Documentation 0950-1194/2

TinkerTool System 9

Reference Manual

Marcel Bresink
Software-Systeme

Version 9.41, March 10, 2025. US-English edition.
MBS Documentation 0950-1194/2

Marcel Bresink Software-Systeme
Ringstr. 21
56630 Kretz
Germany

This publication may contain examples of data used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

This publication could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. The publisher may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Make sure that you are using the correct edition of the publication for the level of the product. The version number can be found at the top of this page.

Special thanks go to Mark Weisz for suggestions for improving the US English translation of parts of the manual.

Main text typeset with Fontin Sans, a font by Jos Buivenga (exljbris Font Foundry).

Contents

Chapter 1

Introduction

1.1 What is TinkerTool System 9?

TinkerTool System 9 is a collection of system utilities assisting you in performing advanced administration tasks on Apple Macintosh computers. All functions can be controlled from one single program which acts as general toolbox and First Aid assistant. This includes

- built-in maintenance features of macOS, usually not visible on the graphical user interface,
- extended file operations, not available in the macOS Finder,
- the possibility to access advanced system settings which are not visible in System Settings,
- graphical user interfaces for "pro" features for which Apple doesn't provide any graphical interface in modern versions of macOS any longer,
- genuine and unique features of TinkerTool System, designed to resolve typical real-world problems of administrators and to fix the effects of certain defects ("bugs") in the operating system,
- features to protect your privacy,
- an emergency tool to troubleshoot and repair macOS in cases where the normal user interface is no longer starting correctly or the user account of the system administrator has been damaged,
- functions to collect advanced information about the hardware, operating system, and applications.

TinkerTool System knows macOS very well. It makes use of a self-adapting user interface which automatically adjusts to the computer model and to the version of macOS you are running. All options available in the current situation are accessible via "panes," very similar to the techniques you already know from the System Settings application.

In the remainder of this manual, we will use the designation "TinkerTool System" for simplicity, omitting the "9." However, there are in fact eight different product generations with slightly different application names.

- **TinkerTool System (Version 1):** for Mac OS X 10.2 Jaguar, Mac OS X 10.3 Panther, and Mac OS X 10.4 Tiger
- **TinkerTool System Release 2:** for Mac OS X 10.5 Leopard, Mac OS X 10.6 Snow Leopard, Mac OS X 10.7 Lion, OS X 10.8 Mountain Lion, and OS X 10.9 Mavericks
- **TinkerTool System 4:** for OS X 10.10 Yosemite and OS X 10.11 El Capitan
- **TinkerTool System 5:** for macOS 10.12 Sierra and macOS 10.13 High Sierra
- **TinkerTool System 6:** for macOS 10.14 Mojave and macOS 10.15 Catalina
- **TinkerTool System 7:** for macOS 11 Big Sur and macOS 12 Monterey
- **TinkerTool System 8:** for macOS 13 Ventura and macOS 14 Sonoma
- **TinkerTool System 9:** for macOS 15 Sequoia

These variants constitute completely separate product lines with different licenses, registrations, and icons.

TinkerTool System is a "real" macOS application and does not make use of unsafe scripting mechanisms. The program follows Apple's latest security guidelines for macOS. The graphical user interface is strictly separated from the operational core which is capable of performing privileged system operations. This core is monitored by macOS's security subsystem which is responsible for permitting or denying each single operation and to ask the user for authentication if necessary. TinkerTool System itself never asks for user passwords, making sure that your credentials cannot be intercepted by malicious user programs.

When resolving typical system problems, TinkerTool System attempts to follow Apple's official support guidelines. This does not mean that TinkerTool System will execute a certain troubleshooting procedure word by word. For example, the program will not simulate the entry of terminal commands if Apple lists them in step-by-step troubleshooting instructions. However, TinkerTool System will execute direct internal commands which will have the exact same effects. Users can click a special help button in TinkerTool System to check whether Apple offers official documents about certain system problems in their database. If such documentation is available, the user can click one or more Internet links to open up-to-the-minute information about the problem in question.

1.1.1 About the different functional areas of TinkerTool System 9

The features of TinkerTool System are divided into four separate areas:

- **System Maintenance:** features to assist administrators in typical troubleshooting operations

- **File Operations:** features to work with advanced operations on files, permissions, and applications
- **System Settings:** controls to access system-wide settings built into macOS
- **User Settings:** features for troubleshooting and maintenance operations which apply to the current user account only.

If you are using the sister application TinkerTool in addition to TinkerTool System, you will be free to integrate the panes of TinkerTool directly into the control window of TinkerTool System. This way you can have the functionality of both applications under one single roof and you no longer need to start the two programs separately. (Both applications must remain present for this to work, however.) TinkerTool's panes will also appear in the section **User Settings**.

1.1.2 System Requirements

To use TinkerTool System 9, you need an *Apple computer* which has one of the following operating systems installed:

- macOS 15 Sequoia

It is recommended to update macOS to the latest version which is available from Apple. This can be done using the **Automatic Updates** feature of the operating system.

> TinkerTool System cannot be used with user accounts that have an empty password. Modern versions of macOS consider this a configuration error and won't allow such users access to privileged parts of the operating system.

1.2 The Security Policy of TinkerTool System

When you launch TinkerTool System for the first time, it will automatically integrate into the security model of macOS. This is necessary because the application can be used to perform critical operations in macOS, for example to alter or even delete operating system files. Only responsible system administrators who manage the respective computer should be allowed to perform such actions.

To guarantee a high security level, TinkerTool System works in two parts: The normal main application with the graphical user interface is coordinating all operations. It also executes all tasks that don't require any special permissions. However, as soon as a *privileged operation* has to be executed, for example changing a setting that takes effect for *all* users of the computer, not only the current one, the application stops, makes you aware of the pending task, and checks whether the current user can identify herself as system administrator. If yes, the task will continue and the privileged operation can start.

The privileged job is not executed by the main application, however. A second component, the so-called *privileged helper* does this work by receiving the request of the main

application via a secure, tap-proof channel. Even if an unauthorized attacker would manage to manipulate the main program, it could not trigger any malicious functions in the computer, because it could not get permission to do that. Only the privileged component, which is monitored and specially protected by macOS has this technical capability. This means we have a *separation of user rights* in this setup. The privileged helper will also be called *security component* in this context.

In case the current user cannot identify as system administrator, the privileged operation will be rejected, denying its execution. You receive a notice in the graphical user interface that the pending task could not be continued due to security reasons.

1.2.1 Approval to use the security component

Apple's policies require an administrator to allow the security component to start automatically before TinkerTool System can be used, since the security component provides services *to all users*. Such programs are referred to by Apple as *Background Item*.

> The security component is started automatically by macOS when you start TinkerTool System. It doesn't run in the background when TinkerTool System isn't running.

Permission can be granted in two ways, either at the first launch of the program or at any time through the **System Settings** program. At the first start, the normal procedure is as follows:

1. Start TinkerTool System for the first time. The program *does not* open its control window, but instead displays an assistant guiding you through all necessary steps for the security component to be approved.
2. macOS displays a request via the Notification Center at the top right, asking whether you like to allow a new background item. In this dialog, select **Options** > **Allow**.
3. Confirm with an administrator's password that you allow this for all users.
4. TinkerTool System removes its message window and starts its full user interface.

> In older versions of macOS, a restart of the computer can be necessary during the very first launch of the application. Unfortunately, this step is enforced by Apple.

You can also grant permission at any time through the System Settings program:

1. Quit TinkerTool System if it is running.
2. Launch **System Settings**.
3. Open **General** > **Login Items**.
4. Find TinkerTool System in the **Allow in the Background** list.
5. Make sure the switch for this entry is on.

1.2.2 Confirming a privileged operation

To create the aforementioned monitored link between main application and privileged component, macOS asks for permission to setup the helper program during the first start of TinkerTool System. After this special trust relationship has been established between main application and privileged component, TinkerTool System will begin to control the special permissions from there on. The following rules apply when verifying the right to execute a protected operation:

For security reasons, only those users can initiate a privileged operation in TinkerTool System for which the option **Allow user to administer this computer** is enabled in the account management of macOS. Such users are called administrators. This special option is the default for the user who owns the computer and has set it up.

The application cannot read your password: Neither the main application, nor its privileged component are involved in the password entry and verification of credentials. Both tasks are exclusively handled by macOS, so that your password cannot be seen by the programs. Only after macOS has checked your identity, the result will be sent to the application.

> The previous rule applies to the authorization of privileged operations, but not for other logins which can also be protected by passwords. If the application has to login to a server process or to another computer in the network, it can be necessary that the program has to temporarily accept the password itself for technical reasons. In such a case you will receive an explicit notification about this circumstance before.

On computers with Touch ID, the confirmation can also be done by fingerprint: If your computer contains Apple's fingerprint reader *Touch ID* , the verification of your identity can also be done by fingerprint. As usual in macOS, you can choose whether to identify by password or by fingerprint.

A confirmation is valid for the pending operation, and optionally for further operations in the next five (5) minutes: In some cases, TinkerTool System has to execute multiple privileged operations in rapid succession to achieve a certain process, for example, a protected file may need to be deleted, and another one must be created in a protected folder. The application is designed to handle such a composite operation as single event, even if the operations are internally considered separate actions requiring different permissions. You only have to authenticate once, not twice in this example. But even operations which don't belong together don't necessarily lead to a renewed password entry: If a time of less than five minutes has passed between a privileged operation and your last authorization, another check of your identity will be avoided.

If you like to repeal this 5-minute rule, protecting each coherent task individually, this will be possible: You can force the application to establish a stricter guideline by a user preference setting:

1. Select the menu item **TinkerTool System** > **Settings**... or press the key combination ⌘ + , .
2. Check the option **Deauthorize administrator after each completed operation**.

An authorization won't be shared with other applications: When you have confirmed your identity to TinkerTool System to execute a privileged operation, this authorization will only be valid for the application itself, but not for other programs. This is also stricter than the usual guidelines of macOS, which would permit to avoid another password entry within five minutes for all applications running in the same login session.

1.2.3 Current limitations of macOS

TinkerTool System adheres strictly to Apple's current guidelines for providing privileged security components. Unfortunately, the latest technologies that Apple prescribes for their implementation are not always mature. This can depend on the macOS version you are using. In particular, the following restrictions may apply at the moment:

- There may only be one copy of the program on your computer. You should avoid having multiple versions or multiple copies on your Mac when launching the program. Only backup copies on Time Machine volumes are accepted.
- After granting the **Allow in background** permission as mentioned above, you should not rename the program or move it to another folder. Otherwise you will have to repeat the entire approval process.
- While you start the Mac, macOS must be able to "see" the application on the startup volume. So it should be in the folder **Applications** on the startup volume or a subfolder of it.

Additional limitations may exist in specific versions of macOS. You may also find detailed information in the chapter Important Release Notes (section 7.2 on page 332).

1.2.4 Removing outdated generations of the security component

TinkerTool System has a long history, protecting many generations of the operating system with its security architecture. Because Apple has changed the guidelines and technologies for this aspect of the system many times, it can have been necessary in the past to modify the security component to use a completely new technology. Usually you won't need to care about this. The application will notify you when an update is due and will perform all necessary steps by itself.

There can be cases however, where an updated security component is so different from its predecessor versions that it will no longer be compatible with them and cannot remove them automatically due to technical reasons. This means an outdated copy of the privileged helper could still be present in the system, even if the main application has been deleted or updated in the meanwhile. This usually doesn't bother, because macOS only starts these programs when necessary. You may like to delete these old components however, to avoid possible misuse and to clean up your computer.

TinkerTool System offers a special maintenance feature to do this. It can search for outdated auxiliary programs and remove them if desired. Perform the following steps:

1. Launch TinkerTool System if it is not running yet.

2. Select the menu item **Reset** > **Clean old security components**….

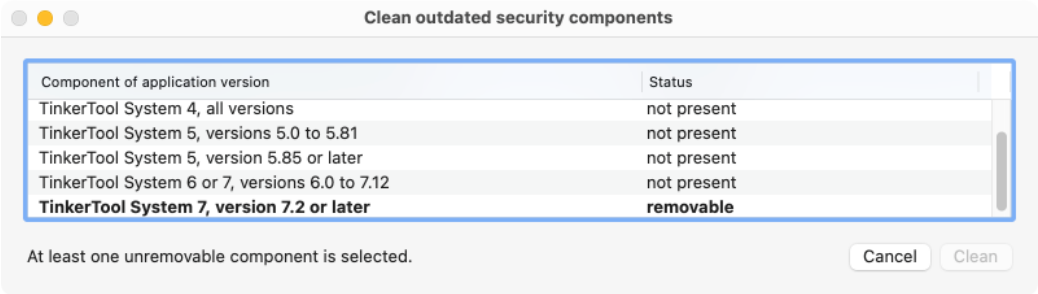


Figure 1.1: Outdated copies of the privileged helper can be removed if desired.

A window like that depicted in the example will open. The table lists all components which could still be installed from old versions of the application. Components marked by bold print are indeed still present and appear with the status **removable**. You can select one or more of these components and click the button **Clean** to delete them. If components are still in use unexpectedly, this will be automatically detected. You can only remove such helper programs after quitting their associated main applications.

1.2.5 Enabling stricter policies for administrator authorization

In older versions of the application, there were special cases for authorizing privileged operations where a login of a user with administrative rights was *not* allowed for security reasons. If desired, administrators can reinstate this previous, more restricted behavior.

Authorization in the current login session of a user who does not have administrative privileges

A user who is not currently logged in to macOS as an administrator can still perform privileged operations if they know the administrator credentials. The current login session does not need to be interrupted. If this option is not desired for security reasons, an administrator can block this by entering the following command on the affected computer:

```
sudo defaults write /Library/Preferences/com.bresink.system.tinkertoolsystem8.plist
MBSBlockAuthForNonAdminLogin -bool true
```

Fallback from local user identification to administrator authorization with name and password

To recognize users as authorized for a privileged operation, the application uses a feature of macOS known as *local user authentication*. macOS checks the user's identity through a dialog window that asks for their credentials. Alternatively, it is also possible to use security hardware, e.g. reading a fingerprint via *Touch ID* or using a smart card.

There are special cases where macOS rejects local user authentication, considering the user as unauthorized:

- The administrator has a blank password and this is not generally prohibited in the running operating system.
- Multiple users are currently logged into screen sessions on macOS and the administrator is accessing either via the feature *Fast User Switching* or through a network connection via screen sharing, but he does not currently have the "front" screen session (on the physical screen), so it is unclear who currently has access to Touch ID or other security hardware. This is called a *non-interactive situation* in macOS.
- Special hardware is available for user identification, but a technical problem has occurred.

In such cases, the program automatically switches to the traditional login of an administrator using name and password. If this option is not desired for security reasons, an administrator can block this by entering the following command on the affected computer:

```
sudo defaults write /Library/Preferences/com.bresink.system.tinkertoolsystem8.plist
MBSBlockLocalAuthFallback -bool true
```

Additional notes on changing security policies

Both policies mentioned above can be turned on or off independently. As a rule, the change takes effect the next time you start the application. However, there may be special operating situations in which macOS delays activation. If you want to ensure that the change takes effect in any case, it is recommended to restart the computer.

The return key may only be pressed at the end of the command, even if a command may be shown on several lines for reasons of space. After command entry, macOS will ask for the password of the currently logged-in administrator. It is entered covertly, so it does not appear on screen.

To switch the behavior back to default, the following commands can be used:

```
sudo defaults delete /Library/Preferences/com.bresink.system.tinkertoolsystem8.plist
MBSBlockAuthForNonAdminLogin
```

or respectively

```
sudo defaults delete /Library/Preferences/com.bresink.system.tinkertoolsystem8.plist
MBSBlockLocalAuthFallback
```

1.3 Basic Operations

1.3.1 The control window of TinkerTool System

After starting TinkerTool System, the main control window will appear. Depending on computer model and system configuration, it may take a few seconds until the window

becomes visible. TinkerTool System is performing a great number of validation and security checks during startup which will need some time until completed. The checks are necessary to ensure that TinkerTool System can indeed run successfully even if you are using it as a kind of first aid utility on a computer with a partially damaged operating system.

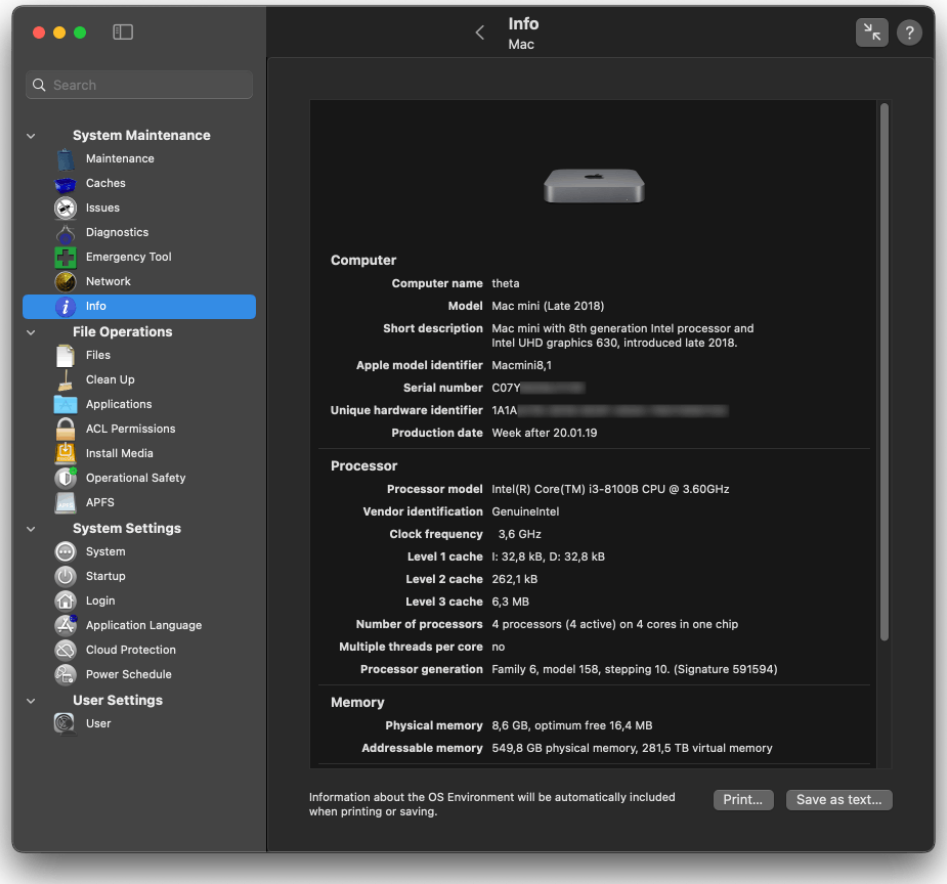


Figure 1.2: The control window of TinkerTool System

TinkerTool System has a long tradition of making its user interface similar to the corresponding version of the System Settings program. On the left is the sidebar, where all the program's functional areas can be found. They are structured as described in in the introduction (section 1.1 on page 1). After clicking on an item, the associated settings pane will appear on the right-hand side of the window. Panes can be further subdivided. Depending on the function, this can be done either by tabs or via sub-items that can be opened via an overview list.

At the top of the sidebar is a search field that you can use to search for a specific feature by keyword. The right-hand part of the window contains the window title at the top, indicating the current pane and any sub-item selected. There is also a button to minimize the window and a button to open context help. These objects are described in the next sections.

You can select a TinkerTool System pane by clicking on its item in the sidebar. Alternatively, you can also use the ↑ or ↓ keys to switch between the individual functional areas. It is also possible to select a pane via the **View** menu. All panes with their corresponding symbols are additionally listed there. You can also use the key combinations ⌘+← or ⌘+→ to switch between the individual panes via the terms **backward** or **forward**. A preference setting (see below) allows you to choose whether this should be understood spatially or temporally. TinkerTool System remembers which card you worked with last time. The next time you start the program, you will be automatically taken back to this point.

1.3.2 Items in the toolbar

In addition to the sidebar, the toolbar at the top of the window is an important element while using the application. At the left, you'll find the common three buttons for closing, zooming or minimizing the window. The icon next to them can be used to hide the toolbar or enable it again. This is useful when you like to focus on a specific program feature and like to the have the largest possible workspace for it.

The free space next to the sidebar icon is reserved for important notices or warnings that affect the entire application. If you see an icon at that location, you can click on it to receive detailed information about a potential issue.

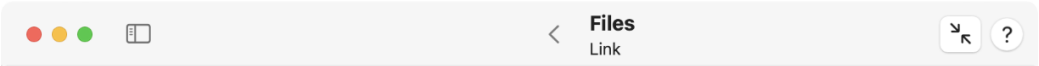


Figure 1.3: Next to the sidebar, the toolbar is an important control element

Approximately at the center of the window, the title of the currently selected pane is shown. If this is a pane with sub-features that are offered via a list (i.e. not via tab items), a second line indicates the name of the respective sub-feature currently selected. The icon < to the left of the title can be clicked to return to the overview again. You can also use the menu item **View** > **Upwards to overview** or press the key combination ⌘+↑. It is also possible to click the respective pane in the sidebar.

The right-hand side of the toolbar contains a button to optimize the window size and an additional button to show the quick context help. Both items are described in more detail in the following sections.

> The toolbar cannot be hidden because it is too important for the operation of the application.

1.3.3 Searching for features by keywords

TinkerTool System offers a large number of different features. For beginners, it can be difficult to know immediately on which pane and in which sub-item a function you are looking for is located. To help you in this case, you can search for features and settings by keyword. Type the search term into the field **Search** at the top left of the window. After each typed letter, TinkerTool System makes suggestions as to which function it could be. The hits are listed in the sidebar together with their associated panes. Depending on the situation, the names of the respective sub-items are also given in parentheses. If the sidebar is too narrow to show the term in its entirety, you can hover over it and all of the text will appear. The pane and the respective sub-item can be opened immediately by clicking on it.

The entered search term can be deleted using the button with the cross in the search field. The sidebar then returns to normal operation.

1.3.4 Minimizing window size

Due to the variety of different functions in TinkerTool System, there are often major differences in the space required by a specific pane in the window. The control window expands automatically if necessary, but you can always enlarge the window yourself by dragging its border, or switch to full screen mode by clicking the green button.

If you want to bring the window back to its optimal size, i.e. set the smallest possible size that TinkerTool System needs to display a certain item, you can click on the button with the two arrows in the title bar of the window. Depending on the currently selected feature, the results will be different.

1.3.5 Context Help

Each pane of TinkerTool System offers a context help panel which can be opened by clicking the round button with the question mark in the upper right corner. A second window will be attached at one of the sides of the main window, displaying short help information for the pane and the sub-item currently open. The help text is structured by the following sections:

- **What it does:** a short description what the feature offered in the opened item will do when you activate it.
- **When to use:** one or more descriptions of typical situations where the feature can be helpful.
- **When not to use:** a list of contraindications when it is not recommended to use this feature or situations where it even can be harmful.
- **Notes:** an optional list of additional notes.
- **Internet information from Apple:** if available, one or more direct links to Apple's web pages which give first-hand, up-to-date information about the topic in question.

1.3.6 The Dock Menu

Some frequently used functions of TinkerTool System can also be activated via the Dock menu: Search for the icon of the application in the Dock, then perform a right-click on the icon to open the context menu. The menu items follow the usual Macintosh standards. If the text of the item does *not* end with an ellipsis character (…), the function will be executed immediately when you select it in the menu. In the other case, TinkerTool System will only open the respective pane and sub-item, so you will have the chance to review settings and to adjust them before anything will happen.

1.3.7 Fields for file system objects

Many features of TinkerTool System work on files and folders. In contrast to other applications, it is often important to know at which exact locations the objects are stored. macOS is using UNIX paths to describe such locations. For this reason, TinkerTool System is using special fields to display file system objects together with their UNIX paths. These fields are a special feature of TinkerTool System and look like this:

Figure 1.4: Path entry field

- At the left side of the field, you see the icon for the selected file system object. This is the same icon the Finder and other applications use to represent this object.
- The top of the field shows the name of the object. It might be translated into your preferred language and file extensions could be hidden.
- The true UNIX path of the object is displayed in a smaller typeface at the bottom of the field. Because paths can become quite long, multiple lines might be used to display a path.
- At the right side, a selection button can be seen. This button will only be available if you are allowed to change the contents of the field. After clicking the button, a standard open panel of macOS will be displayed which allows you to navigate into other folders and to select a different object.

In all cases where TinkerTool System likes you to specify a file system object, you can use any of the following methods to enter the requested data:

- You can click on the selection button if available, as mentioned above. A navigation panel will appear. Alternatively, you can double-click or option-click the field. The latter is especially helpful if you are visually impaired.
- You can click onto the field and enter a UNIX path manually. Note that paths always begin with a leading slash (/). Finish your data entry by pressing the key ↵.

- You can drag a single object from the Finder into the field.

1.3.8 Understanding when Changes Take Effect

When you are using TinkerTool System to modify a system setting of macOS, it tries to let the changes take effect immediately. Note that macOS may ask you to enter name and password of an administrative user first before the actual change takes place. You see that the change has been applied successfully if the user interface keeps its new state, e.g. a check mark you have set "sticks," or a radio button you have clicked keeps the marker in its new position.

For features which do not affect a simple setting but actually execute some operation, for example to delete a selected file, TinkerTool System will show a dialog sheet after the operation has been completed. The sheet will confirm whether the operation was successful or whether it has failed for some reason. More complex operations which might run for several minutes are accompanied by a textual report, displayed either during the operation, or after it has completed, depending on technical situation. The reports can be saved into text files, or be printed for future reference.

1.3.9 General Settings

TinkerTool System supports a few general settings which control some basic policies. You can modify them by selecting the menu item **TinkerTool System** > **Settings**... or by pressing ⌘ + , .

Pane Control

Setting a check mark for the option **Automatically open last used pane when starting** has the effect that the application will remember the pane which was active the last time when you have used and then quit the program. TinkerTool System will automatically switch to this pane and the correct tab item or sub-feature the next time it is started.

The arrow buttons, keys, or menu items allow you to switch between the different panes in the order they are shown in the window. This means you navigate *by position*. In many other applications, e.g. web browsers, the arrows allow you to go backward or forward *in time* instead, following the order how you had selected the items in the past. If you rather prefer this kind of approach, enable the option **Arrows navigate through history**.

As mentioned, most panes are designed, similar to System Settings, in such a way that you have some kind of main menu with a list of sub-features you can access. If you are guided to the previously used feature when launching the application or browsing through different panes, it can be confusing for inexperienced users that you'll only see the last used sub-feature and not all features of that pane. The option **Always return to overview instead of sub-feature (if applicable)** can modify this behavior. Each time when switching to a different pane, its overview with the list of sub-features will become visible. This option is enabled by default as of version 8.4 of the application, but can be disabled again any time if desired.

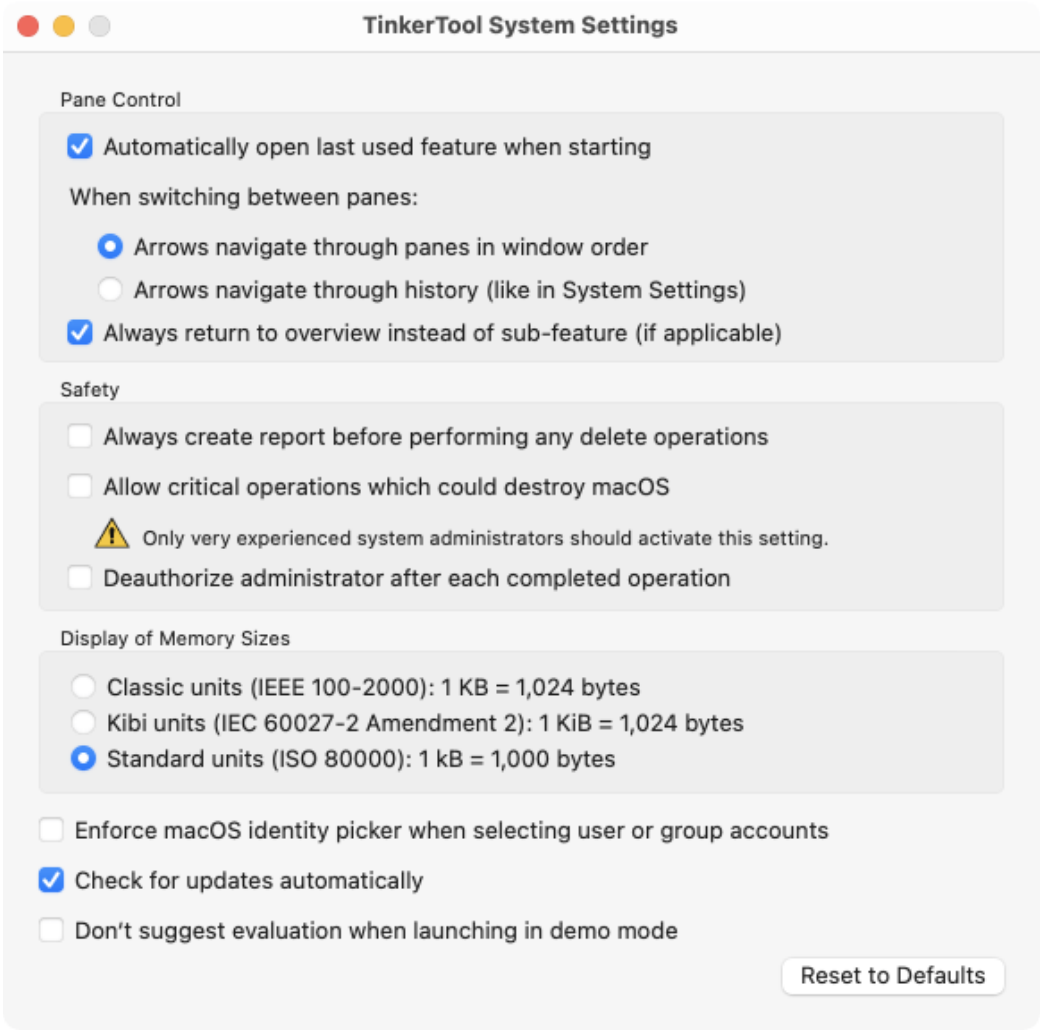


Figure 1.5: The settings window

Safety

The option **Always create report before performing delete operations** controls if TinkerTool System should display a confirmation dialog before removing objects from the file system. It applies mainly to the pane **Clean Up** and to a few other features where TinkerTool System might delete files from folders unknown in advance. In the confirmation dialog you can preview what TinkerTool System will do and which files will be lost after the delete operation has been executed. You can either cancel the entire operation, or deselect particular files or folders from the deletion set. It is recommended to keep this preference setting switched on. Switching it off causes TinkerTool System no longer to wait for confirmation but to remove files immediately. The pane **Clean Up** has additional switches to override this policy for single operations, however.

> The option does not apply to all delete operations. When removing cache files, tens of thousands of files might be affected, so a confirmation for each file would not be useful.

TinkerTool System contains a safety mechanism which tries to detect if you are about to make modifications which could make the whole operating system unusable. Examples are the change of permission settings for files which are part of the operating system, or removing files which belong to macOS. In these cases, changes could cause TinkerTool System or the whole computer no longer to work correctly, so it would also become impossible to revert such a change without reinstalling the whole system.

Very experienced administrators can disable this safeguard, setting a check mark at **Allow critical operations which could destroy macOS**. After this, TinkerTool System will no longer block dangerous file operations. The administrator alone will be responsible for any actions performed.

> 
> It is not recommended to enable this feature. Total data loss can occur. You should know exactly what you are doing when the safeguard is inactive.
>
> You must not understand this safety feature as a guarantee that TinkerTool System cannot be misused to damage important user or system files even if it is left at its recommended setting.

The option **Deauthorize administrator after each completed operation** controls if TinkerTool System should cache and reuse name and password of an administrative user after these credentials have been entered correctly and no more than 5 minutes have passed since the last successful authorization. For further details, please see the chapter The security policy of TinkerTool System (section 1.2 on page 3).

Display of Memory Sizes

The buttons in the box **Display of Memory Sizes** allow you to select how the program should round the number of bytes whenever it needs to represent the size of storage space or main memory:

- **Classic units** use the old common practice of information technology to report memory sizes in multiples of powers of two. 1 kilo byte equals 1,024 bytes. Kilo is abbreviated by a capital K in this case, denoting that it refers to a binary interpretation and does not represent the usual decimal prefix with the meaning 1,000 here. Higher multiples (1 MB = 1,048,576 bytes, not 1,000,000 bytes) don't make this differentiation, however.
- **Kibi units** resolve this ambiguity by additionally marking the prefix with "bi," indicating a binary prefix. 1 kibi byte (1 kiB) equals 1,024 bytes. 1 mebi byte ("megabinary," 1 MiB) are 1,048,576 bytes.
- **Standard units** enforce compliance with "correct" international conventions for quantities and units. 1 kilo byte equals 1,000 bytes, now abbreviated 1 kB. 1 mega byte (1 MB) represents 1 million bytes.

The option **Standard units** is the recommended default for macOS, because many of Apple's applications (unfortunately not all) use the same policy for the display of memory sizes.

Other preference settings

TinkerTool System contains several features where you need to choose a user or a group from the list of accounts available on your Mac, e.g. to change the ownership of a file. In professional network environments, the list of user and group accounts may not be hosted on your Mac alone, but also on one or more *directory servers* in the network. This way, your Mac can work with several thousand user accounts that are known in your network. However, some versions of macOS are affected by performance problems when working with such external account lists. Because TinkerTool System likes to present the complete list of users or groups in situations where you need to select an account, retrieving these lists can take a considerate amount of time. Some versions of macOS may even block the entire user interface for several minutes due to internal design flaws in the way the operating system collects the necessary data.

To avoid such problems, you can force TinkerTool System to use a very simple user interface when it is necessary to choose an account from a list of available users and groups. Set a check mark at **Enforce macOS identity picker when selecting user or group accounts** to use the built-in features of macOS only.

> If the simple account window also has performance problems, this will indicate that this macOS version currently cannot handle this more efficiently.

Apple's account window has the following disadvantages, however:

- It is not possible to preselect an entry to guide you in a specific situation.
- You have to decide from context whether to select a user account or a group account.
- You cannot see the internal identifications of the accounts, only their presentation names.
- You cannot access any system-internal accounts.

The setting **Check for updates automatically** controls whether the application should automatically inform you when new, free updates of the software become available. The automatic check will be performed in regular intervals while you launch the program.

The preference **Don't suggest evaluation when launching in demo mode** only applies if you don't own a valid registration for TinkerTool System. Under normal conditions, TinkerTool System will offer to let you test the application during a limited period for free, which is called *evaluation mode*. When setting a check mark for this option, TinkerTool will no longer make this offer upon each launch (if still available), but directly switch to the locked demo mode. For more information about demo mode, unlocking TinkerTool System, and evaluation mode, please see the respective chapter (section 7 on page 323).

The button **Reset to Defaults** will reset all of the preferences discussed in this section to their recommended default settings. Only the option for update notification will keep its value.

1.3.10 Reverting All Permanent Changes to System Settings

Among the many features of TinkerTool System is the capability to modify system settings built into macOS. When experiencing system problems, you might like to reset all settings to Apple's factory defaults. This is possible by selecting the menu item **Reset** > **Reset all permanent changes**... or pressing the key combination ⇧ + ⌘ + R and following instructions.

This step is also helpful after you have tested TinkerTool System without license in evaluation mode but the evaluation period is over. In this case, TinkerTool System will fall back to demo mode and you can no longer use it to revert system settings you might have changed. The reset feature however will always remain functional, no matter if you are going to purchase a license or not. This makes sure you cannot be locked out from certain settings after the evaluation has ended.

> Note that it is not possible to differentiate which system settings have been changed by TinkerTool System and which have been changed by other third-party applications or by using the macOS command-line. For this reason, TinkerTool System must reset all system settings *it could have changed theoretically* to factory defaults, even if you didn't use it, but something else to make the initial changes. Disabling support for IPv6 is excluded from this rule, because you have full control over this setting in **System Settings** after TinkerTool System has switched the respective option to off.

1.3.11 Searching for Software Updates

TinkerTool System is under continuous development and new versions will be published in irregular time intervals. These updates are usually free unless a completely redesigned product will be released. The latest version is always available for download via the official web site. TinkerTool System can check if a new free update is available for the version you are currently using. To do this, select the menu item **TinkerTool System** > **Check for Updates**. The program will connect to the Internet and inform you about the results. In case a newer version is indeed available, you can choose to open your web browser to be automatically guided to the download page. Instead of performing a manual check by clicking the menu item, you can alternatively enable a preference setting (see above) to let the application perform automatic checks in regular intervals.

> The program does not support any auto-download mechanisms because such features usually do not work and should not work in professional environments where all applications are stored on protected file servers. Automatic replacement of software products might neither comply with security regulations of large organizations, nor with the laws of certain jurisdictions.

1.4 System Integrity Protection

1.4.1 Technical Background

The operating system is protected by a security feature called *System Integrity Protection*. At the technical level, this is also known as *Customer System Restriction (CSR)*. For marketing purposes, Apple also uses the term *rootless*.

System Integrity Protection means that only specific programs of the operating system itself, for example the **Apple Installer**, have permission to modify certain files of the operating system or to use certain features. Not even the highest system authority, the *root* user account can circumvent this restriction. This policy makes sure the system cannot be damaged, or intentionally manipulated by an attacker. Access to the following resources is restricted by System Integrity Protection:

- The modification or deletion of operating system files which are marked with the special attribute *restricted*.
- The modification or deletion of specific NVRAM entries.
- The use of kernel extensions which are not trusted.
- Running the kernel debugger.
- Tracing the execution of specific system processes with the *dtrace* utility.

Some features of TinkerTool System can be affected by System Integrity Protection. For example, when you disable the preference setting **Allow critical operations which could**

destroy macOS and you try to use the function **Files** > **Force Delete** to remove a file which has the attribute **restricted** set, the delete operation will be prevented by macOS. In such cases, TinkerTool System will show an error message as follows:

"Your computer is configured not to permit this operation. The current task cannot be completed because System Integrity Protection is active on this computer. It might be possible to deactivate this feature by changing a hardware setting via the recovery operating system. Please see the reference manual for more information."

System Integrity Protection can be switched off if the owner of a computer prefers to do so. To be effective, System Integrity Protection has to protect itself, however. This means switching this feature off is not possible within the running operating system. In addition, the setting is not stored in any file, but in the system hardware. In case you have installed multiple copies of macOS on your computer, the setting will take effect for all of them.

1.4.2 Disabling Protection

If you need to disable System Integrity Protection for some reason, you can do so as mentioned in the previous section. Perform the following steps:

> The steps are slightly different depending on the processor type of your Mac. If you are not sure whether you are using an Intel processor or Apple Silicon, you will find that information on the sub-item Mac of the Info pane (section 2.10 on page 121) of TinkerTool System.

1. *If you are using a Mac with an Intel processor:* Restart (or switch on) your computer and hold down ⌘ + R to select the Recovery System. You can release the keys when the Apple logo appears. *If you are using a Mac with Apple Silicon:* Make sure your Mac has a connection to the Internet. Switch the computer on by using the power button and hold this button until you see a screen with startup options. Select the item **Options**, which contains a gear icon, then click **Continue**.

2. Depending on the security features active on your Mac, the window **Recovery Assistant** may appear. If it does, follow its instructions to log in as administrative user.

3. Wait until the screen **macOS Utilities** appears, then select the menu item **Utilities** > **Terminal** to launch the Terminal application.

4. Enter the following command in Terminal to disable System Integrity Protection for the entire computer. Press the return key afterwards:

```
csrutil disable
```

> We don't recommended to disable this feature.

The change will take effect after you have restarted the computer. You can restart the system via the corresponding menu item in the Apple menu.

To re-enable System Integrity Protection later, you can use the same steps with the command

```
csrutil clear
```

1.5 Privacy Policy Settings of your Mac

1.5.1 Background Information

As of version 10.14 of the operating system, Apple has added another level of system protection: Nearly all applications are now running in a *sandboxed* environment, which means that each and every request an application sends to the operating system is monitored and checked before it will be executed. Not only Apps from the Mac App Store, but all other software as well, including some of Apple's own applications, are no longer free in executing any command that would otherwise be authorized by user permissions. Access to data that could affect system security or a user's privacy needs explicit approval by an administrator of the Mac first. This approval is granted per program. For example, the administrator could say "program A has permission to access a user's Photos database". Such a privacy definition will then become valid for the entire computer and any user account, for all copies of program A. If program A is running while its privacy settings are changed, the program must be restarted before the new policy takes effect.

The settings for privacy policy are a powerful tool to prevent applications from accessing critical data behind the user's back, no matter whether intentionally or unintentionally. This is especially true for unwanted applications such as adware, computer viruses, Trojan Horses, or other types of malware. However, this additional protection comes with additional work for administrators. After new software has been installed, it should be checked whether the application needs access to protected parts of the Mac in order to fulfill its duties. If the necessary approval is not granted, the affected application cannot execute specific operations. Such operations may either silently fail, or they are stopped with an error message. The necessary approval must be given by an administrator and the application must be restarted.

1.5.2 Privacy Settings affecting TinkerTool System

As the name indicates, TinkerTool System is a an application designed to perform system-related tasks. Some of the areas that can be accessed by TinkerTool System are critical to the users' privacy, e.g. the application is capable of determining the size of the Spotlight index database. The Spotlight index contains information about all files of all users, and parts of this data may be related to persons, or could be confidential, so it is protected by macOS. Without prior approval, TinkerTool System cannot "see" the Spotlight index or its size at all.

TinkerTool System uses special precautions to check whether a certain operation *could* be blocked by macOS due to privacy settings *before* that operation is about to be executed.

This way, “silent failures” should be avoided. TinkerTool System won’t erroneously pretend that an operation was apparently successful although that operation might have been completely blocked by macOS and actually nothing happened at all. In such cases, TinkerTool System shows specific error messages with detailed information which approval needs to be granted before the affected feature can be used.

A special warning marker with a red shield will appear in the title bar of the control window when TinkerTool System detects that basic features of the application won’t work as expected due to the current privacy settings. If you click on this marker, TinkerTool System will show in detail which areas are affected:

- **Full disk access for your user account:** The application cannot access critical files during standard operations which don’t require special privileges.
- **Full disk access during privileged operations:** The application cannot access critical files while executing privileged operations that require you to authenticate as system administrator.
- **Access to other volumes:** The application cannot access data located on secondary volumes, e.g. external disk drives or network file servers. All volumes which are not the system volume (hosting the operating system and your local home folder) can be affected.

If you see the red shield button in the title bar or any of the detail items have a red warning indicator, you should change the privacy settings of macOS using the instructions given in the next section. You can still operate TinkerTool System without doing this, but then some features could fail with an error message.

1.5.3 Changing the privacy settings

In order to use all features of TinkerTool System, the following privacy approval must be granted:

- **Full Disk Access**

If you like to approve full disk access for TinkerTool System, perform the following steps:

1. Launch **System Settings**.
2. Open the pane **Privacy & Security**.
3. Select the item **Full Disk Access**.
4. Check if an entry for **TinkerTool System** is in the table. If yes, set a check mark next to it. If no, click the button **+** below the list of apps and add TinkerTool System to the table.
5. Relaunch TinkerTool System.

1.6 Integrating TinkerTool into TinkerTool System 9

1.6.1 Enabling Integration

TinkerTool System uses some of the technologies found in the free sister product *TinkerTool*, an application to view and edit selected personal preferences, settings which Apple is offering for advanced "pro" users as part of macOS. TinkerTool and TinkerTool System do not overlap in any way, so administrators who like to have access to the full feature set of the two applications must copy both programs to their computers.

All features of TinkerTool can be accessed from within TinkerTool System if users like to do so. In this case, the panes of TinkerTool become plug-ins of TinkerTool System. It is still necessary that both applications are present on the computer. "Present" means that TinkerTool System can access the files of TinkerTool via a known folder. It is not necessary to place the programs into the same folder. You can use different folders, different disk drives, or even different computers (using network sharing).

To integrate the panes of TinkerTool into TinkerTool System, perform the following steps:

1. Launch TinkerTool System.
2. Select the menu item **View** > **Add Panes from TinkerTool**….
3. Navigate to the copy of TinkerTool which should be integrated. TinkerTool System will automatically search for the latest version present on your computer and will offer it as suggestion. Because it is possible to have several different copies installed simultaneously, this might not always be the preferred choice, however. Press the **Open**… button to confirm the correct selection.

After a few seconds, all panes of TinkerTool appropriate for your computer and operating system version will additionally appear in the section **User Settings**. The integration behaves like a user preference and will be maintained upon each start. This also means each user is free to choose if the connection between the two programs should be used or not. Each user account has the additional freedom to integrate different copies of TinkerTool if necessary.

Due to the large number of different variants of TinkerTool and TinkerTool System, some limitations apply regarding the question which variants can be combined with each other. *TinkerTool System 9* and later can integrate copies of *TinkerTool version 10* and later.

> TinkerTool System doesn't support operation in mixed languages due to internal restrictions of macOS and to avoid confusion. For example, if your primary language is French, TinkerTool will run with a French user interface as standalone application, but it will only run in English or German when integrated into TinkerTool System, because TinkerTool only supports these two languages. To control your personal priority of languages, open **System Settings** and go to **General** > **Language & Region**. You can add languages to the table **Preferred languages** and reorder them as desired.

1.6.2 Disabling integration

The connection between the two applications will be detached automatically when the bound copy of TinkerTool can no longer be located in the folder chosen by the user. For security reasons, TinkerTool System will not try to track whether the application might have been moved to a different folder. To detach TinkerTool manually, select the menu item **View** > **Remove TinkerTool Panes**. The change will take effect immediately. It is not necessary to restart the program.

Chapter 2

System Maintenance

2.1 The Pane Maintenance

2.1.1 Clear Directory Cache

macOS contains a background service which communicates with the directory services configured for your system. This service is the central information broker needed to collect data about users, computers, IP addresses, user groups and many other things relevant to an operating system. Under special circumstances, the internal memory contents of this service may contain incorrect or outdated information, especially if your computer is accessing a name server or directory server which doesn't work reliably, or if the network configuration has changed abruptly. This can result in unexpected delays (spinning rainbow cursor) especially when using network functions.

In this situation, clearing the online cache of directory services might correct the problem. The information broker will begin with fresh new data which it fetches from your network and the local computer. Note that this cache is not stored in any file. It is kept in the memory (RAM) of the directory services subsystem of macOS.

> The word "directory" is sometimes used as a technical term for a folder storing files. This is not what is meant here. In this context, the word directory refers to an inventory list of names, objects and network addresses relevant to your computer. macOS is always running a directory service no matter whether the computer is connected to a network or not.

When retrieving data about names and network addresses of other computers, the directory services are not the only source of information which keep records in their internal cache memory for some time. The system service acting as "DNS resolver," responsible for finding addresses for computer names and vice versa, assists the directory services in doing their job. When you clear the memory cache, you can decide whether only the records of directory services as such should be cleared, or if cached DNS information should be removed as well.

To clear the directory cache of macOS, perform the following steps:

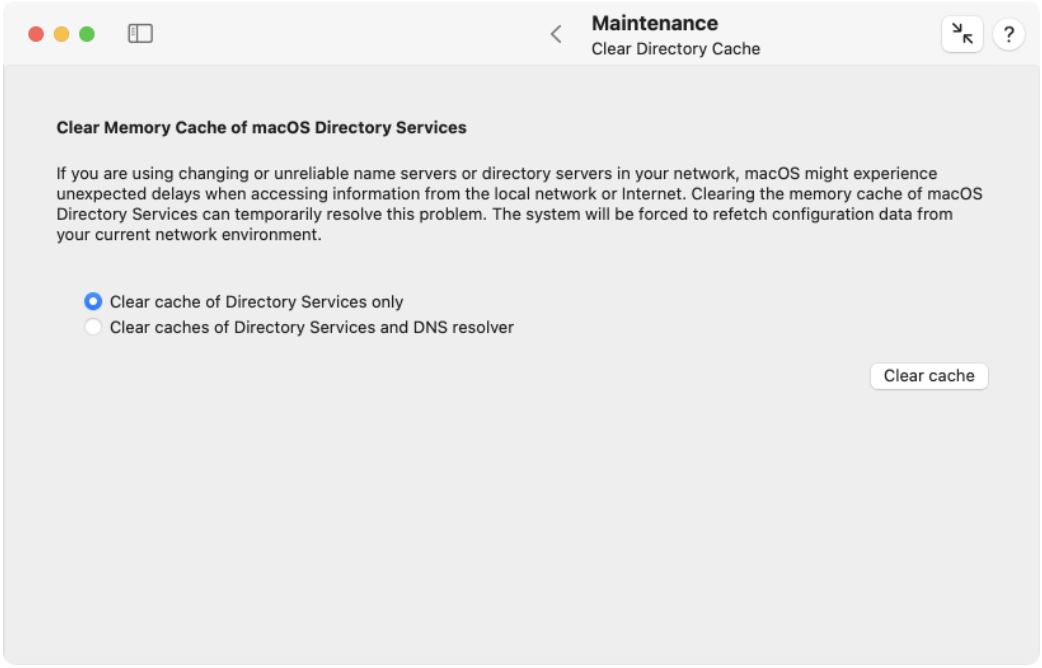


Figure 2.1: Clear directory cache

1. Open the sub-item **Clear Directory Cache** of the pane **Maintenance**.

2. Select one the radio buttons to indicate if the cache of the DNS resolver should be included in the cleaning operation.

3. Click the button **Clear Cache**.

2.1.2 Export directory data

As mentioned in the last section, directory services store important data about the local computer. Such a database is called a *directory node*. In professional networks, it is common not only to have a directory node on each computer, but also having one or more central databases managed by special directory servers. This allows to implement network-wide user accounts, for example, so that a user can log in to any computer in the network, while maintaining uniform file permissions for use on all disks and file servers.

