of your files; our goal is to make the destination files look exactly like the source files.

Some placeholder files won't function as placeholder files on the destination. OneDrive, for example, won't see a placeholder file that is outside of your OneDrive folder (i.e. on your startup disk) as a "true" placeholder file, and will not engage to download the file's data when you attempt to open it. CCC makes a best-effort attempt to not copy OneDrive placeholder files at all. Microsoft's OneDrive client software actively prevents applications from accessing those files — OneDrive placeholders

are impossible to back up.

Dropbox's placeholder files function correctly when you back them up from an APFS volume to another APFS volume, and when you back them up from an HFS+ volume to another HFS+ volume. Because Dropbox uses a **different** proprietary technique for creating the placeholder file on each volume format, though, these placeholder files won't behave correctly when transferred from one filesystem format to another.

Google Drive File Stream uses yet another proprietary device for its placeholder files. These placeholder files (which include all Google document formats) can't be opened by any application other than Google Drive, so CCC does not attempt to back them up.

OneDrive may delete online-only files from the cloud when you restore a OneDrive folder from a backup

Because Microsoft's OneDrive syncing software prevents applications from accessing the contents of OneDrive online-only placeholder files, those placeholder files cannot be present on a backup. If you restore a OneDrive folder from a backup, the OneDrive service should be smart enough to not **delete** files from the cloud simply because the placeholders are now absent. For comparison, Dropbox and iCloud won't delete files whose placeholders are absent, rather those services will only delete a file from the cloud when an actual file removal event occurs. In our own testing, OneDrive does not delete online-only files from the cloud when restoring from a backup. People have [reported this concern](https://answers.microsoft.com/en-us/msoffice/forum/msoffice_onedrivefb-mso_win10-mso_o365b/when-is-microsoft-going-to-fix-onedrive-when-a/45f8e646-7421-4249-9272-03e8f255c28f) <https://answers.microsoft.com/en-us/msoffice/forum/msoffice_onedrivefb-mso_win10-mso_o365b/when-is-microsoft-going-to-fix-onedrive-when-a/45f8e646-7421-4249-9272-03e8f255c28f> on Microsoft's forums <<https://techcommunity.microsoft.com/t5/OneDrive-for-Business/Is-OneDrive-Deleting-Newer-Files-After-Backup-Restore/m-p/228811>>, and two CCC users have reported the same concern to us. If you restore from a backup and encounter this problem, you can restore the deleted files using [these instructions from Microsoft](https://support.office.com/en-us/article/restore-deleted-files-or-folders-in-onedrive-949ada80-0026-4db3-a953-c99083e6a84f) <<https://support.office.com/en-us/article/restore-deleted-files-or-folders-in-onedrive-949ada80-0026-4db3-a953-c99083e6a84f>>.

If you're reading this because you encountered an error in your backup task indicating that CCC dropped a OneDrive placeholder file, take a moment to consider whether you should continue to include your OneDrive folder in your backups. On one hand, having a local backup of the OneDrive files that actually reside on your Mac is really nice to have. On the other hand, if you don't recall that placeholder files will be missing from your backup, then you may have some hassle in the future if/when you restore from that backup.

Related Documentation

- [Excluding files and folders from a backup task](http://bombich.com/kb/ccc5/excluding-files-and-folders-from-backup-task) <<http://bombich.com/kb/ccc5/excluding-files-and-folders-from-backup-task>>

What is CCC's Privileged Helper Tool?

At its core, Carbon Copy Cloner is a product that is designed to make bootable backups of your Mac's operating system. In order for CCC to be able to make copies of system files, CCC needs to have the privilege of copying files that can't be read nor written by just any user – **CCC requires elevated privileges to copy macOS system files**. 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>](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>](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>](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>](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 <http://bombich.com/kb/ccc5/modifying-cccs-security-configuration>](http://bombich.com/kb/ccc5/modifying-cccs-security-configuration)
- [Uninstalling CCC <http://bombich.com/kb/ccc5/uninstalling-ccc>](http://bombich.com/kb/ccc5/uninstalling-ccc)
- [Granting Full Disk Access to CCC and its helper tool <http://bombich.com/kb/ccc5/granting-full-disk-access-ccc-and-its-helper-tool>](http://bombich.com/kb/ccc5/granting-full-disk-access-ccc-and-its-helper-tool)
- [System problems can lead to a failure to install CCC's helper tool <http://bombich.com/kb/ccc5/carbon-copy-cloners-privileged-helper-tool>](http://bombich.com/kb/ccc5/carbon-copy-cloners-privileged-helper-tool)

Downgrading an APFS-formatted Fusion volume from Mojave

If you upgraded your Mac to macOS Mojave and have decided to downgrade for one reason or another, the procedure is [usually pretty straightforward](#). Fusion volumes, however, introduce a complication. Upon upgrading to Mojave, a Fusion volume will be converted from HFS+ to APFS. If you want to downgrade to High Sierra (or any earlier OS), you must reformat that Fusion volume as HFS+. Because APFS Fusion volumes are not handled gracefully by High Sierra, however, the procedure is a bit tedious. The following steps will help you downgrade your Mojave Fusion volume to High Sierra.

Warning: These instructions will permanently delete the contents of the two devices that belong to your Mac's internal Fusion device. If you're uncomfortable with any of the steps in this process, please don't hesitate to [ask us for help <http://bombich.com/software/get_help>](http://bombich.com/software/get_help).

1. Boot from your CCC bootable backup that you intend to restore from (e.g. macOS High Sierra or earlier).
2. Choose "About this Mac" from the Apple menu to verify that your Mac is booted from your backup volume.
3. Open Disk Utility.
4. Choose "Show all devices" from the View menu.
5. Identify the two devices that belong to the APFS Fusion volume. Typically one will be an SSD and the other will be an HDD, and both should be in the "Internal Devices" section of Disk Utility's sidebar.
6. Erase the SSD Fusion member as "Mac OS Extended, Journaled". Name it "FusionSSD" so it's easy to identify later.
7. Erase the HDD Fusion member as "Mac OS Extended, Journaled". Name it "FusionHDD" so it's easy to identify later.
8. Quit out of Disk Utility.
9. Open Carbon Copy Cloner.
10. Click on the "FusionHDD" disk in CCC's sidebar.
11. Click the "Recovery HD..." button at the bottom of the window.
12. Click the "Create Recovery HD" button. If that button is disabled, don't worry – this step isn't essential.
13. Quit out of CCC
14. Open the Terminal application, type the following command, then press the Return key:
`diskutil list`
15. In the list of devices and volumes, find and make a note of the device identifier (in the IDENTIFIER column) associated with FusionSSD and FusionHDD. For FusionSSD, we will use the whole device identifier, e.g. disk1, whereas for the FusionHDD, we will use the volume device identifier, e.g. disk5s2.
16. Type the following command in the Terminal, substituting the device identifiers noted in the previous step, then press the Return key:
`diskutil cs create "Macintosh HD" SSD_Whole_Device_Identifier HDD_volume_identifier`
17. The previous command will create an empty Fusion device, and print out a "Logical Volume Group" identifier. Select that identifier and copy it to the clipboard.
18. Type the following command in the Terminal, substituting the logical volume group identifier



noted in the previous step, then press the Return key:

```
diskutil cs createVolume Logical_Volume_Group JHFS+ "Macintosh HD" 100%
```

19. Quit out of the Terminal application.
20. Open Carbon Copy Cloner.
21. Create and run a new task, specifying your backup disk as the source and the new "Macintosh HD" Fusion volume as the destination.
22. When the restore task is complete, open the Startup Disk Preference Pane in the System Preferences application. Reset the startup disk to Macintosh HD, then reboot.

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 Carbon Copy Cloner and APFS](#) <<http://bombich.com/kb/ccc5/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) <<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](#).

C

Checksumming or "Find and replace corrupted items" — With this option, CCC will calculate an MD5 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 — A copy of a folder or volume; a non-proprietary backup. While not identical (some caches should not be copied as they must be rebuilt on a bootable backup, and files like trash are excluded), clone is a common word used for a CCC bootable backup.

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](#) <<http://bombich.com/kb/ccc5/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 clone of 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 <http://bombich.com/kb/ccc5/backing-up-disk-image>](http://bombich.com/kb/ccc5/backing-up-disk-image)

- **Sparse bundle disk** images appear as a single file but are actually folders with many files inside. This is more efficient, as only the changed parts need to be copied when updated.
- **Sparse disk images** are stored as a single monolithic file. This can make backups less efficient as the entire file must be copied each time.