When a change in the organization of the directory data should become necessary, e.g. because a new computer or a different operating system must be used, it is helpful to export specific types or all directory data from a directory node in order to reuse it on the other system. TinkerTool System supports such an export procedure. It can read all data types supported by Open Directory from all directory nodes bound to a Mac, and save the records to a text file.

Apple announced in April 2022 they would no longer support the software *macOS Server*. This app included a service to provide network-wide directory data via an *Apple Open Directory Server*. If such a server has to move to another operating system in the future, TinkerTool System can help to save its previous data so that all information can still be utilized without modification.

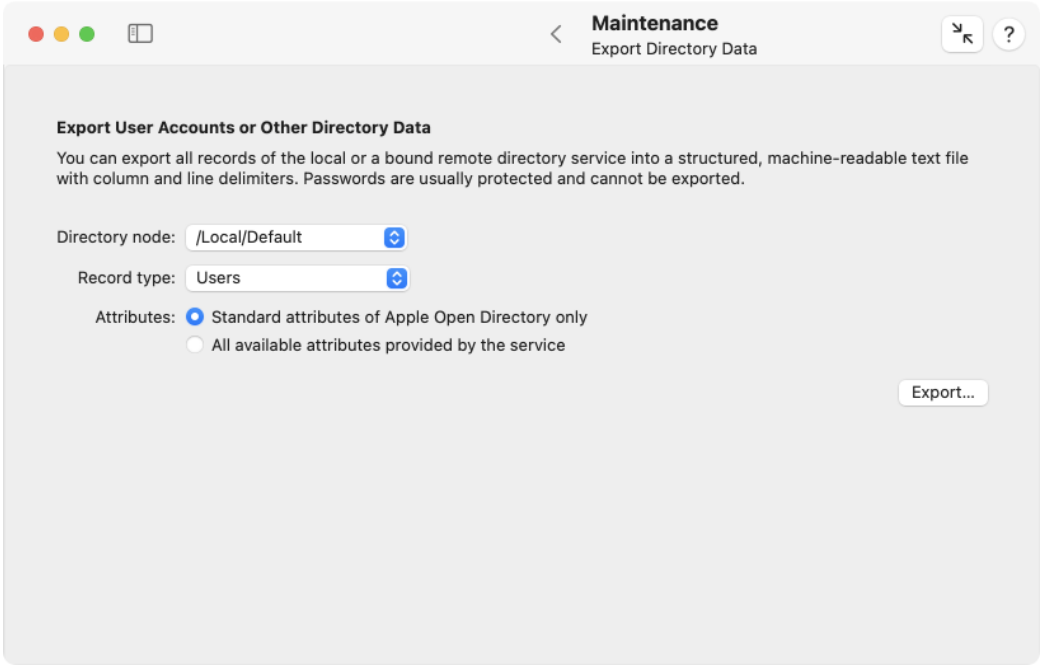


Figure 2.2: Exporting directory data

To export directory data to a text file, do the following:

1. Use the pop-up button **Directory node** to select the service to read data from. The local database of macOS always has the name **/Local/Default**. All other directory data sources compatible with macOS this Mac is currently connected to are automatically listed and can also be selected using their official Open Directory node search paths.
2. TinkerTool System automatically determines which data types are provided by the selected directory node. Choose the type of data to export under **Record type**.
3. Determine whether to export only the common attributes of the selected data type that are dictated by the Open Directory standard, or whether to include all attributes that are “understood” by Open Directory.
4. Click **Export**... and select location and name for the destination file.

If the export is successful, TinkerTool System will automatically open an inspection window after the file was saved. The window contains a table indicating which exact data has been saved, and is designed to provide a final check. The header fields of each column contain the official attribute names currently in use by the directory service. If attributes have been exported that don't contain any text, they will be marked as **Binary Data** and are not evaluated further in this window.

> The second step, i.e. the import into another operating system, usually has to be hand-tailored, so that software like TinkerTool System cannot help here. However, the generated text file has a machine-readable table structure that can be processed with usual standard tools for table or word processing. Experienced system administrators can usually customize the data in a few steps so that the information can be read by other computers. This way, Open Directory data can be imported into a database based on Microsoft Active Directory, Azure Active Directory or a Unix server with an LDAPv3 database according to RFC 2307, for example. Depending on version, target systems with macOS may offer the *dsimport* command to process the text file immediately without any intermediate steps.

2.1.3 Locate Database

Because macOS is a UNIX system, it comes with the program *locate*, a command-line application which quickly finds files by their names or parts of their names. *locate* usually finds names more quickly than Spotlight and includes both visible and invisible files in its search. Like Spotlight, *locate* needs an internal database to do its job. This database is updated in regular intervals to ensure that the program has current information about new and deleted files.

Because most users don't work with macOS command-line programs, the automatic service that updates the locate database is switched off by default. Only administrative users are allowed to check whether the service is on or off. Perform the following steps to see if the update service is active or not:

1. Open the sub-item **Locate Database** of the pane **Maintenance**.

2. Click the button **Show current status**.

The current state will now be displayed by the check mark at **macOS should update the locate database periodically**. You can now either set the check mark to activate automatic maintenance of the database, or remove the check mark to shut down this service.

In a default installation of macOS, the system will update the locate database automatically each Saturday at 3:15 a.m. If your computer is off or in sleep mode at that time, the update is automatically postponed to a later date where the system is active. To enforce an immediate update of the locate database "now," click the button **Update database now**.

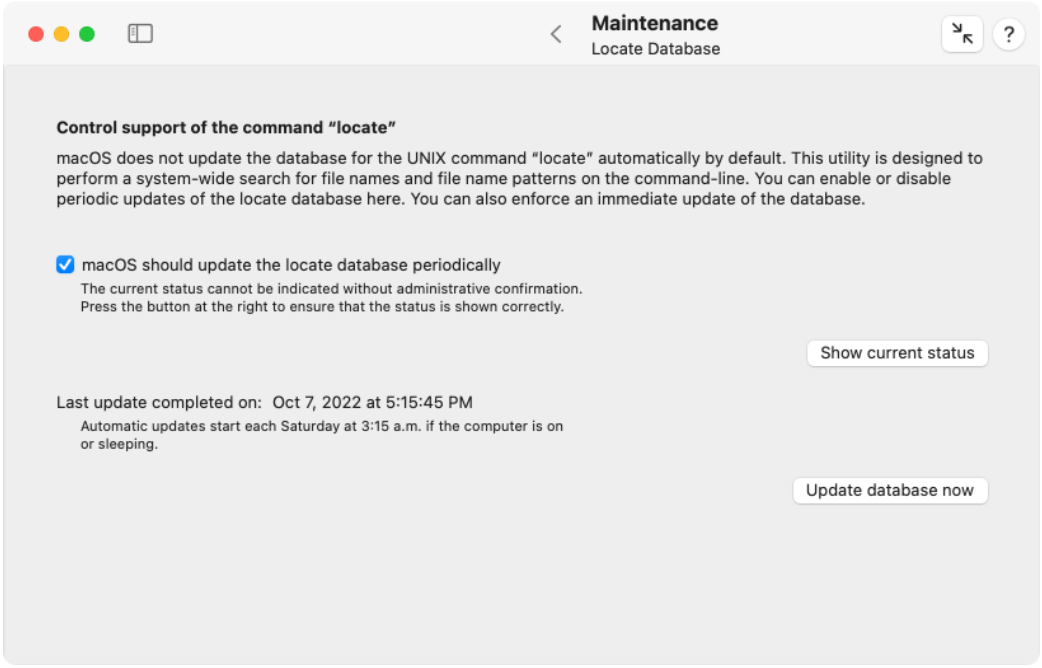


Figure 2.3: Locate database

2.1.4 Antivirus

For many years now, Apple has provided a built-in anti-virus program called *XProtect* as part of macOS. XProtect secures macOS against common computer viruses and malicious software (malware). The software is typically updated by Apple every two weeks in fully automatic fashion, assuming you have not explicitly disabled the option **Install security updates and system files** under **General** > **Software Update** > **Automatic Updates** > **i** in System Settings.

It's part of XProtect's design principle to work completely under cover. Apple does not advertise the program, nor does it point out its existence or activities on its own. However, many users would like to know if XProtect is properly enabled, what exactly it does in the background, and whether the latest version of the program is installed. All this information can be obtained by selecting **Antivirus** on the **Maintenance** pane.

At the top of the **Antivirus** section, under **Current Status**, you can see which version of XProtect is installed and when the last update was performed by your computer. The version code typically increases every two weeks by at least one digit. The status indicator **Launch scanner** indicates whether XProtect will be activated upon each program launch to check the integrity and secure origin of the respective application. The **Background scanner** indicator shows whether XProtect independently searches for known malware in the background, when given a suitable opportunity.

The data in the box **Available Software** can only be shown after you have clicked the

button **Check Apple Server**. After that, you will see the latest version of XProtect that Apple currently offers for your macOS version and since when this is the case. If there is a discrepancy between the published and installed versions, you can click on the **Immediate Update** button to force macOS to download and install the most up-to-date version "now".

> Additional information about XProtect can also be found in the chapter The Pane Info (section 2.10 on page 121). On the Info pane, Apple's list of viruses and malware recognized by XProtect can be retrieved.

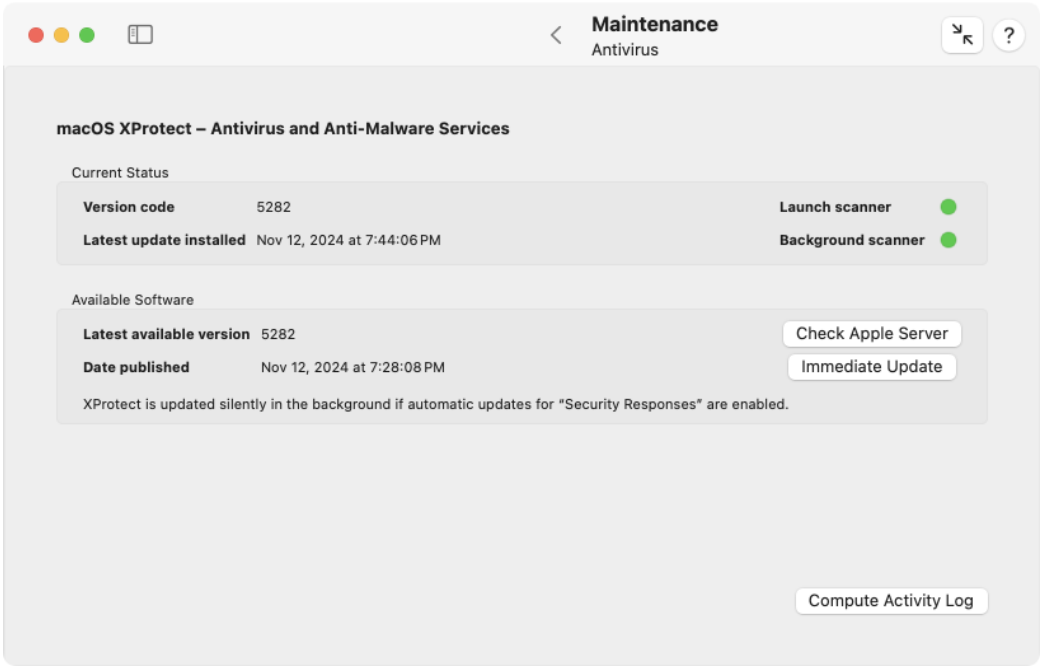


Figure 2.4: Antivirus

Finally, there is also the button **Compute Activity Log** available. Using this, you can retrieve the entire log of XProtect, currently stored in the macOS log database of your computer. This includes all background activities, updates, errors, warnings, and status messages. Administrator rights are required to obtain the protocol. Please note that macOS keeps the protocol in English only.

2.1.5 Shared User Folder

macOS provides a special folder on the system volume which can be found at **Users** > **Shared**. The folder is designed to be utilized by all accounts of a Mac, sharing files locally for common usage. Sharing of data is made possible by specific settings that grant read

and write permissions to everyone. At the same time, other settings ensure that only the creator (and hereby owner) of a file has the right to delete this file at a later time, without the risk to inadvertently remove data of others users.

Many applications by Apple and other vendors use this folder as well, to automatically save data that could be interesting to all users. This includes license or registration data. For example, the application Music uses hidden contents in this folder to store licensing information for the use of copyright-protected media.

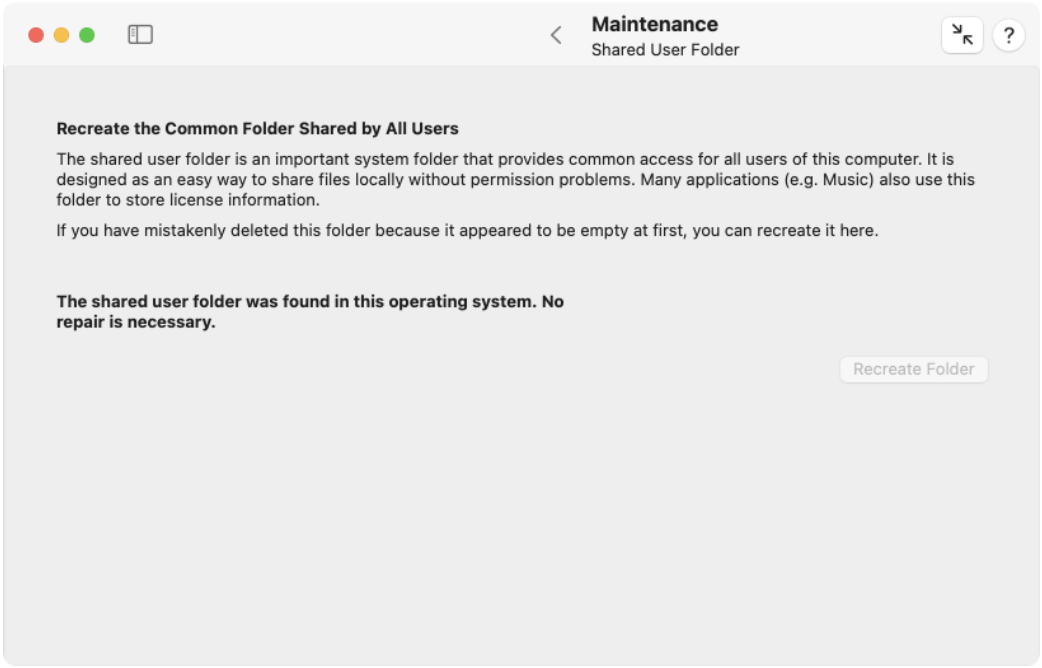


Figure 2.5: Shared User Folder

Some users remove this important system folder because it is initially empty and appears to serve no obvious purpose. This can lead to failures and errors in many applications, however. Due to the special settings for this folder, it is not easy to recreate it correctly.

TinkerTool System checks whether the folder exists on your Mac. If not, you can choose to recreate it in its correct original form, hereby repairing the operating system.

1. Open the sub-item **Shared User Folder** of the pane **Maintenance**.

2. Click the button **Recreate folder**.

2.2 The Pane Caches

2.2.1 Introduction to caching

Nearly all applications running on macOS make use of file caches. These caches are small files which store precomputed or prefetched information needed very often. By "remembering" and reusing previously requested results, applications can be accelerated significantly. They just access the already known data in their cache files, and don't need to recompute or to refetch the information. The data stored in cache files can include, for example, the last few Internet web pages an application has accessed, photos of buddies you chat with, or the data to quickly display your Desktop image, already decompressed, scaled and optimized for your display.

Many applications are not actually "aware" that they are using cache files because macOS may create the caches automatically when the programs initially request data via the operating system. This typically occurs in cases where macOS knows in advance that caching will speed up similar requests later on. For example, each program supporting a "check for updates" feature will usually contact a specific web server to fetch status information. If this is done using standard system procedures, macOS will automatically create a web cache for this application and the affected user account in order to accelerate access to its update server. The application does not really "know" this, but will receive the requested information via macOS more quickly than usual.

Caches are responsible for very significant speed gains, but problems can arise if a cache becomes corrupt. A corrupt cache can contain incorrect, outdated or otherwise unusable information, and any of these conditions can cause very strange effects in the applications using it. Under normal circumstances, macOS or the affected applications should detect corruption within the cache, discard the cached information and automatically rebuild the cache when new data is requested. However, this detection function might not always work in practice, especially after a network connection has been interrupted, after a program has crashed, or when your computer has had problems with its clock, rendering it unusable to track which cached information is up-to-date and which is outdated.

Due to the hidden nature of caches, problems resulting from corruption are very difficult to find. You, the user, only see that "sometimes something is very wrong with some applications." If you experience strange problems with an application, it could be the result of a corrupt cache, but you cannot be sure. The simple, brute-force (and quite possibly harmful) method used to determine whether a cache is corrupt is to delete all the cache files, restart the application, and see if the problem disappears. If it does, you're in luck; if not, you will have lost that valuable data stored in the caches. It may take hours, days, or even weeks before your system has recovered by rebuilding the caches with the recomputed and refetched information. During this recovery period, the computer may run significantly more slowly than usual.

Although cache cleaning can be an effective maintenance step to resolve specific problems, it can have, as we have seen, harmful side effects. For this reason, TinkerTool System introduces a more intelligent approach: You can temporarily deactivate caches, assess whether doing so has a positive effect, and reactivate them if it does not. This more sophisticated approach effectively avoids the problem of cache cleaning often making the

original problem worse.

> Some Internet sites recommend cache cleaning (which is actually just *cache deletion)* as a regular or even scheduled maintenance step. This recommendation is highly irresponsible. We strongly advise you **not** to follow it. Cache cleaning always has the negative side effect of slowing down your computer. It should only be used as a last resort when troubleshooting a well-defined problem, and knowing ahead of time that the positive results will indeed outweigh the negative effects of losing cache data.

2.2.2 Unprotected and Protected Caches

TinkerTool System offers smart deactivation for the following cache category:

- Personal standard caches of the current user

Three other cache categories can only be cleaned, not deactivated, because smart deactivation is prevented by *System Integrity Protection* (section 1.3 on page 8) of macOS:

- Personal high-speed caches of the current user (see the next paragraph),
- System-wide caches used when computer-related information relevant to all users is stored.
- Internal caches of the operating system independent of users and computers.

In professional environments, the private home folders of users are usually stored on a central file server, not on the individual hard disks of local computers. Because network access is typically a bit or even significantly slower than access to a local disk, macOS keeps all caches where fast access is important in a separate area on the system disk. TinkerTool System refers to them as *high-speed caches*. They are used for Internet browsing or for temporarily storing thumbnail images, for example.

2.2.3 Using the Cache Maintenance Functions

Smart Cache Deactivation

Smart deactivation of caches as a troubleshooting procedure is done using the following steps:

1. Define for yourself what exact problem –possibly caused by a corrupt cache– you have to fix. Find a program where you can reproduce the exact problem and test whether only one user account or all user accounts on the computer are affected by it.
2. Start TinkerTool System and open the item **Caches** > **Unprotected Caches**. Click the button **Deactivate caches**.

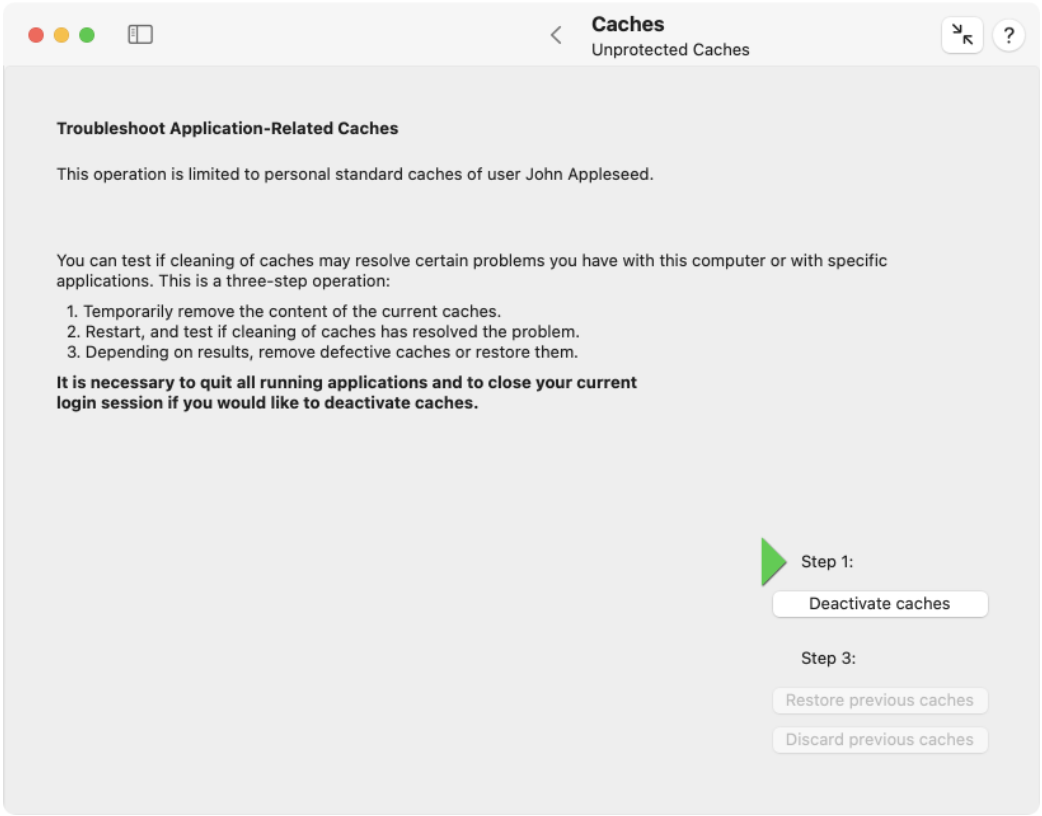


Figure 2.6: Unprotected caches

3. TinkerTool System will ask you to quit all running applications. You can also have TinkerTool System do this automatically for you. The program will then perform a logout.

4. Log in to the system again (with the same user account used in the previous steps). TinkerTool System will start automatically, giving you the option either to restore the caches or to discard them. Keep the application running.

5. Test if the problem you defined during the first step has indeed be resolved by deactivation of the caches. If yes, you might accept the harmful effects of losing the cache data. In this case, click the button **Discard previous caches**. If no (the problem was not fixed and can still be reproduced as before), click the button **Restore previous caches**. In the latter case, TinkerTool System will again perform a log out, and all selected caches will be returned to their previous states. You won't have negative side effects.

Additional Notes

TinkerTool System tries to guide you automatically through the smart deactivation process. A short summary of the instructions, and a large green arrow marker are used to visualize in which state the computer is in. Additional status messages and notes are given in bold face in the lower left corner of the pane.

You should not postpone the decision to restore or discard the caches. Please make the decision as soon as possible.

Cache Cleaning (Protected Caches)

To clean a cache category completely, deleting all its data, perform the following steps:

1. Open the sub-item **Protected Caches** on the pane **Caches**.

2. Select the cache sets which are causing the problem.

3. Click the button **Clean Caches**.

> Remember that cache cleaning should be avoided whenever possible. It will cause your system to run significantly more slowly for some time. Only use cache cleaning as a last resort, if you know for sure that the contents of a specific cache category are causing a technical problem.

2.2.4 Font Caches

macOS uses a specialized background service for font management, the *font registration server*. This background program is responsible for finding out which fonts are available on your system, keeping track of which user has activated which fonts, determining which of the more than 200,000 character glyphs supported by macOS are available in each of

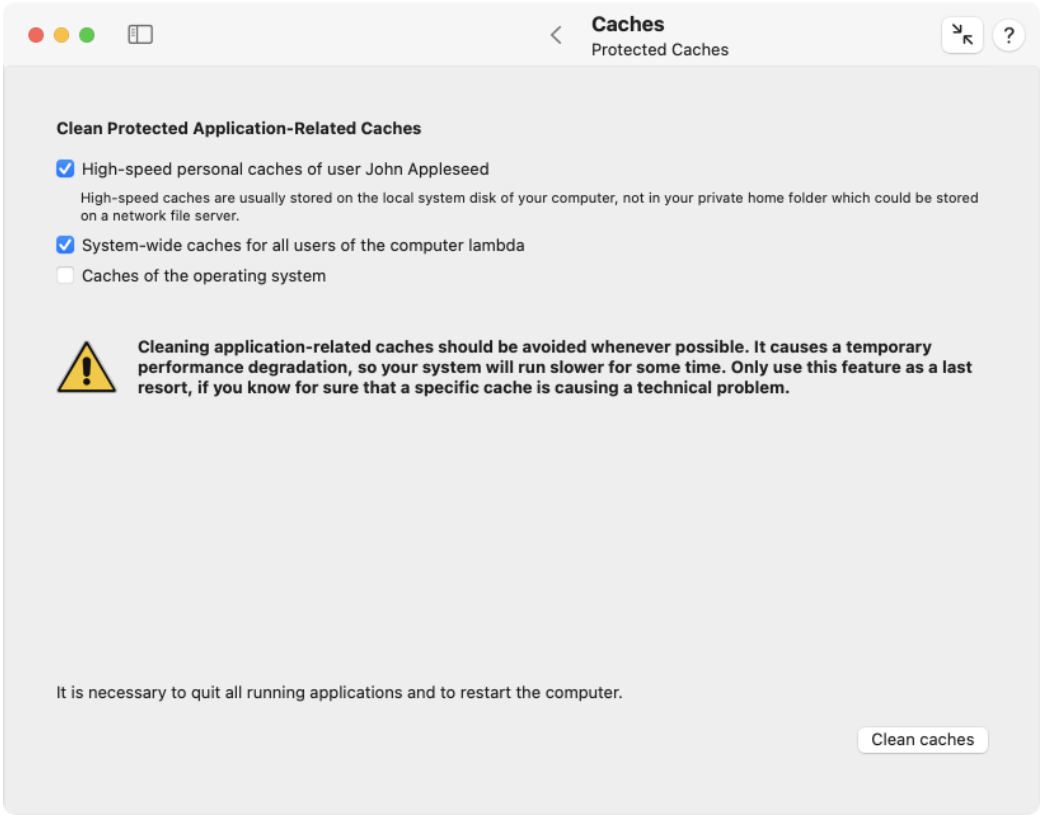


Figure 2.7: Cleaning of protected caches

the fonts, managing the auto-activation of fonts, and performing many other font-related tasks.

Your computer may contain dozens of user accounts, several hundred fonts and millions of different characters. To bring them all together, macOS must maintain sophisticated background databases of glyphs, characters, fonts, and individual user settings. These databases consist of *font caches*. The operating system as a whole and each user account keep their own font caches.

In the event that the font registration server experiences a technical problem, the font caches can become corrupt. This will cause strange effects when working with fonts, e.g. delays after login, unexpected errors in the Font Book application, the spontaneous activation of fonts which should be inactive, or –in the worst case– a complete failure to display the correct characters for certain fonts which basically results in "garbled text."

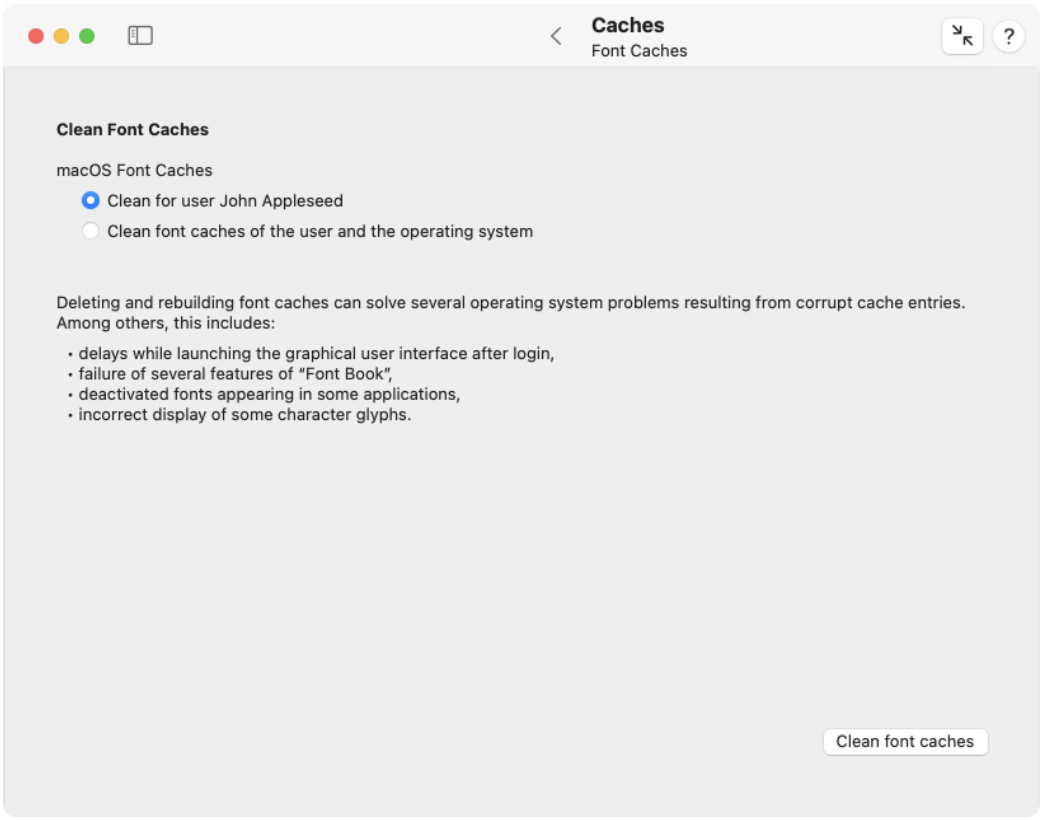


Figure 2.8: Font caches

If you are experiencing such a problem, TinkerTool System can assist you in cleaning the font caches. The clean operation can either be performed for the current user account or for that user account and the whole operating system together.

When cleaning the caches of the font server, a logout will be necessary. macOS will au-

tomatically rebuild the font caches during the next login. This operation should complete within a few seconds or minutes. TinkerTool System automatically guides you through all necessary steps.

Perform the following steps to clean the font caches:

1. Open the sub-item **Caches** > **Font Caches**.
2. Select the macOS font caches which should be cleaned.
3. Click the button **Clean font caches**.
4. Follow the instructions of the program.

2.2.5 Icon Caches

The Dock, the Finder and other parts of the operating system use icons to refer to the applications you have stored on your Mac. To quickly find the correct image for each application, the operating system collects information about the icons in central databases, known as the *icon caches*. The icon caches are usually robust; however, under certain circumstances they can become damaged. In such a case, the application icons may no longer be shown correctly, or some of them are substituted by the generic application icon, a gray square with rounded corners and construction lines.

If you are affected by such a problem, you can let TinkerTool System clear the various icon caches of your user account, causing the operating system to reacquire the necessary information and to rebuild the databases. If all of the user accounts on your computer are affected by application icon failure, you can clear the icon cache of the operating system as well. You'll have to log out in order to complete the operation. If the icon caches of the operating system have been cleared, it will be necessary to restart the computer instead.

Perform the following steps to clean the icon caches:

1. Open the sub-item **Caches** > **Icon Caches**.
2. Select the caches which should be cleaned.
3. Click the button **Clean icon caches**.
4. Follow the instructions of the program.

2.2.6 Kernel Driver Staging

Modern versions of macOS no longer permit that any vendor can install kernel extensions as part of their programs, even if the applications need administrator-authorized installations. The developers need expressed permission from Apple to develop such extensions which is verified by macOS with digital signatures. In addition, the installation of extensions must be explicitly acknowledged in a separate step, using a normally hidden user interface at **System Settings** > **Privacy & Security** > **Others.**

To put all kernel extensions provided by third-party applications under some kind of quarantine, before the user either permits or rejects their use, the respective files are

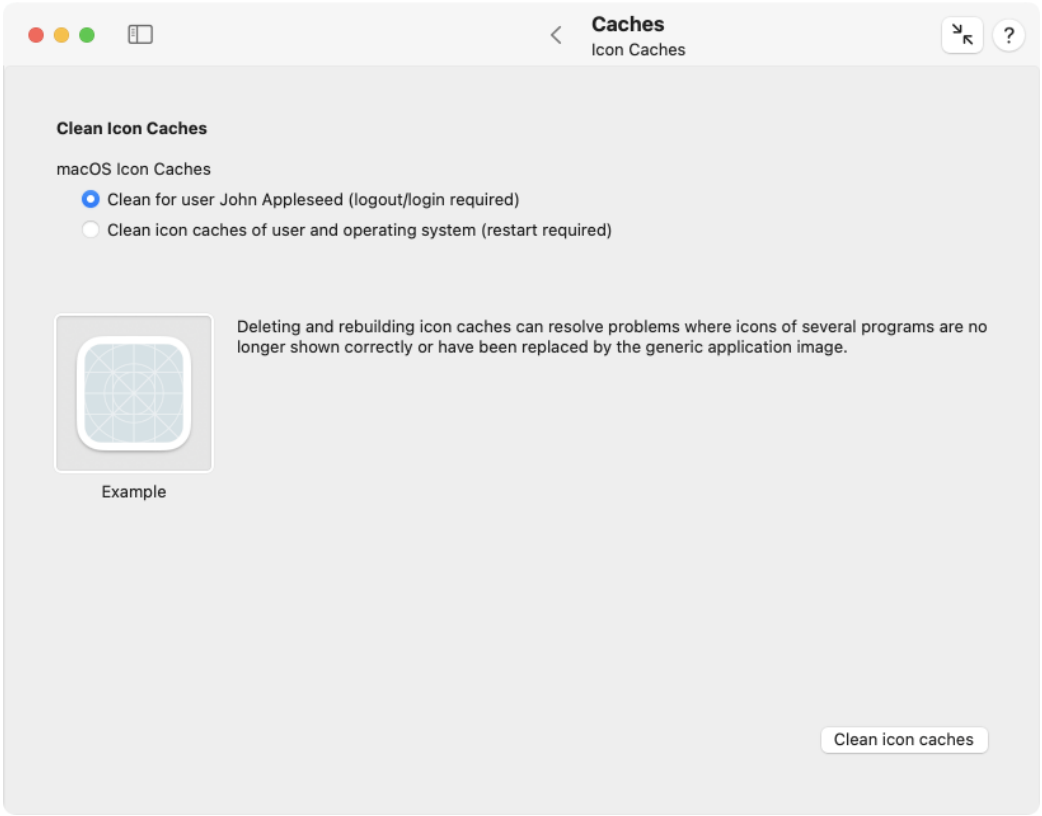


Figure 2.9: Icon caches

collected in a *staging area*, using one or more special system folders. These folders are under *System Integrity Protection* and cannot be modified by anybody, no matter what permissions are used. This means if the user rejected the activation of a specific third-party driver, that driver's files will remain in the staging area basically forever, because they cannot be removed. Folders used for staging are usually

- /Library/StagedDriverExtensions and
- /Library/StagedExtensions

but Apple may change this any time without notice.

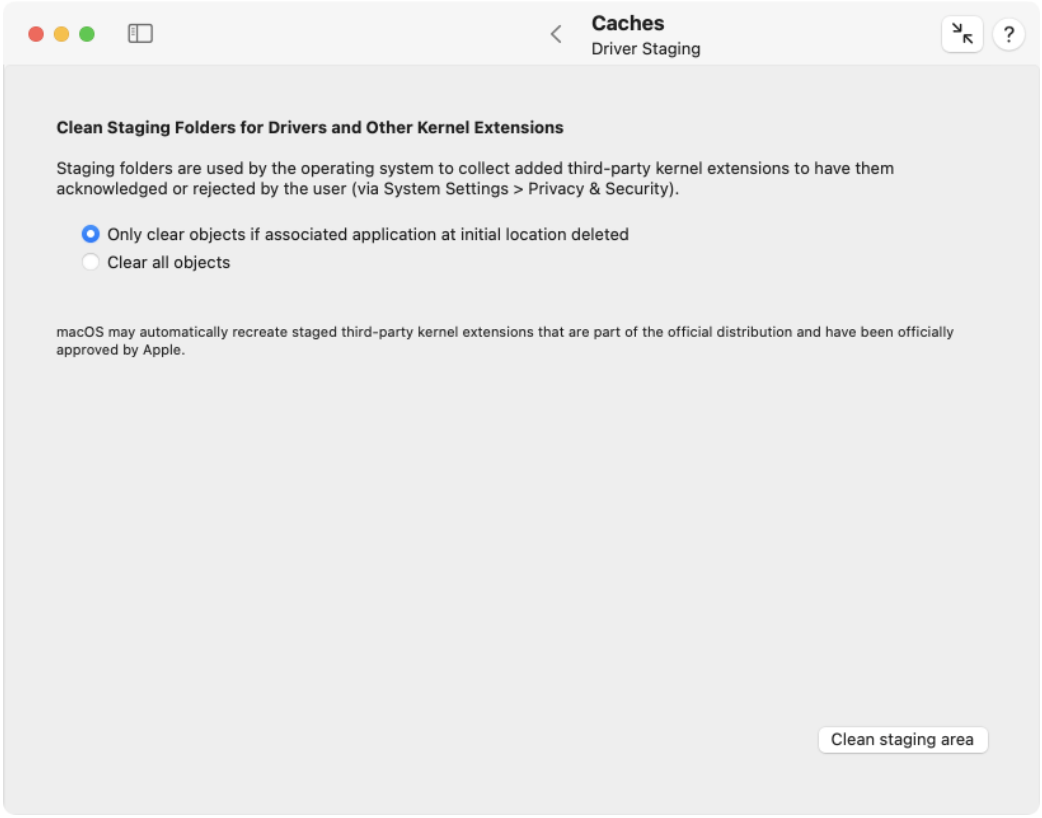


Figure 2.10: Driver staging

TinkerTool System can help in this case, indicating to the operating system it should clear its staged kernel extension files. Perform the following steps to do this:

1. Open the sub-item **Caches** > **Driver Staging**.
2. Use the radio buttons to indicate whether you like to remove *all* staged objects, regardless of their current role in the system (**Clear all objects**), or limit the removal to

cases where the associated applications can no longer be located at their original installation places. (This makes sure that drivers which still wait for approval or denial in the middle of an unfinished installation job cannot be deleted inadvertently.)

3. Click the button **Clean staging area**.

> There are special drivers that have been developed by third parties, but are officially distributed by Apple as part of macOS. These kernel extensions are staged as well and may also be removed if you select the **Clear all objects** option. However, macOS may automatically restore those particular files later.

2.3 The Panes for Time Machine

2.3.1 Time Machine Basics

Time Machine is the name of Apple's technology which automatically creates backup copies of your computer's hard drives. Backups are created silently in the background, typically every hour. Outdated file sets are automatically removed, keeping hourly backups for the last day, daily backups for the last month, and monthly backups until the destination device is full. Each backup set contains a nearly complete snapshot of the contents of all disks for which Time Machine has been activated. "Nearly" means that Time Machine automatically omits files which are considered unimportant or which can be recreated, like log files, the Trash, caches, the Spotlight search index, etc. As of macOS 11, this also includes the operating system itself. Although your files can be restored for each point in time for which a backup is available, Time Machine technically only stores the differences between any two given consecutive backup operations *(incremental backup)*. Differences are handled at the file level, i.e. if a single byte in a file X has changed, the entire file X will be copied during the next Time Machine backup run.

2.3.2 General Notes when Working with the Time Machine Pane

Time Machine can be configured to work with multiple destination devices at the same time. In addition to disk drives, destination devices can be servers in the network (such as Time Capsule), a Mac running Time Machine file sharing (available in old versions of macOS Server and in standard versions of macOS as of version 10.13), or a NAS with Time Machine support. TinkerTool System automatically detects your configuration and always works on the Time Machine destination that is currently defined by macOS to be the "active" one.

The name and type of the destination are shown in the upper box of the Time Machine pane. For disk-based backups, the name of the volume is shown at **Destination**. Network-based backups are indicated by a headline with the notice **network mode**. The upper box also shows whether automatic backups are currently enabled, and if a successful maintenance connection between TinkerTool System and Time Machine could be established. If

an error occurred, e.g. if the current privacy settings of your computer don't permit that you access Time Machine disks, this will be noted in the upper box.

If you use the modern APFS version of Time Machine (see next section), the line **Destination** will also indicate whether the backup is encrypted. In addition, the line **Automatic backups** will contain a notice which backup time interval is currently set.

2.3.3 The different versions of Time Machine for macOS 10 and later versions of macOS

As of macOS 11, the technology of Time Machine has been strongly extended and modified: While earlier versions of the operating system only accepted destination volumes for backups that had been formatted with the file system *Mac OS Extended (HFS+)* , backups onto the *Apple File System (APFS)* are now possible as well. If Time Machine is freshly configured for a new backup disk, it will use APFS and will operate in "modern" mode. When taking over old backup sets initially created with macOS 10, OS X, or Mac OS X, Time Machine will continue working with HFS+.

The feature sets between the macOS 10 and the modern variants of Time Machine are very different. For this reason, TinkerTool System uses different panes to control Time Machine depending on which variant is detected. If running in macOS 10 mode, the respective pane will identify as **Time Machine X**.

> This manual contains two different chapters for the use of both the panes Time Machine X (section 2.4 on page 42) and Time Machine (section 2.5 on page 55).
>
> TinkerTool System won't switch the Time Machine mode of operation while it is running. When you swap the destination disk from HFS+ to APFS while TinkerTool System is open, the application will notice this the next time you will be preparing a maintenance operation and shows an error message in this case. You can simply quit and reopen the program to resolve this situation.

2.4 The Pane Time Machine X

> This chapter applies to the *Time Machine X* pane and describes working with the compatibility mode for macOS 10, i.e. on backup media created in HFS+ format by macOS 10. When using the up-to-date variant of Time Machine (backup to APFS), please continue reading in the next chapter (section 2.5 on page 55).

2.4.1 Maintenance After Replacing a Data Source of Time Machine (macOS 10 mode)

The incremental backup strategy mentioned in the introduction only works if Time Machine can be absolutely sure which files have changed between two consecutive backups

and which haven't. If Time Machine cannot confirm that a given file is identical to the one it saw during a previous run, that file will be freshly copied in the next run.

When the identity of your computer changes, for example if you purchased a new one, or if it had components replaced during a repair, Time Machine has to assume that *all* the files of your computer have changed. This is true even if you have "cloned" or manually copied the files from the old to the new computer. This means that during the next backup, Time Machine will copy all the files again. Only if you use Time Machine itself to perform a full restore operation of the previous data, will Time Machine "know" that it can safely reuse the previous incremental backup.

The same problem arises if you replace a volume of your Mac, but use something other than Time Machine to copy the data back. Replacing a volume can mean

- you replaced a disk drive physically,
- you erased or reformatted a partition,
- you cloned a volume by a third-party application, but the original and copied volumes were attached to the computer at the same time, so that the system had to change the identity of one volume to keep track of which is which.

Only if you copy a disk drive or partition physically (i.e., by a copying the raw data blocks, not file by file) and make sure that the operating system where Time Machine is active doesn't mount both volumes simultaneously, will Time Machine seamlessly continue its incremental operation. In all other cases, Time Machine has to assume that all files on the entire affected volume have changed and therefore must be fully copied again.

TinkerTool System can help here, letting you manually confirm to Time Machine that a computer or a volume should still be considered the same, although its identity changed. This way, the new item will take over the role of the replaced item, and its history in Time Machine can be continued without requiring a full new backup.

> Please note that it is a necessary requirement in all cases that the operating system with all its user accounts has stayed the same. For example, you cannot use these maintenance features if you have a new Mac (with a different installation of macOS) and like to take over data from the Time Machine backup of an old Mac. Even if system versions and names of all users are identical, transferring the Time Machine backup won't be possible in this case, because the backup contains access rights for user accounts of a different system installation. This problem can be resolved by copying accounts and Time Machine data at the same time via Apple's Migration Assistant.

Inheriting a Time Machine Backup Set from a Replaced Computer (macOS 10 mode)

If you need to confirm that Time Machine can safely take over a backup set that was created by a different physical computer or by a different operating system installation on the same computer, you can reassign the backup set to your current system. You should only do this in the aforementioned scenario, where all files have indeed be copied to the new system installation by some other means (not under control of Time Machine). Perform the following steps to do this:

1. Open the tab item **Maintenance** on the pane **Time Machine X**.
2. Click the button **Assign a foreign backup to this Mac**....

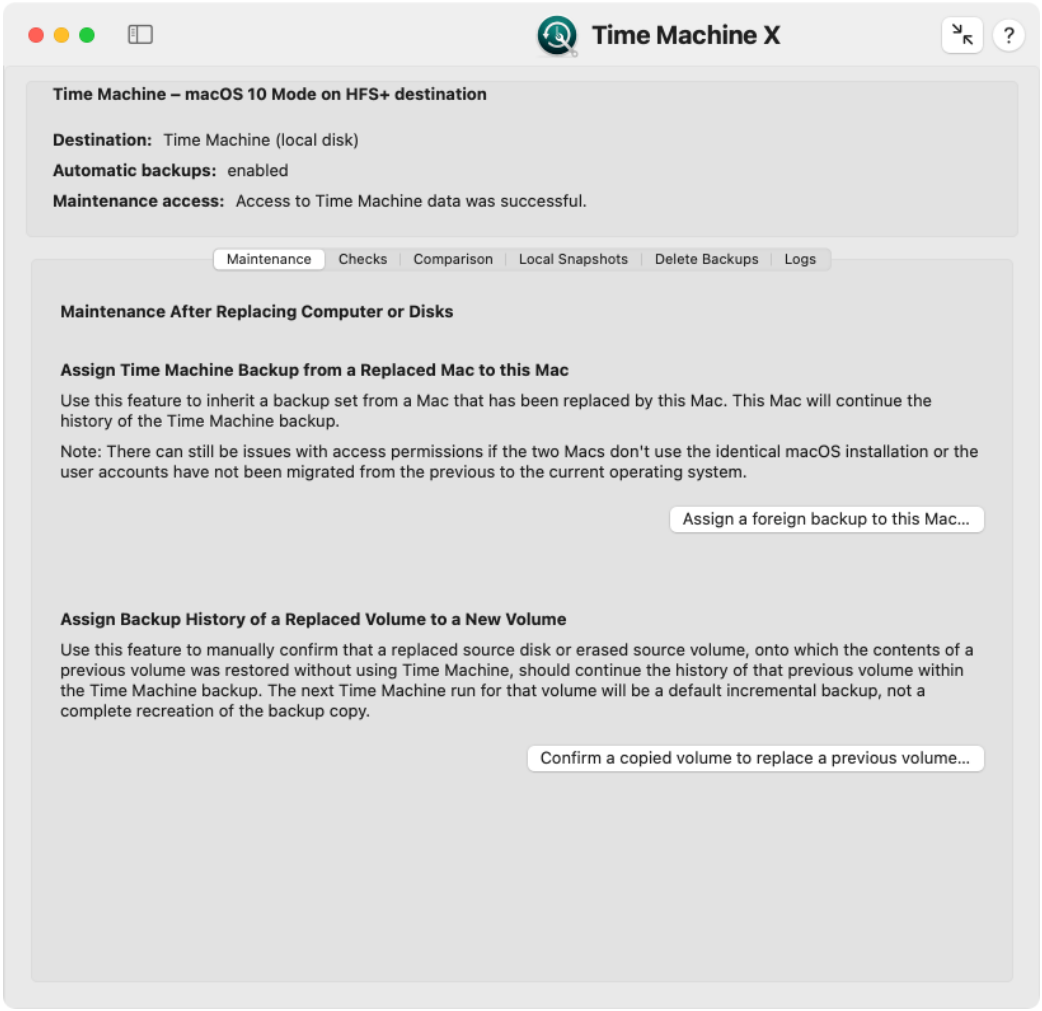


Figure 2.11: Maintenance after replacing Time Machine data sources

TinkerTool System will guide you through all steps of the procedure. You will need to locate the foreign backup set to complete the operation. In case of a local Time Machine disk, this will be the top folder of the backup set. It has the name of the previous computer and is located in the folder *Backups.backupdb* on the destination disk. When using APFS, the folder is the Time Machine volume itself.

Depending on how Time Machine was configured before inheriting the foreign backup set, you might need to re-enable Time Machine in the **General** > **Time Machine** section

of **System Settings** and change the backup destination.

In case the local volumes of the current computer are different from the ones of the previous computer, *inheriting the backup set alone won't be sufficient*. You will additionally need to reassign each volume, which is described in the next section.

Associating a Replaced Volume with a Volume in the Backup Set (macOS 10 mode)

As outlined in the introduction, there can also be cases where you need to confirm to Time Machine that it can safely take over the history of a volume in the backup, although the identity of the original source volume has changed. You can reassign a volume in the backup (for all snapshots recorded by Time Machine) to match a volume of your current setup. You should only do this in the previously mentioned scenario, i.e. where all files have indeed been copied from the previous volume to the new volume (not under control of Time Machine, so that Time Machine did not "notice" it). Perform the following steps to do this:

1. Open the tab item **Maintenance** on the pane **Time Machine X**.
2. Click the button **Confirm a copied volume to replace a previous volume**….

Three items need to be specified:

- a snapshot in the current backup set that includes one of the backups of that volume,
- the name of that volume as it was recorded at the time of the selected snapshot,
- the name of the new volume in your current installation that should match the volume in the backup set.

TinkerTool System reassigns that volume for the entire time line recorded in that backup set, i.e. *for all snapshots*. It does not matter if the previous volume changed its name during the recorded time period. Time Machine identifies the volume correctly tracking its internal history data.

Do not abuse the two maintenance features to manipulate the backup in any other cases that have not been mentioned here. The backup set could become unusable.