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 <http://bombich.com/kb/ccc5/advanced-settings#ignore_xattrs>](http://bombich.com/kb/ccc5/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>](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 <http://bombich.com/kb/cc5/preparing-your-backup-disk-backup-os-x>](#)

Prune — Remove older, archived material that was cached on the destination volume. [Automated maintenance of the CCC SafetyNet folder <http://bombich.com/kb/cc5/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 <http://bombich.com/kb/ccc5/performing-actions-before-and-after-backup-task#scheduler_shell_scripts>](http://bombich.com/kb/ccc5/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>](https://en.wikipedia.org/wiki/RAID) for more details.

Recovery HD — A hidden, Apple-proprietary volume associated with a macOS startup volume. The Recovery HD offers a method to reinstall macOS, and also must be present prior to enabling FileVault encryption on the associated startup volume. The presence of a Recovery HD volume is not required for maintaining a bootable backup of your startup disk, nor for recovering from a bootable backup. [Cloning Apple's Recovery HD partition <http://bombich.com/kb/ccc5/cloning-apples-recovery-hd-partition>](http://bombich.com/kb/ccc5/cloning-apples-recovery-hd-partition)

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 Carbon Copy Cloner SafetyNet <http://bombich.com/kb/ccc5/protecting-data-already-on-your-destination-volume-carbon-copy-cloner-safetynet>](http://bombich.com/kb/ccc5/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 <http://bombich.com/kb/ccc5/performing-actions-before-and-after-backup-task#scheduler_shell_scripts>](http://bombich.com/kb/ccc5/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, Clone button. [Simple Mode](http://bombich.com/kb/ccc5/simple-mode) <<http://bombich.com/kb/ccc5/simple-mode>>

Snapshot — A snapshot is a recording of the state of a system at a particular point in time, an analogy to a photograph. You can restore your system to a prior point in time using a snapshot.

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) <<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-gb/HT201255) <<https://support.apple.com/en-gb/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 \(task chaining\)](http://bombich.com/kb/ccc5/performing-actions-before-and-after-backup-task#chain_tasks) <http://bombich.com/kb/ccc5/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](http://bombich.com/kb/cc5/my-disk-already-formatted-hfs-why-am-i-getting-warning). <<http://bombich.com/kb/cc5/my-disk-already-formatted-hfs-why-am-i-getting-warning>>

The disk usage on the destination doesn't match the source. Did CCC miss some files?

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](http://bombich.com/kb/ccc5/some-files-and-folders-are-automatically-excluded-from-a-backup-task) <<http://bombich.com/kb/ccc5/some-files-and-folders-are-automatically-excluded-from-a-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? <<http://bombich.com/kb/ccc5/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?

For an APFS volume, you may never be able to get accurate disk usage values that can be meaningfully compared on the source and destination. You should, however, always be able to find your files at the same location on the source and destination – you should never find an item to be missing from the destination (unless you excluded it from the backup, of course). [This video <https://www.youtube.com/watch?v=n_7JgLKy_W0>](https://www.youtube.com/watch?v=n_7JgLKy_W0) will help you compare the files on the source and destination so you can verify that you're able to find your files on your backup.

For HFS+ formatted source and destination volumes, a basic enumeration of the files and folders on those volumes will give you meaningful numbers to compare. The [Volume Disk Usage Details <http://bombich.com/software/files/tools/Volume_Disk_Usage_Details.zip>](http://bombich.com/software/files/tools/Volume_Disk_Usage_Details.zip) tool can help you collect this kind of enumeration. When this tool has completed scanning the source and destination volumes, you can compare the reports to find any discrepancies. You can use this tool to enumerate individual folders as well if you need to get more granular details about a discrepancy in a particular folder.

If you find a discrepancy that you cannot explain, or that appears to be errant, [please let us know <http://bombich.com/software/get_help>](http://bombich.com/software/get_help) and we'll help you get to the bottom of it.

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. Carbon Copy Cloner can solve this problem! We lay out a few different scenarios and solutions below.

"I want a bootable backup for each Mac on the same hard drive" (macOS High Sierra and later, APFS-formatted backup disk)

Each APFS volume that you add to your backup disk can hold a bootable backup of macOS High Sierra and later, or any other data that you would like to keep separate from other content on the backup disk.

It's really easy to create separate volumes in an APFS-formatted container. When you're backing up multiple volumes to the same 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

"I want to back up my startup disk and a data volume to the same backup disk" (macOS High Sierra and later, APFS-formatted backup disk)

Same as above — create a dedicated volume on your backup disk for each source that you're backing up:

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/n_arMTq3d58>](https://youtu.be/n_arMTq3d58)

"I want a bootable backup for each Mac on the same hard drive" (Sierra or older, HFS+ formatted backup disk)

Creating a bootable backup requires that you provide a dedicated backup volume for each Mac that you want to back up. If you want to maintain each bootable backup on the same hard drive, you simply create a partition for each computer that you want to back up using Disk Utility:

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. Configure each of your CCC backup tasks to back up to its own dedicated volume on the destination

Related Documentation

- [Learn more about partitioning a hard drive for use with Carbon Copy Cloner <http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x>](http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x)
- [Partitioning a new hard drive \[10.11 and 10.12\] <https://www.youtube.com/watch?v=3AUXkwaVVFQ>](https://www.youtube.com/watch?v=3AUXkwaVVFQ)
- [Partitioning a new hard drive \[10.10\] <https://www.youtube.com/watch?v=WZ1sstRdWjk>](https://www.youtube.com/watch?v=WZ1sstRdWjk)

"I want to back up my startup disk and a data volume to the same backup disk" (Sierra or older, HFS+ formatted backup disk)

Two CCC backup tasks will manage these backups. The first task will back up your startup disk directly to the backup volume for a bootable backup, the second task will back up your data volume to a subfolder on the backup volume. Thanks to CCC's SafetyNet [<http://bombich.com/kb/ccc5/protecting-data-already-on-your-destination-volume-carbon-copy-cloner-safetynet>](http://bombich.com/kb/ccc5/protecting-data-already-on-your-destination-volume-carbon-copy-cloner-safetynet) feature, the two backup tasks will coexist peacefully.

1. Configure a CCC task to back up your startup disk to the backup volume. Choose your startup disk from the Source selector and choose the backup volume from the Destination selector.
2. Verify that the SafetyNet feature is **On**. [Note: If you have modified any Advanced Settings, be sure that the **Protect root-level items** [<http://bombich.com/kb/ccc5/advanced-settings#protect>](http://bombich.com/kb/ccc5/advanced-settings#protect) option is checked.]
3. Schedule the task, if desired, or choose "Save" from Carbon Copy Cloner's File menu. You can run this task immediately or let it run on schedule later.
4. Click the **New Task** button in CCC's toolbar.
5. Choose your data volume from CCC's Source selector.
6. In the Finder, create a new folder at the root level of the destination volume to store your data volume's backup. Finder may prompt you to authenticate if you ran the first task already, and that's OK.
7. Drag the new folder from the Finder onto CCC's Destination selector.
8. Schedule the task, if desired, or choose **Save** from Carbon Copy Cloner's File menu. Again, you can run this task immediately or let it run on schedule later.

CCC's SafetyNet will prevent the first task from erasing the content that you're backing up to a subfolder on that same destination volume.



"I want to back up multiple data volumes (no OS files) to the same backup disk"

The easiest way to back up multiple data-only volumes to the same backup disk is to create a folder on the backup disk for each volume 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. Choose **Choose a folder...** from the Destination selector
4. Select your destination volume in the sidebar
5. Click the **New Folder** button to create a new folder at the root level of the destination to store your data volume's backup, then select that folder as the destination.
6. Schedule the task, if desired, or choose **Save** from Carbon Copy Cloner's File menu. You can run this task immediately or let it run on schedule later.
7. 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](http://bombich.com/kb/ccc5/backing-up-large-files-mounted-disk-images-and-virtual-machine-containers) <<http://bombich.com/kb/ccc5/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](http://bombich.com/kb/ccc5/backing-up-large-files-mounted-disk-images-and-virtual-machine-containers) <<http://bombich.com/kb/ccc5/backing-up-large-files-mounted-disk-images-and-virtual-machine-containers>>
- [Leveraging Snapshots on APFS Volumes](http://bombich.com/kb/ccc5/leveraging-snapshots-on-apfs-volumes) <<http://bombich.com/kb/ccc5/leveraging-snapshots-on-apfs-volumes>>

Some applications behave differently or ask for the serial number on the cloned volume. Did CCC miss something?

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' installation disks 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 when booting from your cloned volume. 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/cloning 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).
- A dialog may appear asking you to locate the "System Events" application (this one appears to be a one-time deal, dismiss the dialog and you shouldn't see it again). If you have many apps that load on login, you can avoid many of these verification dialogs by holding down the Shift key when you log in.
- **Time Machine** may no longer recognize your original source volume because the UUID has changed ([potential solution <http://oldtoad.net/pondini.org/TM/B6.html>](http://oldtoad.net/pondini.org/TM/B6.html))
- **Google Drive** must be disconnected, then reconnected to your account. [Details here <http://bombich.com/kb/discussions/google-drive-reports-google-drive-folder-missing>](http://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 [[Potential solution <https://forums.adobe.com/thread/370733?tstart=0>](https://forums.adobe.com/thread/370733?tstart=0)]
- Finder may not resolve aliases to files on a backup volume if those aliases were created on Snow Leopard or later. Finder will give you the opportunity to "readdress" these aliases when

you try to open them.

- Network settings may not be respected on 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. The Local Items Keychain is only respected on the original volume on which it was created, it cannot be restored from any backup (even Time Machine). If you enable iCloud Keychain syncing (before you find yourself in a need-to-restore position), however, the passwords in this keychain will be stored in iCloud and shared with a restored volume once you log in to iCloud on that restored volume.
- **Little Snitch** settings, or a subset of them, may not be recognized while booted from a backup volume. [The folks at Objective Development recommend <https://forums.obdev.at/viewtopic.php?f=1&t=4874>](https://forums.obdev.at/viewtopic.php?f=1&t=4874) that you export your rules first, then re-import them while booted from the backup volume.
- If you open an **Adobe Lightroom** catalog from a cloned or 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>](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 cloned volume, or [watch this video on our YouTube channel <https://youtu.be/vZE_dY_aVbeo>](https://youtu.be/vZE_dY_aVbeo) to see a demonstration of the problem and solution.
- **TeamViewer** Product Support recommends that TeamViewer be reinstalled when restoring a backup to a different Macintosh.
- If configured to start on login, when booted from a backup, the Box Sync application will delete the contents of your Box Sync folder, then re-download all of the content from Box.com. 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 booting another Macintosh from the backup volume, they're only recognized on the Mac upon which they were created.
- **Apple Pay** may function incorrectly when booting another Mac from your backup. [[Apple Kbase: If Apple Pay on your Mac is disabled because security settings were modified <https://support.apple.com/en-us/HT209016>](https://support.apple.com/en-us/HT209016), [Another potential solution <https://blog.yimin.gliu.com/2017/06/15/resolving-endless-apple-pay-add-card-loop-after-time-machine-restore/>](https://blog.yimin.gliu.com/2017/06/15/resolving-endless-apple-pay-add-card-loop-after-time-machine-restore/>)]

References to third-party solutions/workarounds are provided as information only. We have not tested these solutions and we cannot endorse them.

Can I back up one computer and use the clone to restore another computer?

Often, the answer is **probably yes**. However, there are some caveats.

Don't install older versions of macOS than what your computer shipped with

When you get a brand new Mac from Apple, it has a specific version of macOS installed on it, and further, a **build** that is specific to that exact model of Mac. If you install an older version or build of the OS, for example by cloning your older Mac to it, then it may behave unexpectedly, or it may not boot at all. **If your new Mac is brand new, use Migration Assistant to migrate your data to your new Mac.**

If your **new** Mac is just different, but not really hot off the production lines, then cloning another Mac to the new Mac may work fine. When cloning your source Mac to your new Mac, be sure that your source Mac has been updated to at least one later release than what came on the newer Mac. For example, if your newer Mac came with 10.12.4, update your source Mac to 10.12.5 before migrating. If such an update is not available, use the [Migration Assistant <https://support.apple.com/kb/HT204350>](https://support.apple.com/kb/HT204350) instead.

T2 and Apple Silicon Macs have "personalized" operating systems

When macOS is installed onto a T2 or Apple Silicon Mac, the macOS Installer signs some of the startup resources with a code signature that is unique to your Mac. If you attempt to boot your Mac from the backup of some other Mac, your Mac will refuse to boot from that volume, claiming:

A software update is required to use this startup disk. You can update now or select another startup disk.

The "update" involves downloading system resources and then personalizing the backup volume's OS to the current Mac. This requires an Internet connection. Typically the application of that update works and the backup volume is then bootable, but various factors can cause that to fail. After [confirming that the version of the operating system is compatible with the Mac you're trying to boot <https://support.apple.com/en-us/HT201686>](https://support.apple.com/en-us/HT201686), there are two options to make this work:

T2 Mac

- Hold down Command+R to boot the Mac into [Recovery Mode <https://support.apple.com/en-us/HT201314>](https://support.apple.com/en-us/HT201314) and [change the Secure Boot setting to Medium Security <https://support.apple.com/en-us/HT208330>](https://support.apple.com/en-us/HT208330), then proceed to attempt to boot from the backup volume or
- Hold down the T key on startup to boot the Mac into [Target Disk Mode <https://support.apple.com/en-us/HT201255>](https://support.apple.com/en-us/HT201255), attach the Mac and the backup disk to another Mac, then restore the backup directly to the TDM Mac's internal storage. CCC will ask

macOS to personalize the destination Mac. This procedure requires macOS Catalina or later and an Internet connection.

Apple Silicon Mac

Hold down the Power button on startup, select "Options", then press the Continue button. Then:

- Choose "Startup Security Utility" from the Utilities menu, then change the Security Policy to **Reduced Security**, then proceed to attempt to boot from the backup volume or
- Choose, "Share Disk..." from the Utilities menu, select a volume to share, then click the "Start Sharing" button. Attach the backup disk directly to another Mac, attach the Sharing Mac to the other Mac via USB or Thunderbolt, then restore the backup directly to the Sharing Mac's shared disk. CCC will ask macOS to personalize the destination Mac. This procedure requires macOS Catalina or later and an Internet connection.

Do not attempt to restore the backup of an Intel Mac to an M1 Mac. If you're attempting to migrate data from an older Mac to a newer Mac, you should use [Migration Assistant](https://support.apple.com/kb/HT204350) <<https://support.apple.com/kb/HT204350>>.

Some of your preferences on macOS are considered "host-specific"

Preferences such as these will be ignored if you boot another machine from your cloned operating system and data. For example, the screen saver preferences are host-specific — if you boot another machine from your bootable clone and the screen saver kicks in, you will notice that it has reverted to default settings. Do not fear that you have lost any data, your original preferences will be "restored" when you boot again from your original Mac. To learn exactly what preferences are host-specific, hold down the Option key and choose **Library** from the Finder's go menu, then navigate to Library > Preferences > ByHost.

Network settings may not be respected on another Macintosh

In addition to application-specific preference files, the network configuration of one Mac may not be accepted by another Mac. macOS network settings are stored in /Library/Preferences/System Configuration/preferences.plist, and CCC will copy that file unless you explicitly exclude it. Sometimes a Mac will respect the settings configuration file from another Mac, but often there are enough differences in the networking hardware configuration that macOS decides to ignore the contents of that file.

Some applications may behave differently when you open them on another Mac

This section of CCC's documentation <<http://bombich.com/kb/cc5/some-applications-behave-differently-or-ask-serial-number-on-cloned-volume.-did-ccc-miss>> highlights some of the affected applications that we're aware of.

The macOS Installer applies a firmware upgrade

Older Macs won't recognize APFS volumes as bootable devices until the macOS Installer has applied a firmware upgrade. If you're planning to clone High Sierra or later onto another Mac, you must have used the macOS Installer at least once on that system before you will be successful cloning the newer OS to that Mac.

So how can I find out if it will actually work?

Determining whether this type of clone will work for you is really easy — simply boot the destination Mac from your CCC backup of the source Mac:

1. Attach the CCC backup of the source Mac to the destination Mac with a Thunderbolt or USB cable.
2. On the destination Mac, open the Startup Disk preference pane in the System Preferences application and set the source Mac's backup volume as the startup disk, then click the Restart button.

If the destination Mac successfully booted from the source Mac's installation of macOS, then it works! Open CCC, then clone the source Mac's disk to the destination Mac's internal hard drive. If the destination Mac could not boot from the source Mac's installation of macOS, use the Migration Assistant to transfer your user data and applications instead.