2.4.2 Backup Verification and Statistics (macOS 10 mode)

TinkerTool System gives you access to internal check features of Time Machine. You can learn more about the actual storage size needed by the individual snapshots, and you can initiate a verification run on selected snapshots, ensuring that the contents of the backup are still intact.

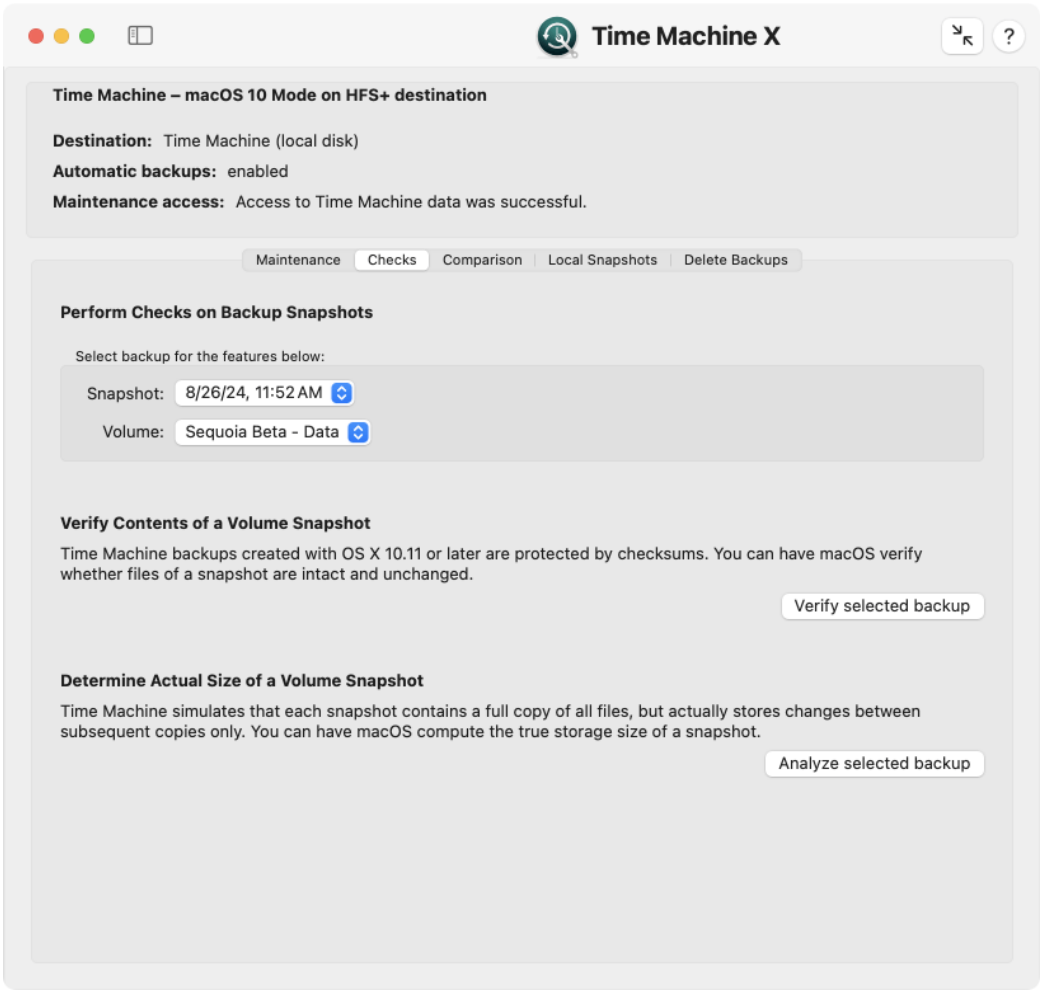


Figure 2.12: Features for backup verification and statistics

Verifying the Contents of a Volume Snapshot (macOS 10 mode)

To be absolutely sure that the backup copy of a volume for a specific point in time can be read without problems and is fully intact, you can force Time Machine to validate its internal checksums. As of version 10.11 of the operating system, Time Machine protects each file in the backup by computing and recording a checksum for the content of that file. To verify a backup run for a volume, perform the following steps:

1. Open the tab item **Checks** on the pane **Time Machine**.
2. Use the pop-up button **Snapshot** to select the time of the backup that should be checked.
3. Use the pop-up button **Volume** to select the volume in the snapshot that should be verified.
4. Click the button **Verify selected backup**.

The check will need a considerable amount of time. If problems are identified, TinkerTool System will show a table with all issues after the verification has been completed. The table will list the full paths of the files in the backup where a problem was detected. There can be two types of problems, indicated as follows:

- **File modified:** the file in the backup did not match its checksum. Either the file could not be read correctly or its contents changed unexpectedly.
- **No check possible:** the file could not be tested successfully because its checksum was not available. This indicator does *not* mean that you shouldn't trust the copied file. It means that it is currently unknown whether the file is OK or not.

Possible reasons for cases where no check is possible could be:

- The snapshot was created with an operating system prior to version 10.11.
- The checksum is currently in use because another Time Machine operation (e.g. a new backup session) is currently running in the background. In this case you should repeat the test, perhaps after temporarily disabling automatic backups.

The list of possible reasons depends on the operating system version and may not be complete.

Computing the Actual Storage Size of a Volume Snapshot (macOS 10 mode)

In addition to the change rates between consecutive snapshots, it can be interesting to know the actual storage size consumed by a snapshot that contains the backup copy for a specific volume. Due to the internal optimization of Time Machine, this size can be very different from the simulated size for the related backup folder shown in the Finder or by similar applications listing files.

To let Time Machine compute the true storage size of a volume snapshot, perform the following steps:

1. Open the tab item **Checks** on the pane **Time Machine X**.
2. Use the pop-up button **Snapshot** to select the time of the backup that should be evaluated.
3. Use the pop-up button **Volume** to select the volume in the snapshot that should be evaluated.
4. Click the button **Analyze selected backup**.

TinkerTool System summarizes the size value in a message that will be shown after the computation has been completed.

> The actual storage size can be zero if the contents of the selected volume did not change between consecutive backup runs.

2.4.3 Comparing Time Machine backup snapshots (macOS 10 mode)

Time Machine does not usually need any maintenance as long as you don't replace the source or destination disks. You just define which disk volumes should be included in the backup, what destination drive should be used, and switch Time Machine on. However, there can be certain instances where Time Machine may not run as expected – for example if there is a file system problem on one of the source volumes, or if there was a power failure during a Time Machine run. TinkerTool System can help you to detect possible problems with backups by controlling one of the diagnostic features of Time Machine with a few simple clicks.

You can select two different backup sets and compare all their files. This will show the "true," incremental contents of a Time Machine backup, rather than the simulated view in the Finder or the Time Machine user interface, which always shows the entire effective backup set at a selected point in time. If some part of Time Machine is failing, this will mean that although specific files have been modified, they have not been included in the next incremental backup copy corresponding to the Time Machine snapshot taken immediately after the modification time. For typical Time Machine problems, the updates for an entire folder would be missing, which can be detected easily when comparing the two backups preceding and following the modification of files in that folder.

You can also use this feature to determine which files have changed on your computer at a particular point in time, or to assess how many files with what storage size are typically part of your backups every hour.

Alternatively, it is also possible to compare the current data on your computer (that is, all files which are selected to be handled by Time Machine) with a specific backup session. This feature is helpful to detect implementation errors in Time Machine. You can immediately see whether the data that *should* be copied has actually been copied. Note that this type of compare operation takes a significant amount of time, because all files on your computer have to be checked.

To start the comparison of two Time Machine backups, perform the following steps:

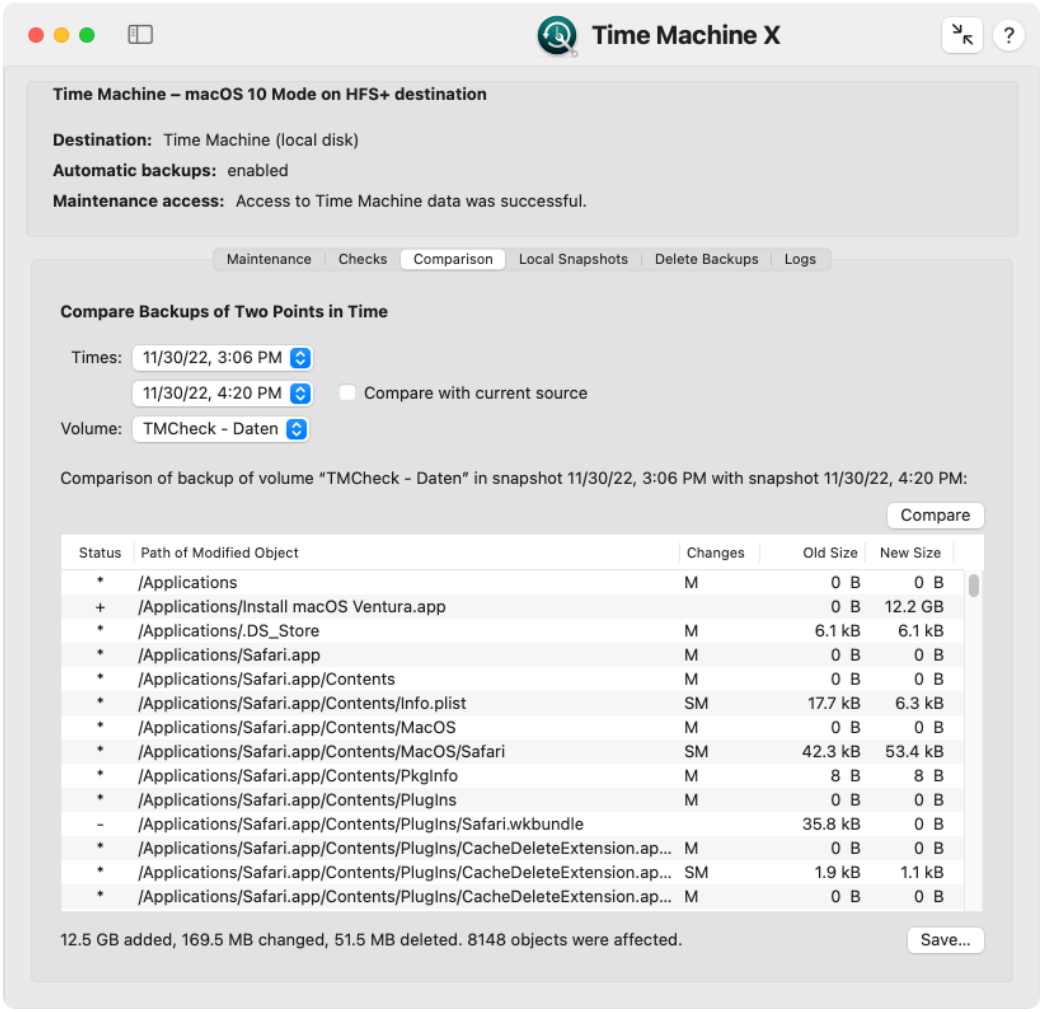


Figure 2.13: Check Time Machine by comparing backups

1. Open the tab item **Comparison** on the pane **Time Machine X**.
2. At **Times**, select the two points in time for which the backup sets should be compared. The order of the times does not matter. To choose the "live" data on your computer for comparison, set a check mark at **Compare with current source**.
3. If Time Machine is configured to create backup copies of multiple disk volumes, select the desired disk to compare, using the pop-up menu **Volume**. (This is not necessary or possible when comparing the current source data).
4. Click the button **Compare**.

Depending on the size of your backup and the amount of data differing between the two selected backup sets, the compare operation may need a few seconds or several minutes to complete. The results will be shown in the table.

- The column **Status** uses a single marker to indicate the overall status of each difference that has been found. The markers have the following meaning:
  - **+:** This object has been added.
  - **-:** This object has been removed.
  - ***:** This object has been modified.
- **Path of Modified Object** shows the UNIX path of the file or folder where a difference was detected. The path must be interpreted relative to the volume you had selected for comparison.
- **Changes** indicates the exact type of modification:
  - **A:** The Access Control List has changed.
  - **C:** The creation time has changed.
  - **D:** The data stored in the object has changed.
  - **G:** The group owner has changed.
  - **M:** The modification time has changed.
  - **O:** The owner has changed.
  - **P:** The POSIX permissions have changed.
  - **S:** The size has changed.
  - **T:** The object type has changed.
  - **X:** The Extended Attributes have changed.
- If the object is a file and the file has been modified, the column **Old Size** shows the storage size required by the file for the older of the two selected points in time.
- Similarly, the column **New Size** displays the storage size at the later of the two selected times.

If you move the mouse cursor over an entry in the column **Changes**, TinkerTool System will display a short textual explanation, so you don't need to learn the abbreviations.

For reasons of efficiency, the entries in the table cannot be rearranged in different sort orders. TinkerTool System shows them in the same order as they are processed by Time Machine during backups. You can use the button **Save**… to create a processed report in text form which can then be saved to a file.

2.4.4 Working with Local Snapshots (macOS 10 mode)

If at least one of the volumes selected to be part of the backup uses the modern *Apple File System (APFS)*, Time Machine will automatically enable additional features:

- Every time a backup session is started, Time Machine will create an *APFS snapshot* of each APFS volume that is about to be copied. An APFS snapshot is basically a frozen image of the source volume, created at the time the backup began. Even if files are changing while the backup session is running, the snapshot will ensure that Time Machine only "sees" a static picture of the volume. If the backup copy must be restored later, the result will reflect a consistent state of the volume, without any files that have been in an "in-between" condition only.

- Each APFS snapshot will be kept by the operating system on each volume as long as this volume has enough storage space. The snapshot is basically invisible during normal operation and only needs a small amount of additional storage space. It is based on the strategy to never reuse any block of the volume that had been occupied by a file for any new files, even when that file has been deleted or this part of the file has been changed.

- APFS snapshots are not only created when normal Time Machine backups are made, the operating system also creates them when major changes in the system are to be expected, e.g. when an operating system update is about to be installed.

- These snapshots can be used as "restore points" that allow you to very rapidly reset an entire APFS volume to a consistent state of the past. This is done via Time Machine (usually after starting the recovery system), selecting the APFS volume itself, not the actual Time Machine volume, as source for a restore operation. For more information, please see Apple's official documentation on macOS.

This basically means that an APFS snapshot can be used as a local snapshot of Time Machine. Working with these snapshots doesn't require access to the actual Time Machine backup volume.

> Other parts of macOS can use the APFS snapshot feature as well. The list shown on the tab **Local Snapshots** considers APFS snapshots created by Time Machine only. If you like to work with the complete list of APFS snapshots, please see the chapter The Pane APFS (section 3.7 on page 232).

It is under sole discretion of the operating system when to automatically create or to remove APFS snapshots. TinkerTool System gives you additional manual control about these local snapshots, however.

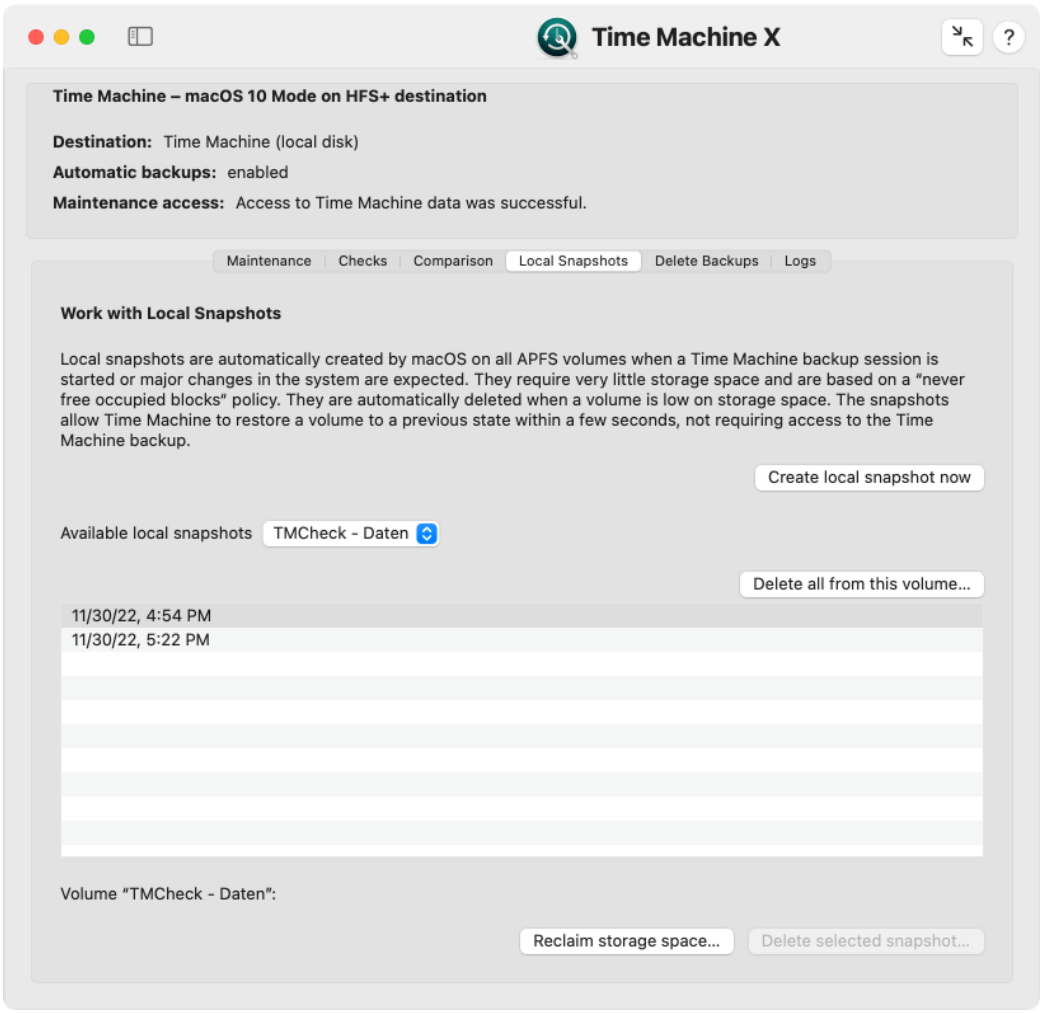


Figure 2.14: Working with local APFS snapshots

- You can create a local snapshot immediately, just by clicking a button. This is helpful to create a well-defined restore point, e.g. when you like to test a possibly "dangerous" action on an APFS volume that might need to be undone in the near future.
- You can review which local snapshots are currently available on each APFS volume.
- You can force macOS to clean up its local snapshots immediately, to bring forward the point in time when this would happen automatically. This is done by specifying

a planned amount of storage space that should be reclaimed during the cleanup. macOS will keep as much snapshots as it can to meet this target.

- You can delete local snapshots of your choice.

To create a new local snapshot on all APFS volumes that are part of your Time Machine backup, perform the following steps:

1. Open the tab item **Local Snapshots** on the pane **Time Machine X**.
2. Click the button **Create local snapshot now**.

Creating the local snapshot should typically require less than one minute.

You can review all snapshots using the table **Available local snapshots** on the same pane. The available points in time are listed as separate lines. By default, you will see a list for the entire computer. If more than one APFS volume is in use, it can also be interesting to see the list of snapshots on each volume. Note that the sets of available snapshots can be different on each volume because some volumes may have less free storage space, so they will automatically remove snapshots earlier than others. To select between different volumes, use the pop-up button above the table.

To reclaim storage space on a particular volume, select the volume with the pop-up button above the table, then click the button **Reclaim storage space**…. TinkerTool System will ask you in a dialog sheet how much bytes you like at least to be reclaimed. You can specify a low value (like 1) to make sure that only the smallest possible number of snapshots will be deleted. The operating system will use its standard policies to automatically select the snapshots that should be removed. At the end of the operation, TinkerTool System will show a summary how many local snapshots have been lost and how much storage space has been freed on the volume.

> In some cases, Time Machine may decide to postpone the cleaning operation for some time. In this particular situation, TinkerTool System may not indicate that storage space has been freed yet immediately after requesting a reclaim procedure.

In order to free up as much space from a volume immediately, select the volume at **Available local snapshots** and click the button **Delete all from this volume**. Time Machine will understand this as urgent request to reclaim the maximum amount of storage space currently in use for local snapshots.

To delete a local snapshot manually, select it in the table and click the button **Delete selected snapshot**….

2.4.5 Deleting Time Machine Backup Data (macOS 10 mode)

Remove a backup snapshot from the currently active Time Machine disk (macOS 10 mode)

As part of its daily routine, Time Machine cleans up backups regularly, if necessary every hour. After a backup session has run, outdated backup snapshots are removed from the

backup disk. Sometimes, you may like to remove a specific snapshot manually, e.g. to free some storage space. *You must never do this via the macOS Finder. This could damage the Time Machine backup set, and in addition also the Trash feature of the Finder.* TinkerTool System offers you a safe way to remove a Time Machine backup for a certain point in time:

1. Open the tab item **Delete Backups** on the pane **Time Machine X**.
2. Select the snapshot that should be removed with the pop-up button at **Delete** in the upper part of the window.
3. Click the button **Delete…** next to it.

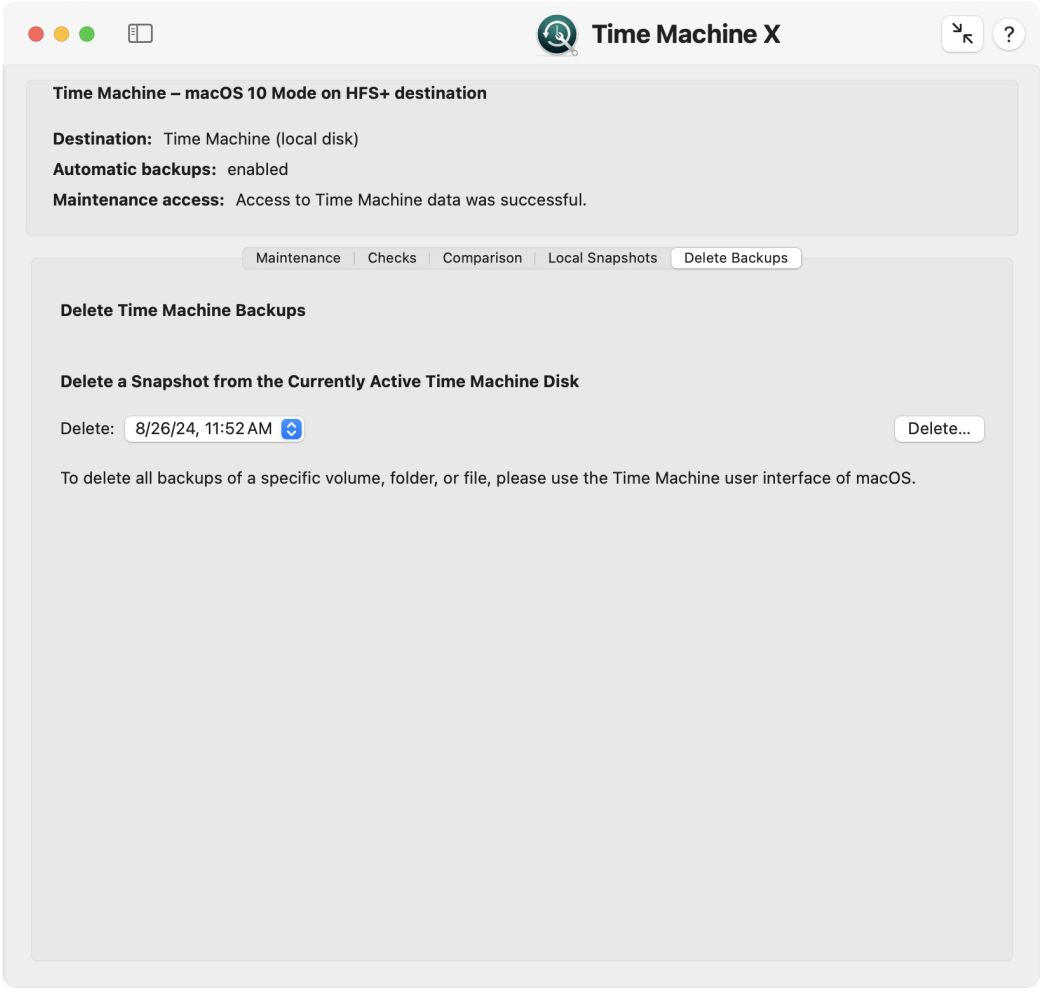


Figure 2.15: Deleting Time Machine backup data

This operation removes items from Time Machine "horizontally": All files and folders of a snapshot will be deleted, so you can no longer "travel back in time" to restore one or all files for this specific moment. All other snapshots remain intact, however. You can additionally remove items "vertically", i.e. you can delete a specific file or folder *from all snapshots* in the backup set. This feature is already built into the Time Machine user interface:

1. Use the Finder to open the parent folder that contains the item to be removed.
2. Open the Time Machine user interface.
3. Select the object you like to remove in the Finder-like window of Time Machine.
4. Use the context menu (right click) to remove the selected item.

2.5 The Pane Time Machine

> This chapter applies to the **Time Machine** pane. When using Time Machine in macOS 10 mode, which automatically activates the pane **Time Machine X**, please read the previous chapter (section 2.4 on page 42) instead.
>
> TinkerTool System won't switch the Time Machine mode of operation while it is running. When you swap the destination disk from APFS to HFS+ while TinkerTool System is open, the application will notice this the next time you will be preparing a maintenance operation and shows an error message in this case. You can simply quit and reopen the program to resolve this situation.

2.5.1 Maintenance After Replacing a Data Source of Time Machine

The incremental backup strategy mentioned in the introduction only works if Time Machine can be absolutely sure which files have changed between two consecutive backups and which haven't. If Time Machine cannot confirm that a given file is identical to the one it saw during a previous run, that file will be freshly copied in the next run.

When the identity of your computer changes, for example if you purchased a new one, or if it had components replaced during a repair, Time Machine has to assume that *all* the files of your computer have changed. This is true even if you have "cloned" or manually copied the files from the old to the new computer. This means that during the next backup, Time Machine will copy all the files again. Only if you use Time Machine itself to perform a full restore operation of the previous data, will Time Machine "know" that it can safely reuse the previous incremental backup.

The same problem arises if you replace a volume of your Mac, but use something other than Time Machine to copy the data back. Replacing a volume can mean

- you replaced a disk drive physically,
- you erased or reformatted a partition,

- you cloned a volume by a third-party application, but the original and copied volumes were attached to the computer at the same time, so that the system had to change the identity of one volume to keep track of which is which.

Only if you copy a disk drive or partition physically (i.e., by a copying the raw data blocks, not file by file) and make sure that the operating system where Time Machine is active doesn't mount both volumes simultaneously, will Time Machine seamlessly continue its incremental operation. In all other cases, Time Machine has to assume that all files on the entire affected volume have changed and therefore must be fully copied again.

TinkerTool System can help here, letting you manually confirm to Time Machine that a computer or a volume should still be considered the same, although its identity changed. This way, the new item will take over the role of the replaced item, and its history in Time Machine can be continued without requiring a full new backup.

> Please note that it is a necessary requirement in all cases that the operating system with all its user accounts has stayed the same. For example, you cannot use these maintenance features if you have a new Mac (with a different installation of macOS) and like to take over data from the Time Machine backup of an old Mac. Even if system versions and names of all users are identical, transferring the Time Machine backup won't be possible in this case, because the backup contains access rights for user accounts of a different system installation. This problem can be resolved by copying accounts and Time Machine data at the same time via Apple's Migration Assistant.

Inheriting a Time Machine Backup Set from a Replaced Computer

If you need to confirm that Time Machine can safely take over a backup set that was created by a different physical computer or by a different operating system installation on the same computer, you can reassign the backup set to your current system. You should only do this in the aforementioned scenario, where all files have indeed be copied to the new system installation by some other means (not under control of Time Machine). Perform the following steps to do this:

1. Open the tab item **Maintenance** on the pane **Time Machine**.
2. Click the button **Assign a foreign backup to this Mac**….

TinkerTool System will guide you through all steps of the procedure. You will need to locate the foreign backup set to complete the operation. In case of a local Time Machine disk, this will be the top folder of the backup set. It has the name of the previous computer and is located in the folder *Backups.backupdb* on the destination disk. When using APFS, the folder is the Time Machine volume itself.

Depending on how Time Machine was configured before inheriting the foreign backup set, you might need to re-enable Time Machine in the **General** > **Time Machine** section of **System Settings** and change the backup destination.

In case the local volumes of the current computer are different from the ones of the previous computer, *inheriting the backup set alone won't be sufficient*. You will additionally need to reassign each volume, which is described in the next section.

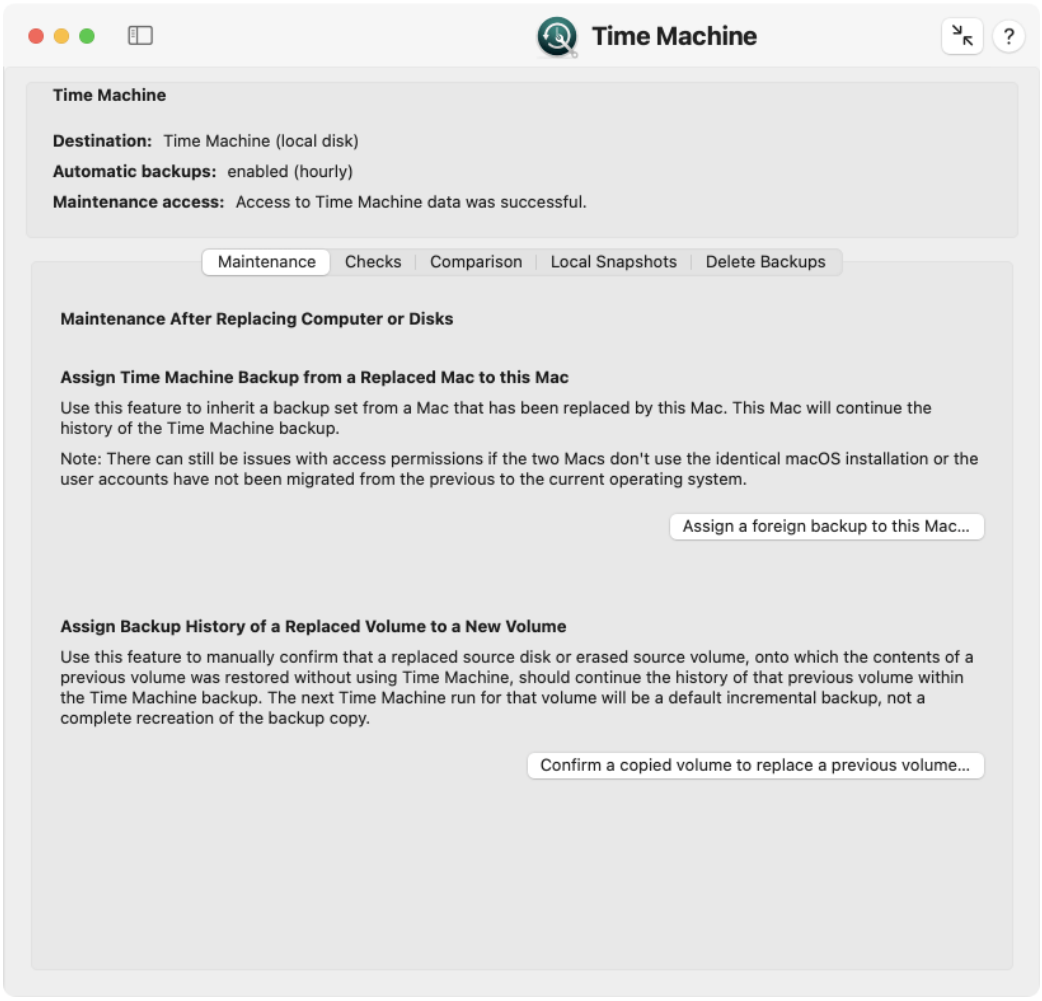


Figure 2.16: Maintenance after replacing Time Machine data sources

Associating a Replaced Volume with a Volume in the Backup Set

As outlined in the introduction, there can also be cases where you need to confirm to Time Machine that it can safely take over the history of a volume in the backup, although the identity of the original source volume has changed. You can reassign a volume in the backup (for all snapshots recorded by Time Machine) to match a volume of your current setup. You should only do this in the previously mentioned scenario, i.e. where all files have indeed been copied from the previous volume to the new volume (not under control of Time Machine, so that Time Machine did not "notice" it). Perform the following steps to do this:

1. Open the tab item **Maintenance** on the pane **Time Machine**.
2. Click the button **Confirm a copied volume to replace a previous volume**….

Three items need to be specified:

- a snapshot in the current backup set that includes one of the backups of that volume,
- the name of that volume as it was recorded at the time of the selected snapshot,
- the name of the new volume in your current installation that should match the volume in the backup set.

TinkerTool System reassigns that volume for the entire time line recorded in that backup set, i.e. *for all snapshots*. It does not matter if the previous volume changed its name during the recorded time period. Time Machine identifies the volume correctly tracking its internal history data.

Do not abuse the two maintenance features to manipulate the backup in any other cases that have not been mentioned here. The backup set could become unusable.

2.5.2 Backup Verification

Verifying the Contents of a Volume Snapshot

To be absolutely sure that the backup copy of a volume for a specific point in time can be read without problems and is fully intact, you can force Time Machine to validate its internal checksums. As of version 10.11 of the operating system, Time Machine protects each file in the backup by computing and recording a checksum for the content of that file. To verify a backup run for a volume, perform the following steps:

1. Open the tab item **Checks** on the pane **Time Machine**.

2. Use the pop-up button **Snapshot** to select the time of the backup that should be checked.
3. Use the pop-up button **Volume** to select the volume in the snapshot that should be verified.
4. Click the button **Verify selected backup**.

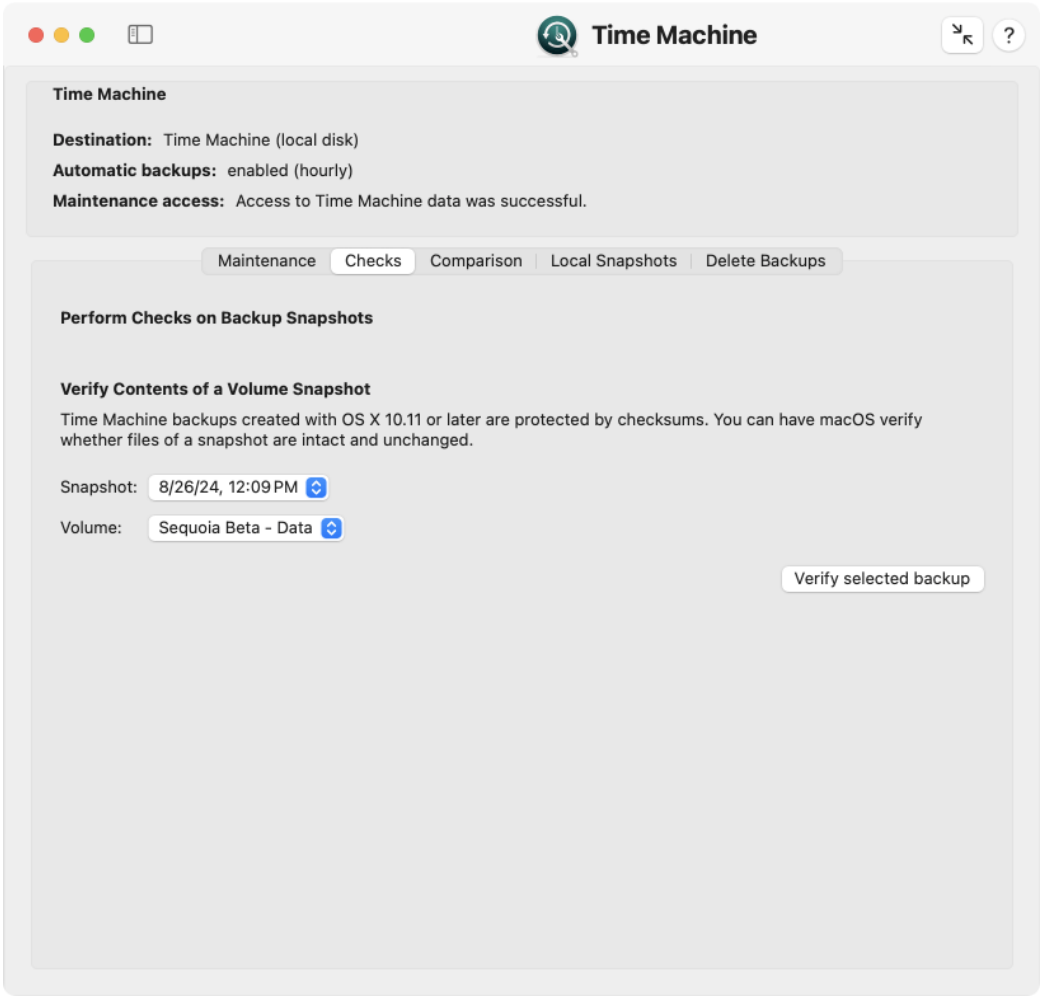


Figure 2.17: Feature for backup verification

The check will need a considerable amount of time. If problems are identified, TinkerTool System will show a table with all issues after the verification has been completed. The table will list the full paths of the files in the backup where a problem was detected. There can be two types of problems, indicated as follows:

- **File modified:** the file in the backup did not match its checksum. Either the file could not be read correctly or its contents changed unexpectedly.
- **No check possible:** the file could not be tested successfully because its checksum was not available. This indicator does *not* mean that you shouldn't trust the copied file. It means that it is currently unknown whether the file is OK or not.

Possible reasons for cases where no check is possible could be:

- The snapshot was created with an operating system prior to version 10.11.
- The checksum is currently in use because another Time Machine operation (e.g. a new backup session) is currently running in the background. In this case you should repeat the test, perhaps after temporarily disabling automatic backups.

The list of possible reasons depends on the operating system version and may not be complete.

2.5.3 Comparing Time Machine backup snapshots

Time Machine does not usually need any maintenance as long as you don't replace the source or destination disks. You just define which disk volumes should be included in the backup, what destination drive should be used, and switch Time Machine on. However, there can be certain instances where Time Machine may not run as expected – for example if there is a file system problem on one of the source volumes, or if there was a power failure during a Time Machine run. TinkerTool System can help you to detect possible problems with backups by controlling one of the diagnostic features of Time Machine with a few simple clicks.

You can select two different backup sets and compare all their files. This will show the "true," incremental contents of a Time Machine backup, rather than the simulated view in the Finder or the Time Machine user interface, which always shows the entire effective backup set at a selected point in time. If some part of Time Machine is failing, this will mean that although specific files have been modified, they have not been included in the next incremental backup copy corresponding to the Time Machine snapshot taken immediately after the modification time. For typical Time Machine problems, the updates for an entire folder would be missing, which can be detected easily when comparing the two backups preceding and following the modification of files in that folder.

You can also use this feature to determine which files have changed on your computer at a particular point in time, or to assess how many files with what storage size are typically part of your backups every hour.

Alternatively, it is also possible to compare the current data on your computer (that is, all files which are selected to be handled by Time Machine) with a specific backup session. This feature is helpful to detect implementation errors in Time Machine. You can immediately see whether the data that *should* be copied has actually been copied. Note that this type of compare operation takes a significant amount of time, because all files on your computer have to be checked.

To start the comparison of two Time Machine backups, perform the following steps:

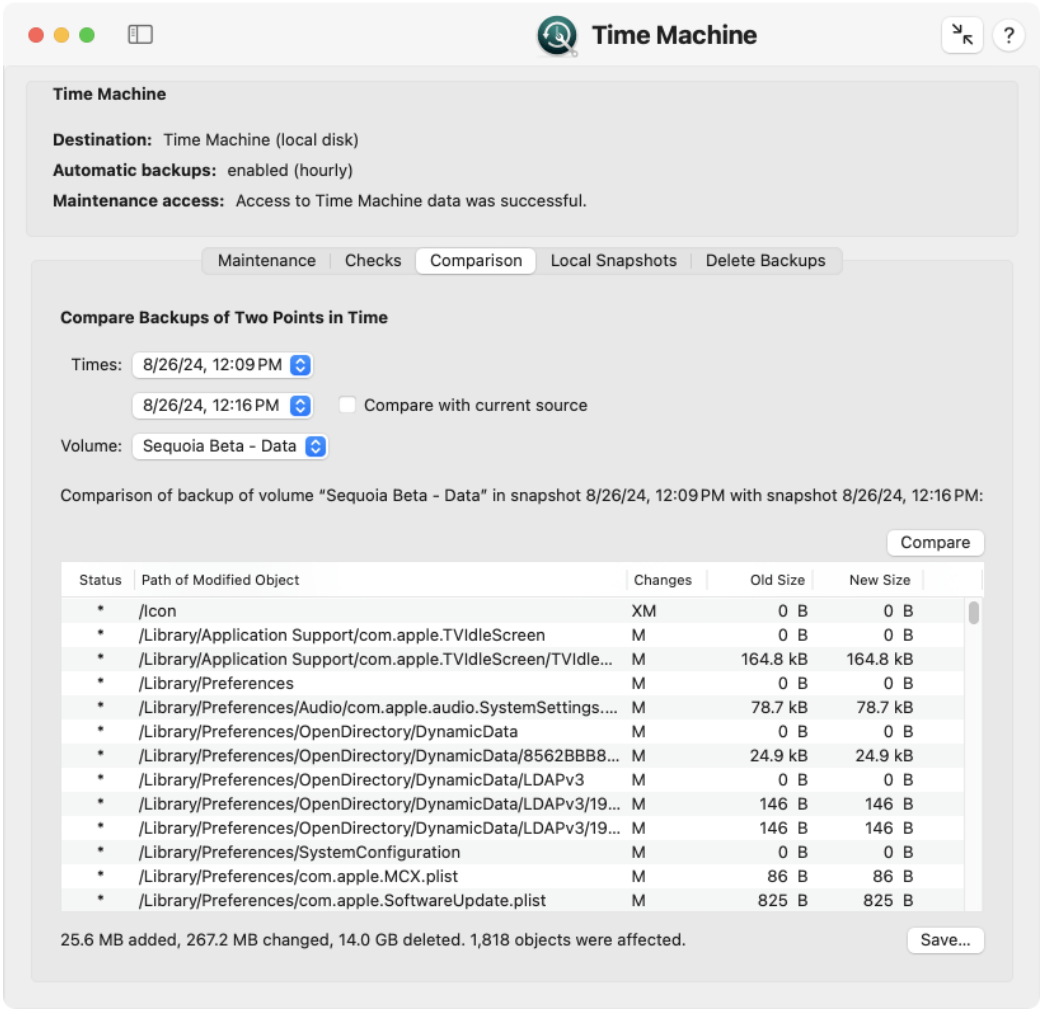


Figure 2.18: Check Time Machine by comparing backups

1. Open the tab item **Comparison** on the pane **Time Machine**.
2. At **Times**, select the two points in time for which the backup sets should be compared. The order of the times does not matter. To choose the "live" data on your computer for comparison, set a check mark at **Compare with current source**.
3. If Time Machine is configured to create backup copies of multiple disk volumes, select the desired disk to compare, using the pop-up menu **Volume**. (This is not necessary or possible when comparing the current source data).
4. Click the button **Compare**.

Depending on the size of your backup and the amount of data differing between the two selected backup sets, the compare operation may need a few seconds or several minutes to complete. The results will be shown in the table.

- The column **Status** uses a single marker to indicate the overall status of each difference that has been found. The markers have the following meaning:
  - **+:** This object has been added.
  - **-:** This object has been removed.
  - ***:** This object has been modified.
- **Path of Modified Object** shows the UNIX path of the file or folder where a difference was detected. The path must be interpreted relative to the volume you had selected for comparison.
- **Changes** indicates the exact type of modification:
  - **A:** The Access Control List has changed.
  - **C:** The creation time has changed.
  - **D:** The data stored in the object has changed.
  - **G:** The group owner has changed.
  - **M:** The modification time has changed.
  - **O:** The owner has changed.
  - **P:** The POSIX permissions have changed.
  - **S:** The size has changed.
  - **T:** The object type has changed.
  - **X:** The Extended Attributes have changed.
- If the object is a file and the file has been modified, the column **Old Size** shows the storage size required by the file for the older of the two selected points in time.
- Similarly, the column **New Size** displays the storage size at the later of the two selected times.

If you move the mouse cursor over an entry in the column **Changes**, TinkerTool System will display a short textual explanation, so you don't need to learn the abbreviations.

For reasons of efficiency, the entries in the table cannot be rearranged in different sort orders. TinkerTool System shows them in the same order as they are processed by Time Machine during backups. You can use the button **Save**… to create a processed report in text form which can then be saved to a file.

2.5.4 Working with Local Snapshots

If at least one of the volumes selected to be part of the backup uses the modern *Apple File System (APFS)*, Time Machine will automatically enable additional features:

- Every time a backup session is started, Time Machine will create an *APFS snapshot* of each APFS volume that is about to be copied. An APFS snapshot is basically a frozen image of the source volume, created at the time the backup began. Even if files are changing while the backup session is running, the snapshot will ensure that Time Machine only "sees" a static picture of the volume. If the backup copy must be restored later, the result will reflect a consistent state of the volume, without any files that have been in an "in-between" condition only.

- Each APFS snapshot will be kept by the operating system on each volume as long as this volume has enough storage space. The snapshot is basically invisible during normal operation and only needs a small amount of additional storage space. It is based on the strategy to never reuse any block of the volume that had been occupied by a file for any new files, even when that file has been deleted or this part of the file has been changed.

- APFS snapshots are not only created when normal Time Machine backups are made, the operating system also creates them when major changes in the system are to be expected, e.g. when an operating system update is about to be installed.

- These snapshots can be used as "restore points" that allow you to very rapidly reset an entire APFS volume to a consistent state of the past. This is done via Time Machine (usually after starting the recovery system), selecting the APFS volume itself, not the actual Time Machine volume, as source for a restore operation. For more information, please see Apple's official documentation on macOS.

This basically means that an APFS snapshot can be used as a local snapshot of Time Machine. Working with these snapshots doesn't require access to the actual Time Machine backup volume.

> Other parts of macOS can use the APFS snapshot feature as well. The list shown on the tab **Local Snapshots** considers APFS snapshots created by Time Machine only. If you like to work with the complete list of APFS snapshots, please see the chapter The Pane APFS (section 3.7 on page 232).

It is under sole discretion of the operating system when to automatically create or to remove APFS snapshots. TinkerTool System gives you additional manual control about these local snapshots, however.

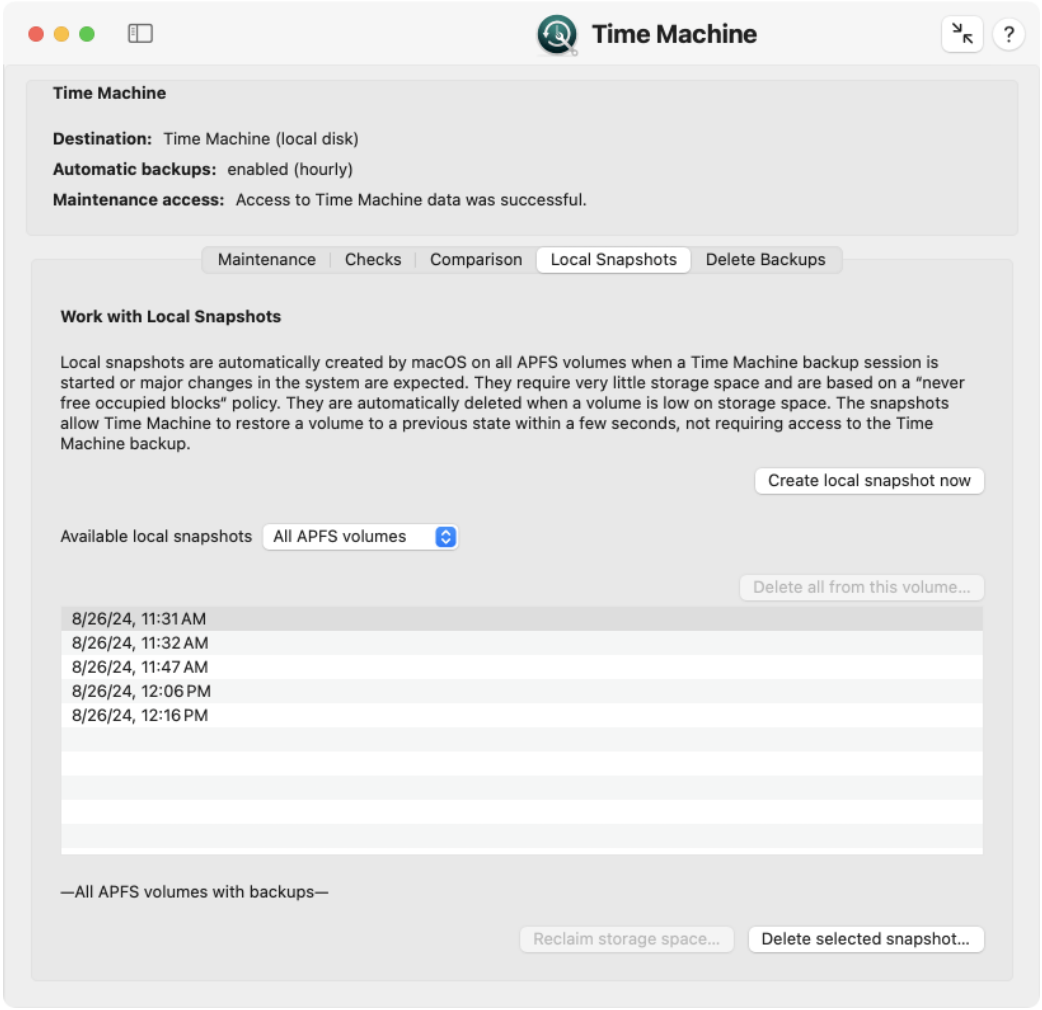


Figure 2.19: Working with local APFS snapshots

- You can create a local snapshot immediately, just by clicking a button. This is helpful to create a well-defined restore point, e.g. when you like to test a possibly "dangerous" action on an APFS volume that might need to be undone in the near future.
- You can review which local snapshots are currently available on each APFS volume.
- You can force macOS to clean up its local snapshots immediately, to bring forward the point in time when this would happen automatically. This is done by specifying

a planned amount of storage space that should be reclaimed during the cleanup. macOS will keep as much snapshots as it can to meet this target.