Related documentation

- [Apple Kbase #HT201686: Don't install older versions of Mac OS than what comes with your computer <https://support.apple.com/kb/HT201686>](https://support.apple.com/kb/HT201686)
- [Apple Kbase #HT204319: macOS versions and builds included with Mac computers <https://support.apple.com/kb/HT204319>](https://support.apple.com/kb/HT204319)
- [Apple Kbase #HT208020: Upgrade macOS on a Mac at your institution <https://support.apple.com/kb/HT208020>](https://support.apple.com/kb/HT208020)

I have a clone created by another application. Will CCC recognize that data, or will it want to recopy everything?

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: Clone created by another cloning utility

If the software you used previously created a non-proprietary clone 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 cloned 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: My backup is in a folder on the destination. Why is CCC recopying everything?

The common use of CCC is to create a bootable clone of your startup disk. To do this, CCC copies all of the stuff from your source volume directly to the destination volume — not into a subfolder, but directly to the destination. At the end of the task, the destination looks exactly like the source. Typically you see **Applications**, **Library**, **System**, and **Users** on the source volume, so that's exactly what you should see on the destination volume.

If your previous backup was placed in a folder, however, then you must instruct CCC to place your backup into that same folder (assuming that's what you want — macOS will not work when placed in a folder on the destination). To do this, choose **Choose a folder** from the Destination selector to select the folder that your backup should be placed into.

Can CCC back up my BootCamp (Windows) partition?

CCC can back up the contents of the Boot Camp partition, but it cannot make a bootable clone of the partition. 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>](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. Choose **Some files...** from the popup menu underneath the Source selector
3. In the Task Filter panel, exclude **WINDOWS** and **Program Files**
4. Click the Done button
5. Click the Save button or choose **Save** from CCC's **File** menu

Will CCC clone 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. These three sections of the documentation address these matters:

[Can I run a backup while I'm using my computer? If I have open files, will they be backed up? <http://bombich.com/kb/ccc5/can-i-run-backup-while-im-using-my-computer-if-i-have-open-files-will-they-be-backed-up>](http://bombich.com/kb/ccc5/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?" <http://bombich.com/kb/ccc5/ccc-reported-destination-full.-what-can-i-do-avoid#destination_is_tight_on_space>](http://bombich.com/kb/ccc5/ccc-reported-destination-full.-what-can-i-do-avoid#destination_is_tight_on_space)

[Example pre and postflight shell scripts \(e.g. how to automatically suspend Parallels\)](http://bombich.com/kb/ccc5/performing-actions-before-and-after-backup-task#examples)

[<http://bombich.com/kb/ccc5/performing-actions-before-and-after-backup-task#examples>](http://bombich.com/kb/ccc5/performing-actions-before-and-after-backup-task#examples)



CCC reported that the destination is full. What can I do to avoid this?

By default, 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 you are not using CCC's default SafetyNet settings and you're running into a "destination is full" error, then you may need to apply a more liberal pruning limit in Advanced Settings. The amount of free space required on your destination depends on the size of files that you normally edit during the day. In general, you should have as much space available at the beginning of the backup task (e.g. right after pruning is complete) as you ordinarily see copied during a backup task. So if CCC ordinarily copies 9GB of data, maybe with a spike to 14GB every once in a while, you should configure your pruning settings to accommodate that maximum value (e.g. leave at least 15GB of free space). Especially if you modify large files on a regular basis, the nominal amount of data copied each time could be fairly high. If you use a Windows virtual container that is 80GB on a daily basis, for example, the nominal amount of data copied during your daily backup task will be at least 80GB, so you will have to accommodate that with your pruning settings.

To change CCC's SafetyNet pruning settings, select your task in CCC's main application window, then do the following:

1. Click the **Advanced Settings** button
2. In the **Before Copying Files** section, indicate how CCC should prune the SafetyNet folder, e.g. based on free space available on the destination, age of the archives, or size of the archives.
3. Specify a limit.
4. If you selected the free space option, consider checking the **Auto adjust** checkbox so CCC can manage this value for you automatically.
5. Save the changes to your task.

Why does CCC report that the destination is full when it appears to have enough room for newer files?

To prevent overwriting a good backup file with a corrupted file on the source, CCC uses a special file copying procedure called an **atomic** copy. If a file has changed since the last backup, it will be copied to the destination using a temporary filename, e.g. `.filename.XXXXXX`. When CCC has finished copying the file successfully, CCC deletes (or moves to the SafetyNet) the older version on the destination, then renames the updated file to the correct filename.

Because CCC uses this special procedure, the **destination volume must have, at minimum, enough free space to accommodate all of the data that will be backed up plus enough room to accommodate a temporary copy of the largest file on the source volume**. If you frequently modify very large files, such as movies, disk images, or virtual machine containers, you should designate a backup volume that has considerably more space than is consumed by your source volume to avoid running out of space during a backup task, and you should configure CCC's SafetyNet pruning settings to accommodate a temporary copy of the largest file on the source volume.

An example to illustrate the dilemma

Consider the following scenario:

- 500GB source volume
- 500GB destination volume
- 450GB of data on the source
- The largest file on the source is 75GB

If the destination is empty, the math is easy — 450GB of data easily fits on a 500GB disk.

Now let's go to a subsequent run of the backup task. Suppose no changes have occurred at all on the source, except to that 75GB file. How shall we proceed to copy that file to the destination? The destination has only 50GB of free space at this point.

Option A: Fast and loose

- Delete the 75GB file from the destination
- Copy the newer 75GB file from the source to the destination

Option B: Atomic copy

- Copy the newer 75GB file from the source to the destination
- Delete the 75GB file from the destination

Option B is impossible in this scenario. But, Option A is foolish. CCC never uses option A, that's just gambling with your data. This isn't theoretical either, we've heard stories of people losing data in this manner with other "backup" software.

CCC uses the atomic file copying method. Rather than deleting a file that will be replaced, and then copying the replacement file, CCC copies the replacement file to the destination first (using a temporary file name). When the file has been copied successfully, CCC then removes (or archives) the older version of the file, and then renames the temporary file to its correct name. This is particularly important should CCC discover that the source file is unreadable due to a media error. With the "Option A" copying behavior, you'd be left with no good copy of the file on the destination and of course the corrupted copy on the source. The downside to the atomic copying method is that the destination needs to have enough free space to accommodate the old version of the file and the replacement version of the file.

If you find yourself in a similar scenario, you have a couple options:

- Get a larger destination disk so CCC can make safe backups. We strongly recommend this option.
- Implement a [preflight script](http://bombich.com/kb/ccc5/performing-actions-before-and-after-backup-task#scheduler_shell_scripts) <http://bombich.com/kb/ccc5/performing-actions-before-and-after-backup-task#scheduler_shell_scripts> that deletes that 75GB file, and just hope that the source file never becomes corrupted. You can [download an example preflight script here](http://bombich.com/software/files/tools/remove_large_file.sh.zip) <http://bombich.com/software/files/tools/remove_large_file.sh.zip>.

One last note – CCC's "Run a deletion pass first" troubleshooting option does not contradict the atomic copying procedure, so it is not applicable in this scenario. The deletion pass removes files from the destination that are no longer present on the source, it does not remove files that will be getting updated during the backup.

I have SafetyNet turned off, how could the destination be too full?

If you have disabled CCC's SafetyNet setting, note that deletions occur as the items to be deleted are encountered. CCC traverses the files and folders on your source and destination volumes in

alphabetical order, so it is possible that CCC will attempt to write new files to the destination before deleting items that were deleted from the source. If you have made large organizational changes on the source (e.g. renamed or moved folders, deleted and created many items), you may want to try the following steps to proactively clear space on the destination:

1. If you did not choose the option to delete the SafetyNet folder from the destination when you disabled the SafetyNet option, choose **Delete a SafetyNet Folder...** from the **Utilities** menu. Drag the _CCC SafetyNet folder from the Finder onto the **Delete a SafetyNet Folder** window to remove that folder.
2. Click the Advanced Settings button.
3. Uncheck the box next to [Protect root-level items on the destination](http://bombich.com/kb/ccc5/advanced-settings#protect) <<http://bombich.com/kb/ccc5/advanced-settings#protect>>.
4. Check the box next to [Run a deletion pass first](http://bombich.com/kb/ccc5/advanced-settings#troubleshooting) <<http://bombich.com/kb/ccc5/advanced-settings#troubleshooting>> in the Troubleshooting Options box.
5. Save and run the backup task.

Related Documentation

- [Why is disk usage different between the source and destination?](http://bombich.com/kb/ccc5/disk-usage-on-destination-doesnt-match-source.-did-ccc-miss-some-files) <<http://bombich.com/kb/ccc5/disk-usage-on-destination-doesnt-match-source.-did-ccc-miss-some-files>>
- [Automated maintenance of the CCC SafetyNet](http://bombich.com/kb/ccc5/automated-maintenance-ccc-safetynet-folder) <<http://bombich.com/kb/ccc5/automated-maintenance-ccc-safetynet-folder>>
- [Creating a separate task to prevent VM container versions from bloating the SafetyNet](http://bombich.com/kb/ccc5/creating-separate-task-prevent-vm-container-versions-from-bloating-safetynet) <<http://bombich.com/kb/ccc5/creating-separate-task-prevent-vm-container-versions-from-bloating-safetynet>>
- [Mail's "Log Connection Activity" setting creates enormous files](http://bombich.com/kb/ccc5/why-ccc-recopying-every-file-during-each-backup#mail_cd_log) <http://bombich.com/kb/ccc5/why-ccc-recopying-every-file-during-each-backup#mail_cd_log>

Can I use Carbon Copy Cloner to clone a Time Machine backup?

No, CCC will exclude the Backups.backupdb folder during a backup task because Time Machine backup folders contain Apple-proprietary filesystem devices. Apple's recommended procedure for copying a Time Machine volume is documented in [this Apple Kbase article](https://support.apple.com/en-us/HT202380) <<https://support.apple.com/en-us/HT202380>>.

Backing up Time Machine sparsebundle disk images

When Time Machine is configured to back up a Macintosh to a network volume (such as a Time Capsule device), Time Machine stores the backup in a sparsebundle disk image. CCC can copy these sparsebundle disk image files without any special configuration; simply choose your network volume as the source of your CCC backup task. In fact, CCC quite capably copies only the bands within the sparsebundle that have changed, so you can add CCC to this type of setup for a second tier backup to an offsite network share.

Note that CCC will exclude the Backups.backupdb folder at the root level of a volume by default. If your source volume has a folder by that name, and you want CCC to copy sparsebundle disk images from this folder, you can choose **Choose a folder...** from CCC's Source selector and choose the Backups.backupdb folder directly to configure CCC to back up the sparsebundle disk images. Note that the only items in a Backups.backupdb folder that CCC will copy are sparsebundle disk images. Other folders, e.g. local Time Machine backups will be excluded. Further, CCC will only consider sparsebundle images for deletion in a Backups.backupdb folder on the destination. Other items in this folder on the destination will be protected from deletion.

Lastly, please note that no application can access the contents of a sparsebundle disk image file **while that disk image is mounted or otherwise deemed to be in use**. For example, if your Time Machine backups are currently running and backing up to a disk image, CCC will not be able to copy the disk image file, rather it will get an error that the files are in use.

Frequently Asked Questions about encrypting the backup volume

- [Can I back up an encrypted volume to a non-encrypted volume?](#)
- [If I back up an encrypted volume to a non-encrypted volume, will the copied files be encrypted on the destination?](#)
- [Will Carbon Copy Cloner enable encryption on my backup volume?](#)
- [Do I have to wait for encryption to complete before rebooting from my production volume?](#)
- [What password do I use to unlock my encrypted volume?](#)
- [What happens if I change my account password on the source volume? Does the encryption password on the backup volume get updated automatically?](#)
- [I enabled encryption on my 3TB USB backup disk. Why can't I boot from that volume any more?](#)
- [Can I create a bootable backup on a pre-encrypted volume? Why do you recommend cloning to a non-encrypted volume first?](#)
- [I restored my backup to another Mac that had FileVault enabled, and now I can't unlock the cloned volume.](#)
- [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 cloning to an APFS volume that previously had FileVault enabled, the destination can't be unlocked on startup](#)
- [After cloning to an APFS Encrypted volume there is a 24-second stall during startup](#)
- [My YubiKey authentication device can't unlock my encrypted backup volume on startup](#)

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](http://bombich.com/kb/ccc5/working-filevault-encryption) <<http://bombich.com/kb/ccc5/working-filevault-encryption>> to enable encryption.

Will Carbon Copy Cloner 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.

I enabled encryption on my 3TB USB backup disk. Why can't I boot from that volume any more?

Some versions of OS X have difficulty recognizing USB devices that have been encrypted with FileVault. The Western Digital My Passport Ultra 3TB disk, for example, works fine as a bootable device when not encrypted. In our tests, however, this device was no longer recognizable when FileVault encryption was enabled. This problem appears to be limited to OS X 10.11 El Capitan. The same volume was accessible using older and newer OSes, and also functioned fine as an encrypted startup device using older and newer OSes.

Can I create a bootable backup on a pre-encrypted volume? Why do you recommend cloning to a non-encrypted volume first?

Catalina users: It is not possible to **create** a bootable backup on a pre-encrypted backup disk, [Apple's tools just don't permit this <http://bombich.com/kb/ccc5/macOS-catalina-known-issues#diskutil_addvolume_encryption>](http://bombich.com/kb/ccc5/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.

We generally [recommend that people establish a bootable backup on a non-encrypted volume](http://bombich.com/kb/ccc5/working-filevault-encryption) [<http://bombich.com/kb/ccc5/working-filevault-encryption>](http://bombich.com/kb/ccc5/working-filevault-encryption), and then enable FileVault while booted from the destination. Some people have discovered, however, that a pre-encrypted volume can function as a bootable device **with versions of macOS prior to Catalina**. So why do we recommend the former? There are a couple notable differences between pre-encrypting the disk vs. enabling FileVault after booting from the not-encrypted disk. When you enable FileVault via the Security Preference Pane:

- You get a sanity check that a recovery volume exists (this avoids spending lots of time copying files only to find out that the volume might not be bootable)
- You get the opportunity to store a recovery key with Apple
- You can unlock the disk with selected accounts
- You get a nicer UI on startup to unlock the disk (e.g. it's similar to the LoginWindow interface), vs. a less-polished looking **Unlock Disk** interface
- APFS-specific: You avoid a 24-second startup delay that occurs when the system can't find the "disk" user in the system's directory service on a pre-encrypted APFS volume.

One drawback to enabling FileVault via the Security Preference Pane, however, is that [changes to account passwords on the source volume aren't immediately reflected on the backup](#) as far as unlocking the disk is concerned. The old account passwords would be required until you boot from the backup and specifically re-enable those accounts in the Security Preference Pane (at which time the disk's EncryptionKey is remastered).

As far as the backups are concerned, there's no difference between these two methods. There is still an order-of-operations concern with pre-encrypting the disk if your disk is formatted using Apple's legacy HFS+ filesystem format (**the steps below are not applicable to APFS**). You'd want to approach it in this manner:

1. Erase the destination device <http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x> > (unencrypted!)
2. Click on the freshly-erased disk in CCC's sidebar and create a recovery volume on that disk
3. Go back to Disk Utility and erase the **volume** now, not the whole disk (as was emphasized in the instructions above). Now you can choose the option to encrypt the volume. By erasing just the volume here, not the whole disk, the hidden recovery partition that CCC created won't be destroyed.
4. Open CCC and configure your backup task

In general, either procedure is fine, it really is the same as far as the backup is concerned. We generally prefer the Security Preference Pane method, however, because it yields the same UI behavior you are expecting if you have enabled FileVault on your production startup volume. Many people become concerned when the Disk Utility-encrypted volume shows any behavioral difference at all with regard to unlocking the disk on startup, and that concern is best avoided by enabling FileVault in the Security Preference Pane.

I restored my backup to another Mac that had FileVault enabled, and now I can't unlock the cloned 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 clone 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](http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x#erase_apfs_container) [<http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x#erase_apfs_container>](http://bombich.com/kb/ccc5/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 cloning to an APFS volume that previously had FileVault enabled, the destination can't be unlocked on startup

After cloning 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 cloning 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 clone 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 clone 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 clone 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 cloned 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. Mojave+ only: 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?](#)
- [What happens if no one is logged in when a task is scheduled to run?](#)
- [Will CCC run when the computer is turned off?](#)
- [Will CCC run when the my laptop's lid is closed?](#)
- [How is system sleep handled?](#)
- [Why does my laptop sometimes go to sleep during a backup task?](#)
- [Why does my screen turn on shortly before a backup task starts?](#)
- [What if the backup drive is not available when a task is scheduled to run?](#)
- [Can I stop a backup task before it finishes?](#)
- [How can I disable/suspend a task?](#)
- [Can I configure a task to run immediately after the computer is turned on?](#)
- [Related documentation](#)

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.cchelper" 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?