- You can delete local snapshots of your choice.

To create a new local snapshot on all APFS volumes that are part of your Time Machine backup, perform the following steps:

1. Open the tab item **Local Snapshots** on the pane **Time Machine**.
2. Click the button **Create local snapshot now**.

Creating the local snapshot should typically require less than one minute.

You can review all snapshots using the table **Available local snapshots** on the same pane. The available points in time are listed as separate lines. By default, you will see a list for the entire computer. If more than one APFS volume is in use, it can also be interesting to see the list of snapshots on each volume. Note that the sets of available snapshots can be different on each volume because some volumes may have less free storage space, so they will automatically remove snapshots earlier than others. To select between different volumes, use the pop-up button above the table.

To reclaim storage space on a particular volume, select the volume with the pop-up button above the table, then click the button **Reclaim storage space**…. TinkerTool System will ask you in a dialog sheet how much bytes you like at least to be reclaimed. You can specify a low value (like 1) to make sure that only the smallest possible number of snapshots will be deleted. The operating system will use its standard policies to automatically select the snapshots that should be removed. At the end of the operation, TinkerTool System will show a summary how many local snapshots have been lost and how much storage space has been freed on the volume.

> In some cases, Time Machine may decide to postpone the cleaning operation for some time. In this particular situation, TinkerTool System may not indicate that storage space has been freed yet immediately after requesting a reclaim procedure.

In order to free up as much space from a volume immediately, select the volume at **Available local snapshots** and click the button **Delete all from this volume**. Time Machine will understand this as urgent request to reclaim the maximum amount of storage space currently in use for local snapshots.

To delete a local snapshot manually, select it in the table and click the button **Delete selected snapshot**….

2.5.5 Deleting Time Machine snapshots

As part of its daily routine, Time Machine cleans up backups regularly, if necessary every hour. After a backup session has run, outdated backup snapshots are removed from the backup disk. Sometimes, you may like to remove a specific snapshot manually, e.g. to free some storage space. *You must never do this via the macOS Finder. This could damage the Time Machine backup set, and in addition also the Trash feature of the Finder.* TinkerTool System offers you a safe way to remove a Time Machine backup for a certain point in time:

1. Open the tab item **Delete Backups** on the pane **Time Machine**.
2. Select the snapshot that should be removed with the pop-up button at **Delete**.
3. Click the button **Delete…** next to it.

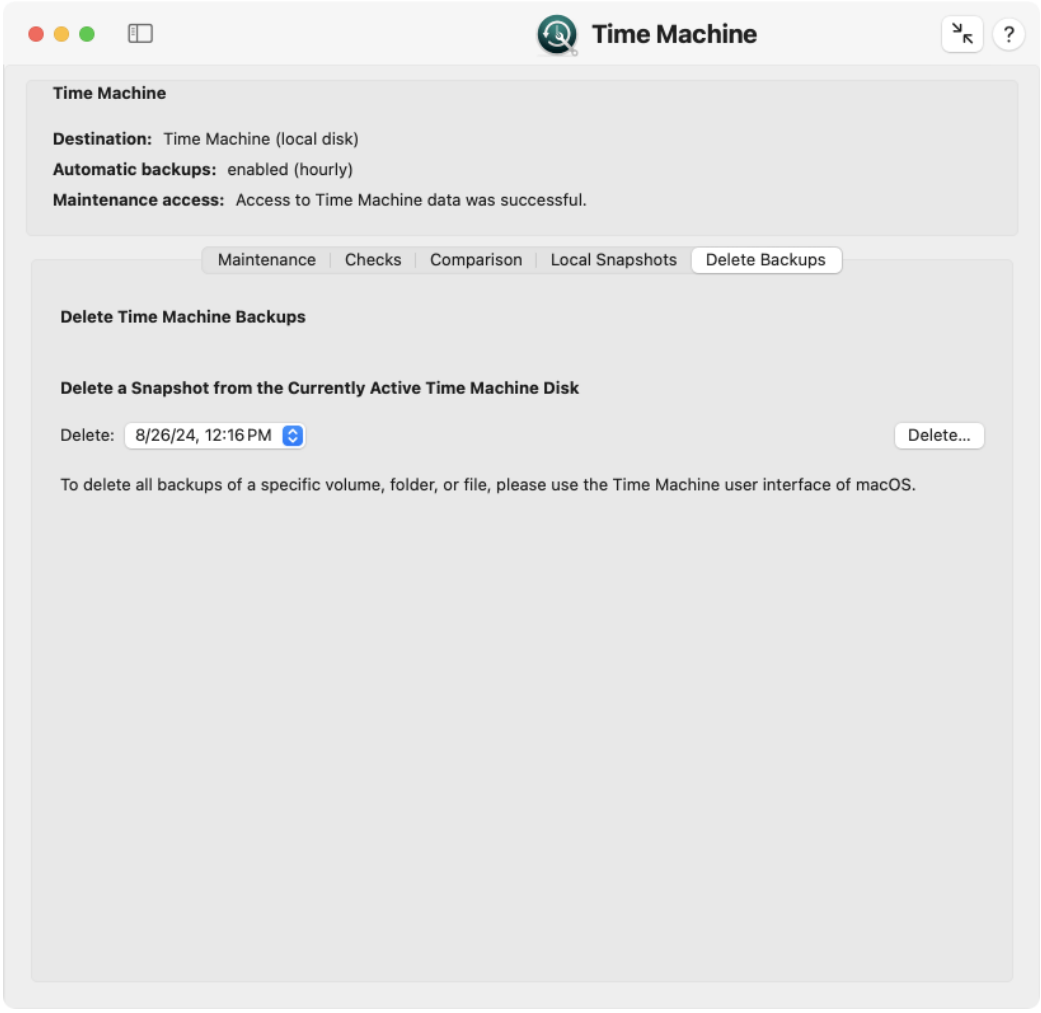


Figure 2.20: Deleting Time Machine backup data

2.5.6 Retrieving Backup Logs

Earlier versions of macOS created a log file each time a Time Machine backup has run and a new snapshot was created. The content was stored as a hidden text file next to

each backup folder. Modern versions of macOS no longer do this. Instead, the general log database of macOS is used for that purpose. Text files with log data are no longer available, but they can be retrieved in hindsight any time later by evaluating the database. Among other information, the log discloses data

- how long the backup run needed to complete,
- whether a full or incremental backup was performed,
- what storage size was needed,
- which files have been omitted,
- whether unusual situations occurred during the backup, etc.

> You need to be logged in as administrator in order to get access to the Time Machine logs.
>
> The logs are only available in English, no matter what language you have chosen for the user interface. The reports are created by macOS, not by TinkerTool System, so their contents can change without notice depending on which operating system version has created them.

To open a log for a snapshot of your Time Machine backup set, perform the following steps:

1. Open the tab item **Log** on the pane **Time Machine**.
2. Select the time of the backup session that is of interest with the pop-up button **Compute log for**. Alternatively, you can click the button **Log for last hour** to get a listing of all Time Machine activities that occurred in the past hour.

TinkerTool System shows the contents of the log in the text area.

2.6 The Pane Issues

2.6.1 Resolving Issues with the macOS Software Update Feature

Under specific circumstances, which depend on your local network, your Internet service provider, and the country you are in, the software update feature of macOS might not always work as error-free as expected. TinkerTool System can help you to resolve typical problems with single mouse-clicks.

What is macOS Software Update?

macOS uses two completely separate technical features to keep software products up-to-date: The operating system itself and additional components which can be seen as parts or add-ons of the operating system are updated via a function called *macOS Software*

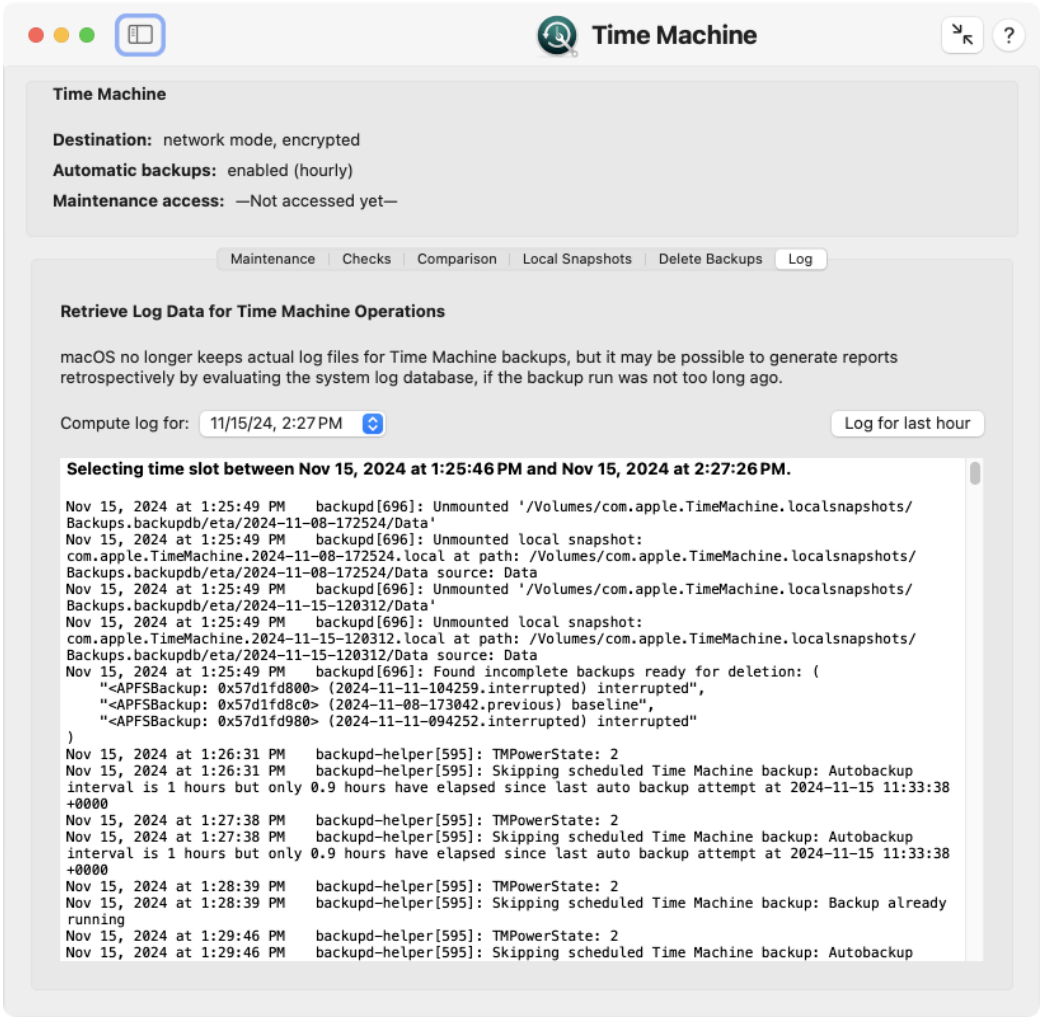


Figure 2.21: Logs for Time Machine backups are no longer created as separate text files, but can be retrieved afterwards

Update. It is based on a newsfeed-like architecture which informs macOS about available downloads. If you participate in one of the *beta software programs* offered by Apple, the standard feed can be redirected to a different one which contains additional beta products, not available to the general public.

For Apps that have been dowloaded from the Mac App Store, no matter if the Apps have been developed by Apple or by third-party vendors, macOS uses a different mechanism which is linked to the App Store itself. This feature is called *App Updates*.

> App updates are presented in the **App Store** application, item **Updates**. On the other hand, macOS software updates are listed in **System Settings**, pane **General** > **Software Update**.
>
> Apple distributes new Macintosh operating systems in form of an App which is in fact the installer for that system. So an *upgrade* of macOS (switching from your current OS to a new generation OS with a different major version number) comes as App from the App Store, while each *update* of the OS (product care which only changes the minor version number) comes via the Software Update function.

Enforcing an Immediate Synchronization with the List of Available Updates

It can happen that macOS doesn't notice the availability of an update immediately. There can be a delay of up to two weeks before an entry finally appears on your local system. In case you have learned from somewhere else, like a press article or news web site, that an update must be available which was not automatically listed by your computer yet, you can force your Mac to contact Apple, retrieving the latest list of update downloads available now. To do this, perform the following steps:

1. Open the sub-item **Software Update** on the pane **Issues**.
2. Click the button **Synchronize List**.

After that, macOS will contact Apple via your Internet connection. TinkerTool System shows a small status panel, indicating live what the operating system is doing. Retrieving and evaluating the up-to-date software list may take several minutes. If new updates are available, System Settings will automatically list them as soon as the synchronization process is completed.

Removing Unsuitable Update Notifications

In some special cases, the opposite of the previously mentioned issue can occur: macOS may list available software updates you are no longer interested in, so you basically have "too many" entries in the list of updates. This can happen shortly after you have changed your personal software feed, for example when you have decided to no longer participate in one of the beta programs. In that particular case, System Settings may still list beta updates although you don't like to see them any longer.

To clear the list of available updates in such a case, perform the following steps:

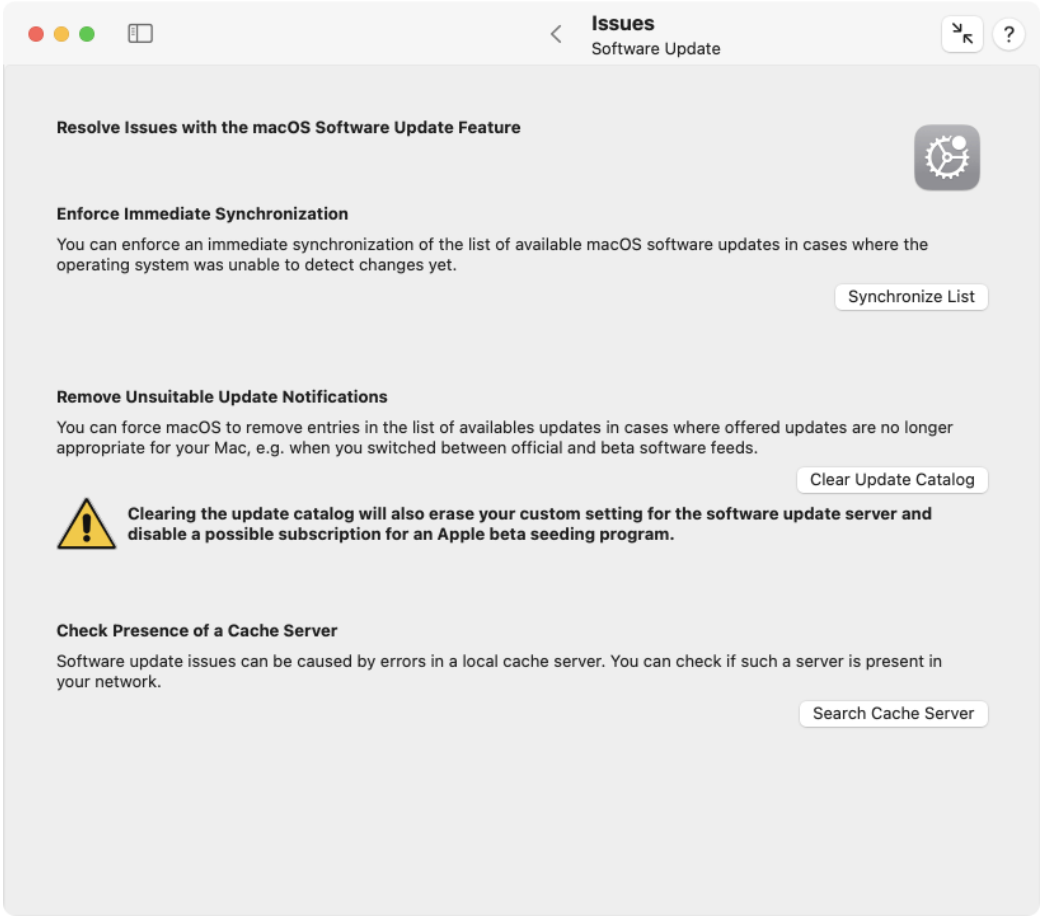


Figure 2.22: Resolving Issues with the Software Update Feature of macOS

1. Open the sub-item **Software Update** on the pane **Issues**.
2. Click the button **Clear Update Catalog**.

Check the Presence of a Cache Server

If you have many Apple devices on your local network, setting up a *content caching server* on your network can greatly speed up access to updates. All you have to do is turn on the corresponding function on a Mac in your network that is running as continuously as possible. This server monitors the data traffic for updates and caches all downloaded data. The other computers on the network detect the presence of the content caching server and can now download updates from it over a fast local line. The update data no longer has to be downloaded again for each computer via the slower Internet connection. If desired, the content caching server can also accelerate read and write access to iCloud services by also caching data locally for this purpose. Multiple content caching servers can be deployed simultaneously for very large networks.

All aspects of a content caching server are fully automated. After turning on the service on the computer that was selected for this purpose and selecting the options, which and how much data should be cached, no further actions are required. Clients do not have to be set up, but use the service automatically as soon as it is available.

For certain combinations of operating system versions of the clients and the operating system version of the server, however, there are known errors in macOS in which the search for updates does not work correctly, or certain update packages are not offered at all or are offered very late. Therefore, when troubleshooting software update issues, it is necessary to know if there are one or more content caching servers on the network. This is not always clear. For example, a mobile Mac user might have accidentally (or even maliciously) turned on the content caching server feature, causing problems when this Mac is present in the local network.

The program can check whether there are content caching servers on the local network and which of them is currently the preferred one used by your Mac to retrieve updates. The IP addresses of a server and the list of detail services offered by the cache can also be determined.

1. Open the sub-item **Software Update** on the pane **Issues**.
2. Click the button **Search Cache Server**.

If one or more servers are available, they will be listed in a separate sheet. The window contains the following data:

- **Client implementation version:** the version number of the software that the currently running version of macOS uses when working with content caching
- **Public IPv4 Address:** the network address currently used by the client when accessing the Internet

A table lists all local content caching servers with a brief description. After selecting a line, the details for each server appear in the lower part of the window:

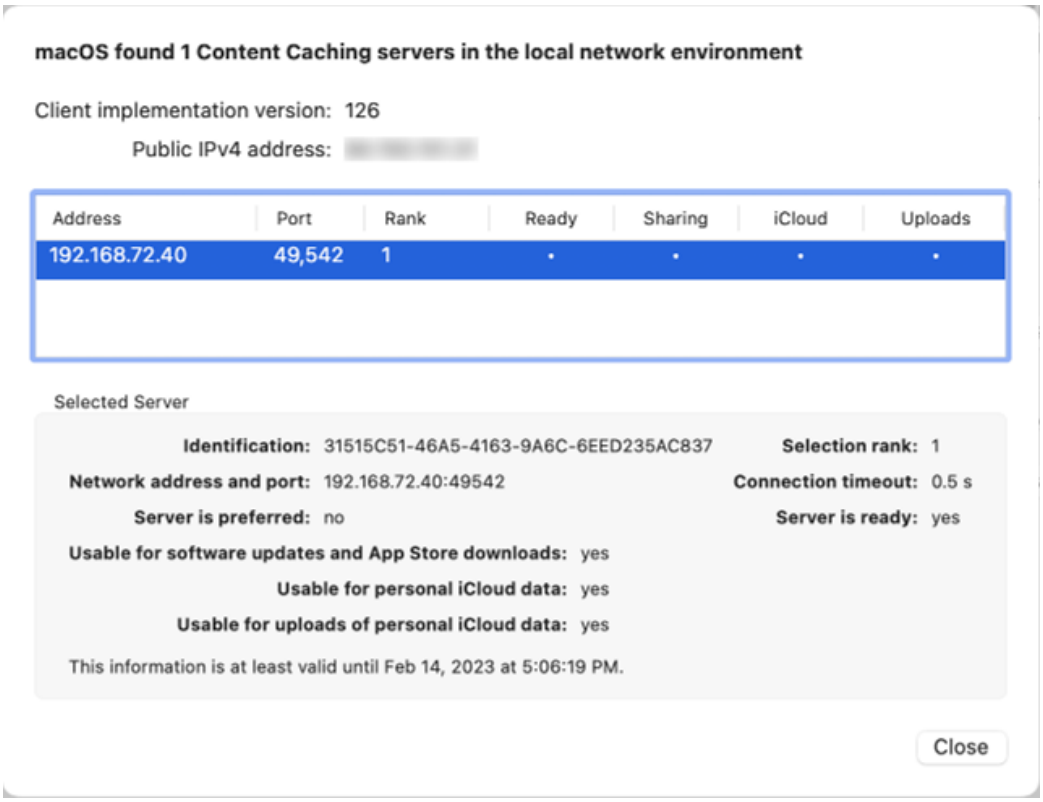


Figure 2.23: If one or more content caching servers are available, they will be presented in an overview

- **Identification:** a *UUID* that uniquely identifies each server worldwide
- **Network address and port:** the IPv4 address of the server in the local network and the port number for accessing the cache service
- **Server is preferred:** a flag indicating whether this server should be preferred over other existing servers
- **Selection rank:** the priority used to select this server if there are multiple servers in the network
- **Connection timeout:** the time after which an access attempt will be aborted
- **Server is ready:** a status indication of whether this server is currently operational
- **Usable for software updates and App Store downloads:** a status indication of whether this server caches software updates and app updates
- **Usable for personal iCloud data:** a status indication whether this server can be used to read iCloud data from users in the local network
- **Usable for uploads of personal iCloud data:** a status indication whether this server can be used for writing iCloud data by users in the local network

In addition, information is given as to when this Mac considers the specified data to be valid. At this point in time at the latest, the information will be refreshed again.

2.6.2 App Store Update

The App Store application introduces an annoying problem as of macOS Big Sur where users receive update notifications for Apps they have updated already, sometimes several months ago. This can happen if you are using your Mac with multiple users and only one of them usually downloads updates for Apps, or if you have multiple Macs and use the App Store on only on one of them, then copying the Apps manually to the others.

A reset of the App Store information for the affected user should usually fix this problem. TinkerTool System offers you to reset either the current user account or all active user accounts of the Mac. In this context, an “active” account refers to a user who has a home folder at the default location on the local Mac (usually in the folder **/Users**).

The reset operation will also clear the overview page of the App Store that lists the recent updates this user has downloaded. The list of purchases or any other data for the user who might currently be logged into the App Store won’t be affected, however.

To reset the App Store application, perform the following steps:

1. Open the sub-item **App Store Update** on the pane **Issues**.
2. Use the buttons at **Select user accounts to perform an App Store reset** to choose whether you like to run the reset for the current user or for all users of this Mac.
3. Click the button **Reset**.

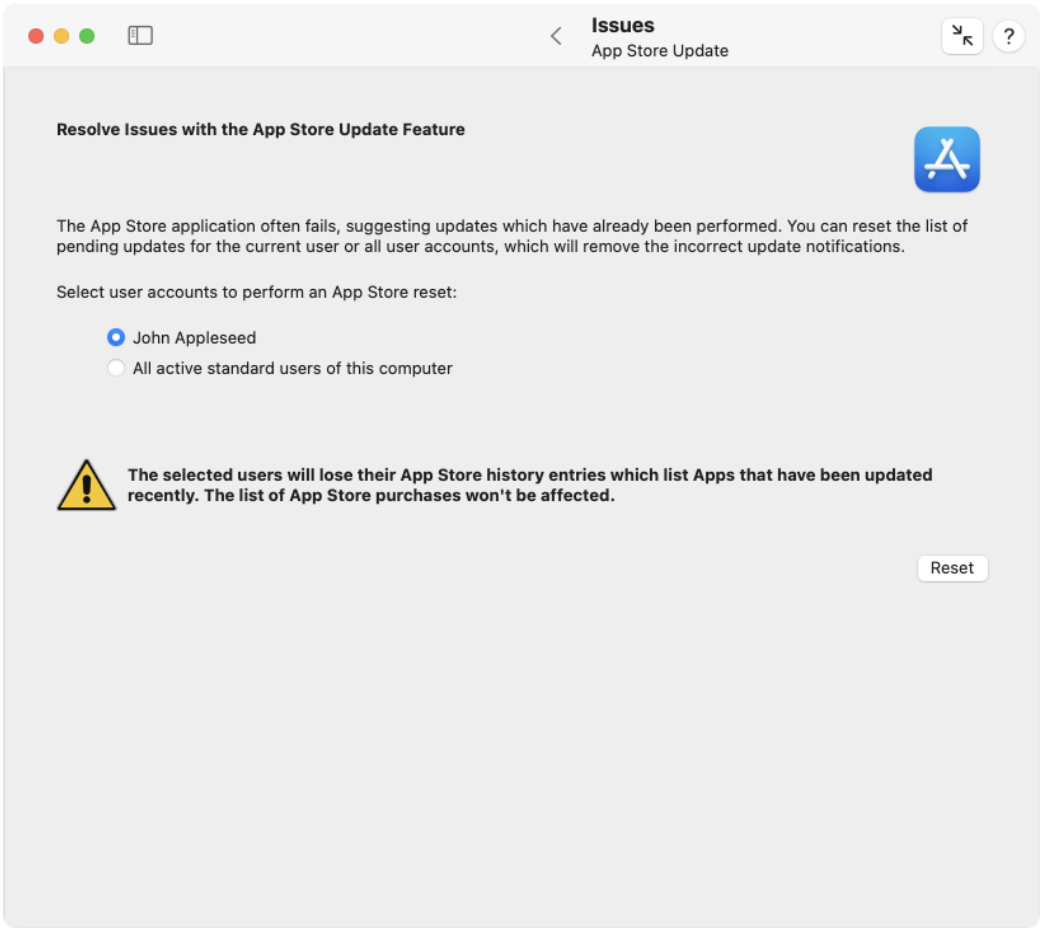


Figure 2.24: Resetting the App Store application can remove invalid update notifications

You should quit the App Store application before you run the reset operation, and you should also make sure that no downloads or updates from the App Store are currently running in the background.

2.6.3 Background Items

With macOS 13 Ventura, Apple had integrated a strongly revised version of system service management into the operating system. The most important change is that helper programs that provide services for "big" applications no longer have to be placed in central folders of the operating system (such as */Library/PrivilegedHelperTools/* for privileged utilities). Instead they can remain in their associated main programs. This has the advantage that nothing needs to be installed or uninstalled for new applications. Once the main application has been copied to the Mac, its embedded utility is automatically present with no special setup required. If the program is later deleted, the embedded helper program is automatically removed as well. To do this, macOS must monitor in the background whether the existing applications contain helper programs that can provide services. The type of each service can be determined based on description files that are hidden in the main program.

Both, new helper programs and old ones, that still want to be compatible with operating systems prior to macOS 13 and therefore cannot use the modern way of embedding in the main application yet, are called *Background Items* by Apple. All detected helper programs are listed on the pane **Login Items** of **System Settings** , under the heading **Allow in the Background**.

Unfortunately, the new term "background item" and the way it is presented is very confusing. Users get the false impression that the listed items are programs that macOS would always start automatically. Additionally, the brief explanation given on the pane **Login Items** provides a similar, incorrect definition.

In reality, "background items" are just *permissions* granted to macOS to *potentially* start a helper program in case the main application would request its services. In some cases, this can mean that a helper program is indeed started automatically by macOS every time the system starts, namely when this makes sense due to the functions of the helper program. But it can just as well mean that a utility is never started, e.g. because the user does not need its services at all. The associated main application specifies the conditions under which a helper program is to be started via an internal definition file.

In addition to the misleading description of what a background item actually is, the new service management in macOS is anything but correct and reliable. There are a large number of internal defects and general design flaws. Among other things, there are the following problems:

- The name of an item is often determined incorrectly and displayed in different ways for different users.
- The associated main application of a background item cannot always be determined.
- In some cases, items are grouped under the name of the software developer for whom Apple has notarized one of the associated main applications. This doesn't make sense, since the user can no longer validate and turn off items individually.

- In many cases, the name of the software developer cannot be determined.
- In many cases, the name of a software developer does not allow the user to deduce which application it belongs to.
- In some cases, a main application calls a utility that is included with macOS. System Settings is unable to indicate “Apple” as a developer.
- It is not clearly distinguished whether the name of the helper program or rather the name of the associated main application is shown.
- A button with an info icon is displayed in some cases, designed to determine the location of a helper program. This button often has no function.
- In cases where indicating the storage location actually works, the user may be tempted into simply deleting the helper. However, deleting it can cause significant damage in the system.
- The notification that a newly added background item should be approved often appears far too late. Sometimes it only appears after restarting the computer.
- Users that have network accounts instead of local accounts cannot approve background items.
- Even if a user approves a background item, macOS often does not start the associated helper, ignoring that the main application may urgently need it. A restart of the computer is required.
- In some cases, approving a background item doesn’t work permanently. After each restart of the computer, the user will again receive requests to add already granted background items, often with dozens of notifications.

Of course, TinkerTool System cannot really fix the many errors and design flaws that occur in different ways in the different versions of macOS, but it can provide two features that offer good workarounds in practice:

On the one hand, you can force macOS to delete the entire service management data for background items, to have it rebuilt with the current system version. Some deficiencies are then rectified for some time. On the other hand, you can have TinkerTool System create its own list of background items. It tries to take the list from macOS, but display it in an error-free way. This can help to understand why macOS considers a particular program a background item and what is actually meant by the often dubious entries in System Settings.

> As explained above, background items are actually user preferences that control which helper programs are allowed to be launched on demand for your user account. The list of background items can therefore be different for each user.

Perform the following steps to reset the service management for background items in macOS:

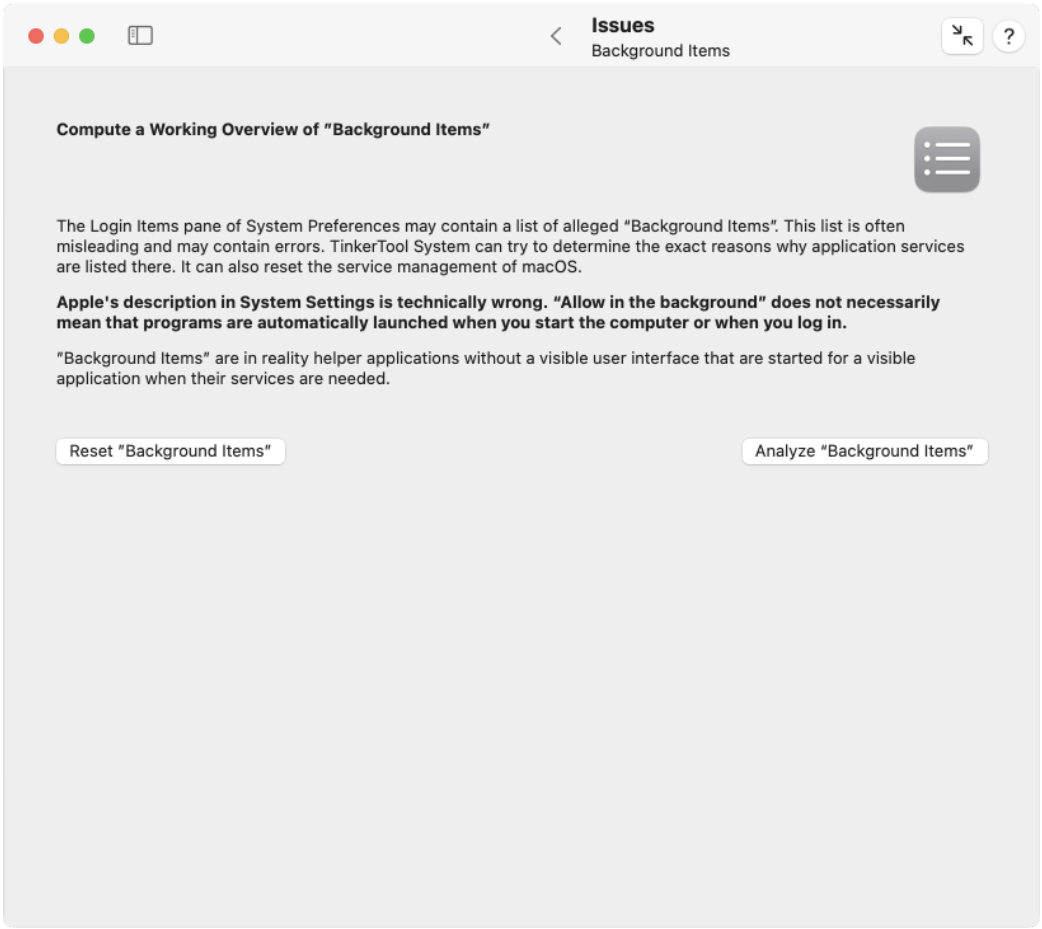


Figure 2.25: TinkerTool System helps to resolve issues with "background items" and to understand Apple's defective list of these items in System Settings

1. Make sure you can restart the computer.
2. Open the sub-item **Background Items** on the pane **Issues**.
3. Click the button **Reset "Background Items"**.
4. Follow the program's instructions. TinkerTool System will restart the computer.
5. Log back into the computer using the same user account.
6. TinkerTool System will automatically restart and confirm that the reset is complete.

Perform the following steps to have TinkerTool System analyze the list of background items. The program will then display a similar list as error-free as possible. You can compare this list to the list shown by macOS in System Settings.

1. Open the sub-item **Background Items** on the pane **Issues**.
2. Click the button **Analyze "Background Items"**.

You receive the following information for each entry of a background item:

- an icon and the name under which the item is listed
- a status display, whether the utility can be started on demand (green) or whether you do not allow the start (red)
- **Developer:** the name of the developer of this program, if it can be determined
- **Component of:** the name of the main application this helper program probably belongs to. For older software which has not been adapted to macOS 13 or higher yet, it is technically not possible to determine this exactly in every case.
- **Type:** the type of helper being launched (see below)
- **Program file:** the actual filename of the helper program being launched
- a button to reveal the program file in the Finder

TinkerTool System distinguishes between the following types of background items:

- **Startup service for all users:** the helper is allowed to be started if necessary once macOS has booted
- **Login service for all users:** the helper is allowed to be started if necessary once any user has logged into macOS
- **Login service for you:** the helper is allowed to be started if necessary once your own user account has logged into macOS
- **Embedded startup service:** the utility resides in the main application and is allowed to be started if necessary once macOS has booted

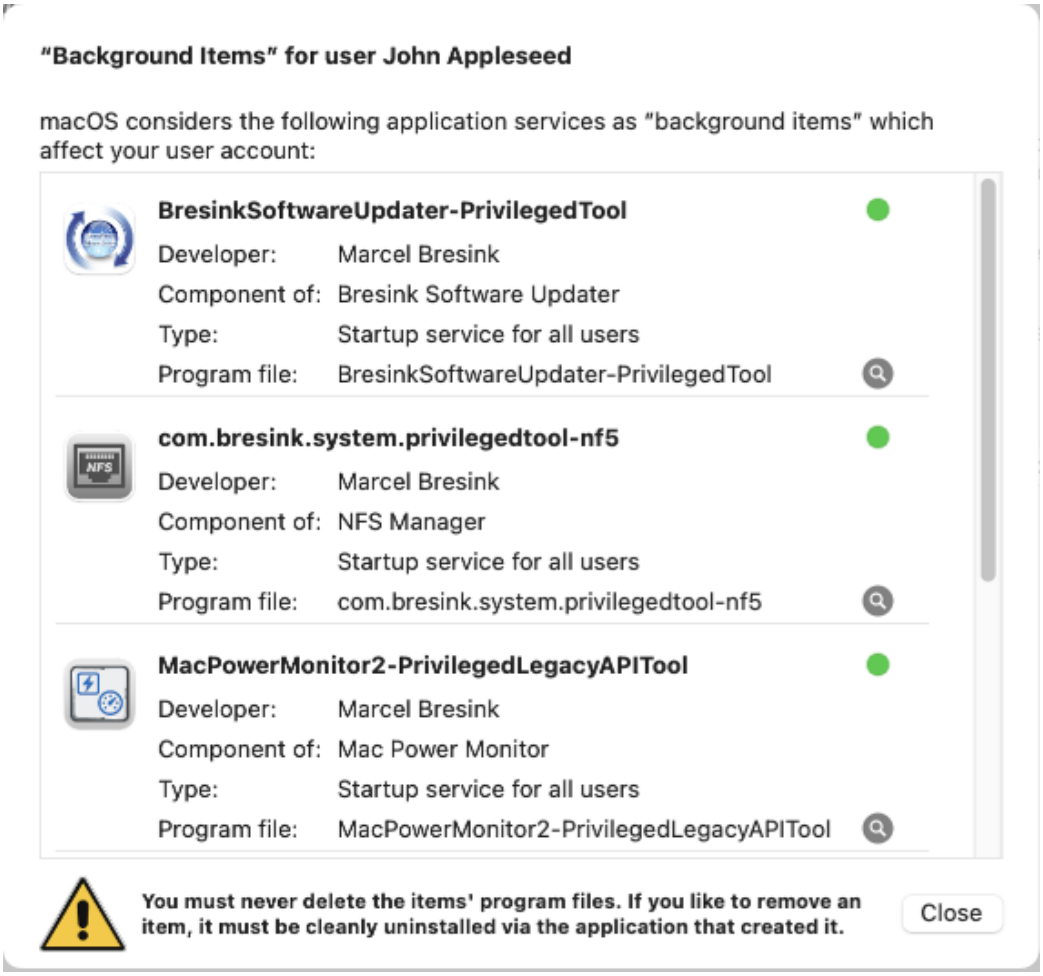


Figure 2.26: The list of background items maintained by macOS can be shown by TinkerTool System in a more understandable way with as few errors as possible

- **Embedded login service:** the utility resides in the main application and is allowed to be started if necessary once any user has logged into macOS
- **Embedded hidden login item:** the utility resides in the main application and will be launched in any case once your own user account has logged into macOS. It is similar to a login item, but it is set up by the associated main application and not via visible user settings.

If you do not know the exact purpose of a background item, it is not recommended to block the start in System Settings. This corresponds to the behavior of all macOS versions prior to version 13. Some main applications can no longer work if you block their helper programs.

Warning: You must never delete a background item's program file. In case of embedded helper programs, this would destroy the main application. With older services, this can result in macOS searching for the missing program every 10 seconds. This permanently leads to numerous log entries and performance problems. If you really want to delete an entry for a background item, you will have to validate in the list (at **component of**) which main application it belongs to. In the documentation for the main application, you will usually find information on how to cleanly uninstall either just the helper program or the complete software (main application and helper program) from the computer.

2.6.4 Fix Problems with Automatic Time Synchronization

There is a known design flaw in newer versions of macOS: If the Mac is switched off without shutting the operating system down correctly, which can, for example, happen in the event of a power failure or, in the case of portable Macs, if the battery is empty, date and time settings may be wrong the next time the computer is switched on again, but they can also no longer be set correctly. In this special case, macOS repeatedly changes the date and time to incorrect values. This can lead to significant additional problems when communicating with other computers on the network or logging in to user accounts.

You should check first whether the system settings for automatic time synchronization are correct.

1. Open the sub-item **Time** on the pane **Issues**.
2. Click **Show Date & Time Settings**.

The corresponding pane in System Settings will open. The normal settings are:

- **Set time and date automatically:** switched on
- **Source:** Apple (time.apple.com.)

- **Time zone:** the timezone valid for your current location

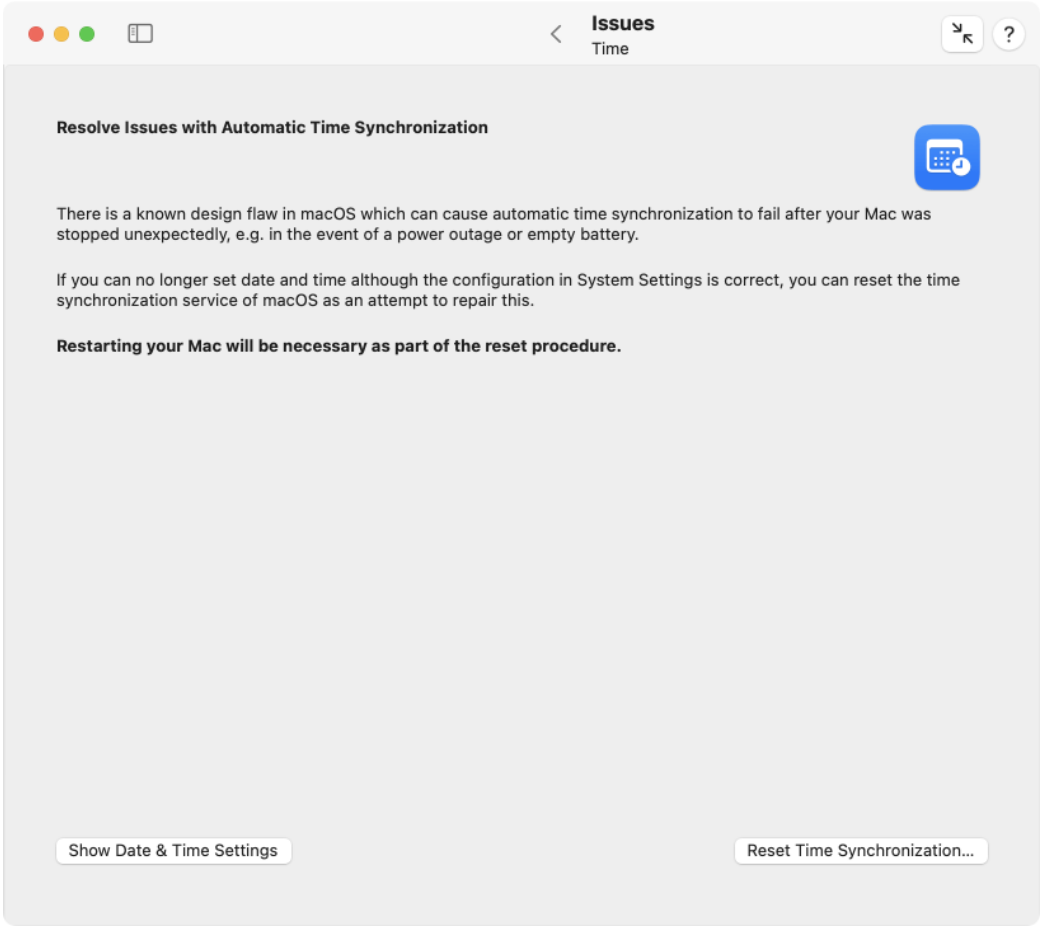


Figure 2.27: A failure to set date and time correctly can be fixed in many cases

If all settings are correct, but time and date are still wrong, you can try to have TinkerTool System fix this problem by resetting the macOS time synchronization service and deleting incorrect data. Note that this process requires restarting the computer. To attempt repair, follow these steps:

1. Open the sub-item **Time** on the pane **Issues**.

2. Click **Reset Time Synchronization**....

3. Follow the instructions given by the application.

2.6.5 Erasing the Partitioning Info of Disks to Resolve Issues with Disk Utility

The application *Disk Utility,* as shipped with modern versions of macOS, is affected by several technical defects. One of the issues can prevent the reorganization of used disks: Depending on the partitioning scheme and previous contents, Disk Utility may reject or fail to erase a disk, so you cannot use the drive for new purposes. All attempts to remove the previous file systems are unsuccessful. TinkerTool System can help in this case, clearing the partitioning info that causes problems in Disk Utility.

Warning: Clearing the partitioning info means that all file systems on the drive in question become inaccessible. All data in all volumes on that disk will be lost. The disk drive will behave similar to a brand new device.

To prepare the disk for successful reuse in Disk Utility, perform the following steps:

1. Open the sub-item **Disk Drives** on the pane **Issues**.
2. Select the disk that should be cleared with the pop-up button **Disk to erase**.
3. Review the current partitioning layout of the selected disk in the overview at **Affected volumes**. TinkerTool System shows the layout in hierarchical order as it was detected by macOS. The application tries to indicate the names and sizes of all volumes found which helps you to identify the correct disk. Note that the overview might include invisible system partitions which might not be shown by Disk Utility.
4. Click the button **Erase Disk**....

Be absolutely sure that you have selected the correct disk for the clear operation before clicking the **Erase** button.

The disk itself is shown by its device name, often supplemented by a serial number or bus identification, which can help you to differentiate between similar disks if you have multiple drives of the same model. Volumes which are currently not mounted are inaccessible which means that TinkerTool System may not be able to indicate the volume names to which you are accustomed. Instead, the internal names of the associated partitions may be shown. If you are not completely sure about the identity of a specific disk, try to mount it in Disk Utility to see the volume names in TinkerTool System, then unmount the volumes again.

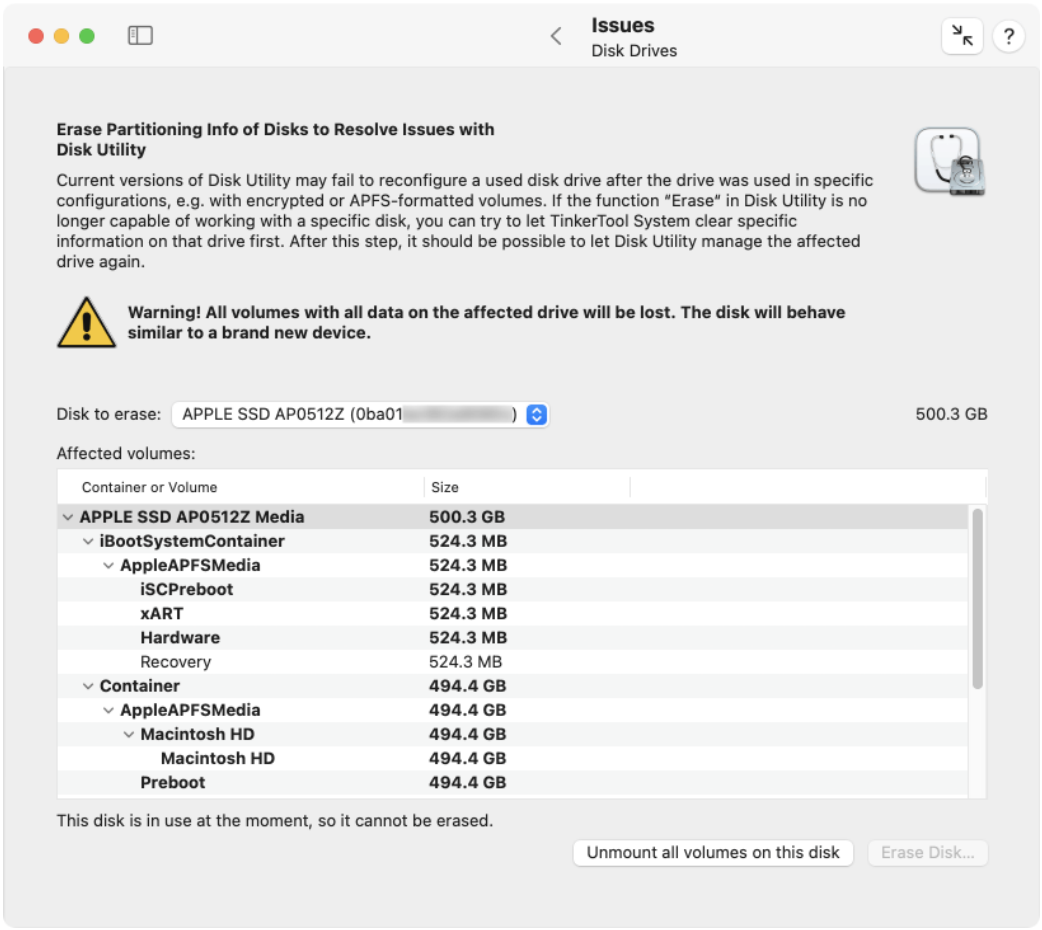


Figure 2.28: Clear disks which can no longer handled by Disk Utility

You can only select a drive for erasure when all of its volumes are inactive. If a disk is still in use, unmount the respective volumes by clicking the button **Unmount all volumes on this disk** below the table.

After TinkerTool System has successfully performed the clearing procedure, you can try to reuse the drive with Disk Utility, using its own **Erase** feature which should work correctly now.

2.7 The Pane Diagnostics

2.7.1 Evaluate RAM Size

Introduction to virtual memory

The amount of main memory *(RAM, Random Access Memory)* installed in a computer can be very important for the system's achieved computing performance. If not enough memory is available, the speed of the computer will significantly decrease. If too much memory is installed, however, capacity that is not really needed will be unused. Unnecessary costs will be the result.

The optimal amount of RAM will depend on how you use your computer, and, in particular,

- which applications you are using,
- which data is processed by the applications, and
- the degree to which programs are being used simultaneously, causing them to be held in memory at the same time.

macOS keeps detailed internal statistics about the amount of memory used by each running program. TinkerTool System can evaluate these statistics to assess whether the total amount of RAM installed in your computer is appropriate for your typical work. This evaluation will allow you to assess whether additional memory will actually enhance performance.

Background Knowledge

As is the case with all modern operating systems, macOS does not allow any running program to access main memory directly. This access is granted only to the inner core (kernel) of the operating system. For each running program (or *process*), the hardware simulates a separate memory space. Each process runs in its own, completely separate space, which appears to be exclusively owned by it. For any given process, the only memory it can "see" is its own; other processes' spaces are completely invisible. That process is incapable of spying on the data space of other processes, and it cannot intentionally or unintentionally write data in their spaces. This is one of the most important methods of ensuring that an operating system is stable and safe. Programs are strictly shielded against each other. Even "rogue" applications cannot crash other processes or the operating system.