By default, any scheduled events that elapse when the computer is off will be skipped, and those tasks will run at their next scheduled run time. If you would like to schedule a task to occur when the system is typically powered off, choose the "Wake or power on the system" option from the System Sleep popup menu in the CCC Scheduler. With that configuration, 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 <http://bombich.com/kb/ccc5/how-modify-scheduled-backup>](http://bombich.com/kb/ccc5/how-modify-scheduled-backup)

Will CCC run when the 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 in to 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 wake your computer when your tasks are scheduled to run. You can change this setting in the **Runtime Conditions** section when scheduling a task. As long as your Mac is running on AC power, CCC will prevent the system from sleeping for the duration of a backup task.

Related Documentation

- [Handling system sleep events <http://bombich.com/kb/ccc5/configuring-scheduled-task-runtime-conditions#sleep>](http://bombich.com/kb/ccc5/configuring-scheduled-task-runtime-conditions#sleep)
- [How to modify a scheduled backup <http://bombich.com/kb/ccc5/how-modify-scheduled-backup>](http://bombich.com/kb/ccc5/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?

By default, CCC schedules a wake event to occur 20 seconds before a scheduled task is configured 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. If you prefer that your display does not turn on, e.g. in the middle of the night, use the **Run this task when the system next wakes** setting 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 <http://bombich.com/kb/cc5/performing-actions-before-and-after-backup-task#power_mgmt_options>](http://bombich.com/kb/cc5/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? <http://bombich.com/kb/cc5/how-set-up-scheduled-backup>](http://bombich.com/kb/cc5/how-set-up-scheduled-backup)
- [Configuring Scheduled Task Runtime Conditions <http://bombich.com/kb/cc5/configuring-scheduled-task-runtime-conditions>](http://bombich.com/kb/cc5/configuring-scheduled-task-runtime-conditions)

Frequently asked questions about the Carbon Copy Cloner SafetyNet folder

Note: The topics in this article are not relevant to APFS-formatted destination volumes that have [CCC snapshot support enabled](http://bombich.com/kb/ccc5/leveraging-snapshots-on-apfs-volumes) <<http://bombich.com/kb/ccc5/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?](#)
- [Why can't I open some files in the _CCC SafetyNet folder?](#)
- [Can I restore a previous version of the OS using one of the archives in the _CCC SafetyNet folder?](#)
- [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](#)
- [Why can't I delete some items from the SafetyNet folder? The Finder says that some items are in use.](#)
- [How can I prevent Migration Assistant from copying the CCC SafetyNet folder during a migration?](#)
- [I have SafetyNet enabled, why can't I find a "_CCC SafetyNet" folder on the destination?](#)
- [I selected "Don't delete anything", why is CCC placing items in the "_CCC SafetyNet" folder on the destination?](#)

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. 2017-07-27 (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 <http://bombich.com/kb/cc5/leveraging-snapshots-on-apfs-volumes#srp>](http://bombich.com/kb/cc5/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, or [from a snapshot <http://bombich.com/kb/cc5/leveraging-snapshots-on-apfs-volumes#restore>](http://bombich.com/kb/cc5/leveraging-snapshots-on-apfs-volumes#restore).

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 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.

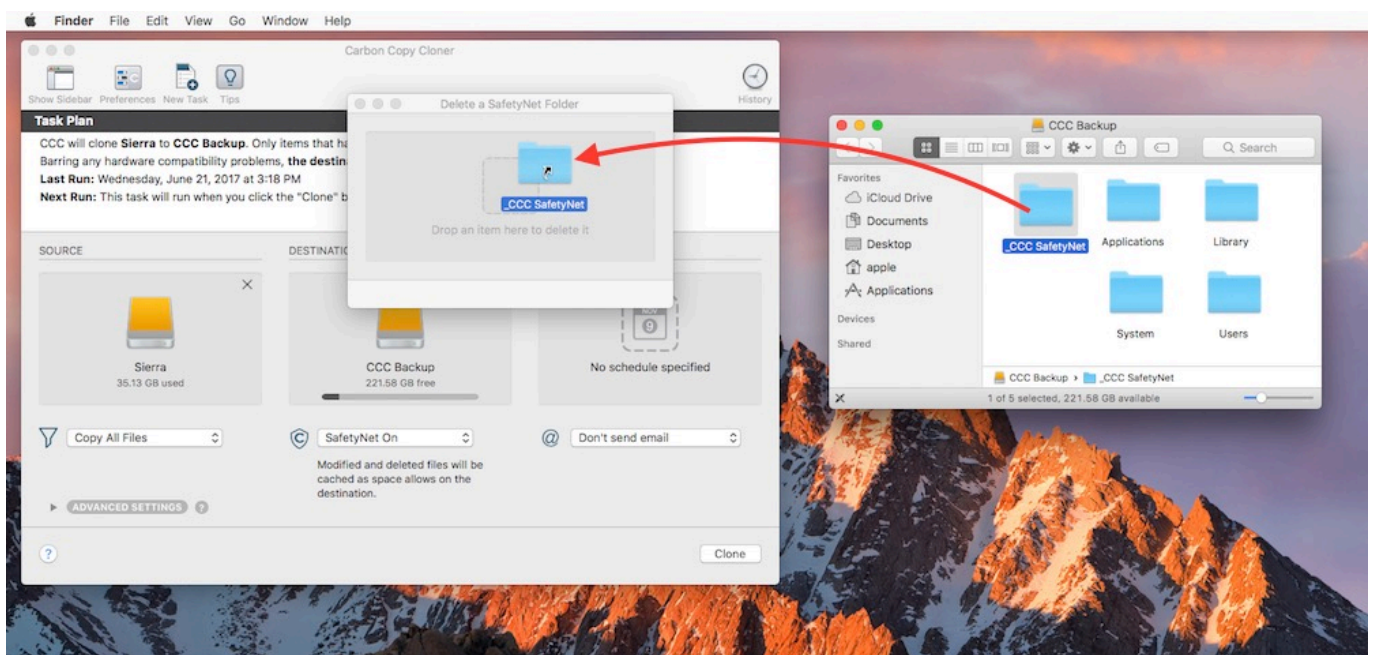
Not all applications have this kind of internal Trash folder, so be sure to see how it works for other applications before applying these exact steps. The general idea, though, is that you should deliberately archive the items that you're removing from your source volume in a way that makes sense to 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.

In OS X El Capitan, Apple introduced a new feature called **System Integrity Protection (SIP)**. SIP works by preventing any user from deleting certain protected system items on the startup disk. If you boot your Mac from a backup volume and restore system files to your startup disk, CCC will place outdated versions of those system files into the SafetyNet folder. These modifications are allowed because CCC is making changes to that volume while it is not the current startup disk. When you restart your computer from that destination volume, however, SIP re-engages and may then prevent you from deleting the protected items that were placed into the SafetyNet folder. If you attempt to delete these items, the Finder will report that they 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 the item you're trying to remove is on your current startup disk, CCC will move the item to the root of your startup disk, then instruct you to boot your Mac from some other volume (e.g. your backup disk). Once booted from the backup volume, you can repeat the same steps with CCC to remove the SafetyNet folder.

If you're still having trouble after trying that, don't hesitate to [ask us for help](#) <http://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](#) <<http://bombich.com/kb/ccc5/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](#) <<http://bombich.com/kb/ccc5/legacy-safetynet-folder-not-used-when-snapshots-are-enabled-on-destination>>
- [SafetyNet snapshots vs. Backup snapshots](#) <<http://bombich.com/kb/ccc5/leveraging->

[snapshots-on-apfs-volumes#safetynet_vs_backup>](#)

- [Where did the CCC SafetyNet folder go after upgrading to Catalina? <http://bombich.com/kb/ccc5/frequently-asked-questions-about-ccc-and-macos-catalina#safetynet>](http://bombich.com/kb/ccc5/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.

Frequently Asked Questions about cloning Apple's "Recovery HD" partition

Reminder: Recovery HD volume cloning is not applicable to APFS-formatted destination volumes (i.e. Catalina and later)

Carbon Copy Cloner offers complete support for archiving, cloning, and recreating Apple's Recovery HD partition. See the [Cloning Apple's Recovery HD partition <http://bombich.com/kb/ccc5/cloning-apples-recovery-hd-partition>](http://bombich.com/kb/ccc5/cloning-apples-recovery-hd-partition) section of CCC's Disk Center documentation for instructions to create a Recovery HD volume on your backup disk.

When do I need to create a Recovery HD volume?

CCC bootable backups offer similar functionality to the Recovery HD volume, so the Recovery HD volume is not strictly required on a backup volume. Unless you have a specific reason to not create a Recovery HD, though (e.g. because it could affect a Boot Camp partition on the same disk, you don't want to give up the 1GB, etc), we recommend that you maintain a Recovery HD volume on your backup disk. Especially if you intend to use your destination volume in production (e.g. you are migrating to a larger disk, or restoring to a replacement disk), or if you intend to enable encryption on the backup volume, then you should create a Recovery HD volume for the destination volume. If you intend to enable encryption on the destination volume, we recommend that you create the Recovery HD volume **before** enabling encryption. **A Recovery HD volume is not required for restoring an installation of macOS from a CCC bootable backup.**

What is the difference between archiving the Recovery HD and creating a new Recovery HD?

During the course of an ordinary backup of a volume that contains macOS, CCC will **automatically** create an archive of the Recovery HD associated with that volume. This archive is stored on the source volume, and is subsequently backed up to the backup volume along with everything else. This archive of the Recovery HD volume can be used in the future to create a new Recovery HD, and it's the first source that CCC considers when you choose to create a Recovery HD. The archive is not, however, an **operational** Recovery HD volume, it's just a backup file.

CCC's Disk Center offers the ability to create an operational Recovery HD volume as well. This functionality is completely separate from creating an archive of the Recovery HD. Unlike the archiving of the source Recovery HD, creating a new Recovery HD is not something that happens automatically, you have to ask CCC to do this in the Disk Center. When CCC creates a new Recovery HD, it borrows space from your destination volume to create a new, hidden volume on that disk. The resulting Recovery HD is fully operational — you can boot your Mac from it and reinstall macOS. Refer to the previous section to determine if creating a Recovery HD is required in your situation.

Why were other volumes on my disk unmounted when I created a Recovery HD?

CCC uses a command-line version of Disk Utility to resize the donor volume. Resizing that volume requires making changes to the partition table on the disk, and Disk Utility may choose to unmount other volumes on the disk while it makes those changes. CCC will specifically remount the donor

volume, but whether Disk Utility remounts the other volumes is a function (or bug) of Disk Utility. You can remount these volumes manually in Disk Utility.

Can I create a Recovery HD on an Apple Fusion (aka "CoreStorage") volume?

No, not with CCC. Creating a Recovery HD requires borrowing space from a physical volume, and that is not a modification that we recommend making to an underlying member of an Apple Core Storage logical volume. The only Apple-supported method of creating a Fusion volume is via Disk Utility or the macOS Installer, and each of those will create a Recovery HD volume before the Fusion volume is created. If you intend to create your own HFS+ formatted Fusion volume using one of the various tutorials available on the Internet, and if you want that volume to have an associated Recovery HD volume, we strongly recommend that you create a Recovery HD volume **before** creating the Fusion volume. You can use CCC to create the Recovery HD volume on the slowest disk that you intend to add to the Fusion logical volume group. See the following document for a demonstration.

[Creating a Fusion volume with a Recovery HD](#)

[<http://bombich.com/software/files/tools/Creating_a_Fusion_volume_with_a_Recovery_HD.pdf>](http://bombich.com/software/files/tools/Creating_a_Fusion_volume_with_a_Recovery_HD.pdf)

Why is the option to create (or remove) a Recovery HD disabled?

If you are booted from the volume that you have selected in CCC's sidebar, the option to Create or Remove the Recovery HD associated with that volume will be disabled. This is commonly encountered when you have booted from your backup volume. To make changes to the Recovery HD associated with your startup disk, first boot your Mac from some other startup volume.

This option will also be disabled if the selected volume is a Fusion or FileVault-protected volume (i.e. a "CoreStorage" volume). CCC cannot create a Recovery HD volume on a Fusion or FileVault-protected volume, therefore CCC will never allow you to remove the Recovery HD volume that is associated with a Fusion or FileVault-protected volume.

CCC says there is a Recovery volume associated with my startup disk. Why can't I see this Recovery HD volume in the Option key startup manager?

Apple uses an abstract volume type, the CoreStorage volume, for some startup disks. Because these volumes are abstract, your Mac's firmware cannot boot directly from them; a small piece of macOS needs to assemble the abstract volume first. To accommodate this limitation, Apple associates a "helper" partition with CoreStorage volumes. In many cases, the Recovery HD volume plays that role. When you hold down the Option key on startup, your Mac's firmware can't detect the abstract CoreStorage volumes, but it can detect these helper partitions. To avoid confusion, the label given to these Recovery volumes is the label of the associated volume. So if you have a startup disk named "Macintosh HD" and an associated helper partition named "Recovery HD", you will only see one volume in the startup manager — the Recovery volume, but with the Macintosh HD label. If you want to boot from the Recovery volume, click on the Macintosh HD-labeled volume while [holding down Command+R](#) [<https://support.apple.com/en-us/HT204904>](https://support.apple.com/en-us/HT204904).

I'm backing up an APFS startup disk to an HFS+ backup disk. Will CCC automatically create a Recovery HD volume on the destination?

For logistical and data safety reasons that are specific to the shortcomings of HFS+, CCC will not **automatically** create a Recovery HD volume on an HFS+ formatted destination volume; CCC will only automatically create recovery volumes on APFS destination volumes. But you will be able to create a Recovery HD on the destination regardless of the format of the source. During the backup



task, CCC will create a format-agnostic archive of the Recovery volume that is associated with the source. At the end of your first backup task, CCC will prompt you to create the Recovery HD volume on the destination, and will then walk you through the simple procedure. You may also select your HFS+ destination in CCC's sidebar and click on the **Recovery HD...** button at the bottom of the window to create that volume.

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 Preferences button in CCC's toolbar to access settings related to running tasks while on battery power.

Can I run my backups more frequently than Hourly?

CCC offers hourly, daily, weekly, and monthly scheduling options, which suits the needs of most users. Some usage scenarios, however, demand higher frequency backups. For example, photographers might prefer to have their SD cards offloaded to a tethered computer every 5-15 minutes during a photo shoot. When the shoot is complete, though, the backup task should not run at all. Special cases like these demand more flexible execution options, which can be achieved by leveraging CCC's built-in command-line utility. These simple steps demonstrate how to set up a high-frequency backup task that you can easily start and stop and the beginning and conclusion of a photo shoot:

1. Open CCC and click the **New Task** button in the toolbar to create a new backup task. Name it something like "Location Backup".
2. Click on the Source selector and choose your tethered camera's SD card as the source.
3. Drag a folder from the Finder onto CCC's Destination selector to specify that folder as the destination.
4. Save the task (do not schedule this task).
5. Download this example [Frequent Backups script](http://bombich.com/software/files/tools/frequent_backups.command.zip) <http://bombich.com/software/files/tools/frequent_backups.command.zip> and open it in TextEdit (Applications > TextEdit.app).
6. Modify the script to specify the correct location of CCC on your Mac (the default is correct if it is located in your Applications folder), the name of your backup task, and the frequency at which you prefer it to run. Save the changes. You can store this script wherever you like.
7. When you're ready to start your shoot, simply double-click the frequent_backups.command script. The script will run the specified task at the specified frequency.
8. When your shoot is finished, quit the Terminal application to stop the script.

If you have questions about this sort of setup or need some help getting the configuration suited to your needs, please don't hesitate to [reach out to us for help](http://bombich.com/software/get_help) <http://bombich.com/software/get_help>.

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, nor even a notification that something is wrong that should be corrected.

Solution

The solution to this problem is to remove the affected system folder and recreate it with the correct ownership and permissions. To avoid exposing yourself to potential security vulnerabilities, it is imperative that you **remove** this folder and its contents rather than simply correcting the ownership and permissions.