This method is called *virtual memory*. Virtual memory is essentially managed by a hardware component inside the processor, called *Memory Management Unit* or *MMU*. For each access to (virtual) memory, the MMU decides which memory should be actually accessed internally: Virtual memory is either being mapped to real main memory, or to special files on the system disk, known as *swap space*. Mapping virtual memory to real memory is done in blocks, organizational units that are called *pages*. With macOS, each page always has a size of 4 KiB.

The system tries to map virtual memory to real main memory as long as real main memory is available. However, if too many processes are running simultaneously, or too much data is being processed, the amount of main memory available will no longer suffice to host all pages of needed virtual memory. In this case, a page from main memory will be transferred to disk to make room. To do this, the system constantly evaluates how discrete processes are using their memory and selects a memory page in RAM which is deemed least likely to be required by its process in the immediate future. Transferring that page's contents to disk frees up the page for use by another process. This transfer is called a "page out" or "swap out." Later on, if that page, now on disk and not in RAM, is accessed by its associated process, it has to be swapped back into main memory. The system will now select another page to be swapped out, and the two pages trade places.

Because accessing main memory is much faster than accessing hard drives, access to swapped out memory can be 10,000 to 100,000 times slower than accessing memory in RAM. For this reason, the perceived speed of a computer can decrease drastically if too many swap events take place, i.e. there is not enough main memory to hold as many of the used memory pages in the quickly accessible area as necessary. (With up-to-date computers that use flash-based storage instead of magnetic disks, the speed difference has decreased, but it is still very significant.) Theoretically, the best usage of memory has been attained when main memory is being used completely (almost no memory is free), and no swap space is in use. In this case, all data will be in the fast RAM and no part of that RAM is left unused.

In addition to swapping out memory pages to the system's disk drive, the latest versions of macOS are capable of using another location to hold pages which no longer fit into available RAM. Because a hard drive is so significantly slower than RAM, the operating system can decide to sacrifice a small part of the RAM, which would otherwise be available for applications, and use this part to store swapped-out pages after *compressing* their contents. This is called *compressed memory*. Instead of swapping a memory page to disk, the system compresses the page and writes it to a specific RAM area reserved for fast retrieval. This process, of the system's reducing the amount of memory available to applications for its own memory compression area is a critical step of course. The system has to consider very carefully whether the gain of compressing/decompressing data in RAM instead of reading/writing to swap space outweighs the effect of losing that RAM for applications' use.

Evaluating the available memory size

As mentioned above, assessing the optimal use of memory is only possible when relating it to the typical usage of memory during the daily work with your computer. Whether you have enough memory will depend on what applications you are using and how you

are using them. *For this reason, a meaningful evaluation of memory size will be possible only if the operating system had the chance to monitor typical usage of memory within a certain time interval.* Perform the following steps to let TinkerTool System evaluate the memory usage statistics:

1. Open the sub-item **RAM Size** in the pane **Diagnostics**.
2. Click the button **Refresh Values**.

The current statistical readings will now appear in the upper box, the evaluation in the lower box **Results**. An evaluation is possible only after the system has been switched on for at least 2 hours.

> The time period in which macOS has collected statistical data is shown in the last line of the upper box. You have to decide whether the computer has been used under a "typical" workload during this period. If the usage has been more untypical, e.g. because you have had more applications open simultaneously than normal, or because you have worked on an unusually large document (or data set) which has consumed an extraordinary amount of memory, the results will not be meaningful.

If you decide that the usage of the computer has not been typical enough to allow for a meaningful assessment, perform the following steps:

1. Restart macOS.
2. Use your computer for at least two hours with the typical workload this computer has been purchased for.
3. Launch TinkerTool System again, and once more navigate to the feature **Evaluate RAM size**.

The upper box lists selected data from the memory statistics maintained by macOS:

- **Installed memory size:** The amount of actually available main memory which can be used by macOS and running processes. This value is usually identical to the total size of RAM modules installed in your computer. In some cases, however, the reading shown here could be lower due to limitations of the hardware. The computer's chip set, or the "shared memory" feature of graphics chips, can reduce the usable amount of memory on specific computer models.
- **Cache memory:** Memory used by macOS to speed up the computer's operation when accessing files or when restarting recently used applications.
- **Used memory:** The size of main memory which is currently used by running processes and the system kernel. It is further subdivided into three different parts, also listed in the following order: pages used by running processes *(application memory)*, pages which are not permitted to be swapped *(wired-down memory*, sometimes also called *reserved memory)*, and pages for memory compression (*compressed swap space* in RAM).

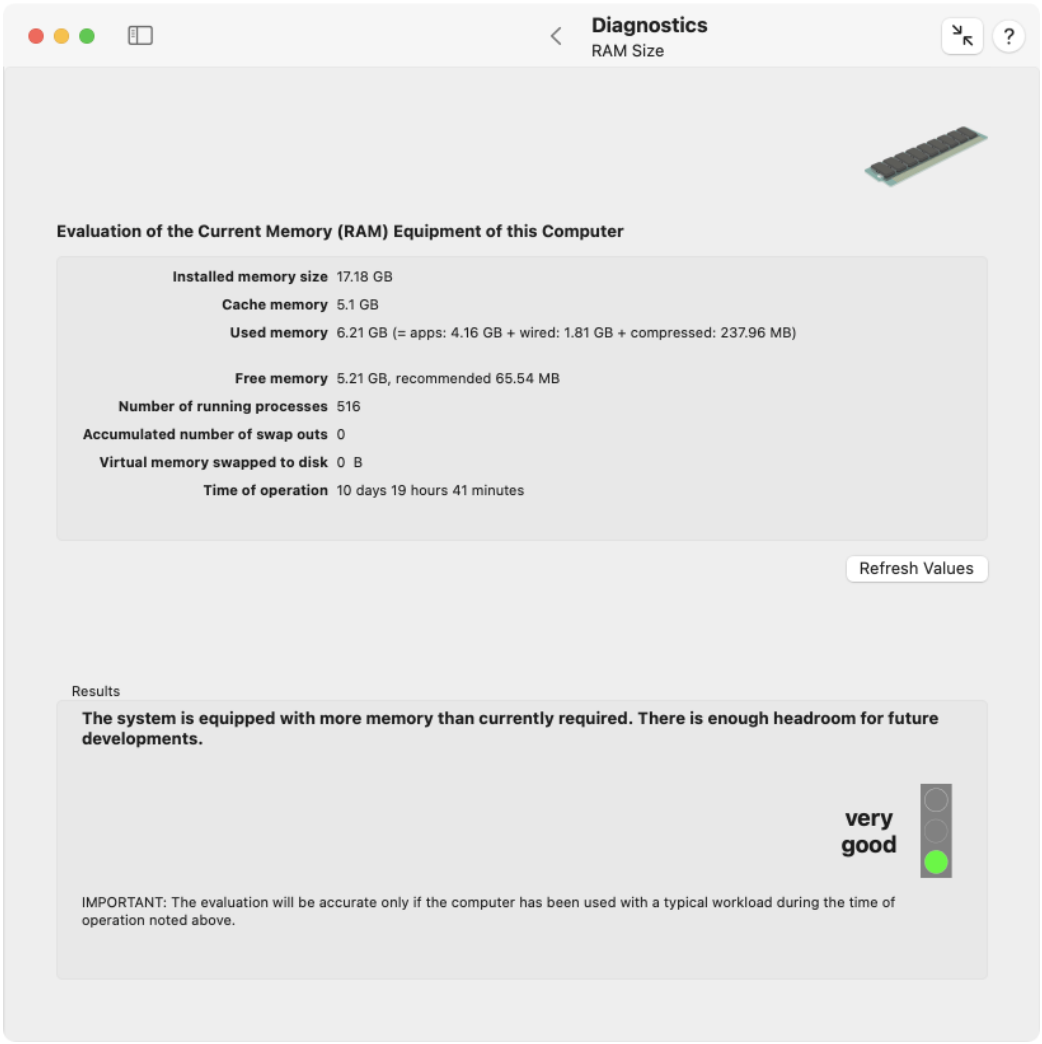


Figure 2.29: Evaluate RAM size

- **Free memory:** The size of main memory which is currently not mapped to virtual memory. This RAM is left unexploited and is not in use. TinkerTool System also shows the recommended free memory size. The system runs best if nearly all RAM is in use, and a very small free part for current handling is left. This recommendation is computed by macOS. The shown reading is the value on which the system bases its memory usage policies.
- **Number of running processes:** The number of processes currently running. Each process is using virtual memory.
- **Accumulated number of swap outs:** The total number of swap-out operations that have occurred during the time of operation of macOS.
- **Virtual memory swapped to disk:** The size of the swap space currently used by running processes.
- **Time of operation:** The time since the last start of macOS. The listed data has been collected during that period.

The box **Results** shows the current evaluation based on the statistics shown in the upper box. The assessment contains a textual explanation and a short overall result like "good" which is additionally represented by the image of a traffic light. The program differentiates between the following results:

- **very good:** The system is equipped with enough main memory and currently has even more memory than is actually needed. With this configuration, the system will have enough reserve performance for future developments.
- **good:** The amount of main memory matches the amount actually needed rather well. A good balance between price and performance has been reached. From an economical point-of-view, this is the best solution.
- **fair:** The system could run slightly better with a bit more memory. The available amount of memory is not in such a short supply, however, that the situation is critical. Expanding memory will increase performance for some degree, but the effect will not be great.
- **bad:** The system does not have enough memory for its typical usage and is significantly slowed down for this reason. If technically possible, you should increase its RAM size. Expanding memory will result in a perceivable performance gain. If the maximum amount of memory has been reached already, you should migrate to a larger computer or reduce your workload.

2.7.2 Inspecting Optical Disks

If your computer contains one or more optical disk drives with write capabilities, you can use TinkerTool System to retrieve detailed information about inserted disk media, such as CDs, DVDs, or Blu-Ray Discs. This feature can help determine the actual manufacturer of a

storage medium, or retrieve information about the recording format of a disk. Depending on the type of medium and its storage format, the amount of data you can retrieve will be very different. With appropriate media, TinkerTool System may include the following detail information in the results:

- identification name of the drive
- firmware revision of the drive
- type of the inserted medium
- media behavior, i.e. compliance with a recording standard
- number of recorded disk sessions
- manufacturer of the disk
- number of recording layers
- diameter of the disk
- supported rotational speeds for this combination of media and drive
- storage capacity of the medium

Whether specific items can be retrieved or not depends not only on the type of storage media, but whether data has already been recorded on the disk.

To inspect optical disk media, perform the following steps:

1. Open the sub-item **Optical Disks** on the pane **Diagnostics**.
2. If multiple optical drives are connected with your computer, select the desired drive with the pop-up button **Disk Drive**.
3. Ensure that the media to be inspected has been inserted into the selected optical disk drive. You can use the button with the eject symbol to eject a disk, or, in case of a drive with a disk tray, use it to open and close the tray. Wait until drive and macOS have recognized the inserted disk.
4. Click the button **Inspect Disk**.

The analysis will be shown in the **Results** box after a few seconds.

Note the difference between the items **Media Type** and **Media Behavior**: If you have recorded digital video on a disk of type DVD+R and have correctly finalized this recording session, the physical type of medium will be **DVD+R**, but the disk will ultimately behave like a **DVD-ROM**.

> If you are not using the typical Apple “Superdrives”, the application will only support optical drives that can both read and write disks.

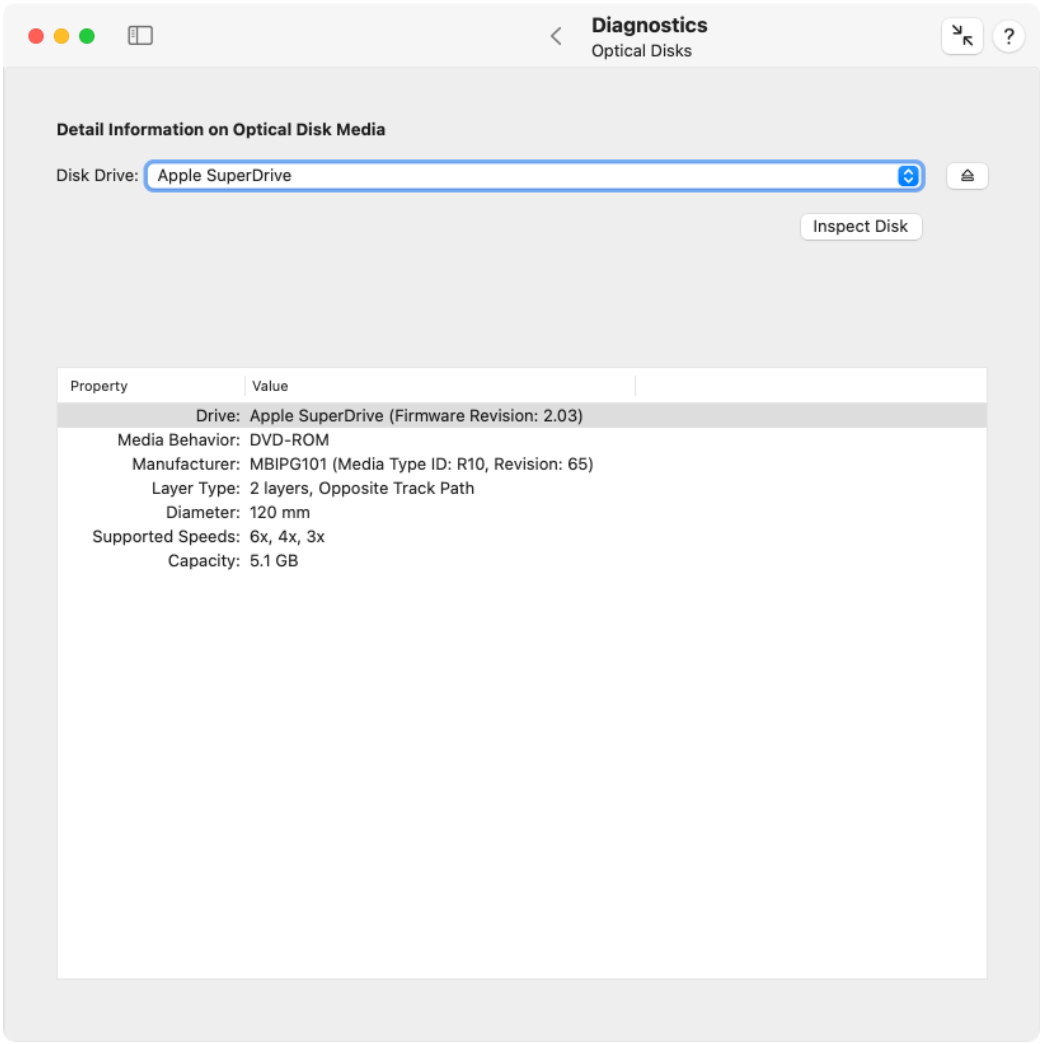


Figure 2.30: Inspect optical disks

2.7.3 SSDs

Before discussing solid state drives (SSD) , also called "flash storage" by Apple for previous generations of Macintosh systems, we should first review how conventional magnetic hard disk drives handle file deletion. On hard disks, file deletion is a simple, quick operation. The operating system erases the file's entry from its folder and informs the file system that the disk blocks used by the file are now free and available for reuse. The old data remains in the blocks until the disk drive overwrites them with data from a new file.

For technical reasons, the deletion procedure is not so straightforward for SSD storage. Although, from the point-of-view of the operating system, an SSD data block is exactly the same as a hard drive block, they cannot be simply overwritten with new data. It is first necessary to explicitly clear them completely, a time consuming operation, before writing new data. The controller of the SSD has to erase each bit of a data block at the physical level, internally resetting all flash memory cells that make up each block. A write operation on a flash storage device will thus be significantly slower if the drive does not have a reserve of empty storage blocks that can be used for the incoming data. The operating system may have to wait for the SSD to prepare an empty block that can be used for a pending write operation. "Empty" in this case means either that this is a brand new, never used storage block, or is a previously used block which has already been cleared.

If large amounts of data have been written to an SSD in the past, the likelihood that either unused or cleared blocks are still available will be lower. The speed of write operations decreases as more data is written. To resolve this problem, the drive must try to clear unused blocks as early as possible. This way, the chance to have empty blocks in reserve, available immediately for incoming write operations, is much higher. But how should the drive "learn" which blocks are no longer in use? On magnetic disks, the drive did not need to "know" that.

To indicate to a storage device that a particular block is considered free by the operating system, so that this block can be prepared for later reuse, the *Trim* command was introduced. Trim commands are part of the ATA8-ACS2 industry standard which specifies how computers should communicate with modern disk drives. So in addition to just updating its own file system information that show which blocks are free, the operating system can now inform the disk drive, too, which blocks are no longer in use. When an SSD receives a Trim command for a specific storage block, it will place that block on its to-do list for cleaning. When the drive has time for cleanup operations, it will then clear the corresponding flash cells in the affected blocks. The likelihood that incoming write commands will find immediately usable free blocks increases, so write operations should be executed as fast as possible.

In a default configuration, macOS won't send Trim commands to all SSDs, but only to flash storage drives provided by Apple, because in this case the operating system is safe to assume that the Trim commands are implemented correctly by the drive, so the commands won't lead to data loss or data corruption.

Very old SSDs (from a time before Trim was standardized) can have internal design flaws, and as a result may not handle Trim commands correctly. This is dangerous, because it can actually lead to situations where the drive clears the *wrong* block. This could result in 512 bytes of zeros overwriting the actual data within a file. To avoid this danger of data loss or corruption, macOS, by default, only sends Trim commands to Apple flash

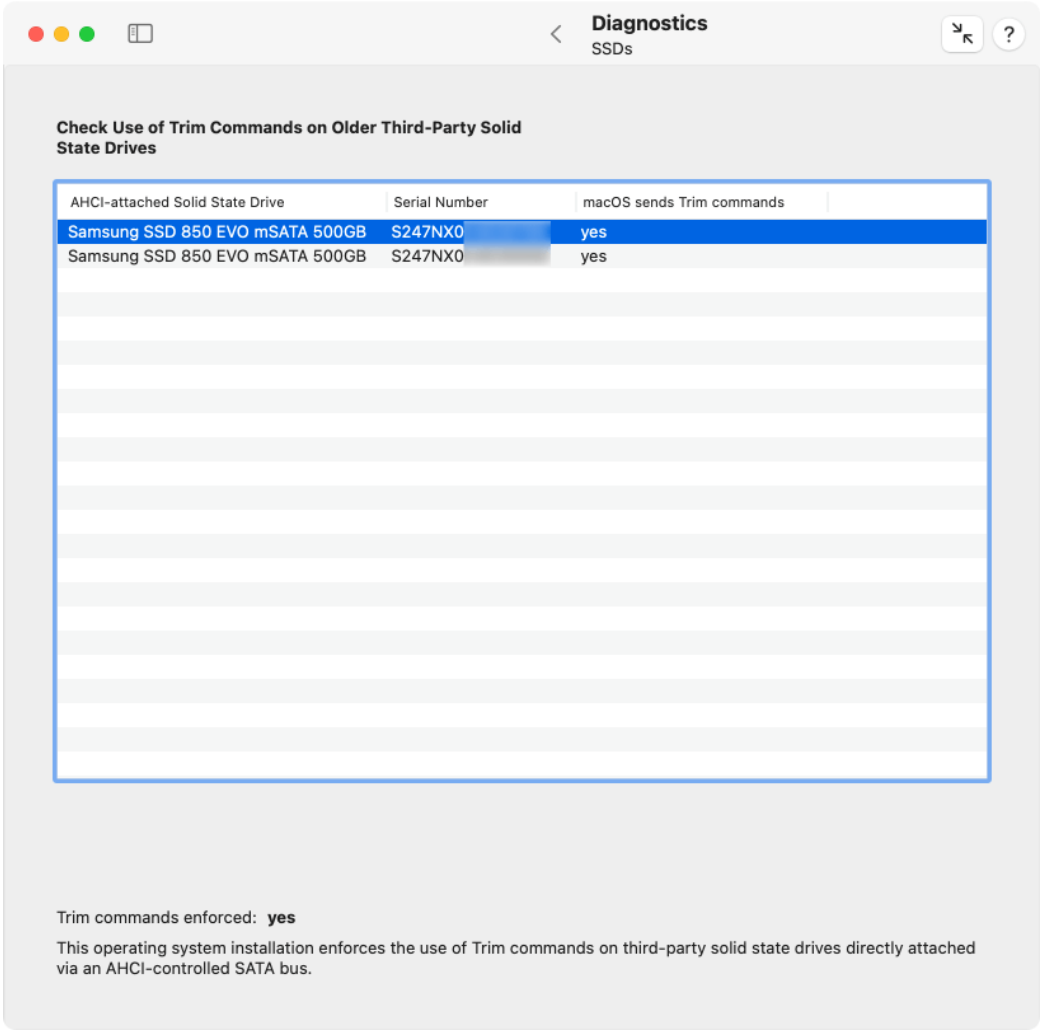


Figure 2.31: macOS can send Trim commands to third-party AHCI-connected SSDs

drives, because it knows that the commands will be implemented correctly.

However, Apple lets you decide whether to use Trim commands with all third-party solid state drives (SSD) attached to your system via a SATA bus and a bus interface based on the AHCI standard (Intel Advanced Host Controller Interface). Changing the mode of operation can be done with Apple's program **trimforce** which must be executed on the UNIX command line. System Integrity Protection ensures that only Apple software can be used to either enable or disable this setting. We won't describe the usage of **trimforce** here. For more information, please see Apple's documentation.

TinkerTool System can check the actual mode of operation currently chosen by macOS to communicate with solid state drives. Open the sub-item **SSDs** on the pane **Diagnostics** to do that.

> SSDs with SATA interfaces and AHCI protocol are outdated technology. Modern Macs use SSDs with the NVMe protocol or "raw" flash memory chips that are directly connected to the processor. Here, the former Trim lock for old SSDs does not matter any longer. TinkerTool System won't show such modern flash devices in the table.

The table on this sub-item shows you all relevant SSDs currently attached to your Mac, and also lists whether Trim commands are sent by macOS. You may like to verify the status of all SSDs before and after reconfiguring the operating system with trimforce (after the computer is restarted). The status line below the table indicates whether the trimforce setting is currently enabled in the operating system or not.

2.7.4 Flash Health

SSDs, or more exactly, the flash memory chips that comprise such storage media, are subject to wear and tear, just as magnetic hard drives. Although there are no mechanical parts that could wear out, each flash memory cell can only withstand a limited number of erase or write operations due to its design. When a certain amount of reprogramming operations is exceeded, the memory cell can no longer switch between its *0* and *1* states reliably. The affected bit "gets stuck" and the entire storage block in which this bit is located must be blocked, because it is no longer working correctly. The controller of the flash storage is prepared for such cases and ensures internally that all blocks wear out as evenly as possible. In addition, the storage space is overprovisioned, i.e. there is more hidden space available than is reported to the outside world. The "superfluous" space is used on one hand to compensate for the slow speed of erase operations (see previous section), by always having enough pre-erased blocks available on reserve for pending write operations. On the other hand, it is used to replace worn-out storage blocks.

You can check the health of flash memory in your Mac by letting TinkerTool System read out internal SSD statistics. Among other items, you can retrieve the number of read/write operations that have been executed, how long the SSD was in operation, whether there is still enough spare storage available, and how much of the expected lifespan has already been consumed. It does not matter whether this is a real SSD drive, or whether the Mac uses pure flash memory chips (as is common with all modern Macs), where an Apple processor simulates the presence of an SSD drive. However, it is important that the

device is an original component of Apple for the respective Macintosh model. The health of third-party SSDs is not automatically monitored by macOS, so it cannot be retrieved by the pane **Flash Health** in that case.

> Accurate values are only guaranteed if communication with the flash unit is based on *NVMe technology (Non-Volatile Memory Express)*. This is the case for all modern Macintosh systems, but for some older Macs which used AHCI communication, macOS will support a very small number of health readings only. TinkerTool System will display this accordingly.
>
> It is not necessary that the flash storage is in use or contains a mounted volume to let it appear in the overview. SSD units which are part of an Apple Fusion Drive are also automatically included in the list.

To let TinkerTool System read out the data that has been collected about Apple flash storage, perform the following steps:

1. Open the sub-item **Flash Health** on the pane **Diagnostics**.
2. Click the **Refresh** button in the lower right hand corner.

All recognized flash drives provided by Apple will now be listed in the upper table. If there has been a problem while retrieving the data, or no original parts of Apple could be found, the table will stay empty and the message **–no entries–** will be shown. After clicking a line of the table, the readings for the selected drive are shown in the lower half of the window.

The meaning of the different items is as follows:

- **Model:** The official model designation Apple uses for this SSD (or simulated SSD, respectively).
- **Revision:** The model revision of the SSD, related to both hardware and firmware.
- **Serial number:** The serial number of the SSD. The numbers of real SSDs can usually be recognized by the use of capital letters. Simulated SSDs often have a fix random code containing the digits 0 to 9 and the small letters a to f only.
- **Current temperature:** The currently measured operation temperature of the flash memory. The unit is determined by your personal locale settings.
- **Data read:** The absolute amount of data which has been read from flash memory during the past lifetime of the SSD.
- **Read commands:** The number of read commands sent from the attached computer to the SSD during its past lifetime.
- **Data written:** The absolute amount of data which has been written to flash memory during the past lifetime of the SSD.

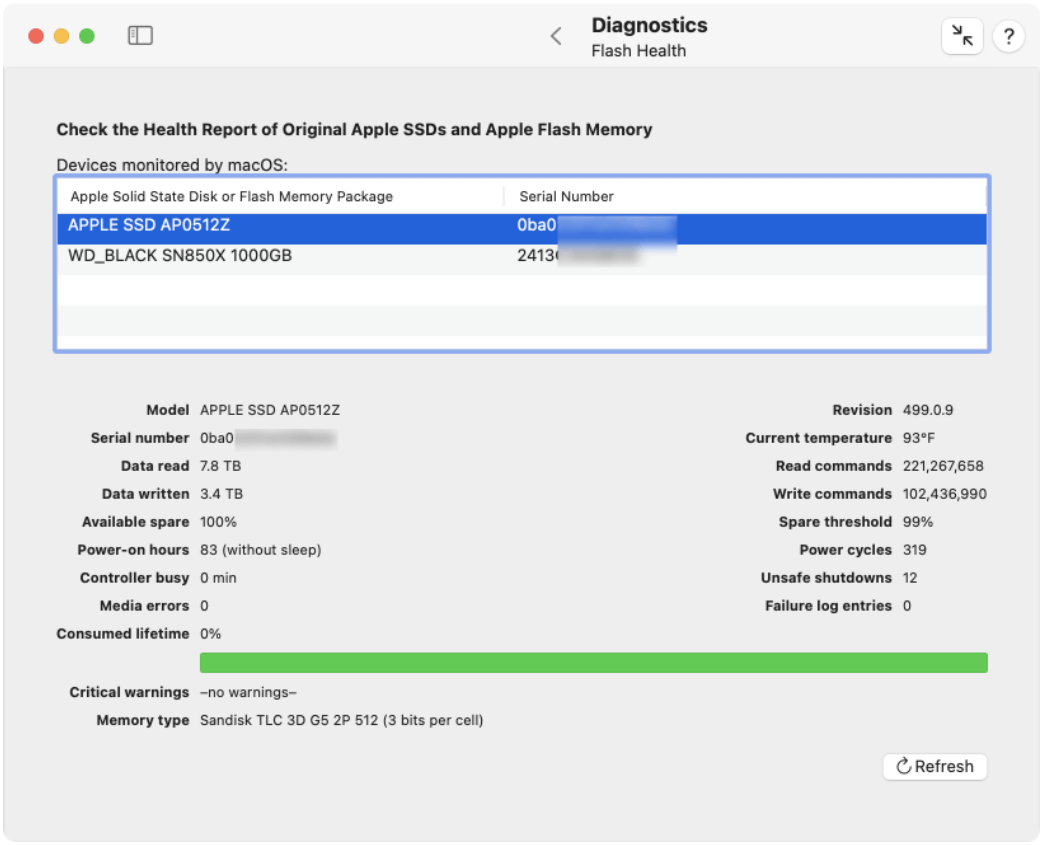


Figure 2.32: Check the health of original Apple flash storage

- **Write commands:** The number of write commands set from the attached computer to the SSD during its past lifetime.
- **Available spare:** The still available amount of spare memory that can be used to replace defective flash storage blocks. The absolute amount is usually a trade secret of the manufacturer. For this reason, the amount is presented as percentage value since manufacturing. The initial value is 100% and decreases with age.
- **Spare threshold:** The value set by the manufacturer at which the remaining spare is considered critical. When the percentage value for the spare falls below this value, the lifespan of the flash memory unit is about to end shortly. The SSD or the logicboard should then be replaced.
- **Power-on hours:** The duration in hours in which the SSD was switched on completely. Sleep mode of SSD or computer does not count as uptime.
- **Power cycles:** The number of on/off cycles during the past lifetime of the SSD.
- **Controller busy:** The number of minutes where the controller of the SSD was so under load that it could not execute pending commands immediately. This value can be used to assess how strong activity and workload on the SSD have been in the past.
- **Unsafe shutdowns:** The number of events where the SSD has lost power without having been previously informed by the attached computer to prepare for a shutdown. This happens, for example, in the event of an unexpected power failure. The controller of the SSD protects itself against such incidents by using its own miniature emergency power supply.
- **Media errors:** The number of errors in flash memory that could be detected via checksum operations, but could not be corrected. Incorrect data was stored or delivered.
- **Failure log entries:** The number of error situations the controller has observed and recorded internally during the lifetime of the SSD.
- **Consumed lifetime:** The percentage of estimated lifetime which has already been consumed by operating the flash storage. For a brand new device, the value is 0%. When the SSD has reached its expected endurance, considered normal by the manufacturer, the value will be 100%. If the unit lasts longer than expected, values between 100% and 255% can be shown. The adjacent bar symbolizes the estimated remaining lifespan. For brand new storage, the bar is completely green. With aging, the green bar becomes smaller and is replaced by gray. The estimation is made by the SSD controller, not by macOS or by TinkerTool System.
- **Critical warnings:** A list of warnings related to the health of flash memory which has been recorded by the controller in its permanent error log. Common warnings are:
  - the amount of spare storage has fallen below the critical threshold

  - the specified operating temperature has been exceeded
  - a high number of media errors has been observed
  - storage media has been set to read-only mode via a hardware setting
  - the controller's internal emergency power supply has failed at least once

- **Memory type:** This information is only available for specific models of the latest Mac model series. It refers to flash memory directly attached to an *Apple Silicon* processor. If possible, the manufacturer and marketing name of the flash memory will be shown. The basic flash technology used may also be indicated, specifically the number of bits which can be stored per cell. Flash memory of type *TLC (Triple Level Cell)* can hold 3 bits per cell, for example. A higher number of bits usually means more storage space at a lower price, but also less operational reliability.

2.7.5 Performing a Quick Test on Cooling Fans

Many Macs need to be cooled constantly, which is done by one or more blowers which pull fresh air into the computer and push out hot air. Most of these fans are continuously monitored and are controlled by an independent auxiliary computer built into your Mac. In older Macs, this is the *System Management Controller (SMC)*, in later Macs an *Apple T2* processor running Apple's BridgeOS operating system, and in modern Macs with Apple Silicon, the M processor itself. Fans are mechanical components which are constantly in use when the computer is active, and as such they are subject to wear and tear. If you hear unusual noise from your Mac and you suspect that one of its fans is no longer working correctly, it is helpful to quickly test the fans without having to open the Mac.

TinkerTool System can do so by temporarily forcing a fan to accelerate to its specified maximum and showing you the current rotational speed values. By listening to the fan's response, you can easily identify its location and determine whether it appears to be behaving normally.

> As of December 2017, Apple has begun to protect the fan control hardware of some Macintosh model series from access by applications. In this case, TinkerTool System cannot determine the names and locations of the fans.

To run a test on one or more fans, perform the following steps:

1. Open the sub-item **Fans** on the pane **Diagnostics**.
2. Select one or more fans in the table that should be tested.
3. Click the button **Test selected fans**….
4. When you like to end the fan check, click the button **Finish test**.

The current speed values are shown in the table and are updated continuously. If you select a single line in the table, technical details about the fan and its approximate location within the Mac's case are shown below the table.

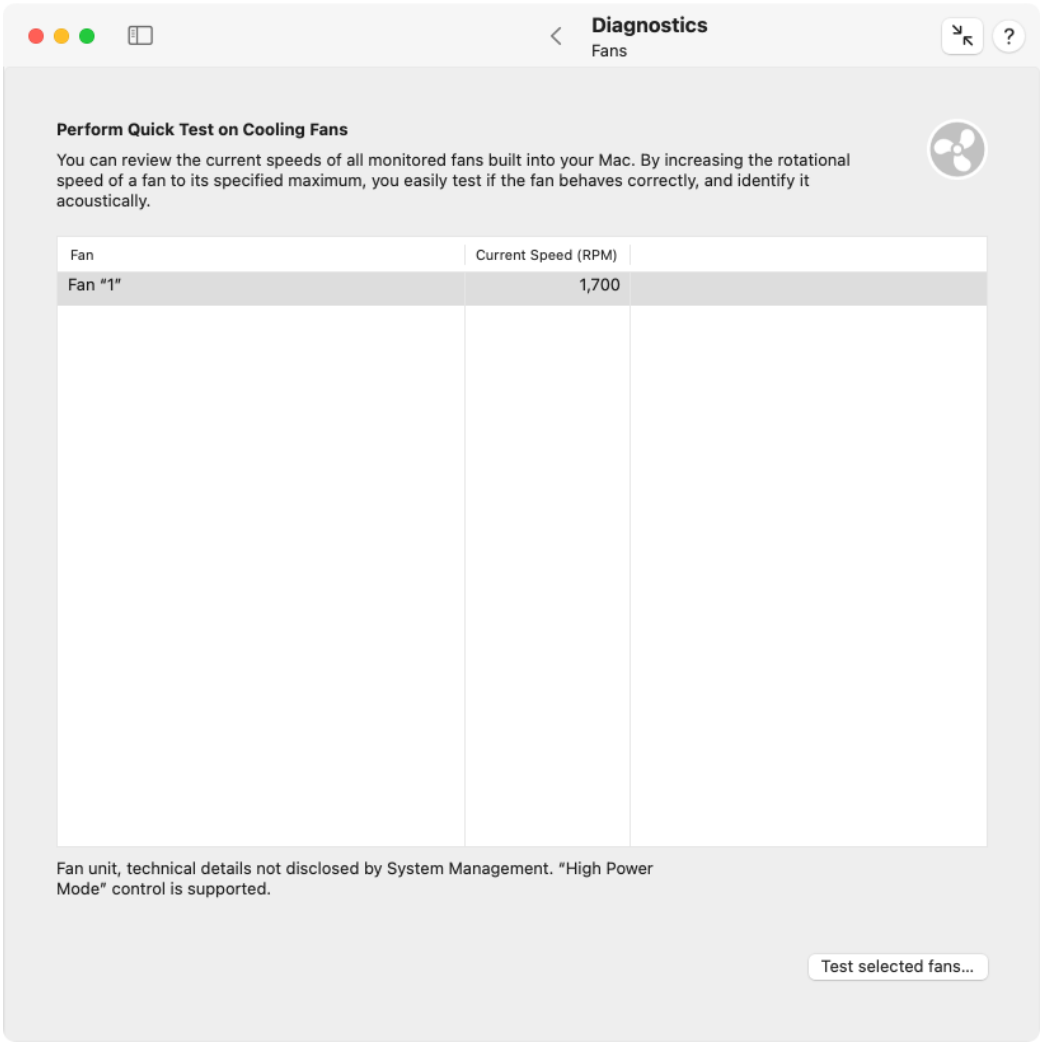


Figure 2.33: Check the cooling fans of your Mac

> If you are using a third-party application to manipulate the built-in standard fan control of the Mac, TinkerTool System will not interfere with that application and an error message is shown in the pane. To run fan tests you will need to deactivate the other application first, then restart TinkerTool System.

Additional considerations for modern Macs

For some computer models released as of November 2023 or later (M3 processors or higher), the fans *and the fan control unit* can be powered down completely if the system is not warm enough to require any cooling. Different from earlier hardware generations, applications like TinkerTool System cannot override this any longer. The fans remain switched off as if they didn't exist. The application tries to detect this, signaling this special situation with an error message shown below the fan table. To test the fans in this particular setup, perform the following steps:

1. Put computational load on the system so that the processor cores are enabled and generate heat.
2. Wait until the **Current Speed (RPM)** indicators in the table switch from **0** to a higher value. This will indicate that the fan hardware was switched on.
3. Quit TinkerTool System.
4. Restart TinkerTool System. The fan control error message should no longer appear and you can test the fans as described previously.

If you don't have an application that forces the Mac to execute a continuous workload, you can download our free utility **SystemLoad**:
`https://www.bresink.com/osx/SystemLoad.html`

2.7.6 Login Time Accounting

macOS is a Unix system, so it has its roots in classic *time-sharing computing* that was used as of the 1950s and onwards. Users connected to a large central computer via a terminal line, logged in with their accounts, ran some programs, and disconnected again. Use of the computer had to be paid per minute. The connection time statistics necessary for this type of accounting are still kept today. TinkerTool System allows you to get access to the data. You can retrieve either the total connect time per user or the total time the Mac was used per day.

1. Open the sub-item **Usage** on the pane **Diagnostics**.
2. Select one of the report types listed in the lower left corner.
3. Click the button **Compute**.

The results are shown in the table. Please consider the following:

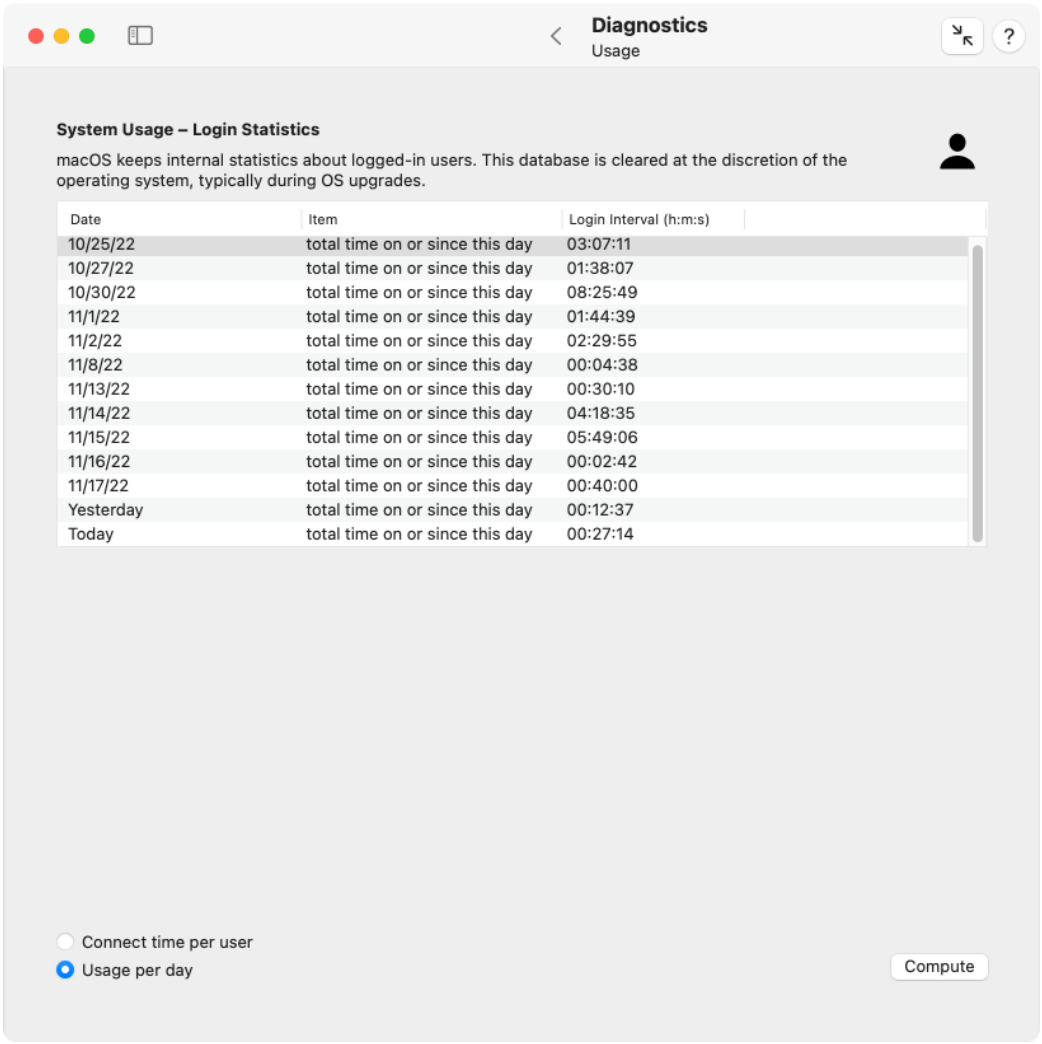


Figure 2.34: Retrieve the login time statistics kept by macOS

- Login intervals are listed in the format hour/minute/seconds, separated by colons (:). If a time interval is longer than one day, the number of days will be shown additionally with the unit *d*.
- The connect time records are collected automatically by macOS. TinkerTool System has no effect on the accuracy of the data. The operating system may delete the internal statistics at its own discretion. This usually happens during operating system upgrades.
- Login time is the time interval between the event where a user logged in (either automatically via macOS or FileVault, or manually by entering her password) and this user logged out (either automatically during a shutdown of the computer, or manually).
- All logins are considered. This includes working at the Mac's screen (which is called a *console login* in time-sharing terms), Fast User Switching, logins via a Terminal session, or remote logins via network. The use of file sharing, however, is usually *not* counted as login. This can depend on the file server.
- Time intervals are measured based on real wall-clock times. If a user is logged in while the computer is sleeping or in standby mode, the sleep time will still be counted as login time.
- Statistics per user are managed by the *short* user names which were valid at the times where these users had access to the computer. So old renamed accounts or deleted accounts may still be found in the list. The short user names are called *account names* in the **Users & Groups** pane of System Settings and are identical to the names of each user's home folders.
- The statistics can contain records for users called *root* and *_mbsetupuser* which are accounts used internally by macOS during system updates.
- Although no privileged operation is necessary in order to use this feature, read permission for the login records is required, because this affects personal data of others. You must be logged in as administrative user to retrieve the data.

2.7.7 Testing Displays

Depending on their quality, display screens can have certain defects already from factory: Individual picture elements (pixels) may not work at all or not always reliably. Aging of the device can also lead to such image errors. Based on the display technology used, the individual colors of the pixels are generated either by making them radiate themselves or by shining white light onto a pixel from behind, letting the picture element filter out specific colors while letting others through. The final color impression of each pixel arises from the fact that a certain amount of red, green and blue light, either generated or filtered, is mixed with one another.

The technical components responsible for the red, green and blue light of a pixel are separated from each other. If there is a defect in a specific pixel, the mechanism responsible for creating or filtering out one of these three colors will have usually failed. A

primary color of that pixel can either no longer be switched on (“dead pixel”), or no longer be switched off (“hanging pixel”).

You can use TinkerTool System to test an attached display screen, by switching all primary colors and their individual mixtures on and off for all pixels on the screen. By selecting red, green, or blue color areas, dead pixels will become visible as black dots. By selecting a mixed color, or by switching from white to a primary color, hanging pixels can be recognized as white or flickering dots. If all pixels are in order, the colors will be displayed correctly over the entire image area.

Some particular Macintosh models with a built-in display are notorious for having screens where the glass and foil lamination elements that make up the display are not perfectly sealed against the outside. This allows dust and moisture to penetrate, leading to streaks, especially at the corners of the picture. Such defects can easily be identified with a completely white test image. A fully black picture, on the other hand, can be useful to clean the glass of the screen without turning off the computer first. Dirt on the surface can be seen easily with this setup.

The following test images are provided by TinkerTool System:

- black picture
- pure white color
- pure red color
- pure green color
- pure blue color
- pure cyan color (“white without red”)
- pure magenta color (“white without green”)
- pure yellow color (“white without blue”)
- vertical bars with all the mentioned colors, similar to the test card of the European Broadcasting Union

When the solid screens are shown, it is additionally possible to overlay a pulsing black grid that moves back and forth. Pressing the key 1 creates a grid with a distance of 1 physical pixel, pressing 2 a grid with a distance of 2. This means you will see a very fine checkerboard pattern, whose fields constantly move back and forth. This way, faulty pixels are even easier to see. You can switch this additional function off again using the 0 key.

> Epilepsy notice for photosensitive people: The application makes sure that the alternating effect does not exceed a frequency of 2 Hz. The flashing pattern caused by this is considered harmless.
>
> The grid is not active when displaying color bars. Naturally, it is not visible on a black screen.

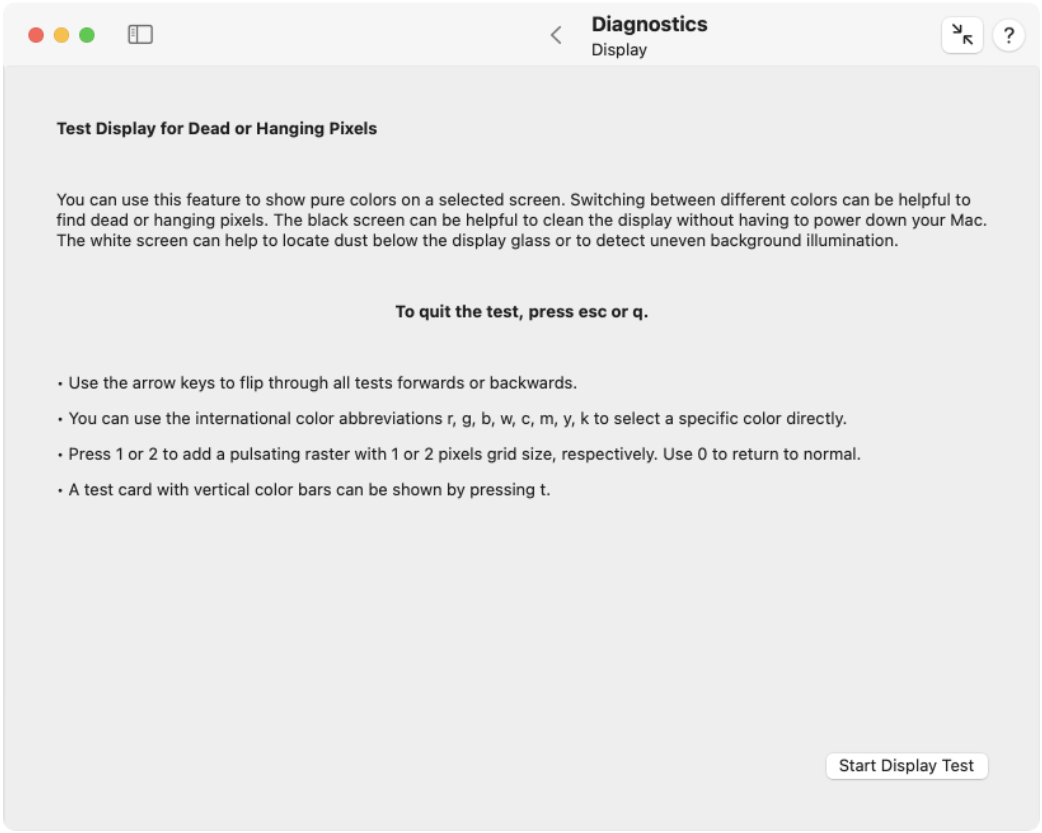


Figure 2.35: Attached screens can be tested with color areas

You can access the test cards as follows:

1. Open the sub-item **Display** on the pane **Diagnostics**.
2. Click the button **Start Display Test**.
3. If more than one monitor is connected, you will be asked which one to test. Select the display screen you like to check and click **OK**.
4. You can choose the individual test cards with the keyboard (see below). The test can be quit by pressing esc.

Table 2.1: Keys for controlling the test cards

Key	Function
esc or q	quit test
↓ or → or ␣	next test
↑ or ←	previous test
k	black
w	white
r	red
g	green
b	blue
c	cyan
m	magenta
y	yellow
t	test card with color bars
1	add moving black grid of size 1
2	add moving black grid of size 2
0	disable the grid feature

2.8 The Pane Emergency Tool

2.8.1 Introduction to the Emergency Tool

Under critical circumstances, your installation of macOS could be damaged by a disk drive failure or by a third-party application which used administrative permissions in such a way that the operating system is no longer starting correctly or does not start at all. When you cannot work with the operating system any longer, utility programs like TinkerTool System also can no longer be of any help to resolve this problem.

Similarly, macOS might still be running, but an important system component which is needed by TinkerTool System could be damaged. Even if TinkerTool System is capable of repairing this failing component during normal operation, this will not help in this

particular case, because you might not be able to launch TinkerTool System due to the damage.

However, TinkerTool System offers a solution which can help you even in those two critical cases. The application contains a mini version which can be launched in the special recovery operating system of macOS. The recovery operating system is installed as an addition to each standard operating system into a special read-only volume. It should always launch, even in emergency situations. The small standalone version of TinkerTool System is called *TinkerTool System for Recovery Mode*, or abbreviated *ttsfrm*.

> Note that you should inform yourself *beforehand*, before a critical problem occurs, how to launch TinkerTool System in Recovery Mode. You will then be prepared for an emergency. The respective instructions can be printed. **They can be different for each computer.**

2.8.2 Printing the Instructions

To print the instructions how to launch *TinkerTool System for Recovery Mode*, perform the following steps:

1. Open the pane **Emergency Tool** of the section **System Maintenance**.
2. Click the button **Print these instructions**….