1. Quit CCC if it is open
2. Choose **Computer** from the Finder's Go menu
3. Navigate to your startup disk > Library
4. Drag the **LaunchDaemons** folder to the Trash, authenticating when prompted
5. Open the Terminal application (`/Applications/Utilities/Terminal.app`)
6. Paste the following into the Terminal one line at a time, pressing the Return key at the end of each line. Type in your admin password when prompted.

```
sudo mkdir -m 755 /Library/LaunchDaemons
sudo chown root:wheel /Library/LaunchDaemons
```

7. Open CCC and try again to save and run a backup task

Related Documentation

- [What is CCC's Privileged Helper Tool? <http://bombich.com/kb/ccc5/what-cccs-privileged-helper-tool>](http://bombich.com/kb/ccc5/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](http://bombich.com/kb/ccc5/frequently-asked-questions-about-carbon-copy-cloner-safetynet) <<http://bombich.com/kb/ccc5/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.
- You can restore older versions of the operating system.
- Deleting snapshots is really simple, you'll never run into permissions problems or failures of the Finder to empty the Trash.

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 bundle files and of the whole OS.



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 clone 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 clone to your current startup disk.

Frequently asked questions about CCC and APFS Volume Groups

If you have applied the macOS Catalina or Big Sur 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](http://bombich.com/kb/ccc5/working-apfs-volume-groups) [<http://bombich.com/kb/ccc5/working-apfs-volume-groups>](http://bombich.com/kb/ccc5/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.

[Do I have to make any changes to my backup disk before running my backup task?](#)

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](http://bombich.com/kb/ccc5/i-want-back-up-multiple-macs-or-source-volumes-same-hard-drive)

[<http://bombich.com/kb/ccc5/i-want-back-up-multiple-macs-or-source-volumes-same-hard-drive>](http://bombich.com/kb/ccc5/i-want-back-up-multiple-macs-or-source-volumes-same-hard-drive)

Video: Preparing your backup disk on macOS Catalina (and later) [<https://youtu.be/n_arMTq3d58>](https://youtu.be/n_arMTq3d58)

[Do I need to create separate backup tasks for "Macintosh HD" and "Macintosh HD - Data"?](#)

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 a hard drive for use with Carbon Copy Cloner <http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x#high_sierra>](http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x#high_sierra)

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/n_arMTq3d58?t=86>](https://youtu.be/n_arMTq3d58?t=86) 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 <http://bombich.com/kb/ccc5/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 <http://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 <http://bombich.com/kb/ccc5/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/MXHNeCHnpnl>>

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/MXHNeCHnpnl)
<<https://youtu.be/MXHNeCHnpnl>>

[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](http://bombich.com/kb/ccc5/macOS-catalina-known-issues#diskutil_addvolume_encryption) <http://bombich.com/kb/ccc5/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 a hard drive for use with Carbon Copy Cloner](http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x#high_sierra) <http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x#high_sierra>.

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? <http://bombich.com/kb/ccc5/frequently-asked-questions-about-ccc-and-macos-catalina#conversion_encrypted_decrypt>](http://bombich.com/kb/ccc5/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? <http://bombich.com/kb/ccc5/frequently-asked-questions-about-ccc-and-macos-catalina#encrypted_non_bootable>](http://bombich.com/kb/ccc5/frequently-asked-questions-about-ccc-and-macos-catalina#encrypted_non_bootable)
- [Working with FileVault Encryption <http://bombich.com/kb/ccc5/working-filevault-encryption>](http://bombich.com/kb/ccc5/working-filevault-encryption)
- [Frequently Asked Questions about encrypting the backup volume <http://bombich.com/kb/ccc5/frequently-asked-questions-about-encrypting-backup-volume>](http://bombich.com/kb/ccc5/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? <http://bombich.com/kb/ccc5/frequently-asked-questions-about-ccc-and-macos-catalina#encrypted_non_bootable>](http://bombich.com/kb/ccc5/frequently-asked-questions-about-ccc-and-macos-catalina#encrypted_non_bootable)
- [Working with FileVault Encryption <http://bombich.com/kb/ccc5/working-filevault-encryption>](http://bombich.com/kb/ccc5/working-filevault-encryption)
- [Frequently Asked Questions about encrypting the backup volume <http://bombich.com/kb/ccc5/frequently-asked-questions-about-encrypting-backup-volume>](http://bombich.com/kb/ccc5/frequently-asked-questions-about-encrypting-backup-volume)
- [Catalina Known Issue: Apple's volume group manipulation tool doesn't work with encrypted volumes <http://bombich.com/kb/ccc5/macos-catalina-known-issues#diskutil_addvolume_encryption>](http://bombich.com/kb/ccc5/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. Drag the Macintosh HD - Data volume from CCC's sidebar into the Source selector
4. 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.

If your backup disk is a "mobile" 2.5" rotational disk (i.e. that spins at 5400RPM or less), we recommend that you format that device as "Mac OS Extended, Journaled" (aka HFS+) and use it for data-only backups. [APFS offers unacceptable performance on these devices <http://bombich.com/blog/2019/09/12/analysis-apfs-enumeration-performance-on-rotational-hard-drives>](http://bombich.com/blog/2019/09/12/analysis-apfs-enumeration-performance-on-rotational-hard-drives), we simply can't recommend nor support the use of these devices for bootable backups.

[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/MXHNeCHnpnl>](https://youtu.be/MXHNeCHnpnl)

Yes, you can dismantle a volume group in Disk Utility. You may want to do this if, for example, you cloned 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 <<http://bombich.com/kb/ccc5/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. <http://bombich.com/kb/ccc5/frequently-asked-questions-about-carbon-copy-cloner-safetynet#sip_prevents_delete>

Frequently asked questions about CCC and macOS 11

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.

How are bootable backups different on macOS Big Sur?

CCC uses Apple's APFS replication utility, "ASR", to establish an initial bootable clone of your startup disk. This 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 new backup 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 clone
- Add a new, dedicated backup volume to an existing APFS destination (if there is enough free space)
- Proceed with a Data Volume 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 Clone" see [Cloning macOS System volumes with Apple Software Restore](http://bombich.com/kb/ccc5/cloning-macos-system-volumes-apple-software-restore) <<http://bombich.com/kb/ccc5/cloning-macos-system-volumes-apple-software-restore>>.

Does my CCC backup have to be bootable for me to restore data from it?

No. 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).

After CCC has established an initial bootable backup, will it keep the destination System volume up to date?

No. We would like to offer this functionality, but doing so involves a tradeoff that we think most users would find unacceptable. Due to an [inflexibility in Apple's APFS replication utility \(ASR\)](http://bombich.com/kb/ccc5/macos-big-sur-known-issues#asr_volume_group) <http://bombich.com/kb/ccc5/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. Doing so would remove all snapshots on the destination, and would take quite a bit longer than an ordinary incremental backup.

Fortunately, updating the System volume on the destination is not something that you have to do frequently, nor even proactively, it's something that you can do if and when required. Simply boot your Mac from the backup volume and apply any updates via the Software Update preference pane

in the System Preferences application. This is something that you could even defer until the need arises to restore from the 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 <http://bombich.com/kb/ccc5/best-practices-updating-your-macs-os#commit>](http://bombich.com/kb/ccc5/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

- [Frequently asked questions about CCC and APFS Volume Groups \(Catalina and Big Sur\) <http://bombich.com/kb/ccc5/frequently-asked-questions-about-ccc-and-macos-catalina>](http://bombich.com/kb/ccc5/frequently-asked-questions-about-ccc-and-macos-catalina)
- [Cloning macOS System volumes with Apple Software Restore <http://bombich.com/kb/ccc5/cloning-macos-system-volumes-apple-software-restore>](http://bombich.com/kb/ccc5/cloning-macos-system-volumes-apple-software-restore)
- [Restoring from a bootable backup <http://bombich.com/kb/ccc5/how-restore-from-your-backup>](http://bombich.com/kb/ccc5/how-restore-from-your-backup)
- [Restoring from a snapshot <http://bombich.com/kb/ccc5/leveraging-snapshots-on-apfs-volumes#restore>](http://bombich.com/kb/ccc5/leveraging-snapshots-on-apfs-volumes#restore)
- [Migrating data from a data-only backup using Migration Assistant <http://bombich.com/kb/ccc5/creating-and-restoring-data-only-backups#migrate>](http://bombich.com/kb/ccc5/creating-and-restoring-data-only-backups#migrate)
- [Best practices for updating your Mac's OS <http://bombich.com/kb/ccc5/best-practices-updating-your-macs-os>](http://bombich.com/kb/ccc5/best-practices-updating-your-macs-os)
- [macOS Big Sur Known Issues <http://bombich.com/kb/ccc5/macos-big-sur-known-issues>](http://bombich.com/kb/ccc5/macos-big-sur-known-issues)