TinkerTool System will automatically adjust the output to the paper size of your printer.

2.8.3 Structure of the Launch Command

The individual launch command for your computer is shown at the end of the instructions. The command is different depending on the location of the program and the names of your volumes, folders, and application. It could be, for example:

```
"/Volumes/Macintosh HD - Data/Applications/TinkerTool System.app/
Contents/SharedSupport/ttsfrm.app/Contents/MacOS/ttsfrm"
```

The actual call that must be typed as one single line into the **Terminal** window to launch the application, can be reconstructed as follows:

1. The command always begins with **"/Volumes/**.
2. The name of the volume where TinkerTool System is stored follows, together with a slash at the end.
3. The path through the hierarchy of folders where TinkerTool System is stored on this volume follows, each part divided by slashes. If you are not working with macOS in English, please make sure to use the real folder names, not any presentation names established by the Finder. For example, if you copied TinkerTool System to your Desktop with the Finder running in French, the folder name will presented as **Bureau**. The actual folder name is **Desktop**, however.

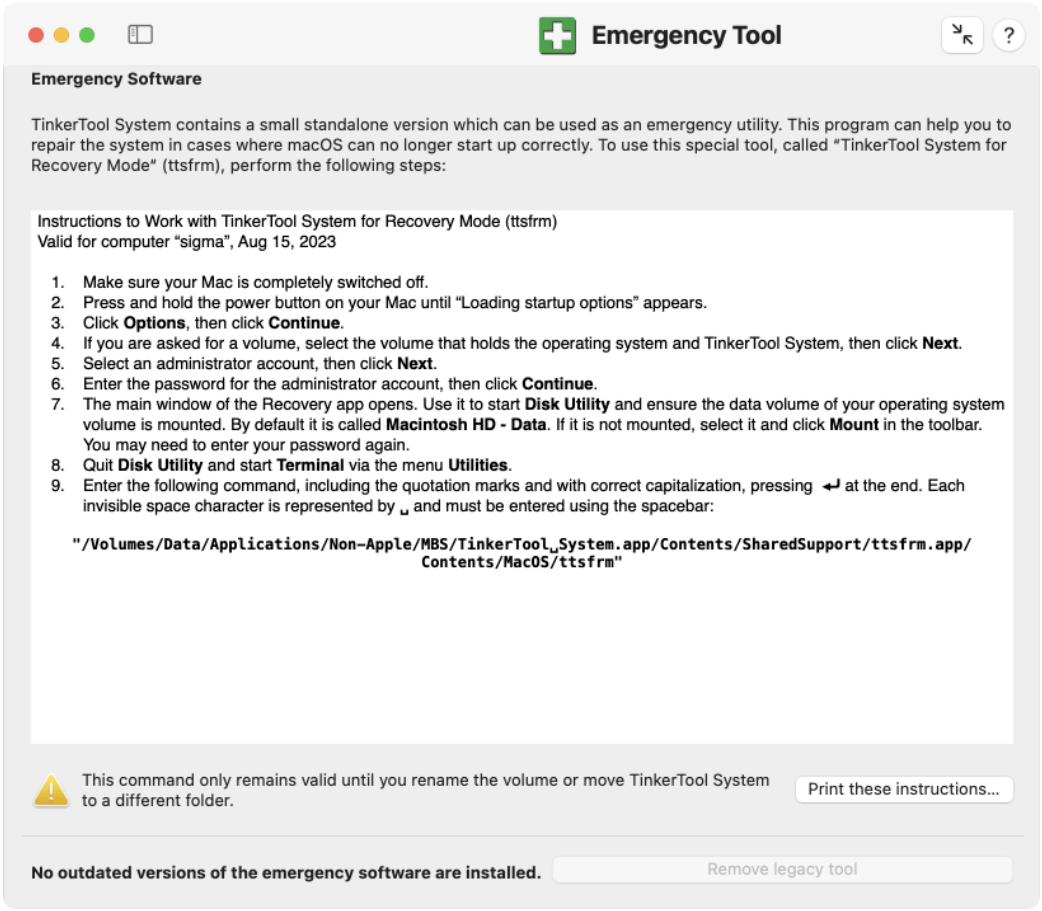


Figure 2.36: Emergency Tool - The instructions shown in the picture are individual for each computer and may not apply to your situation.

4. The name of the application follows, in this case **TinkerTool System**, followed by the ending **.app** and a slash.

5. The command always ends with **Contents/SharedSupport/ttsfrm.app/Contents/MacOS/ttsfrm"**.

6. After the end of the command, the return key must be pressed.

This means the pattern of the call is

```
"/Volumes/<volume>/<folder1></.../><folderX>/<program>.app/
Contents/SharedSupport/ttsfrm.app/Contents/MacOS/ttsfrm"
```

where all parts within angular brackets must be replaced by the actual names that are established on your computer. Don't omit the quotation marks and don't replace them by typographical variants. Press the return key only at the end, even if the command above is written in multiple lines for reasons of space. To make it easier for you to recognize spaces, they are marked with the special character ␣ in the instructions.

Correlation between file position and repair options

If you have multiple disk volumes on your Mac or even multiple operating systems are installed, there will be restrictions which volumes will later be accessible in Recovery Mode and which operating system can be repaired. The following basic rule applies:

TinkerTool System for Recovery Mode only works on the volume group and its associated operating system where the application itself has been stored.

This results in the following consequences:

- TinkerTool System should always be placed on the volume group where the operating system is located.

- If you work with multiple operating systems, each of the system volume groups should have its own copy of TinkerTool System.

> A volume group for macOS consists of the system volume, its associated snapshot volume, and its data volume. You can review the details of this grouping via the pane APFS (section 3.7 on page 232).

2.8.4 Using the Emergency Tool

TinkerTool System for Recovery Mode can only be used after the recovery operating system of macOS has been started. Detailed information on this topic can be found in the chapter Working in macOS Recovery Mode (section 6 on page 307).

2.8.5 Old Versions of the Emergency Tool

Older variants of TinkerTool System had been shipped with a different type of emergency tool which was designed for the *Single User Mode* of macOS. This program had to be installed expressly in a separate step. Apple no longer supports Single User Mode of macOS officially and many Macs are now pre-configured by default to prohibit Single User Mode for security reasons. This has made the old version obsolete, so it should be removed. TinkerTool System detects automatically whether an outdated version of the previous software is available in the running operating system. It will show this at the bottom of the **Emergency Tool** pane. In this case, simply click the button **Remove legacy tool** and follow the application's instructions to clean your Mac.

2.9 The Pane Network

The pane **Network** can be used to replace the functions that have been lost from the previous **Network Utility** which had been part of the operating system in older versions of macOS. TinkerTool System provides a similar range of functions and additionally contains modernized features, in particular to support today's default network protocol IPv6.

2.9.1 Information About Network Interfaces

You can review technical details and statistics on all network interfaces of your Mac that are currently active. Active means that at least one IPv4 or IPv6 address has been assigned to the network port which can be used to communicate with other devices. To get the data, perform the following steps:

1. Open the sub-item **Info** on the pane **Network**.
2. Use the pop-up button to select the interface for which you like to get information.

The items shown in the window are automatically updated every 10 seconds.
The following details are available:

- **Hardware Address:** the predefined address built into the hardware of the network port, used for communication at the *Media Access Control (MAC)* level. This address is also called *MAC address*.
- **IPv4 Address:** the currently assigned address for Internet Protocol version 4.
- **Link Speed:** the detail type of the network connection. The exact meaning is determined by the kind of network port. In most case, the currently selected data rate will be shown.
- **Link Status:** the current status of the network connection as defined by the operating system.
- **Vendor:** the manufacturer of the physical hardware port

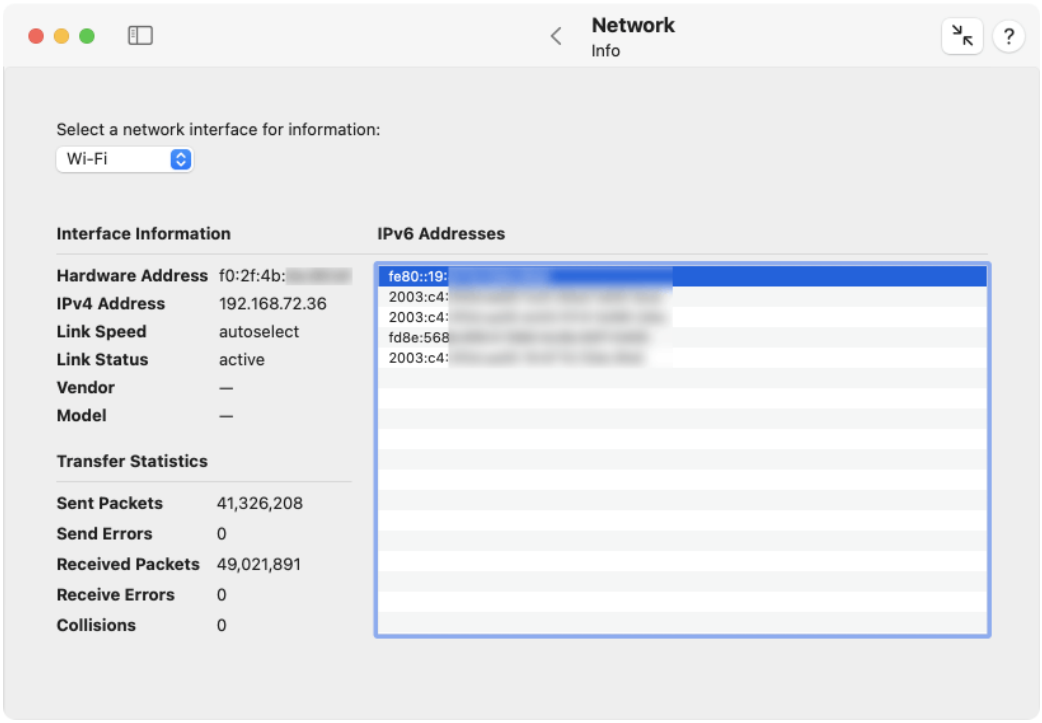


Figure 2.37: Determine details about each active network interface

- **Model:** the type of port or its hardware model number
- **IPv6 Addresses:** the currently assigned addresses for Internet Protocol version 6.
- **Sent Packets:** the number of data packets that have been sent since the operating system was started.
- **Send Errors:** number of sent packets for which an error was detected.
- **Received Packets:** the number of data packets that have been received since the operating system was started.
- **Receive Errors:** number of packets received for which an error was detected.
- **Collisions:** for network technologies where it is possible that multiple devices send data unsynchronized at the same time, which causes data packets to interfere with each other, the number of cases where such transmission collisions have occurred.

2.9.2 Routing Tables and Network Statistics

Via the item **Netstat**, you can review further statistics from the network management of macOS, relevant for all network ports.

1. Open the sub-item **Netstat** on the pane **Network**.
2. Select one of the radio buttons to choose the item for which you like to retrieve data.
3. Click the button **Netstat**.

The application will determine the information and show it in an additional dialog sheet. You can also print the results or save them as text file.

> Please note that macOS may need several minutes of computation time before data will be shown. The information comes directly from the UNIX level of the operating system.

The following statistics are available:

- the routing table of the operating system: the table indicates which interface port is used to communicate with which destinations, or address ranges, respectively. This means this table decides for each outgoing network packet which interface port will be selected for the transmission.
- statistics for each communication protocol: sorted by the typical transmission protocols, like TCP, UDP, IPv4, ICMP, IGMP, IPsec, IPv6, ICMP6, and IPsec6, this item will show statistics about the number of transferred packets, errors, fragmentation, memory use, and similar data.

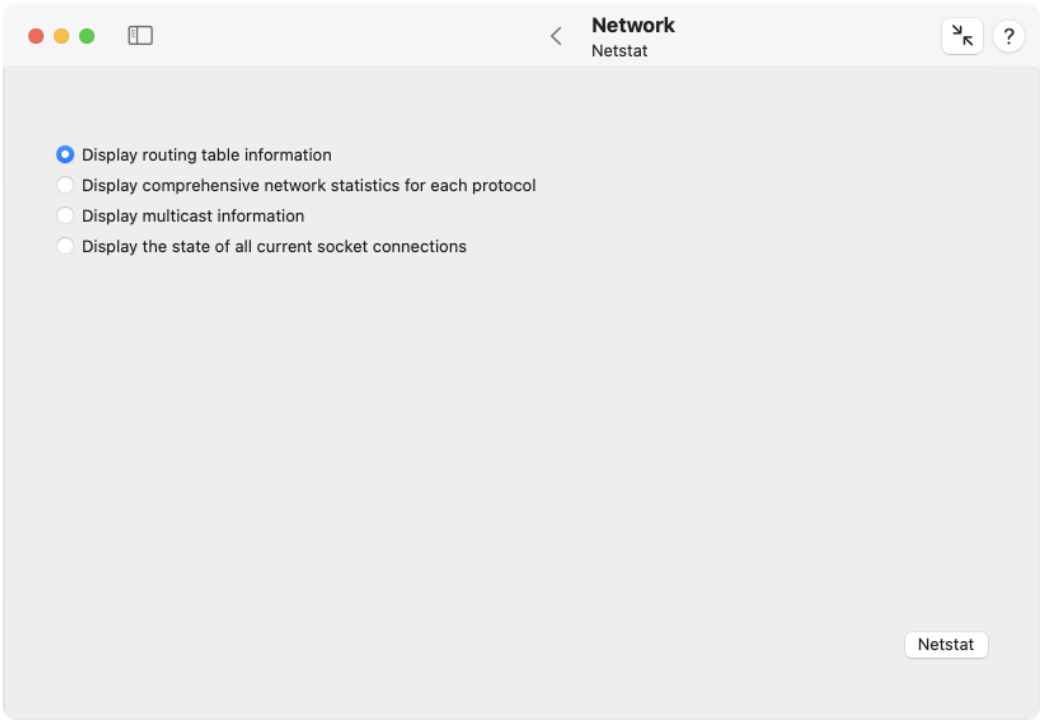


Figure 2.38: Statistics and routing tables can be retrieved from the operating system

- statistics on membership in multicasts: Multicasts are network transmissions that are received simultaneously by a whole group of devices.
- statistics related to logical network connections (sockets) that are currently established: a table shows all endpoints to which communication links are currently established in the network.

2.9.3 Checking Network Connections via Echo Signals

To check the connection to another device in the network, it can be useful to send this device a request to report back. A test packet is sent to the other device, asking to reflect it like an echo. From the technical slang of working with echo sounders (sonars), sending a test signal back and forth is called *ping*.

Perform the following steps to run such a communication test:

1. Open the sub-item **Ping** on the pane **Network**.
2. Enter the desired destination into the text field either by address or by name and press the return key.
3. Check the field **Use IPv6 protocol** if the test should not be performed based on IPv4, but based on IPv6.
4. Choose whether a specific number of test signals should be sent, or whether the test should run endlessly until you click the **Stop** button.
5. Click the **Ping** button.

The report that is shown during the individual ping signals indicates how many bytes have been sent to which address, the current running number of this signal *(icmp_seq, Internet Control Message Protocol sequence number)*, the maximum number of intermediate stations the sent packets are allowed to pass *(ttl, time-to-live)*, and how long (in milliseconds) it took until the echo came back again *(time)*. An additional summary is shown at the end of the report, indicating among other things, how many test packets have been sent, as well as the minimum, average, and maximum echo times, together with their standard deviation during the entire test.

> Not all devices will respond to ping requests. For security or performance reasons, some devices may refuse to answer. Such a case cannot be distinguished directly from cases where the destination host could actually not be reached.

You can use the normal copy/paste or drag-and-drop features of macOS when you like to transfer an address or computer name into the text field. Note however, that a paste operation won't be accepted if you try to transfer text containing characters that are officially forbidden by the Internet standards, an underscore (_), for example. TinkerTool System doesn't perform a full syntax check, but may reject pasted text with characters not compliant with the rules of RFC 952.

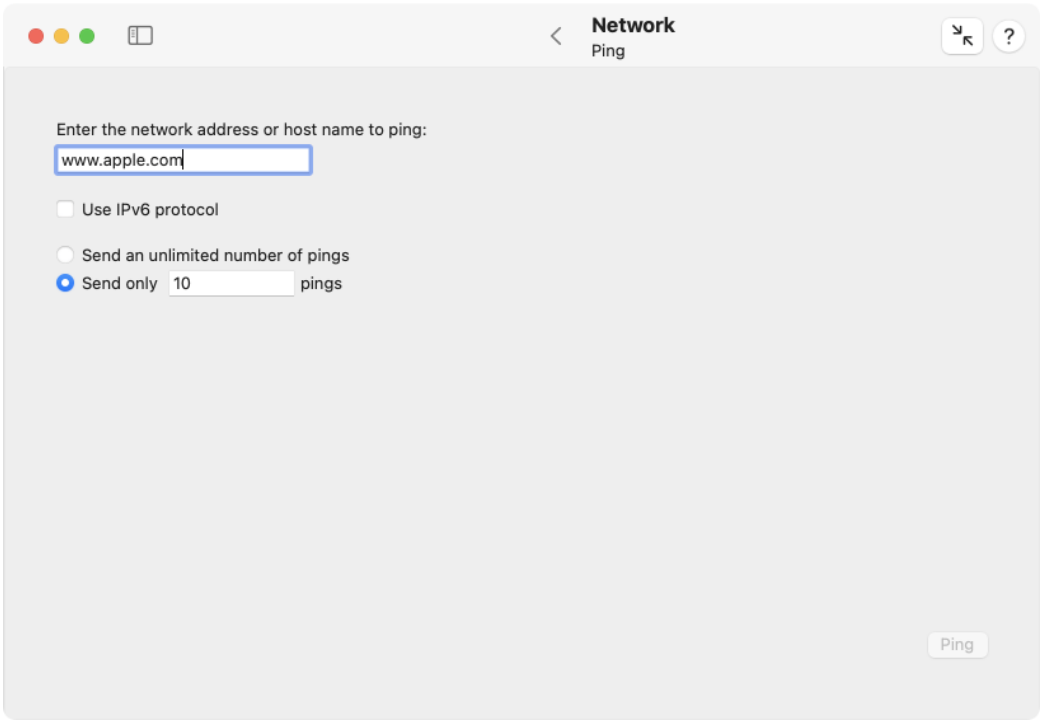


Figure 2.39: To check a connection, an echo request can be sent

> Other fields in the Network pane for entering addresses or host names also follow this policy.

2.9.4 Determine the Assignment Between Host Names and Addresses

The *Domain Name Service (DNS)* is designed to make it possible to reach other devices in the network not only by their addresses, but also by their names. This service either looks up the name for a valid address, or in reverse direction, determines the assigned name(s) for an address. You can submit such a request to the service manually any time. To do this, perform the following steps:

1. Open the sub-item **Lookup** on the pane **Network**.
2. Enter either the name of the device, or its IPv4 address, or its IPv6 address into the text field and press the return key. This will be interpreted as request to look up the missing parts via DNS.
3. If you like to receive a lot more details about the internal query sent and the associated response from DNS in addition to the plain answer to your request, check the field **Use "dig" for more detailed information**.
4. In case you have selected the detailed variant in item (3.), you can additionally choose whether you like the request to be sent via IPv6 only, and whether the IPv6 address should be looked up as well.
5. Click the button **Lookup**.

The response contains in each case

- which server (with its name and address) has sent the answer, and
- how the answer is, i.e. name(s) and address(es).

To evaluate the lookup request, the system will use the DNS server currently configured in the network settings of macOS.

2.9.5 Trace the Path of Data Packets

In larger networks such as the Internet, destination points can only be reached if the data packets can travel along multiple intermediate stations. The individual nodes of the network determine the currently best route, based on network maps, connection costs, and current utilization of the network components. It can be interesting to display the currently selected route for communication with a specific destination. This operation is known as *packet tracing* or *traceroute*.

1. Open the sub-item **Traceroute** on the pane **Network**.

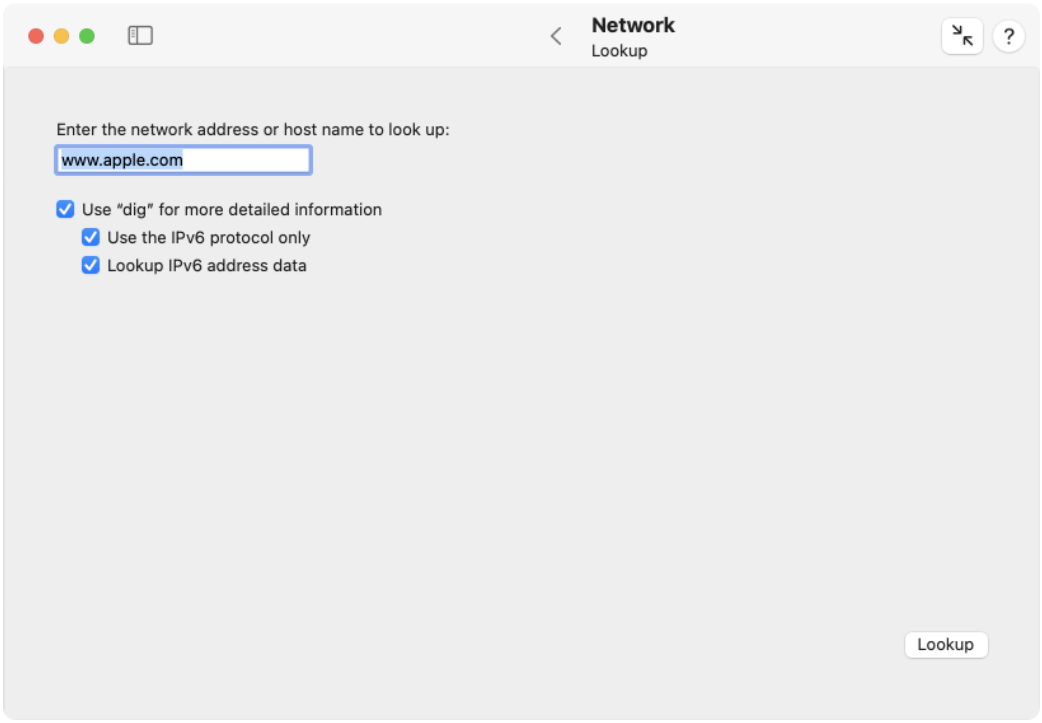


Figure 2.40: The relationships between names and addresses can be reviewed

2. Enter either name or address of the destination into the text field and press the return key.
3. Click the button *Trace*.

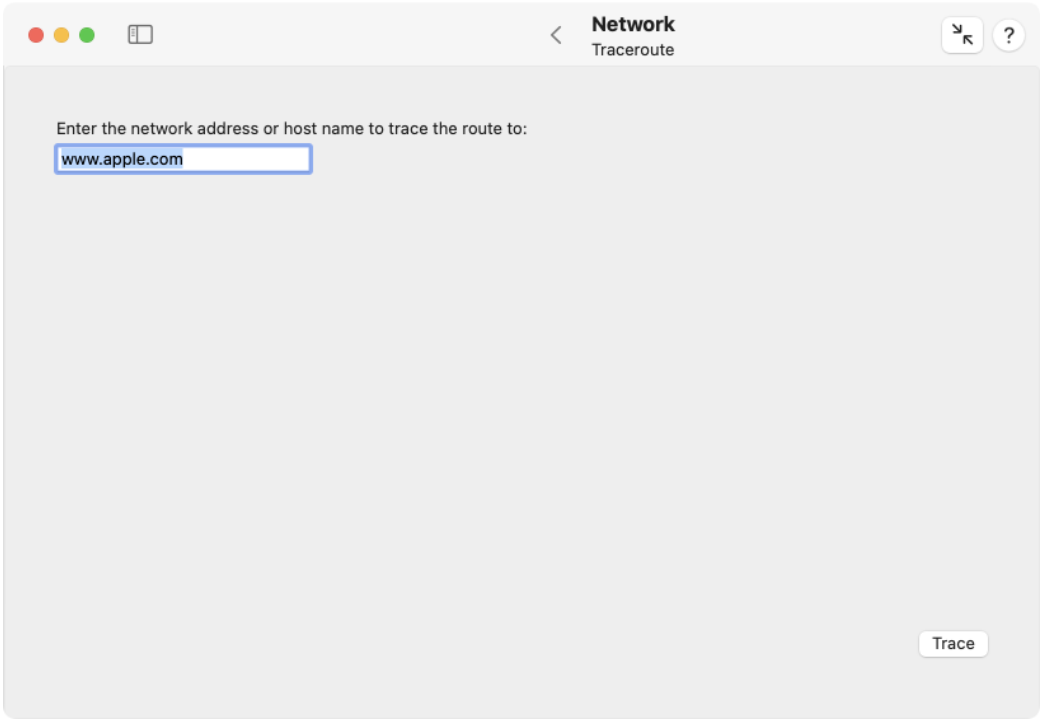


Figure 2.41: The currently chosen route for data packets can be traced in the network

The current route is determined and measured using a series of test data packets (similar to the ping operation). For each intermediate station, called *hop*, you will get one line of output. If available, it will indicate its name and address, as well as the transmission times to reach the next node. Determining the entire route can take a few seconds. Data that cannot be retrieved at the moment is replaced by asterisks.

2.9.6 Querying Databases of the Whois Service

On the Internet, names of the individual network devices, or their ports, respectively, are assigned using a hierarchical system. The names are registered for a fee at specific registration authorities. These registries establish the *whois* service, a database that lists all domain names currently in use. The databases can be accessed publicly to determine information about the owner of a name, a contact person for administration, a contact for technical questions, one for name abuse, the date of registration and the validity period, the responsible registration authority, and the authoritative DNS service.

> For data protection reasons, not all of this information can be retrieved in each country or from every registration authority. The amount of available data can vary greatly depending on the domain name.

To find information about a registered domain name, perform the following steps:

1. Open the sub-item **Whois** on the pane **Network**.
2. Enter the domain name into the text field and press the return key.
3. From the overview of whois servers, select the server which presumably belongs to the responsible registration authority for that domain, or enter the name of another whois server.
4. Click the button **Whois**.

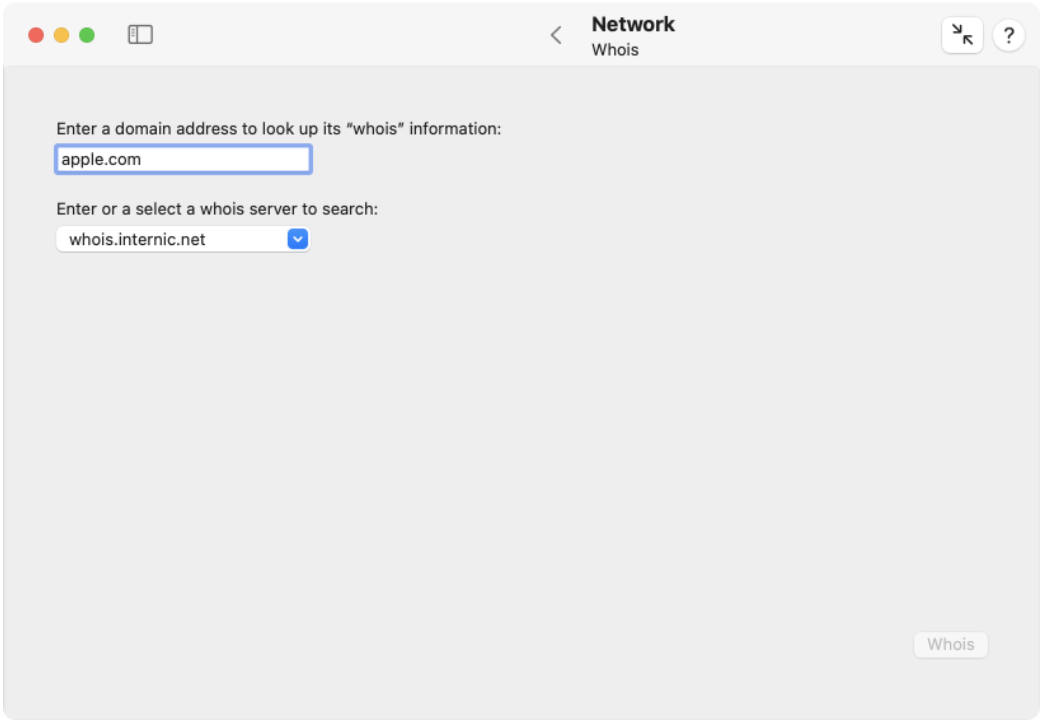


Figure 2.42: The whois service of the Internet can be queried

The publicly available data provided by the selected whois service will be shown. As always, you can print the result or save it as text file.

2.9.7 Determining User Information via the Finger Service

The *finger* protocol describes an information service that provides data about network users live, mainly to determine how and where a user can be reached within a company or similar organization. In addition to contact details, such as phone numbers, room numbers, or email addresses, finger is designed to indicate at which computer of the network a user is currently logged on, and for how long. Querying the finger service is done via text patterns similar to email addresses, namely

```
name@domain
```

where *name* is the short account name of the user, and *domain* is the domain name of the network.

Perform the following steps to get finger data about a network user:

1. Open the sub-item **Finger** on the pane **Network**.
2. Enter the finger specification into the text field and press the return key.
3. Click the button **Finger**.

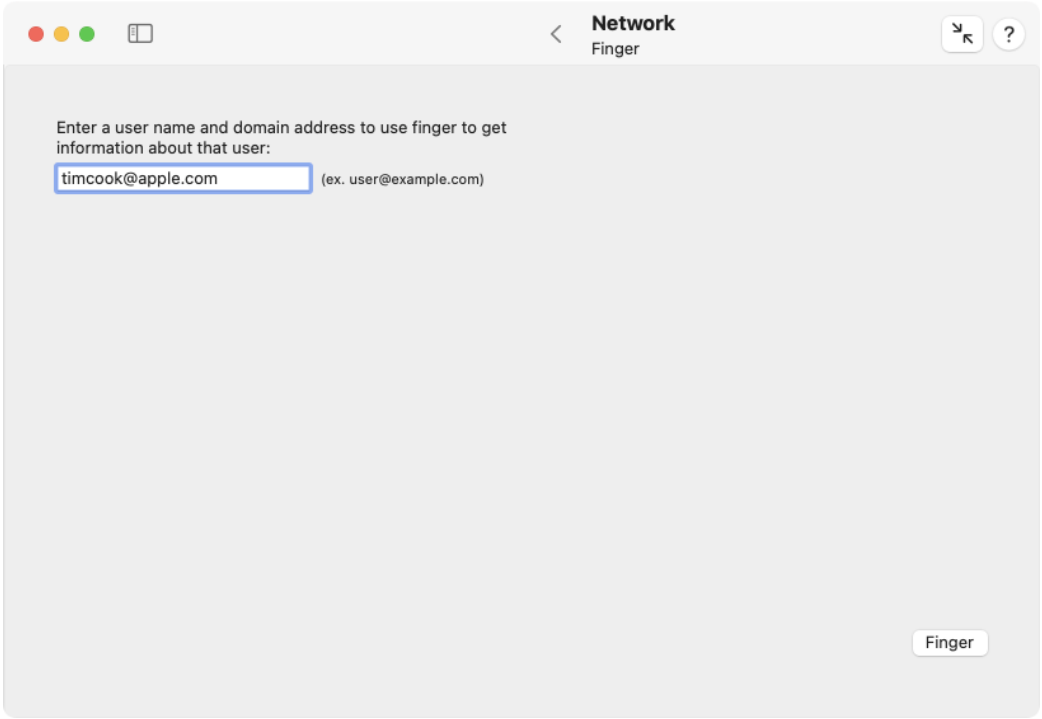


Figure 2.43: The finger service may provide information on network users

> The finger protocol was developed between 1971 and 1977 and is considered obsolete. For data protection reasons, as well as for labor law and security reasons, it is rarely used today. If it is actually used, data will usually be available in the local network only, not across the Internet.

If the finger service is unavailable, you will typically receive an error response that includes the message

```
finger: connect: Connection refused.
```

2.9.8 Responsiveness

macOS contains a built-in speed test that is able to assess the quality of your local network and its Internet connection. You can run the test, which usually takes less than half a minute, via a simple mouse click. The test basically estimates how well your Internet connection will react when several devices or applications are using it at the same time. The results of the test can be particularly useful if you are using an Internet gateway whose performance can be optimized manually, for example by configuring features such as *Smart Queue Management (SCM)*. You can run several tests under similar conditions to experiment which changes lead to better performance.

Please note that both, the network between this computer and your Internet gateway ("router"), the network between the gateway and your Internet provider, as well as the link between your provider and the Internet are part of the measurement. macOS records the following metrics during the test:

- **Upload capacity:** the current net throughput when sending data to the Internet
- **Download capacity:** the current net throughput when receiving data from the Internet
- **Upload flows:** the maximum number of typical Internet send connections possible simultaneously until the network is fully utilized
- **Download flows:** the maximum number of typical Internet reception connections possible simultaneously until the network is fully utilized
- **Idle Latency:** the typical transit time of data between this computer and a server when the communication link is not under load
- **Responsiveness:** the maximum number of packet round-trips per minute that can be expected during typical transactions, when multiple programs send inquiries and wait for replies from the network. A higher number means higher quality of the "felt" network behavior.
- **Overall quality assessment by macOS:** a summary of the total result as a simple catchphrase (see below).

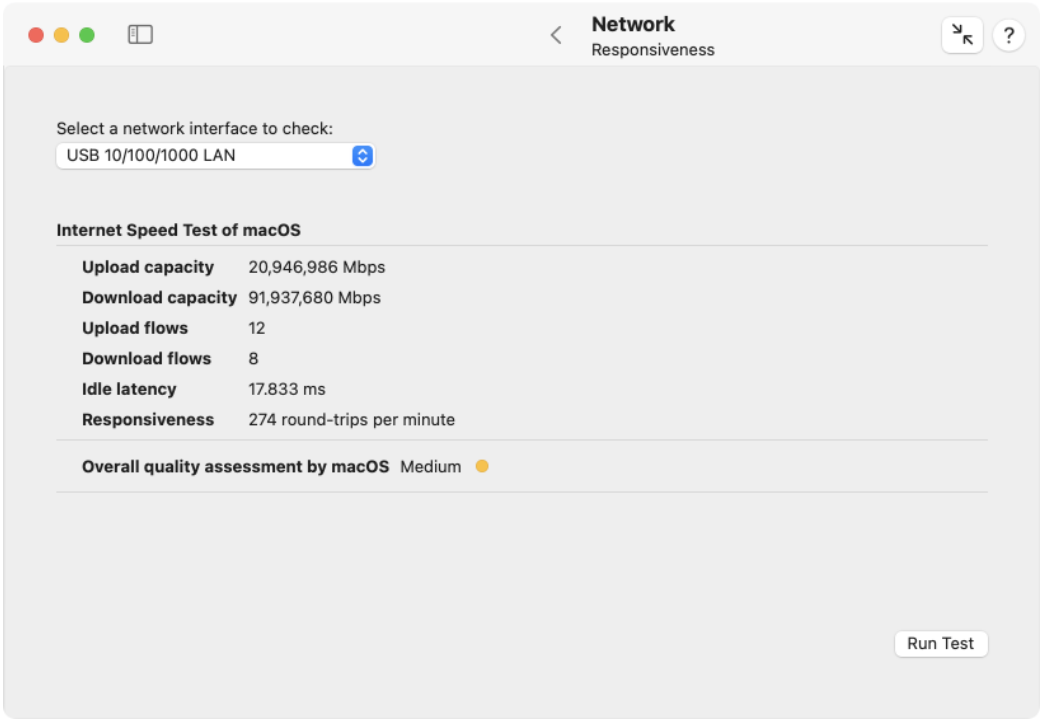


Figure 2.44: macOS can measure the typical responsiveness of your network and assess its quality

During the measurement, a large amount of test data is transferred between your computer and one or more Apple Internet servers. Which servers are involved can be dynamically controlled by Apple and change any time.

Perform the following steps to get an overall assessment of your network quality:

1. Make sure that the pop-up button **Select a network interface to check** is set to the desired option. TinkerTool System offers all physical and virtual network interfaces that currently have an active IP address. Please note that not all interfaces are usually connected to the Internet, so they cannot be used for testing. Usually, it is sufficient to keep the selection **Default interface for Internet access** which causes macOS to automatically choose the network link currently in use for Internet data transfers.
2. Click the button **Run Test**.

The test will then be run by macOS and TinkerTool System will show its results. The overall assessment is at the discretion of macOS and is not influenced by TinkerTool System. Apple provides the following documentation to understand the end result:

- **Low:** If any device on the same network is, for example, downloading a movie or backing up photos to iCloud, the connection in some apps or services might be unreliable, like during FaceTime video calls or gaming.
- **Medium:** When multiple devices or apps are sharing the network, you might see momentary pauses or freezes, like during FaceTime audio or video calls.
- **High:** Regardless of the number of devices and apps sharing the network, apps and services should maintain good connection.

2.10 The Pane Info

2.10.1 Mac

The sub-item **Mac** lists technical details about the current computer system. This includes data not accessible by the **System Information** application of macOS.

The section **Computer** contains the name of the system as you have defined it (which may not be identical to the name used to identify this computer in the network), Apple's official model name (also known as *marketing name*), a short description of this model series, the Apple model identifier which is the code Apple and macOS internally use to identify this series, the computer's serial number, its unique hardware identification, and the week of production. If you are using a Macintosh model available in different colors, a small color field next to the line with the model identifier shows the color of the enclosure. A typical image of the computer model is also shown at the top above the text.

> For Apple devices manufactured after August 2021, Apple may no longer permit that the actual manufacturing date can be determined. In this case, TinkerTool System will indicate this with a respective message.

If your Mac is based on an *Apple Silicon* processor, Apple's short description text for the model series won't be available, but the following information is added instead:

- the Apple order number of this Mac,
- the model code of the enclosure.

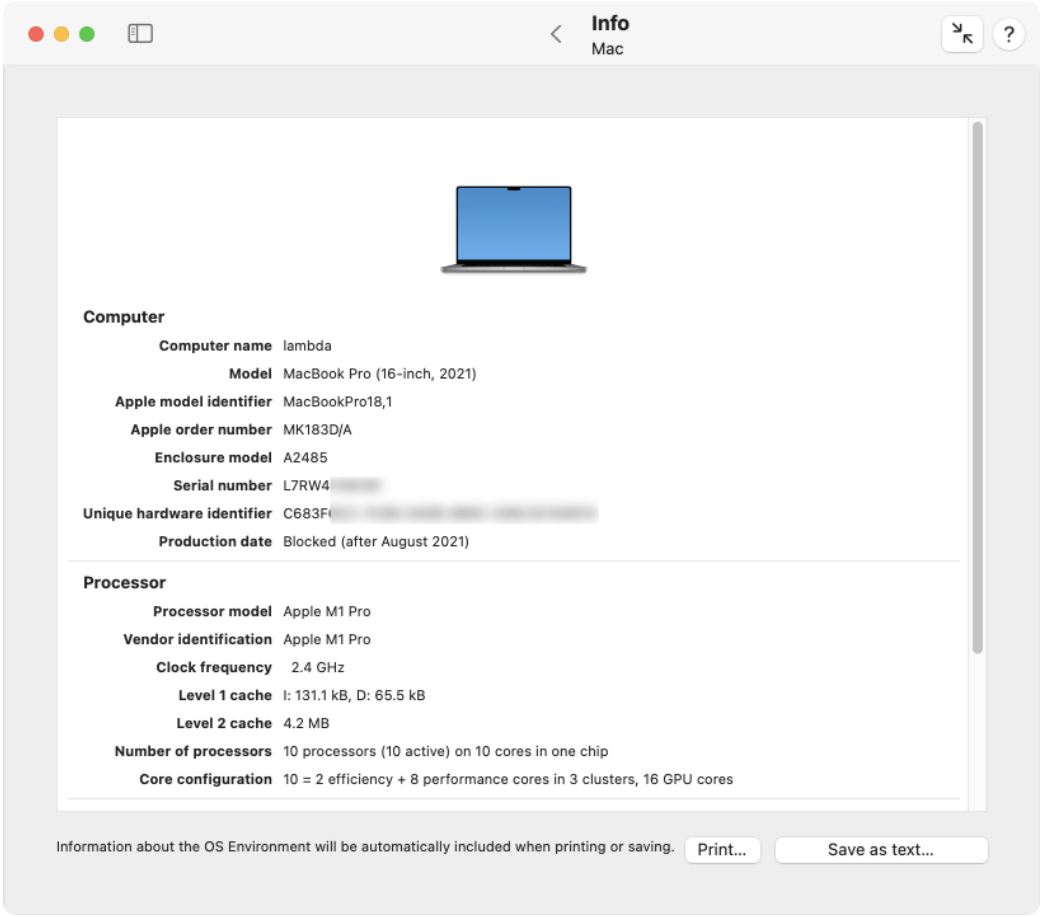


Figure 2.45: System information (version for Macs with Intel processor)

The second section **Processor** lists details about the processor configuration, as well as the available cache sizes. This includes the official processor model identification, the vendor identification, the number of processors, the number of available processor cores and active cores.

For Intel processors, the information whether each core is capable of executing multiple threads of instructions (Simultaneous Multi-Threading) follows. If active, the hardware will simulate twice the number of processors. In addition, you will find the processor

generation specifier for x86 systems, which includes the family number , model number, stepping number (hardware version), and the decimal signature which compresses all identification codes into one single number.

Intel processor generation data is naturally unavailable for Macs with Apple Silicon processors. Here, you will find the exact configuration of processor cores instead: The number of efficiency cores, high-performance cores, their distribution on processor clusters, and the number of Apple GPU cores.

Also listed are the processor's main clock frequency, the sizes of the level 1 caches (I for instructions, D for data), and the sizes of the level 2 and level 3 caches (Intel only).

The section **Memory** shows the size of physical memory (Random Access Memory, RAM) currently built into your computer and the optimum free size. This size specifies the small amount of physical memory the operating system should try to keep free for best performance. The optimum is reached when no RAM is wasted (nearly everything is in use), but a small remainder is left free for current handling. The line **Addressable memory** defines the size of physical and virtual memory the processor can internally manage. This does not mean that this amount could actually be used in practice. The number of slots available for memory modules and other limitations of the computer's chipset will reduce these theoretical values. For more information on memory management, please also see the section Introduction to virtual memory (section 2.7 on page 84).

The fourth section **Logicboard** contains detail data about the computer's main logic board, namely the vendor information, its internal model code, and its serial number. Macs based on Apple Silicon don't use a visible model code for the logicboard and the corresponding line will be omitted in this case.

Additional data for Intel-based Macs

> These items cannot be retrieved if you are using a Mac with Apple Silicon. SMC and bridge are part of the main processor, so they no longer need to be separate parts. System management data compliant with the SMBIOS standard is no longer supported. Instead, product records are available. Please see the next section for more information.

The fourth section also shows the version number of the *System Management Controller (SMC)* and its firmware. The SMC is an auxiliary processor which manages the computer's internal sensors and its power management features. It operates the "always-on" parts of the system, still running when the actual computer is in sleep mode or shut down. It is also responsible to identify the computer as genuine Apple-branded product, constituting the main difference between a generic personal computer and a Macintosh.

A special detail sheet, available via the button **Show management records** lists technical information which has been stored into the management memory of the computer. It includes:

- data about the system unit
- detail information on each processor

- detail information on each cache unit
- detail information on each memory slot or memory device
- a description of the system's firmware
- management data about the system board
- management data about the system enclosure
- detail information about each connector on the system board or system enclosure
- detail information on each expansion slot
- list of built-in system devices
- list of jumpers and switches on the system board.

> These management records are not computed by TinkerTool System but only retrieved by it. They have been stored by the manufacturer into the so-called *System Management BIOS* area of the system's firmware when the computer was assembled. Some parts are also computed dynamically by macOS by retrieving the necessary data from the available hardware.

Another detail sheet **BridgeOS Info** is available if your computer is equipped with *Apple BridgeOS Processor* technology. This can either be the original *iBridge* system or the *Apple T2 Security Processor*. The BridgeOS system is a secondary computer built into your Mac which controls security features such as the TouchID fingerprint sensor or SSD encryption, depending on model. This auxiliary system runs its own operating system *Apple BridgeOS* and may always be on if power is available. The entry **Apple BridgeOS Processor** indicates whether such technology is used in your Mac. If yes, you can press the **BridgeOS Info** button to learn more details about its configuration.

Additional data for Macs with Apple Silicon

Instead of SMBIOS data, Macs with Apple Silicon store Apple product information internally. The most interesting items will be listed after clicking **Show product records**:

- the type of **System on a chip (SoC)** used in this Mac,
- the **Macintosh compatibility level**, which is basically a virtual Mac that defines a certain set of features. For example, a "generation 15" Mac may support more modern features than a "generation 14" Mac, and omit certain outdated features. The level defined by the first Apple Silicon Macs that were published in 2020 is called "generation 20".
- the **Mobile device compatibility level**: similar to the previous item, it defines a set of capabilities this Mac has when it falls back to be used like one of Apple's mobile devices, usually an iPad Pro.

- the **number of built-in microphones**, which defines how many audio sensors are built into this Mac.
- **Memory upgradable:** an indicator whether RAM can be upgraded in this Mac or not.
- **Touch Bar serial number:** if this Mac has a Touch Bar or finger print sensor unit, the serial number of the part which has been paired with this computer.
- **Ambient light sensor serial number:** as before, but referring to the light sensor unit.
- **Cover glass serial number:** as before, but referring to the cover glass of the display.
- **Display assembly part and serial numbers:** if this Mac has a built-int display, the serial numbers and/or part numbers of all components that comprise the display. The cover glass may be included in this list.
- **Power Supply:** Specific Mac series allow access to data about the internal power supply unit. If you are using such a Mac model, the tab **Power Supply** will be shown additionally. It lists technical details such as manufacturer, model type and serial number, as well as nominal secondary voltage, maximum amperage and power. This feature is usually available if the Mac is internally designed like a "portable computer without battery".

It is possible to either print the contents of the main information window, or to save it into an HTML-based text file. Such documents can be used to automatically generate inventory records for all your computers. Click the buttons **Print**... or **Save as text**..., respectively. Created text files can be opened by any web browser or by the TextEdit application included with macOS.

In addition to the **Mac** data, other information from the sub-item **Operation Environment** (see next section) are included in the printed report as well.

> The startup time of the system is a volatile item that is not included in text reports.

2.10.2 Operation Environment

The item **Operation Environment** summarizes the version information about the computer's firmware , the Darwin operating system on which macOS and iOS are based, the kernel version and revision codes, as well as the operating system version and build numbers. The line **System update source** indicates whether you are using an officially released version of the operating system, or whether your computer is set up to receive updates from one of Apple's pre-release distributions *(seeding programs)*.

> Note that the field reflects participation in one of the pre-release update programs, not the status of the currently running operating system. Usually, both specifications are equivalent, but if you have not carried out a pending update yet, there will be temporary differences.

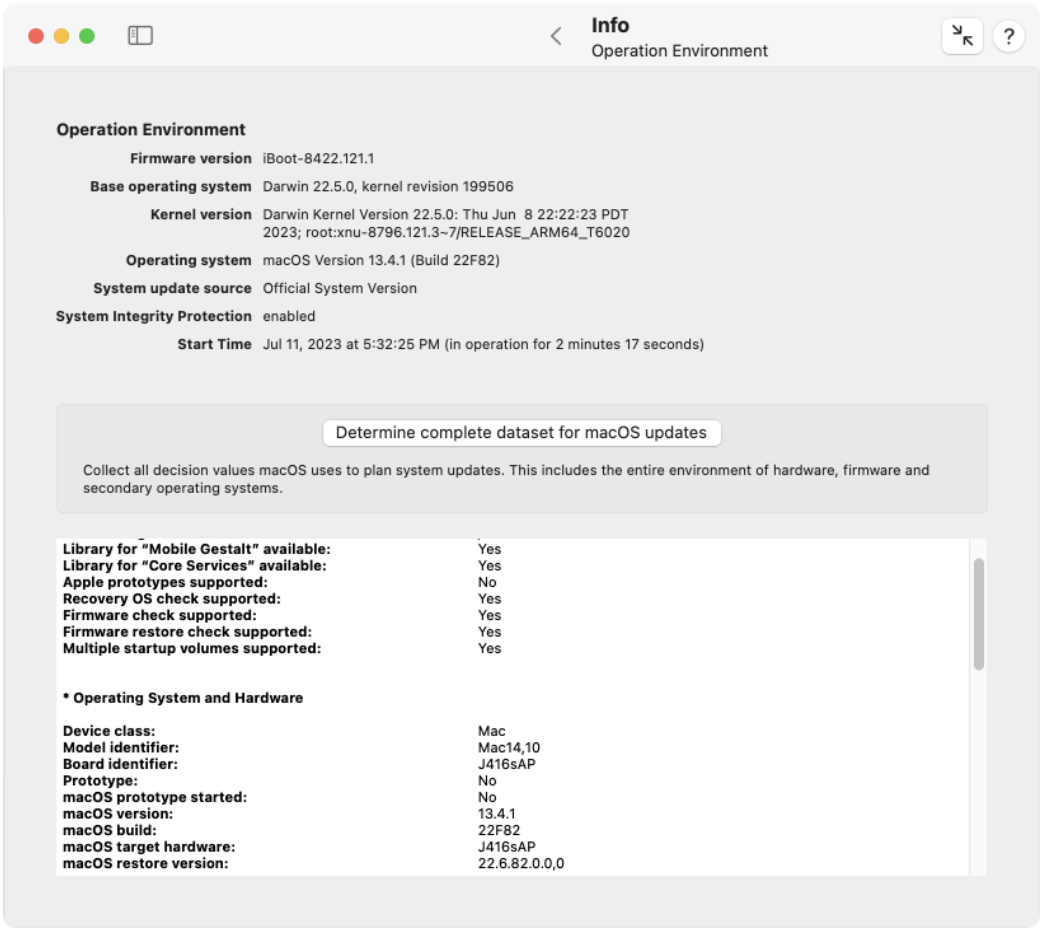


Figure 2.46: Operation Environment

This section also shows the computer's hardware setting for **System Integrity Protection** that is currently taking effect for the operating system. (For information on the technical background of this feature, please see the end of the chapter Basic Operations (section 1.3 on page 8).) The feature can either be fully enabled, completely disabled, or enabled partially. In the partial case, TinkerTool System uses the following abbreviations to indicate which operations are permitted by the current computer settings:

- **kext:** untrusted kernel extensions can be loaded into the system kernel.
- **fsac:** the system has permission to modify or delete objects in the file system for which the attribute *restricted* is set.
- **tpid:** the system has permission to use features that determine which process is belonging to a specific process identification number.
- **kdbg:** kernel debugger features can be used.
- **appl:** the system has permission to use functions which are considered *Apple-internal*.
- **trac:** the system has permission to use program execution tracing (based on *dtrace* technology) without limitations.
- **pram:** the system has permission to modify *all* entries in the non-volatile RAM (NVRAM).
- **devc:** device configuration is permitted.
- **reco:** the computer has permission to use any of the available recovery operating systems.
- **akex:** the system can load trusted third-party kernel extensions which are not approved by an administrator yet.
- **expo:** the system has permission to override the security policy for executable applications.
- **stur:** the operating system can start from an unauthenticated root file system which has not been cryptographically sealed by Apple.

All protection items *not* listed by TinkerTool System are in full effect. The exact meaning of these settings is defined by Apple and can be changed without notice.

The last line of the overview shows the **start time** of the operating system, both as absolute time and as interval that has passed since then, the so-called **uptime**.

If you press the **Determine complete data set for macOS updates** button, TinkerTool System collects further information, namely the entirety of all decision data that macOS uses when it searches for system updates. This includes the hardware, the firmware, the running operating system and all auxiliary operating systems, such as bridge systems, start systems, recovery systems. The data is shown in tabular text form and is usually self-explanatory.

> This data may not be available if the computer has been running for an extended time without restarting it. A restart fixes this issue.

2.10.3 Malware Protection

macOS offers multiple built-in security measures against malicious software (malware). One of these security features works like a virus scanner which automatically scans downloaded files, searching for known code patterns (signatures) in the background. Apple refers to this technology as **Safe Downloads List**. It is also known under the name *XProtect*. Its function is enabled by default. The virus signatures are automatically updated when the option **Install Security Responses and System files** is enabled at **General** > **Software Update** > **Automatic Updates** > **i** in **System Settings**. In addition to detecting malicious software, this component also monitors the version numbers of specific Internet plug-ins installed in the system. Such plug-ins are used by Internet browsers to support optional web technologies like Adobe® Flash® or Java™.

By use of the sub-item **Protection**, you can review the current contents of the Safe Downloads List. The upper table shows the malicious programs which can be recognized by the operating system at the moment. The name of the malware, as defined by Apple, and the file types used for the distribution of the software are listed.

The lower table lists the Internet plug-ins which are monitored by the operating system, checking them for outdated versions. The name of each plug-in and the versions which are considered to be critical are shown.

Below the tables, TinkerTool System displays when Apple has revised the list for the last time, when the list has been transferred to this computer, and whether the system checks automatically if a new version of the list is available. The version specifications differentiate between the malware definitions and the software XProtect for malware handling.

Please note the following points:

- The tables show which threats can potentially be detected by the operating system. They give no indication if this computer had encountered such malicious software in the past or had removed it. So if there is an entry *abc* in one of the tables, this will only indicate that macOS would detect the component *abc*, but it doesn't mean that *abc* is currently on your system.

- Entries in the table can be repeated multiple times, in cases where the malware appears in different variants with different signatures, but Apple decided not to give each version its own name.

- Names in the columns can vary, depending on which version of macOS you are using and which other programs are available on your computer. For example, an internal, technical designation could be listed, an English name, or a name in the primary language you have currently selected.

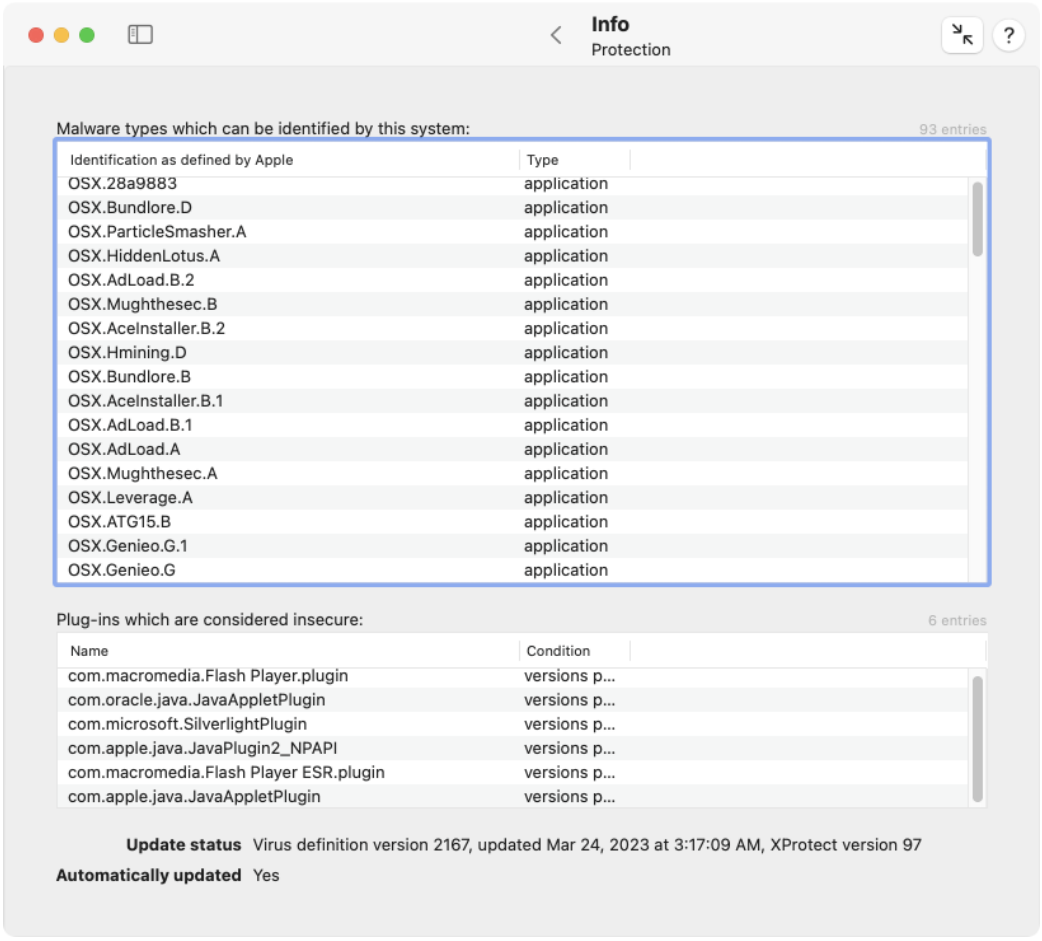


Figure 2.47: Malware protection

2.10.4 App Deny List

After you open the sub-item **App Deny List**, TinkerTool System shows you the operating system's currently list of known applications that should be excluded from using certain features, or should be prevented from running at all. This list is also updated when the option **Install Security Responses and System files** at **General** > **Software Update** > **Automatic Updates** > **i** in **System Settings**.

Three different types of deny lists are shown on this tab:

- The upper table lists applications which should not use the feature **App Nap** by default. App Nap is an Apple technology for saving energy at the application level: When the operating system detects that a running program is currently not visible or audible to the user (all its windows are hidden and the application is currently not playing any sounds), and is also not performing any background services (like downloading a file), this program will be slowed down automatically, basically putting it into a certain kind of sleep mode, waking it up only in longer time intervals, checking if there is something to do. Some older software products are not prepared for this technology yet, and won't work correctly when App Nap becomes active. macOS "knows" the affected applications listed here and automatically disables App Nap for them.

- The middle table lists applications which are known not to work correctly with the **High Resolution** features of macOS, also known as *HiDPI (High number of Dots Per Inch)*. If you are working with a Macintosh system equipped with a *Retina*, *4k-* or *5k* display, macOS will automatically rescale all graphics to make use of the sharp, high-resolution screen. Some older applications don't work correctly in this mode. If they are listed here, macOS won't enable Retina functions for them.

- The lower table lists applications which are known not to work at all with the current version of the operating system, or which will even cause technical problems. macOS will refuse to launch or migrate these applications when they are detected on your system.

Each table has three columns with the following meaning:

- **Name or identification:** the name or internal identification code of the application that is listed to be denied. If the affected application is available on your computer, TinkerTool System tries to show the name of the software product in your preferred language. In that case, the whole entry will also be shown in bold print. Programs which cannot be found on your system are shown with their unique identification code only.

- **Enforced:** If a dot is shown in this column, macOS will strictly enforce blocking the corresponding application. The user cannot override this decision.

- **Affected versions:** This column identifies the exact application versions for which the deny list entry should become effective. In some cases, only old, outdated versions of a software product should be blocked.

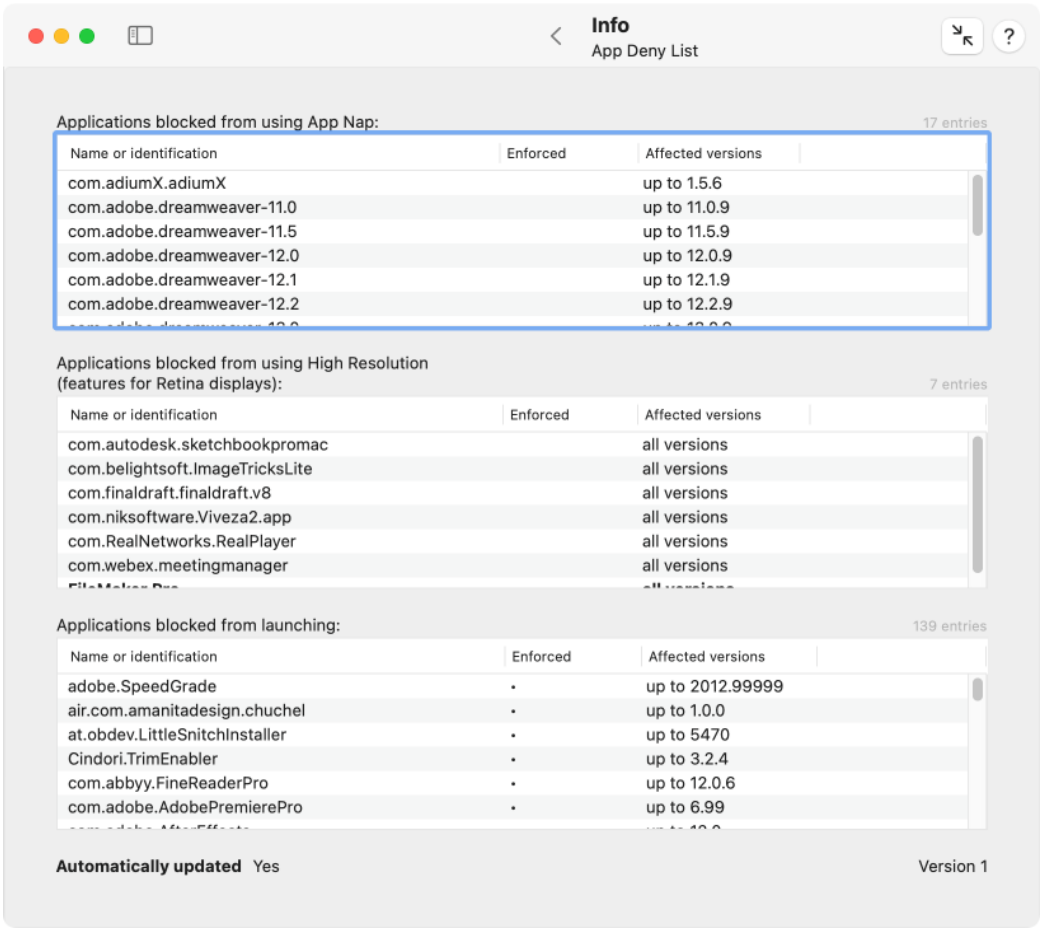


Figure 2.48: App deny list

2.10.5 Classic Logs and Reports

After selecting the sub-item **Classic Logs & Reports**, you will have direct access to a high number of log recordings kept by macOS. The operating system collects notification, warning and error messages in such files, especially for components of the system which don't have a direct graphical user interface. Administrators can use this information to keep track and analyze problem situations which occurred in the past. The classic logs are simple text files which are filled line by line over time. Most services also note time and date in each line, so it becomes easier to understand the series of events that occurred.

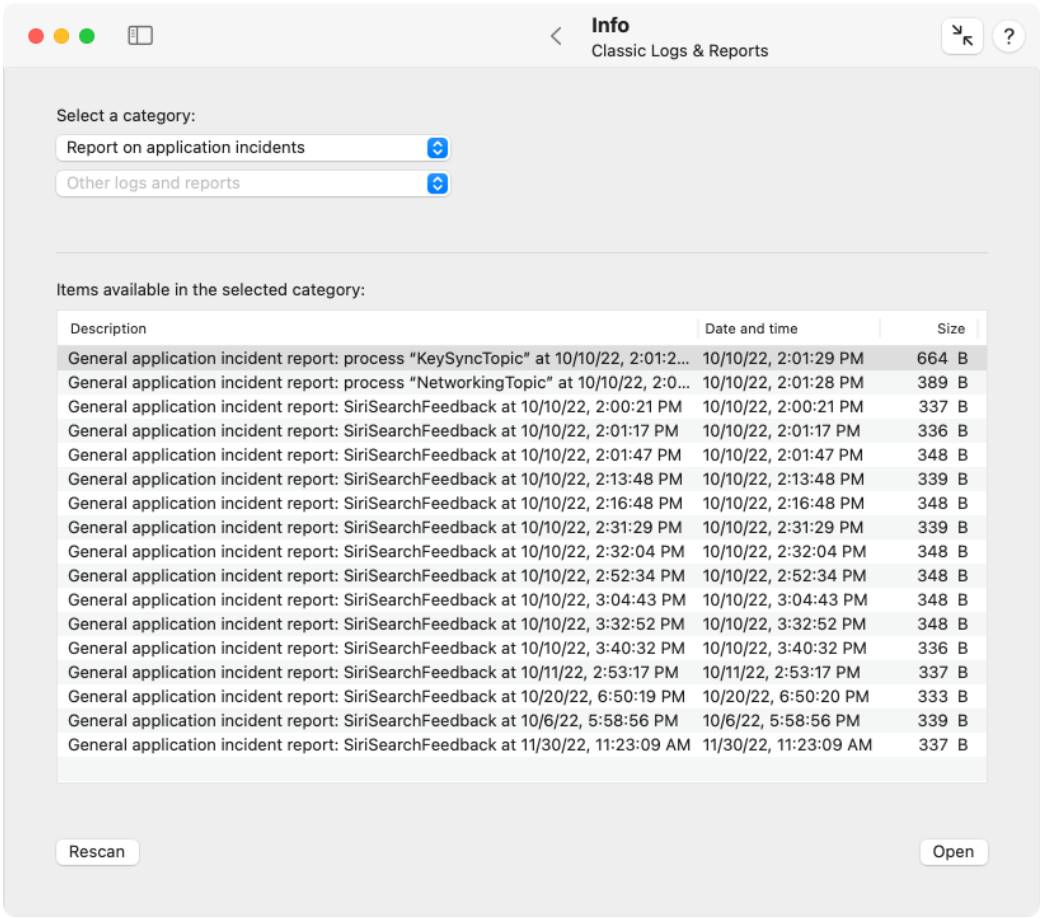


Figure 2.49: Logs and reports

The possibly available logs and reports are accessible via two pop-up buttons. The upper button **Standard logs and reports** allows you to select the most important log files maintained by macOS:

- **System logs:** The main system log which collects the warnings and error messages

of all running applications.

- **Application crash reports:** Detail information about all events where an application had to be quit unexpectedly because a serious internal error occurred.
- **Application crash reports (iOS style):** In 2022, Apple has begun to unify their crash reports across all platforms. macOS is also affected by this, and now usually creates crash reports in a variant which was originally developed for iPhones. Internally, the data is no longer stored as immediately readable report, but in a machine-readable format. TinkerTool System automatically tries to make this as readable as possible.
- **Application hang reports:** Details about events where an application entered a non-responding state. The affected program hung, i.e. it only performed some internal processing but could no longer react to user activity, like mouse clicks, for example.
- **System crash reports:** Technical information about events where a serious error was detected by the inner core of the operating system, the system kernel, so the entire computer had to be shut down immediately to avoid damage of data. In older versions of macOS, such an event was also known as *kernel panic*.
- **System emergency power-off:** These are reports about events where the user has triggered the emergency power-off feature of the Mac, i.e. an enforced shutdown by keeping the power button pressed for several seconds.
- **Apple Silicon issue base reports:** Technical information about events where the secondary operating system for the "Always On" part of Macintosh computers with Apple Silicon detected a problem which required a hardware restart. This can include hardware and system management issues.
- **Apple Silicon issue full reports:** This is a more advanced version of the previous item.
- **High CPU activity reports:** These reports keep track of incidents where macOS detected that an application consumed a lot of processing power, occupying one or more processor cores for an extended period of time. Those events can be normal for specific types of applications, so the reports may not indicate abnormal activity. The reports can be used to become aware of applications that need more energy than others, which can be interesting on battery-powered mobile computers.
- **High application activity reports:** The reports on high application activity refer to events where a program was woken up very frequently in a short time frame. Very similar to high CPU activity, these reports are also not critical but help to understand energy usage.
- **High memory usage reports:** If it makes sense, software developers can define a typical memory usage behavior of their applications. When such an application starts to behave unusual, i.e. it needs more memory than expected, this problem can be reported, or countermeasures can be initiated. For example, the application could try to reduce its memory usage or it could be shut down. These reports keep track of such events and contain the related memory statistics.

- **Disk write activity reports:** Because most Macintosh computers use flash-based storage, which is subject to wear, Apple collects statistics how many write operations occur on specific storage units. This allows to estimate the remaining lifetime of the flash memory cells.

- **Slow response reports:** macOS monitors whether applications respond to user interactions such as a key press or a mouse click within acceptable time intervals. If an application is currently too busy to respond to an event quickly enough, or experiences a technical problem, macOS will show a spinning cursor. It will also create this type of report.

- **Slow shutdown report:** A special kind of slow response is a computer that needs an unusually long time to shut down. To find the cause of such issues, macOS will create a slow shutdown report when such a problem occurs.

- **Differential Privacy submissions:** Apple devices collect information about how the different products, applications, and services are used. If your privacy settings grant Apple permission to do so, this information is sent to Apple from time to time, anonymizing the data by a technique called *differential privacy*. Each submission to Apple is logged.

- **Apple Wireless Diagnostics report:** When the operating system observes specific issues with WiFi operation, it automatically collects diagnostic data about each event. The data may contain private information about networks in the neighborhood. For this reason, the logs are usually encrypted and can only be decoded by authorized Apple service engineers.

- **Report on iCloud services:** These logs contain diagnostic information and statistical data about communication with Apple's iCloud services.

- **Report on baseband processing incidents:** For technical reasons, all operations that convert radio signals to digital data and backwards are collectively called *baseband processing*. This log category is used to record special events that occur in any of the radio-based components of the Mac, such as WiFi or Bluetooth.

- **Report on telephony monitoring:** These logs contain information collected by the telephony features of macOS.

- **Report on trust checks:** Trust checks are used by macOS to assure that a software component is genuine. This usually involves checking a digital signature of executable code and its certificate chain.

- **Report on iPhone updates:** The system creates a report each time you are using macOS to update iOS on an attached iPhone.

- **Report on iPad updates:** The same type of report is created for each operating system update of an iPad.

- **Proactive events reports:** macOS collects statistical data each day how many times Siri could "learn" something new about the user in order to improve its behavior as personal assistant. For example, Siri might have identified a family relationship between the user and another person.
- **Report on application incidents:** these are general diagnostic reports which are triggered by specific programs when they encounter special internal events, for example an unusually high number of write operations on a disk. It is at the discretion of each application which events are considered special.

The second pop-up button collects **Other logs and reports**. This includes known activity reports of macOS, e.g. related to the App Store, Disk Utility, the Resume feature, power down monitoring, etc., as well as unknown logs created by third-party applications. In the latter case, TinkerTool System cannot know the exact contents and meaning of the log files in advance, so the respective items are listed with their raw file names in the menu.

> For security reasons, logs that may keep potentially confidential or security-critical information cannot be opened by every user. You must be logged in as administrative user to ensure that you are capable of seeing and opening the complete set of log files. TinkerTool System will give you a warning in this respect if you are not using an administrator account.

After you have selected a log category with one of the two buttons, the table will give you an overview of the available logs. Each one is listed with a short description, date and time, which usually corresponds with the last entry recorded in the log, and file size. Either double-click a listed entry or click the button **Open** to open the respective log. A text window will show you the contents of the selected log file. Note that you can open as many windows simultaneously as you like. The logs can also be printed or saved into text files, using the buttons at the lower right corner of each window.

> For some logs, the additional button **Open with "Console"** will be shown. This applies to logs which macOS doesn't store as readable text in the clear, but in machine-readable form. TinkerTool System always tries to make this as readable as possible, but in some cases, the application **Console** (from the **Utilities** folder) can use internal know-how of Apple to refine the results even further. So as a test, you can additionally open a log in Console to check whether it is processed differently there. In some cases Console, in other cases TinkerTool System will produce better results.

If you assume that macOS has created new reports while TinkerTool System was running, click the button **Rescan** in the lower left corner of the sub-item to update the pop-up buttons accordingly.

2.10.6 Modern Logging and Tracing

In addition to classic logging where message lines are added at the end of several text files, macOS supports a modern log technology, based on databases. They contain structured,

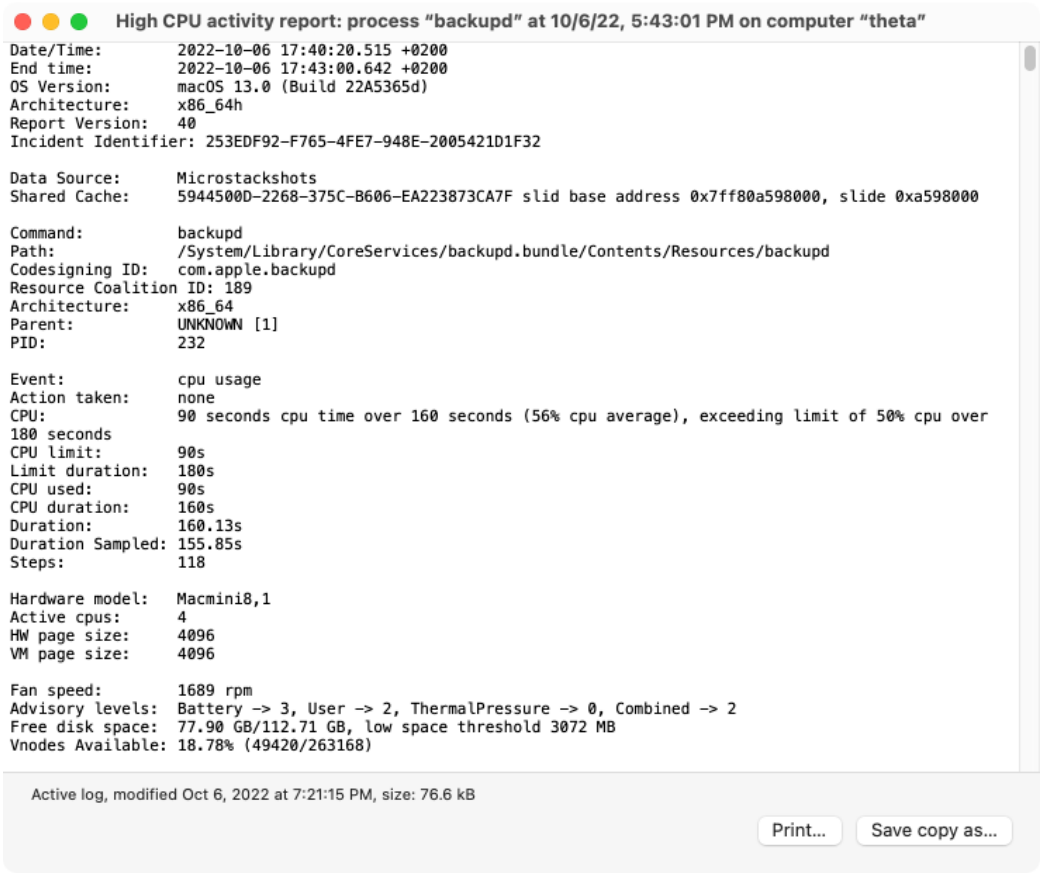


Figure 2.50: The contents of a log or report is shown in a separate window.

compressed records which are distributed between files and main memory, depending on case.

> Apple sometimes uses the term *Unified Logging* for this modern technology. It is designed to replace and supersede all previous logging methods, such as text logs, syslog, or ASL (Apple System Log).

The structure of today's applications create new challenges:

- Programs are separated into different processes, e.g. to handle privileges more safely.
- Processes are divided into different threads, to distribute work onto multiple processor cores.
- Threads might be executed in parallel or in random order, unknown in advance.

When trying to diagnose problems with applications by the use of old-fashioned text reports, it can become difficult or even impossible to track related events between all those processes and threads. Their problem messages might have been recorded in chaotic order and it might not be clear how they are connected with each other. Generating text lines with detailed diagnostic information (which might not be needed under normal circumstances) puts the applications and the operating system under unnecessary stress.

macOS tries to solve these problems by establishing techniques which are more appropriate for current applications:

- Instead of using text files, logging and tracing information is recorded in high-performance databases.
- Applications no longer need to prepare complex text lines themselves (e.g. by computing a textual presentation of a network address which should become part of an error message). They can send such data in raw form to a central logging component. The component can later create the text *on demand, if and when it is actually needed*. This way, the decision to generate text and to format diagnostic data is postponed as far as possible. In many cases, the data can just be discarded after some time, without ever being processed.
- The same technology is used on all system levels. The inner system kernel uses exactly the same technology as a high-level application with graphical user interface.
- There are system-wide severity levels that define how important a message will be. Unimportant messages that are only useful for debugging purposes can be hold in memory for a short, limited time instead of saving it permanently to files. Discarding, archiving and cleaning of logs can be controlled more precisely.
- Messages can be associated with so-called **activity identifiers**. They make it easier to track which messages belong to a certain operation in the system, even if the computations needed to execute that operation are distributed onto several processes and threads.

- The log entries in the database can be enriched with additional information. When logging data is needed to fix a problem, database filtering can be used to find the necessary information, hiding all entries which are unrelated. So-called **subsystem identifiers** and **category identifiers** can be used to organize log entries.
- References to user data which could be critical for the users' privacy can be removed before processing or storing them in the log database. This makes it easier to share logging data with technicians, avoiding the risk that private information or trade secrets are accidentally transferred to unauthorized individuals.

Activities contain a short clear-text description together with a numeric identifier. TinkerTool System shows an activity identifier as hexadecimal number with 16 digits. What to identify as separate activity and how to describe it is left to the author of the application that created an activity record.

Subsystem and category identifiers are also defined by the individual applications. So if you like to filter log messages associated with a specific software component, you'll need information from the software developer what identifiers to use. Subsystem identifiers should be used to define a location within a program, e.g. a specific module. Category identifiers should be used to define a certain mode of operation, e.g. "test mode" or "network-related."

> TinkerTool System automatically analyzes your current operating system and tries to "guess" some of the most important subsystem identifiers. The names appear in the combo box at **Filter by macOS logging subsystem identifier** and can be selected as menu items. You can also overwrite the entry field and enter any other valid name not listed here.

macOS uses five different levels to define the role or severity of a log message:

- **Fault:** a message reporting an error situation that affects the entire operating system or multiple components of a software product.
- **Error:** a message for a problem that is related to a single software component only.
- **Default:** a message which does not indicate an abnormal behavior, but is still so important that it might be worth noting it in the log.
- **Info:** a message of purely informational nature. Such messages are not stored permanently by default. They are usually retrieved on specific request only.
- **Debug:** a message which is only of interest for software developers, helping to track the behavior of a program at the source code level. Such entries are suppressed by default and may occur at very high frequencies, e.g. several hundred log items per second.

TinkerTool System can be used to either

- extract selected entries from the live logging database or from an exported archive, converting them to readable text which can be shown and saved, or to

- export selected or all entries from the logging database, so that they can be reviewed on a different computer.

Apple has defined a specific file format, the **macOS Log Archive** with the name extension **logarchive** to transfer logging and tracing data between different macOS systems. The archives cannot be used directly with previous system generations (OS X or Mac OS X).

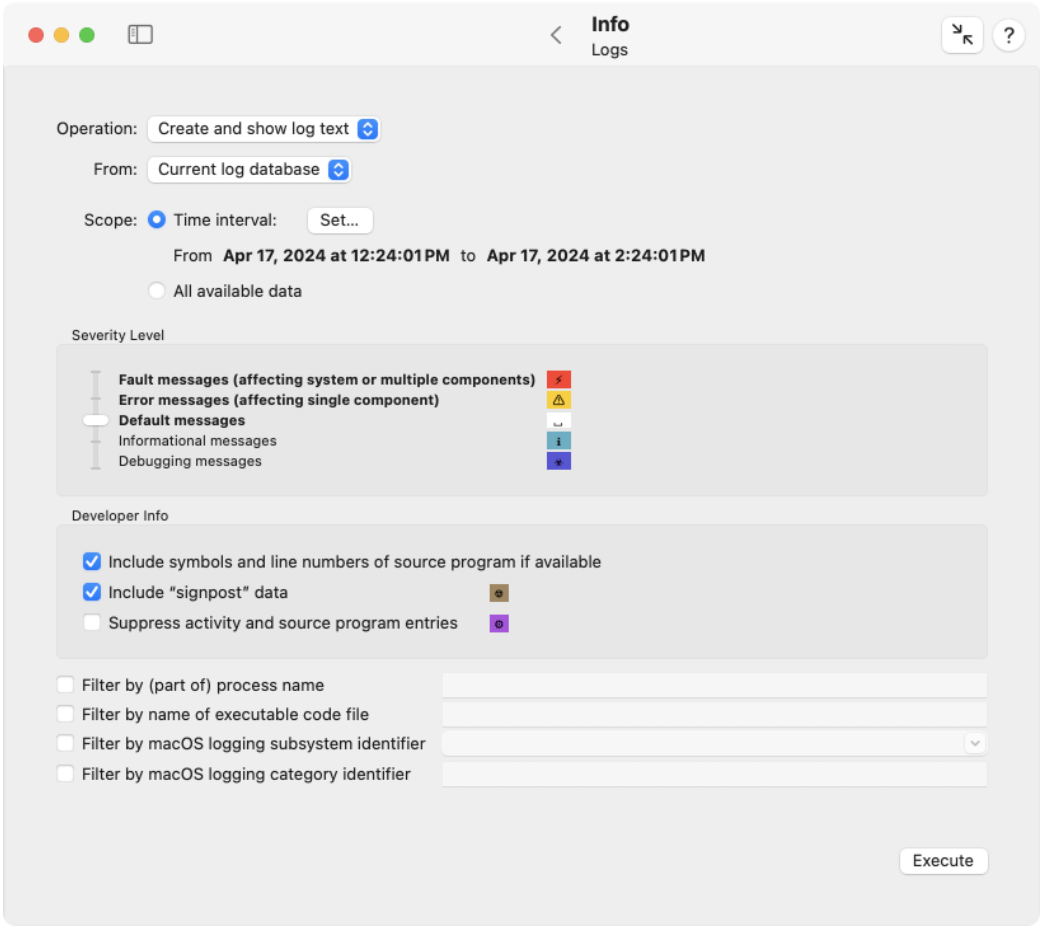


Figure 2.51: Working with modern logs

To work with modern macOS logs, perform the following steps:

1. Open the sub-item **Logs** of the pane **Info**.

2. Select the **Operation** that should be executed. You can either **create and show log text** or **export log data**.

3. Select the source for the operation (if applicable). This can either be the **current log database** of the local computer or **imported log data** taken from a macOS Log Archive file.

4. Use the buttons **Scope** to select the time interval that should be considered. Either you can specify a specific time interval via the **Set**… button, or select **all available data**. The time interval can be set with the **From** and **To** calendar/clock elements. You can either move the clock handles or enter the time as text. The button **+12h** can be clicked to quickly switch from AM to PM or vice versa, respectively. You can also set a **pre-computed time** as explained below.

5. Choose the **Severity level** with the slider. A lower level includes all messages of all higher levels, which is visualized by using bold labels.

6. If you like to add information for software developers to the log when available, set the respective check marks at **Developer Info**.

7. Enable or disable the filter options you need.

8. Click the button **Execute**.

By default, TinkerTool System will choose a time interval that includes the last two hours before the application was launched. If you don't restrict the log by additional filters, this interval might be too large, because typically more than 2 million events are recorded within this period. If you know when a certain event happened you are interested in, you can set an appropriate interval via the time entry sheet with the box …**or use precomputed time**.

There, you can enter date and time of an event manually, and let TinkerTool System set a window between 1 second and 999 minutes around this event automatically. The characteristic point in time can be chosen to be the beginning, the end, or the center of the interval. You can also set the **system startup time** or the current time (button **"Now"**) by mouse click.

To use a filter, enable the respective check mark, then enter the name or identification for this filter into the field right next to it.

> It is not recommended to let TinkerTool System generate very large log texts. The system may have problems to format and show such a long text in a standard window within an acceptable time. For this reason, the application automatically limits text reports to 500 megabytes of processed raw data.

TinkerTool System uses the small icons and background colors shown next to the controls to also mark messages with the corresponding severity level or activity messages in the result text. The icons are shown at the beginning of the associated line. You can remove all color markings by clicking the button **Remove colors**. This cannot be reverted.

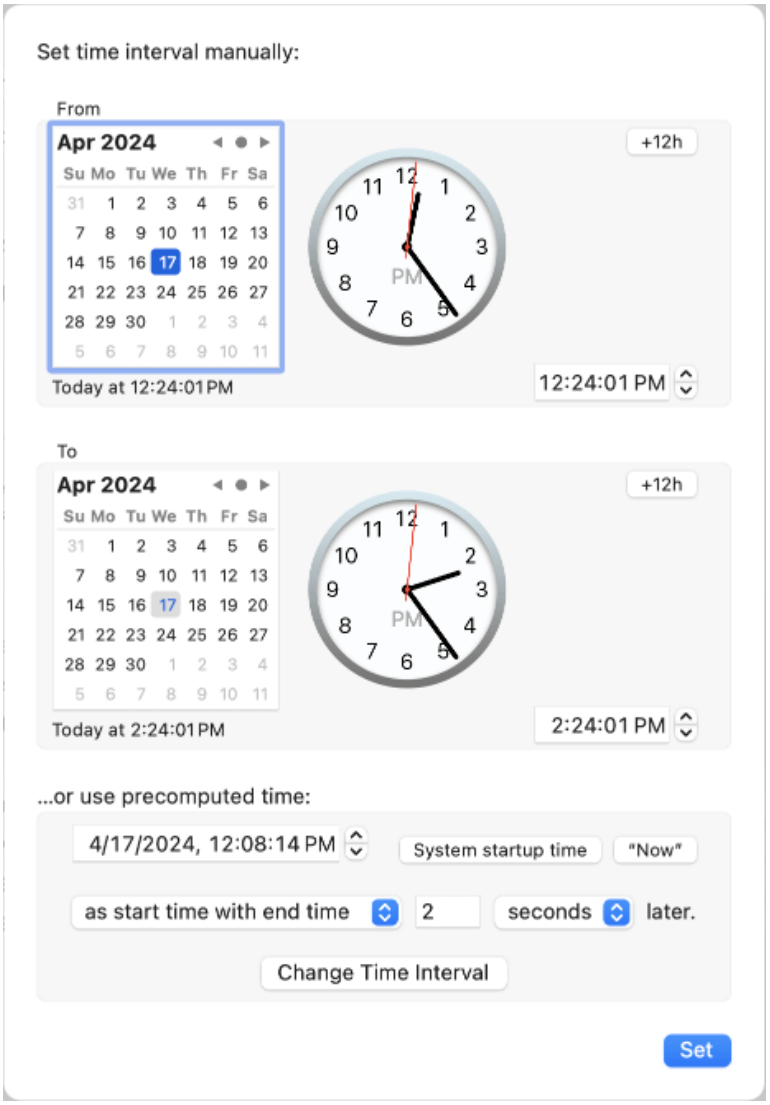


Figure 2.52: The time entry sheet assists you in specifying the time interval of interest

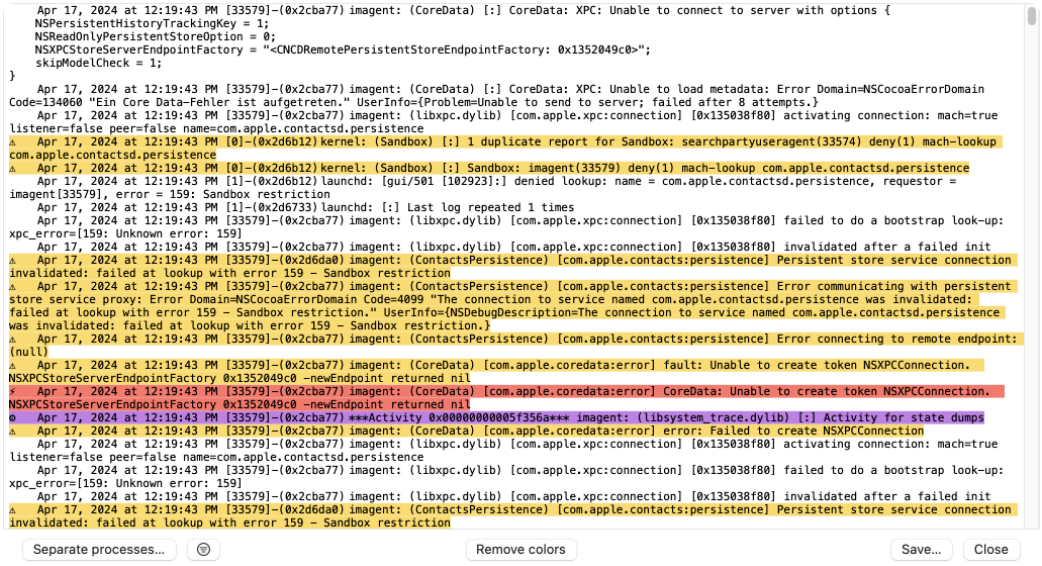


Figure 2.53: Display of a macOS log

> A black bar in the log text indicates that the macOS logging subsystem has removed some information from the output, because the application which had logged the message did not explicitly confirm that the text can be considered public. The removed part might contain data which could affect a user's privacy or could otherwise be subject to data protection. This behavior ensures that log excerpts can be transferred to third parties, respecting national data protection laws. TinkerTool System cannot make these "censored" parts visible. If you remove colors, the black bars will be shown with the text **private**.

If you have activated the option **Include symbols and line numbers of source program if available** and the respective information is included in a log entry, this data will be added with a marker

```
>>> source:
```

at the end of the message line. "Signpost" events are marked by a brown background. In addition to their actual text they contain an indicator of the pattern

```
[spid 0x123456789, ABC, DEF]
```

where the number behind **spid** is the hexadecimal signpost identifier, followed by a scope and a type specification.

You can save the generated log text by clicking the button **Save**... in the display sheet. It will be stored in *Rich Text Format (RTF)*, so it can be opened by any professional text

editor, like **TextEdit** for example. To search for text in the logs, use the **Edit** > **Find** menu items or press ⌘ + F.

If the log text is very long, but you know roughly what you are looking for, you can establish a belated text-based filter in addition to the plain find feature. It allows you to focus on specific message lines, hiding all others. To do this, click the button with the filter icon at the bottom left. In a dialog window, you can now define and apply a key word to search for. After that, only the lines which contain the search term will be shown. Another click on the filter button makes the hidden lines appear again.

By using the button **Separate processes**..., it is possible to isolate entries for individual process instances that are of particular interest from the overall log panel, displaying them in separate windows. After clicking, a dialog appears in which you can select the process instances that have been detected. The program name is given in each case, followed by the process identification (PID) within parentheses. After selecting the processes to be displayed, each instance will be shown in its own window. In order not to overload macOS, the simultaneous output is limited to a maximum of 40 windows.

Chapter 3

File Operations

3.1 The Pane Files

3.1.1 Link

A file system link is an additional representation of an existing file, or —in some cases— a folder. It can be used to refer to the file at a different location, in another folder or on another disk drive, or by using a different name. macOS is supporting three different types of links:

- **Alias:** an object referring to another file or folder which is capable of tracking the original object in case it should move or has been renamed. An alias becomes invalid when the original object is deleted.
- **Symbolic Link:** an object referring to another file or folder via its UNIX path name. If the original object is moved or renamed, the link will intentionally break. When trying to open an object via a broken link, you will receive an error message.
- **Hard Link:** an additional entry in a folder which is referring to a file. Neither the user nor the operating system can distinguish a hard link from the "first" folder entry of a file, so we can no longer speak of an original object here. Hard links are just one or more additional names pointing to the same file. Hard links are restricted to files, they cannot be used for folders. They also cannot cross volume boundaries, so the file a hard link refers to must lie on the same disk volume as the link.

The macOS Finder can create aliases only. If the Finder displays a symbolic link, it will also represent it as alias to simplify the situation for unexperienced users. Such objects are shown with a black curved arrow in addition to their icons. Aliases are a technology taken over from the classic Mac OS, and in some specific cases, applications must explicitly support the alias technology in order to access the original item the alias is pointing to. Links however are evaluated by the operating system itself, so they should work with any application.

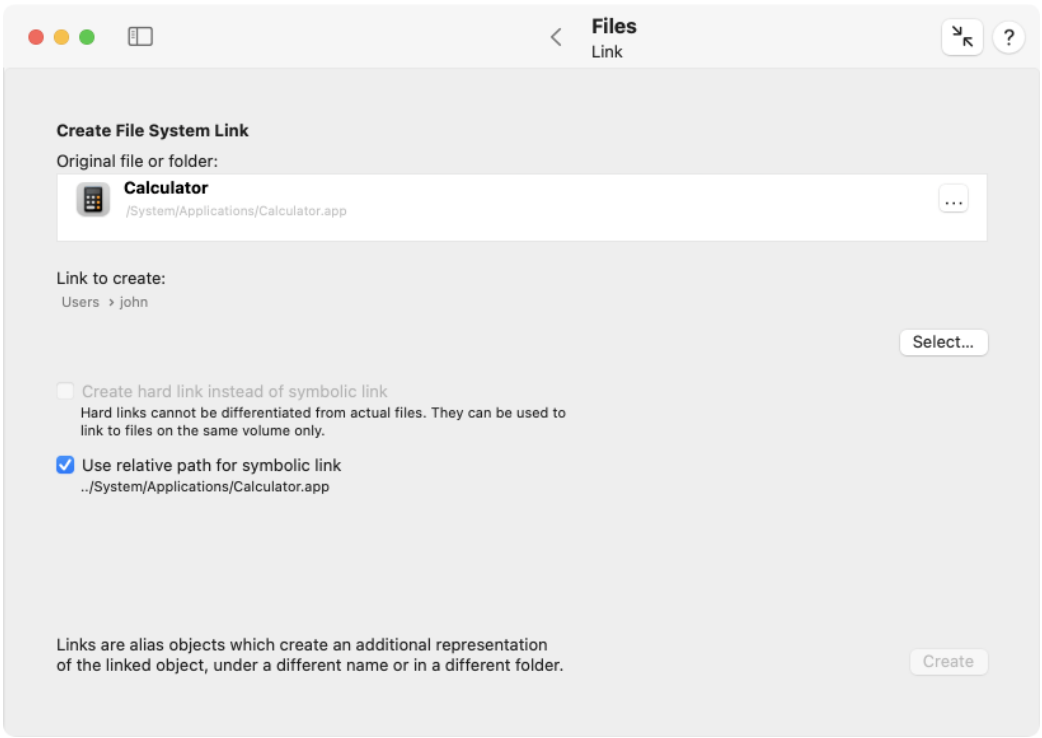


Figure 3.1: Link

> In fact, modern versions of macOS internally differentiate between classic Mac OS aliases, which are now deprecated, and modern aliases based on so-called *bookmarks*.

Because the Finder cannot create symbolic links or hard links, TinkerTool System adds these missing functions. Perform the following steps to create links:

1. Open the sub-item **Link** on the pane **Files.**
2. Drag the original file or folder from the Finder into the field **Original file or folder**. You can also click the button [...] to navigate to the object, or click on the white area to enter the UNIX path of the object.
3. Click the button **Select**... to specify the location and name where you like the link to be created.
4. By default, a symbolic link will be created. If you like to create a hard link, check the option **Create hard link instead of symbolic link**. Remember that hard links are restricted to point to files on the same disk volume.
5. If you have chosen a symbolic link, decide whether to create it with an absolute or relative path, using the option **Use relative path for symbolic link**. A relative path won't break in cases when you later move an entire folder hierarchy to another location, and both the link and link destination are within that hierarchy. The relative path that will be used is shown below the option.
6. Click the button **Create**.

3.1.2 Protection

macOS supports a special protection attribute which can be attached to files or folders. When you mark an object as being protected, it is no longer possible to change or delete it. Any change requires that the protection is being removed first. The macOS Finder uses a lock symbol displayed in addition to the usual icon to represent a protected object. Sometimes, the terms "locked" and "unlocked" are used for protected and unprotected objects, respectively. However, locking can also mean a different thing, namely to mark an object as being in exclusive use by a program, so we don't use this term to avoid confusion.

TinkerTool System has the option to set or remove protection flags not only for single objects but for a whole hierarchy of files and folders included in a top folder. To work with protection attributes, perform the following steps:

1. Open the sub-item **Protection** on the pane **Files**.
2. Drag a file or folder from the Finder into the field **File or folder**. You can also click the button [...] to navigate to the object, or click on the white area to enter the UNIX path of the object.

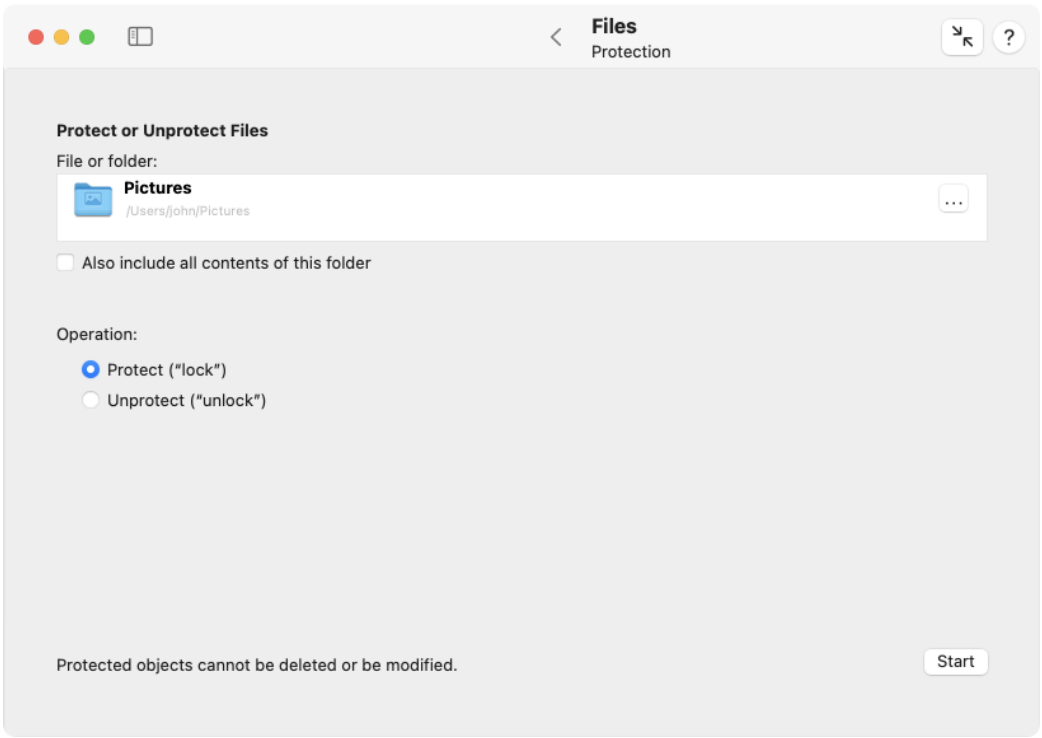


Figure 3.2: Protection

3. If you have selected a folder, decide if the protection should only be modified for the folder itself or all its contents, too. Set the option **Also include all contents of this folder** accordingly.
4. Switch the radio buttons **Operation** either to **Protect** or **Unprotect**.
5. Click the button **Start**.

> Some non-Macintosh file systems are not capable of supporting protection attributes. In this case, the operating system may confirm that the protection marker has been set successfully, but the object remains in the unprotected state.

3.1.3 Attributes

In addition to the protection marker, which is also supported at the UNIX level of macOS, the operating system is supporting some high-level attributes which have been adopted from the classic Mac OS.

- A file can be associated with an **HFS type code**: The type code is designed to indicate what kind of document the file should represent. By help of the type code, the system can quickly determine what is expected to be stored in a given file, without needing any special markers in the file name (like file name extensions) and without having to analyze the contents of a file.
- A file can also be associated with an **HFS creator code**: The creator code was designed to indicate which application should open this file. By help of the creator code, the system could quickly determine which application the user prefers to open a given document, hereby overriding the default connection between the file type and the associated standard program to open documents of this type. Creator codes enforced a strict binding between a specific document and an application. Today, creator codes are a thing of the past. TinkerTool System can still show and edit creator codes, but they are no longer in use in macOS.
- Files or folders can be associated with a visibility marker: If an object is marked as being invisible, the Finder and all **Open** panels will no longer display this object. You can only refer to the file by specifying its full UNIX path name, or by using applications which do not respect the visibility attribute. Invisible objects are also called *hidden*.

> Although we are referring to type and creator attributes as being HFS codes, these codes are not restricted to be used on HFS and HFS+ file systems only. macOS is capable of emulating these attributes on nearly any file system.

To change one or all of these high-level attributes, perform the following steps:

1. Open the sub-item **Attributes** on the pane **Files**.

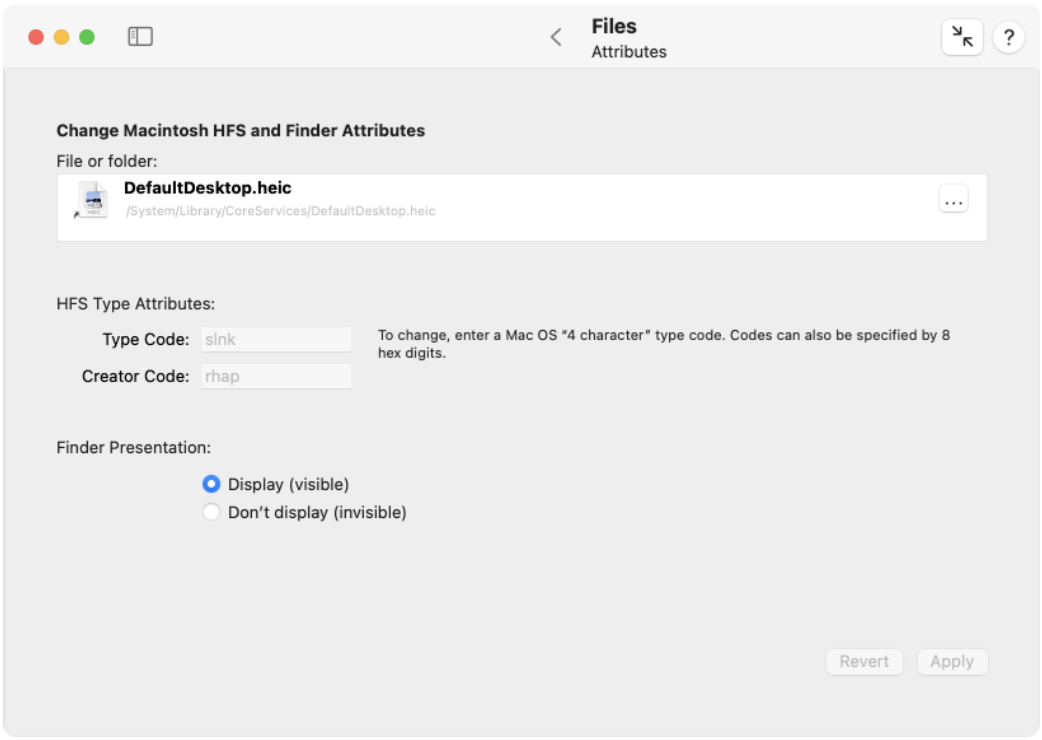


Figure 3.3: Attributes

2. Drag a file or folder from the Finder into the field **File or folder**. You can also click the button [...] to navigate to the object, or click on the white area to enter the UNIX path of the object.
3. Modify the attributes, entering new values into the code fields, or clicking one of the **Finder Presentation** buttons.
4. Click the button **Apply** to set the new attributes, or click the button **Revert** to discard your changes and reread the current attributes from the selected object.

Type codes and creator codes must be specified either by four characters of the ASCII character set, or by four arbitrary bytes which have to be entered using eight hexadecimal digits (the digits 0 to 9 and the letters a, b, c, d, e, f, or A, B, C, D, E, F). The program will automatically detect what you mean depending on the length of your input. Note that codes specified by ASCII are always case-sensitive. Examples for valid codes are:

- PREF
- ilge
- 8BPS
- A4B7C1D1

To remove a type or creator code from a file, delete the entry in the respective code field completely and click **Apply**. TinkerTool System cannot assist you in selecting type or creator codes for known document types or known applications, respectively. You'll have to know the correct codes in advance.

> Although it is technically possible to store HFS type attributes for folders, the meaning of this was undefined in the classic Mac OS, and Apple never supported this officially. For this reason, TinkerTool System also won't permit to attach these attributes to folders.
>
> Keep in mind that you can no longer use drag-and-drop or file dialogs for objects which are invisible. You'll have to enter the object's full UNIX path to access it by an application. This also includes TinkerTool System. However, you can press the key combination ⌘ + ⇧ + . in a Finder window to let it show invisible objects. Pressing the key combination in the Finder once more will disable that feature again.

3.1.4 Changing Time Attributes

Among the many attributes stored with each file and each folder are various time specifications:

- Time of creation
- Time of last modification

- Time of last access
- Time of last backup
- Time of last status change

The times of last change and last access are mandatory. Whether other times are also saved depends on the respective file system. For example, HFS+ is able to store the time of last backup while APFS cannot. Information that is not available is marked by TinkerTool System with greyed-out labels.

> macOS and other UNIX systems use the date **01/01/1970** to indicate that a valid time has not been set yet.

There can be various reasons for adjusting or correcting the time information manually, for example if a file contains a digital image from a camera with an incorrect clock setting. TinkerTool System allows the existing time information to be overwritten with other values.

The time of last status change plays a special role in the operating system and is usually not displayed by applications such as the Finder. This time specification is used, among other things, to control the internal administration of the file system and *cannot* be changed in order to avoid errors in the system.

To modify one or more time attributes of an object, perform the following steps:

1. Open the sub-item **Times** on the pane **Files**.
2. Drag a file or folder from the Finder into the field **File or folder**. You can also click the button [...] to navigate to the object, or click on the white area to enter the UNIX path of the object.
3. Change the time specifications as desired by entering new values into the fields, or by clicking their arrow buttons, respectively.
4. Click **Apply**.

You can use the button **Revert** any time to go back to the original values currently stored.

> Caused by activities of the operating system, the value for **time of last access** may unexpectedly change after TinkerTool System has saved it. This is mainly due to how the Finder's preview functions work and cannot be prevented.
>
> The Finder additionally shows a time **Last opened**. This is not an attribute actually stored in the file system, but a value calculated by Spotlight. Therefore it is not included in the list of times.

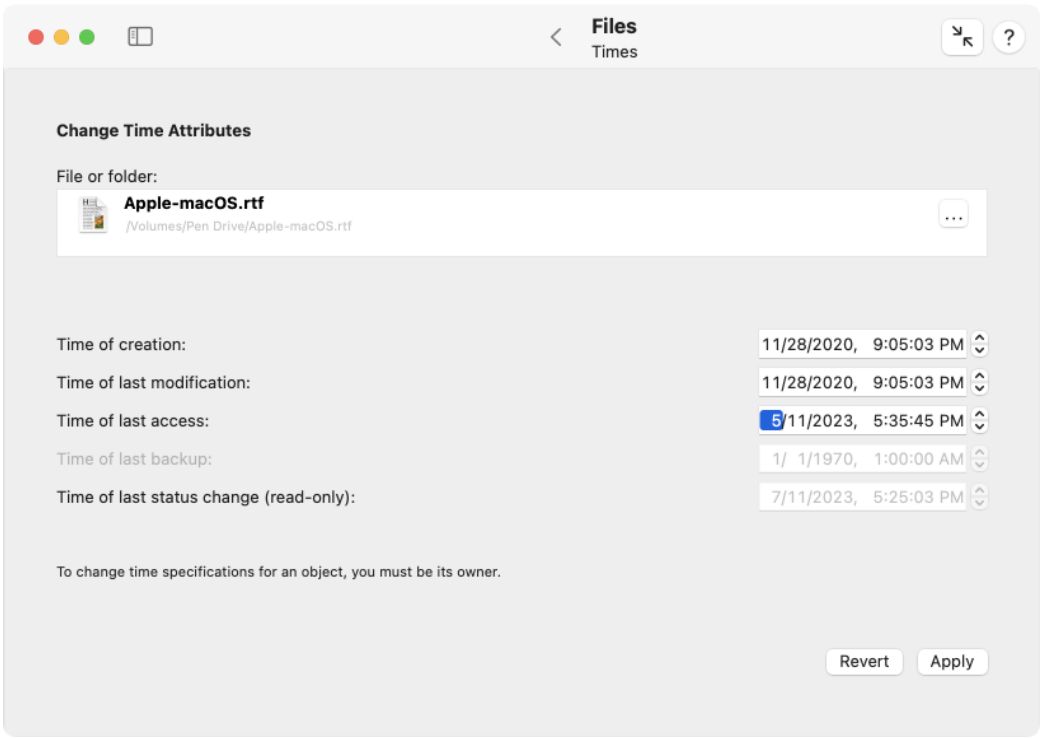


Figure 3.4: Time specifications for an object can be changed

3.1.5 Quarantine

An important part of the security infrastructure built into macOS is its capability to track potentially dangerous files coming from untrusted sources, or having been transferred via unsafe channels like the Internet. When you open such a file or program, you will receive a warning message which asks for reconfirmation whether you actually trust the file. The source of the file and the time when it was loaded onto your computer is noted in the message.

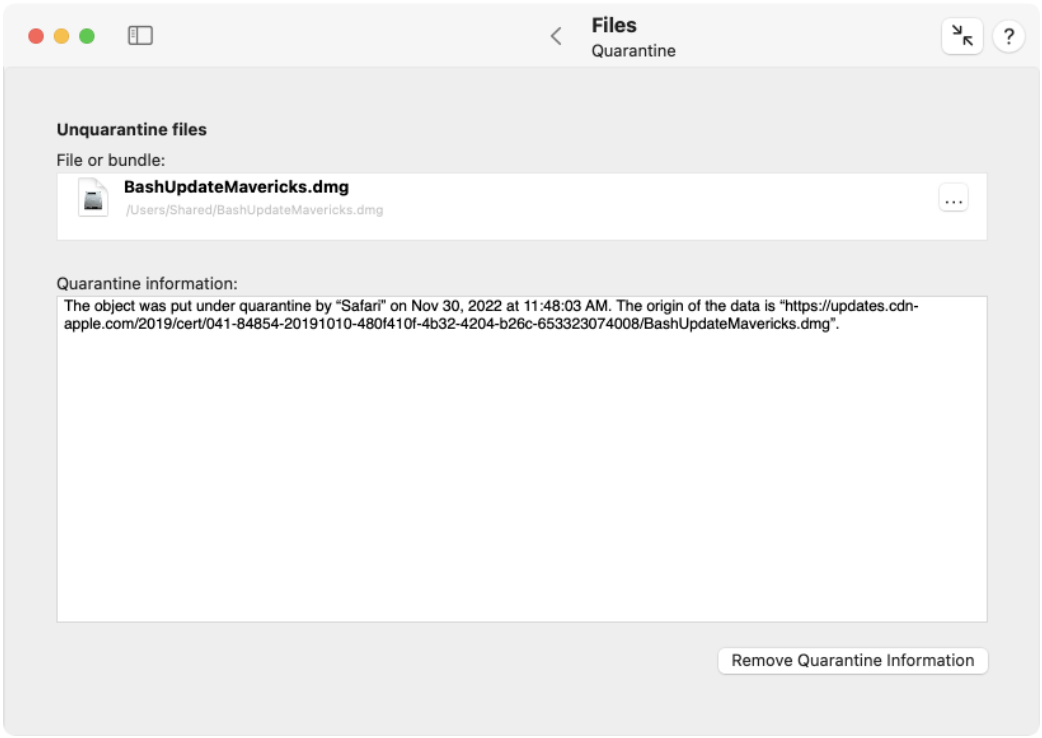


Figure 3.5: Quarantine

This feature is technically implemented by adding special quarantine attributes to the affected files. TinkerTool System can display this information, giving you the option to remove the attribute, hereby "un-quarantining" the files. This can be helpful if you know that the file comes from a trusted source and you like to "re-publish" it on your own computer, for example before placing it into the public folder **/Users/Shared** or before uploading it to your local file server. This way you can avoid that other users are confronted with the warning message. They might not be able to successfully confirm they trust the files because they might not have the necessary write permissions for the shared folder.

> Removing quarantine information from an application will also disable the security feature "Gatekeeper" for that program. macOS will no longer recognize that the

> application has been downloaded from the Internet, so its files will become irrelevant to Gatekeeper.

To remove quarantine information from a single object, perform the following steps:

1. Open the sub-item **Quarantine** on the pane **Files**.
2. Drag a file or bundle from the Finder into the field **File or bundle**. You can also click the button [...] to navigate to the object, or click on the white area to enter the UNIX path of the object.
3. Verify the current status displayed in the field **Quarantine information**.
4. Click the button **Remove Quarantine Information**.

3.1.6 Contents

You may sometimes receive files of unknown origin or with unknown document types. In other cases, files may have invalid type markers or file name extensions, for example a file displayed by the Finder to be a PNG image although it actually contains a JPEG image. To find out what is really contained in a file, you can have macOS look into the file letting it analyze what its contents may be. To do this, perform the following steps:

1. Open the sub-item **Contents** on the pane **Files**.
2. Drag a file from the Finder into the field **File to analyze**. You can also click the button [...] to navigate to the object, or click on the white area to enter the UNIX path of the object.
3. The result of the analysis will be displayed in the field **Results**.

> The analysis is done by the underlying operating system, not by TinkerTool System. For this reason the results may slightly vary in different operating system versions. The report is always displayed in English, no matter what preferred language you have set in your personal preferences.

You can only select one file at a time. It is not possible to analyze applications or other bundles. They will be simply identified as being a **directory**, the technical term for a folder. This analysis is correct, because bundles are actually folders which may contain a large number of different files although the Finder represents them by single file icons. To select one of the files inside a bundle, select it in the Finder and use the Finder's feature **Show package contents** to open it as a folder. Then drag one of the contained files into the field of TinkerTool System.

In some cases, it might also be helpful to know which metadata the Spotlight search engine of macOS has collected about a particular object. To additionally display the Spotlight data, click the button **Also show Spotlight metadata** below the **Results** field. A table will appear which contains the complete list of Spotlight attributes for the selected object.

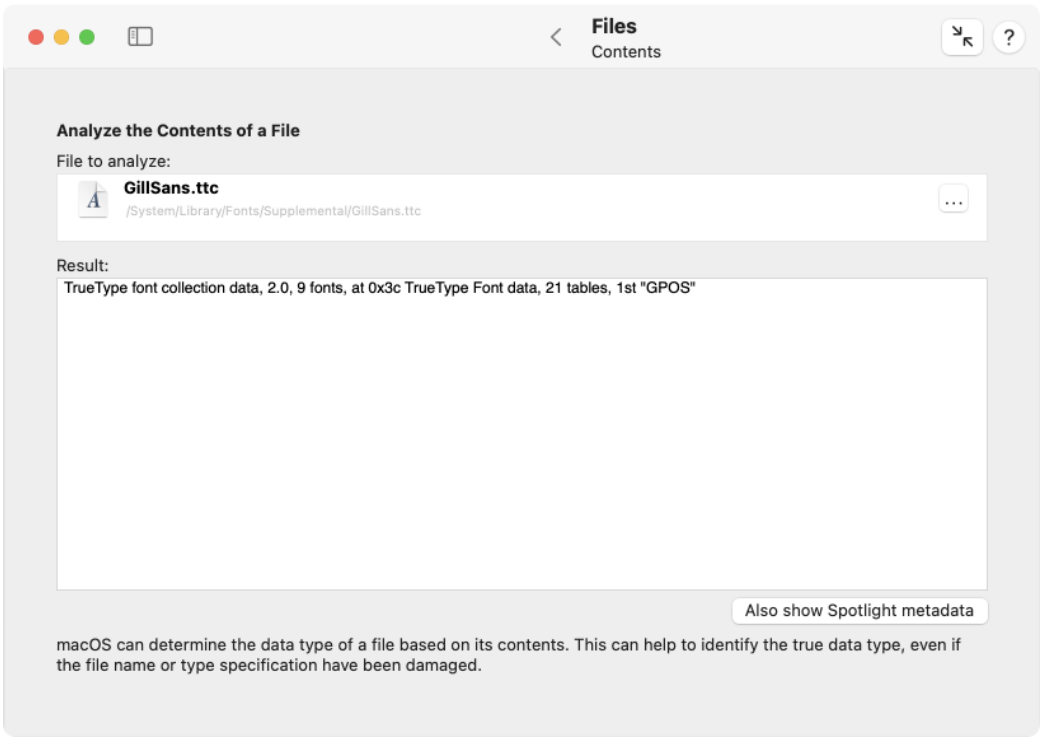
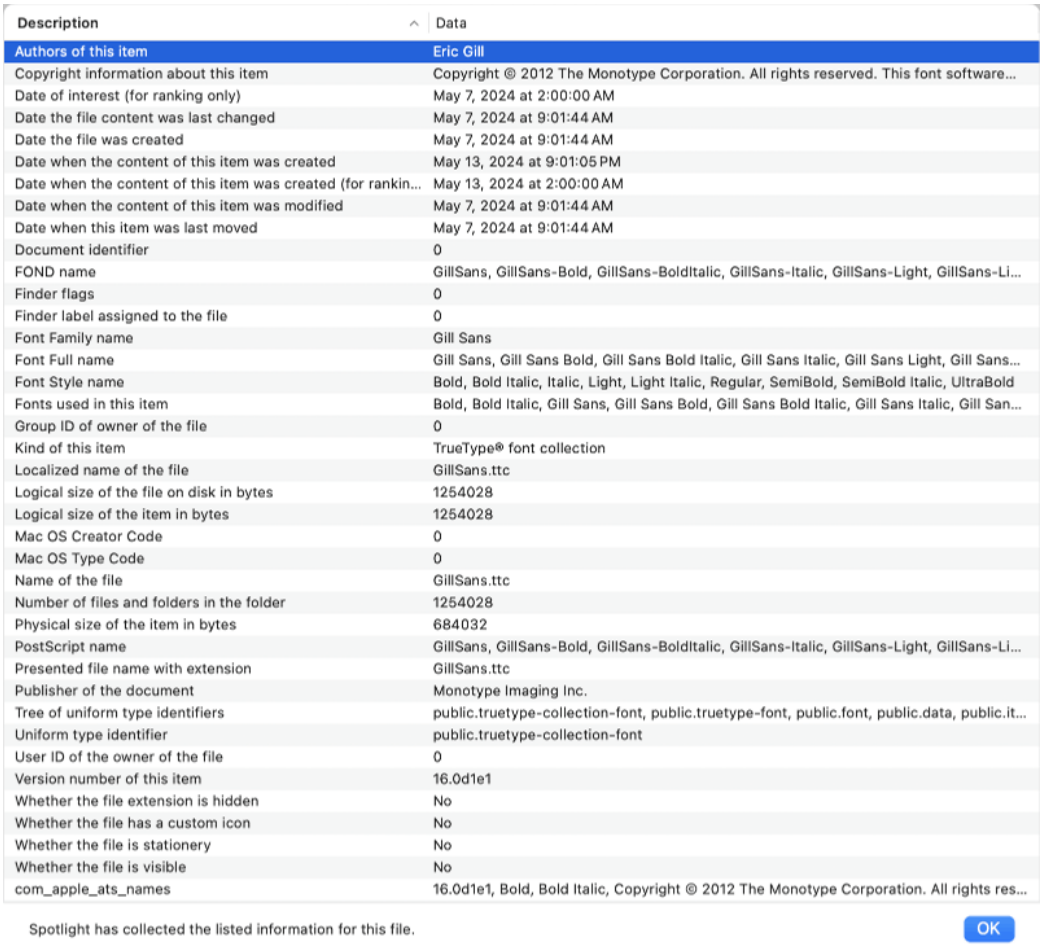


Figure 3.6: Contents



Description	Data
Authors of this item	Eric Gill
Copyright information about this item	Copyright © 2012 The Monotype Corporation. All rights reserved. This font software...
Date of interest (for ranking only)	May 7, 2024 at 2:00:00 AM
Date the file content was last changed	May 7, 2024 at 9:01:44 AM
Date the file was created	May 7, 2024 at 9:01:44 AM
Date when the content of this item was created	May 13, 2024 at 9:01:05 PM
Date when the content of this item was created (for rankin...	May 13, 2024 at 2:00:00 AM
Date when the content of this item was modified	May 7, 2024 at 9:01:44 AM
Date when this item was last moved	May 7, 2024 at 9:01:44 AM
Document identifier	0
FOND name	GillSans, GillSans-Bold, GillSans-BoldItalic, GillSans-Italic, GillSans-Light, GillSans-Li...
Finder flags	0
Finder label assigned to the file	0
Font Family name	Gill Sans
Font Full name	Gill Sans, Gill Sans Bold, Gill Sans Bold Italic, Gill Sans Italic, Gill Sans Light, Gill Sans...
Font Style name	Bold, Bold Italic, Italic, Light, Light Italic, Regular, SemiBold, SemiBold Italic, UltraBold
Fonts used in this item	Bold, Bold Italic, Gill Sans, Gill Sans Bold, Gill Sans Bold Italic, Gill Sans Italic, Gill San...
Group ID of owner of the file	0
Kind of this item	TrueType® font collection
Localized name of the file	GillSans.ttc
Logical size of the file on disk in bytes	1254028
Logical size of the item in bytes	1254028
Mac OS Creator Code	0
Mac OS Type Code	0
Name of the file	GillSans.ttc
Number of files and folders in the folder	1254028
Physical size of the item in bytes	684032
PostScript name	GillSans, GillSans-Bold, GillSans-BoldItalic, GillSans-Italic, GillSans-Light, GillSans-Li...
Presented file name with extension	GillSans.ttc
Publisher of the document	Monotype Imaging Inc.
Tree of uniform type identifiers	public.truetype-collection-font, public.truetype-font, public.font, public.data, public.it...
Uniform type identifier	public.truetype-collection-font
User ID of the owner of the file	0
Version number of this item	16.0d1e1
Whether the file extension is hidden	No
Whether the file has a custom icon	No
Whether the file is stationery	No
Whether the file is visible	No
com_apple_ats_names	16.0d1e1, Bold, Bold Italic, Copyright © 2012 The Monotype Corporation. All rights res...

Spotlight has collected the listed information for this file. OK

Figure 3.7: The list of Spotlight metadata maintained by macOS for this file can also be shown

3.1.7 Analyze Alias Objects

In 1991, Apple introduced a new file system object, the *alias*, in what was then the operating system Mac OS 7. Via the menu item **Make Alias** you can create a reference to an existing file or folder and thus address the same object under different names or at different locations, without having to store it multiple times. In other operating systems, aliases are also known as shortcuts or links.

Aliases still exist in today's macOS. However, they are technically implemented differently, since the original way of storing aliases is too insecure by today's standards and has certain disadvantages. Since the base of the operating system has been switched to the professional UNIX, other types of alias-like objects have also been added, since file references have existed in UNIX for much longer. All of these different ways of linking files are presented as alias by the Finder for convenience, although there are often subtle differences in their properties and capabilities. TinkerTool System allows you to determine how an alias is actually implemented. You can also check which target object the alias refers to and how much storage space it requires.

macOS currently uses the following types of alias objects:

- **Classic Mac OS Alias:** This was the original file type to store aliases. It was a special description file in which a kind of search specification for the target object was stored. In addition to name and storage folder, things such as the approximate file size and files in the neighborhood were also specified. If a program wanted to open an alias object, it had to take special steps itself, namely passing the object to the *Mac OS Alias Manager* for evaluation. This sent a kind of search request to the operating system to find the original file using the existing description data. This way, an alias could often remain functional even if the original file was renamed or moved. This was quite convenient, but had the disadvantage that every program had to actively support working with aliases. In addition, by today's standards, the idea of finding the original using a search request in case of doubt is too dangerous: an attacker could replace an original file with a fake that is so similar to the original that the Alias Manager uses the manipulated copy instead of the original as the target of the alias. This could make users open a file that triggers malicious functions with their current rights. Modern versions of macOS no longer create such classic aliases. However, for compatibility reasons, these aliases can still be opened, but they are subject to special security restrictions.

- **macOS Bookmark:** If you create an alias via the Finder, recent versions of macOS save the alias as a *macOS Bookmark file*. This behaves similarly to a bookmark in a web browser and saves the target via a file-related URL ("Internet address"), which can also be protected with security information. For security reasons, if you move the original object to a different location, the reference is intentionally invalidated and the alias can no longer be resolved. When working with files and folders via the usual macOS **Open** dialog windows, the evaluation of bookmarks is supported automatically by the higher layers of macOS, so that applications don't have to take care of it.

- **absolute symbolic link:** on the UNIX level of macOS, aliases can be implemented

even more simply: you store the absolute file path of the target in a text file and add a marker that it is a link, in this case a *symbolic link*. Working with and creating symbolic links has already been described in the first section of this chapter. Here, the link will also become invalid by intention when the original object is renamed or moved. Symbolic links are resolved fully automatically by the operating system, without the opening application having to "know" this. Only if a program actively states that it explicitly *does not* want to have symbolic links evaluated, it will be able to recognize a symbolic link as such.

- **relative symbolic link:** This is a special variant of a symbolic link, where the file path is not saved as an absolute location, but relative to the location of the alias (e.g. as "go up one folder, then go to object X in subfolder Y"). In this case, an entire subfolder hierarchy can be moved to a new location and the link will still be valid.

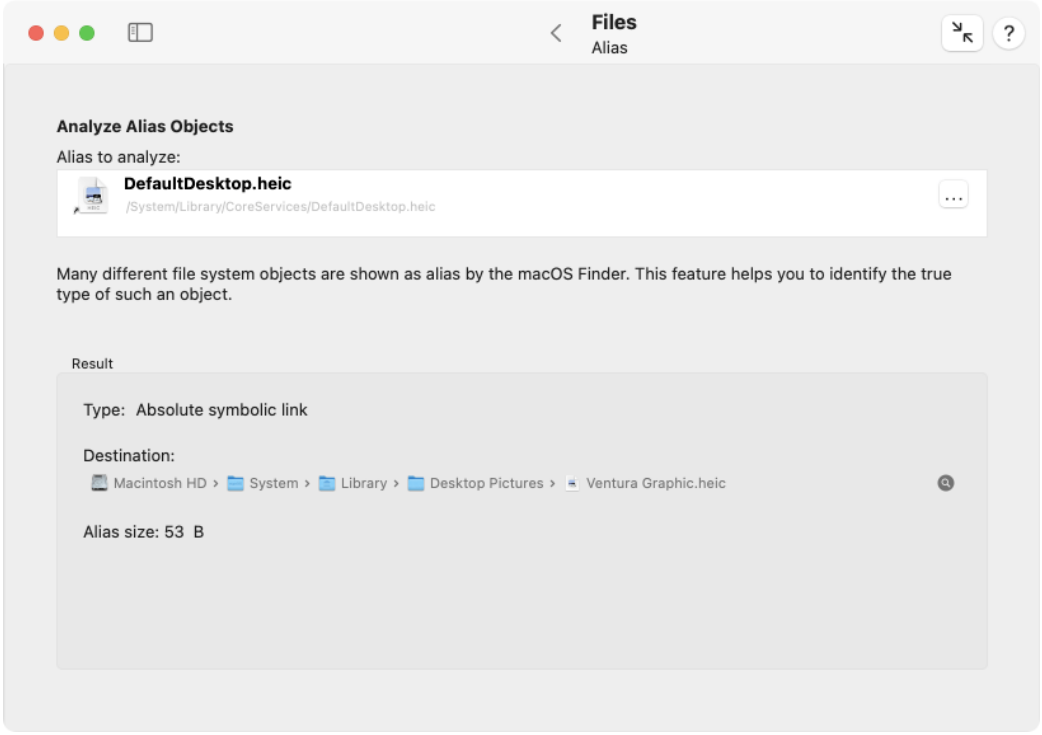


Figure 3.8: The Finder uses the generic term alias for different types of objects

To determine the actual type of an item presented as alias by the Finder, do the following:

1. Open the sub-item **Alias** on the pane **Files**.
2. Drag an alias from the Finder into the field **Alias to analyze**. You can also click the

button [...] to navigate to the object, or click on the white area to enter the UNIX path of the object.

The evaluation is shown in the **Result** box. You can use the magnifying glass icon to reveal the original object in the Finder.

3.1.8 Force Delete

Badly written applications and installers which don't handle permissions properly may leave files or folders on your system that cannot be moved into the Trash very easily. In other cases, applications may create a large number of files with write protection which also cannot be removed quickly. If you want to enforce removal of a large number of protected files, or if you want to remove a file from a folder with inappropriate permission settings, you can do so with the **Force Delete** feature:

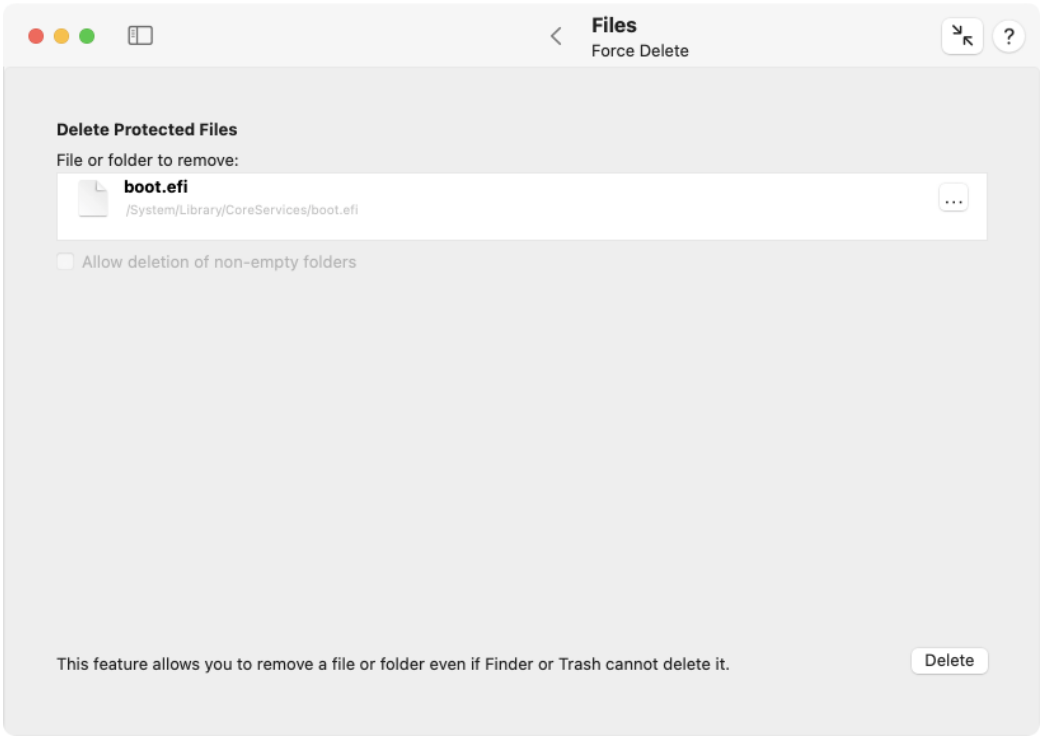


Figure 3.9: Force delete

1. Open the sub-item **Force Delete** on the pane **Files**.
2. Drag a file or folder from the Finder into the field **File or folder to remove**. You can also click the button [...] to navigate to the object, or click on the white area to enter the UNIX path of the object.

3. If you have selected a folder for removal and this folder contains objects, you must confirm that you are going to delete the folder together with its objects inside. In that case, set the check mark **Allow deletion of non-empty folders**.

4. Click the button **Delete**.

3.1.9 Nesting

Limits of the Local Operating System

Modern operating systems and file systems have no limit how deep you can nest folders. However, there is a technical limit in the paths that are used to refer to these folders or the files they contain. In compliance with the POSIX industry standard, an operating system does *not* need to support file access paths with unlimited lengths when addressing a file system object in an application, command, or any function that works with file names.

In practice, this means that access to a file in a hierarchy of very deeply nested folders with long names may just fail, when the operating system does not accept that file's *absolute path* because it is too long. Objects in such folders may become invisible on the graphical user interface, e.g. in the Finder, or in Open/Save panels, because the system is no longer capable of processing their oversized paths.

Note that paths depend on context and present situation. If a file is on your system volume named "Macintosh HD," it may have an absolute access path like

```
/Users/MyName/Documents/Some/Nested/Folder/Example/Document.txt
```

If this disk is now mounted as external drive by a different Mac, the very same file may now be addressed by

```
/Volumes/Macintosh HD/Users/MyName/Documents/Some/Nested/Folder/Example/Document.txt
```

so the length of the path has increased by the part needed for "/Volumes/Macintosh HD" that the other Mac uses to refer to this external disk volume. Paths for identical objects can vary depending on how you combine multiple disks to build the entire file system hierarchy of the running computer. In enterprise networks, objects on file servers can become visible in arbitrary folders the network administrator has chosen for the client computers to use. In this case the paths are also just appended at run time. They are not stored anywhere.

Such deep folder hierarchies with overly long access names can be created by using *relative* paths instead of absolute paths. We won't go into further details here, but the operating system alternatively supports the concept of a *current working folder*. You can tell the system to "go" into the folder at

```
/Users/MyName/Documents/
```

then to navigate to the subfolder **Some**, then to navigate to its subfolder **Nested**, and so on, only using *relative* "navigation" instructions with short paths, instead of packing the entire specification of the file's location into one single path specifier.

When referring to path lengths, not the plain number of characters, but the amount of memory used to store the characters when handling the path plays the crucial role. All modern operating systems use the Unicode UTF–8 encoding when processing file paths. With this encoding system, Latin characters, including characters with accents for many European languages usually need one byte per character. Characters of many Asian languages are stored as two bytes. Very specialized characters, such as Emojis, need four or even more bytes.

TinkerTool System can determine the maximum number of bytes the currently running version of macOS guarantees to be supported when referring to files via paths. It can also check whether all files in a folder hierarchy of a specified top folder can currently be addressed by absolute paths without exceeding this given limit.

- The check can be performed for any folder, no matter if it is on the system volume, an external disk, or a file server.
- To avoid privacy issues, the check will be limited to files and folders which you are permitted to open.
- The scan is automatically limited to the volume on which the top folder is located. If you like to test all disks, you'll have to run separate checks, selecting each of their top folders.
- Objects marked as *dataless files,* which refer to synchronized data in iCloud or cloud solutions of other vendors, are automatically excluded by the operation. Otherwise, macOS would automatically trigger downloads for the affected files when their folders are scanned.

You can activate an additional option not only to check the paths as they currently are, but also to check *possible* paths that could be created if an application attempts to copy the tested files to a different volume, and that application is using absolute paths to do that. As we had explained previously, the path for the mount point of the destination volume would need to be added to the already existing paths if a program tried to create a "clone" of a volume, copying its contents file by file to a different one.

Perform the following steps to check a folder hierarchy for overly long access paths:

1. Open the sub-item **Nesting** on the pane **Files**.
2. Drag the folder where the test should start from the Finder into the field **Top folder for check**. You can also click the button [...] to navigate to the folder, or click on the white area to enter the UNIX path of the folder.
3. Decide if you like to check the paths of the selected objects as they are, or to check their paths under the assumption that each object would be copied to all currently attached volumes. In the latter case, set a check mark at **Check whether theoretical path lengths could be exceeded if cloning objects to locally attached volumes**.
4. Click the button **Check selected folder**.

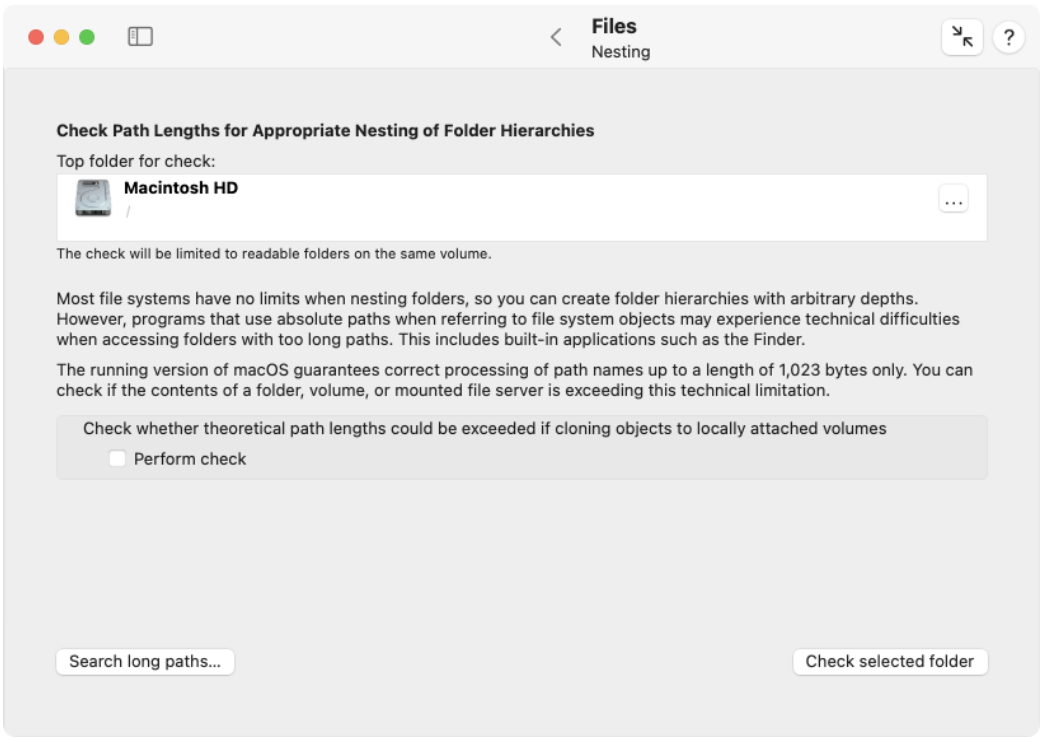


Figure 3.10: Find absolute paths that may be too long for many applications

The scan will begin. It can be canceled any time by clicking the **Stop** button in the status sheet. After all tests have been completed, the results will be shown in a different panel. If all objects are expected to be accessible, a green check mark symbol is shown. If one or more problems have been detected, the result panel will show

- a list of all files and folders which may not be accessible by all applications, (or cannot be copied to a currently attached local volume, respectively),
- the number of bytes used to store the path of each possibly inaccessible object,
- a reveal button for each object to navigate to the problematic folder in the Finder,
- a separate table that lists all folders that could not be tested due to permission problems.

When using a reveal button, the Finder may *not* open the indicated file system item, because it is affected by the path problem itself, so it cannot correctly process the location of that item. Instead, TinkerTool System will instruct the Finder to open the "deepest" folder in the hierarchy that can still be safely displayed.

Although the shown folder can still be handled by the Finder, some or all of the folder's contents may be invisible in the related Finder window, because the Finder is no longer capable of processing the items' names at that deep level of the hierarchy. If you delete the supposedly empty folder, you may lose data!

You should rename the folder at this or a higher level, giving it a shorter name to resolve the problem. You could also move the affected folder to a higher position in the hierarchy instead. It would not be appropriate to do this automatically, so TinkerTool System won't assist you further in this matter. The reorganization of folders should be done by the owner of the files who created the nested hierarchy.

Arbitrary Limits for Other Systems

In some cases, the question how long a file system path can be in order to be processed correctly may not affect the local system, but the collaboration with other systems. For example, you may have set up a folder which should be automatically synchronized with a remote folder via network, but that network server uses different limits for acceptable path lengths.

In addition to the detailed local checks, TinkerTool System also offers a simple quick check that tests a selected folder hierarchy against a path limit you can specify yourself. Perform the following steps to do this:

1. Open the sub-item **Nesting** on the pane **Files**.

2. Drag the folder where the test should start from the Finder into the field **Top folder for check**. You can also click the button [...] to navigate to the folder, or click on the white area to enter the UNIX path of the folder.
3. Click the button **Search long paths**....
4. Specify whether you like to validate **absolute** paths (as they currently are on the volume of the local computer), or **relative** paths (as seen from the selected top folder) and specify the limit in bytes. Click **OK**.

TinkerTool System now checks the folder and all its subfolders on the same volume where you have read permission, and collects all file system objects in a list that indicates where the specified path length is exceeded. The results are displayed at the end of the search procedure, listing paths and their respective lengths. After selecting a line, the corresponding path will be shown with its complete length, and you can also open it in the Finder, as far as technically possible.

The minimum limit you can specify is 200 bytes, the maximum is the local limit of the running operating system.

3.1.10 Extended Attributes

Many of the additions to files already mentioned in this chapter, like HFS attributes or quarantine markers, constitute records of additional information, attached to a file or folder. Several other elements can be attached in such a manner as well, like Finder tags, Spotlight comments, backup markers of Time Machine and many other things. All modern versions of macOS collect such additional records as so-called *Extended Attributes*. Each Extended Attribute has a certain name, defined freely by the application which created and uses this attribute. Connected with each name is a certain sequence of bytes, representing the *value* or *contents* of the attribute. What exactly is stored as contents is at the discretion of the respective program. The number of Extended Attributes which can be attached to a file system object is theoretically unlimited.

Older versions of macOS or the classic Mac OS have used a similar concept known as *named forks* of a file. In particular, the so-called *resource fork* played the most important role. The advantage of using Extended Attributes or forks is that additional information can be stored *together* with the actual contents of a file (usually called *data fork*), using a single icon and single name for administration and transport. A disadvantage is that not all file systems (e.g. the FAT format of MS-DOS) are capable of storing such attributes. If a file, which has many attributes attached, is copied onto a disk not prepared for such operations, the additional streams of data can simply be lost. It also becomes more difficult to specify the true amount of storage space needed for a file, compared to the simple case.

> Modern versions of macOS handle a resource fork internally as Extended Attribute with the name **com.apple.ResourceFork**.

There can be many different reasons to remove Extended Attributes from files. Here two typical examples:

- You have received a large amount of image files originally created with the classic Mac OS. The files contain resource forks which contain file icons, each representing a preview thumbnail image for the corresponding picture. These resources unnecessarily need a lot of storage space. Today's computers with multi-core processors are so fast that they can compute the previews for the Finder directly from the image contents, on the fly and in parallel while listing the files. Preview thumbnails computed in advance are no longer needed. In this case you could remove all Extended Attributes named **com.apple.ResourceFork** from the whole folder of pictures.
- In some case of emergency you have restored files from a Time Machine backup, by copying files directly on the command-line from the Time Machine disk to the system disk, without using the Finder or the Time Machine user interface. In this case, the internal processing markers, used by Time Machine to control which versions of files are available for which points in time, may have mistakenly got on the system disk as well. In order to avoid conflicts with future backups, you like to remove these marker attributes from the restored files, by deleting all Extended Attributes prefixed with **com.apple.TimeMachine**.

You can specify a single file or a whole folder of files in TinkerTool System to let the program display all Extended Attributes associated with the objects. Afterwards, you can choose to remove one or all attributes with a certain name from the set of file system objects. Please note that read permission is needed for the affected folder and Extended Attributes. For the delete operation, write permission is needed, respectively.

Perform the following steps to display Extended Attributes, or to delete them, respectively:

1. Open the sub-item **Extended Attributes** on the pane **Files**.
2. Drag a file or folder from the Finder into the field **File or top folder from which to remove Extended Attributes**. You can also click the button [...] to navigate to the object, or click on the white area to enter the UNIX path of the object.
3. Click the button **Remove...** to review the Extended Attributes of the selected objects.

Before any attribute is actually going to be deleted, TinkerTool System uses a dialog sheet where all found attributes and the file system objects they belong to will be listed:

- The upper part of the window is listing the names of all found attributes and the number of objects (files or folders) that have this attribute attached. By removing or setting a check mark in the column **Remove?**, you can define whether this attribute should be removed or not.
- After selecting an attribute in the upper half of the window, the lower half will be listing all paths of the objects containing such an attribute. If you like to restrict the operation to single files, you'll have to drag each object one by one into the field **File or top folder from which to remove Extended Attributes**.

The removal operation will start after clicking the button **Delete** in the sheet. No object will be touched if you click the **Cancel** button instead.

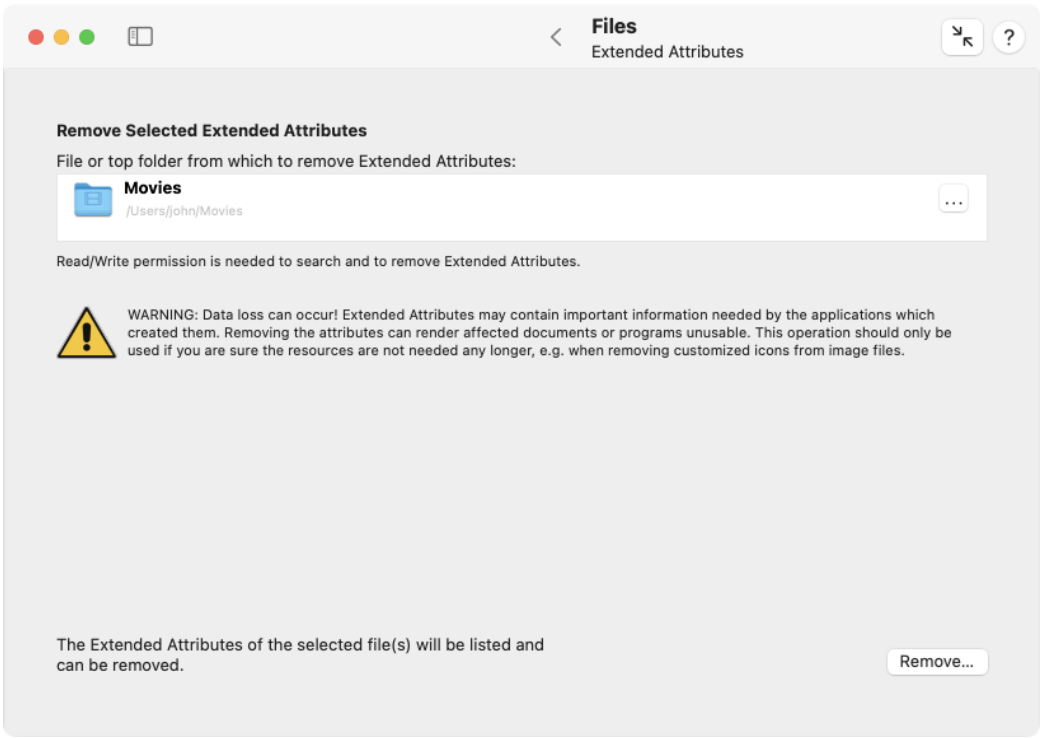


Figure 3.11: Remove Extended Attributes

You should only use this feature if you know exactly what you are doing, in particular, which attributes are needed for what purpose. Specific documents may no longer open after their attributes have been removed.

3.2 The Pane Clean Up

3.2.1 General Policy when Deleting Files

The pane **Clean Up** is designed to remove files from your computer which might not be needed any longer. Note that TinkerTool System cannot release you from your decision whether certain files are indeed not needed or should be kept. To avoid that the program cleans your system from files without your explicit permission to do so, it is recommended to always keep the option **Display analysis before deleting anything**, which you'll find at the bottom line of each sub-item, in the "on" position. The option will be active by default if you have set the preference **Always create report before performing any delete operations** in the settings panel of the application (section 1.3 on page 8).

With this feature switched on, TinkerTool System always displays a confirmation panel which will list all files and folders that are about to be removed before the actual delete operation will take place. You will have a final chance to review the list of files. By deselecting specific files from the list, you can also take them away from the delete operation individually. Each entry also has a "reveal in Finder" button marked with a magnifying glass that can be clicked to open the affected folder, showing the respective object, in a Finder window.

3.2.2 Hidden Support Files

macOS uses several types of hidden support files to fulfill specific tasks. If you are transferring disks to users of operating systems where these hidden files could become visible, e.g. when uploading files to a shared server, or when working with external drives for transport, these files might cause confusion or may be considered to be disturbing. Some hidden files contain important data while others might not be of use when working with foreign systems. TinkerTool System supports the removal of two specific types of hidden files:

- **Desktop Services Store files:** These files always have the name **.DS_Store**. The Finder is creating a .DS_Store file in every folder a user has ever opened with the Finder, under the condition that the user had write permission for each folder in question. A .DS_Store file contains all view settings the Finder was using the last time a user opened the folder containing that file. View settings include the size of the Finder's display window, the view mode (icon, list, columns, gallery), the position of the

icons, the sorting settings, background images, and much more. The Finder's view settings are either set indirectly, by just opening a new default window which has certain current view settings, or explicitly by using the menu item **View** > **Show View Options** of the Finder. When a .DS_Store file is removed, its folder will fall back to using default view settings. A new .DS_Store file will be created automatically the next time the folder is opened via the Finder again.

- **AppleDouble files:** These files are also called "dot underscore files" because they always have file names that begin with "._". The macOS kernel creates these files automatically when it is necessary to store certain Macintosh-specific attributes on file systems which cannot support such attributes natively. Examples for these additional attributes are the type codes, the visibility markers, quarantine info, or the resource forks already mentioned in the chapter The Pane Files (section 3 on page 145). Such files will only be created if it is necessary to emulate these attributes on a foreign file system, for example when storing a classic Mac application onto an MS-DOS disk. For this reason you will rarely find such files on HFS+ disks. They can exist on such disks nevertheless, for example after document files with emulated attributes have been copied back to an HFS+ disk using an operating system different from macOS. The connection between the main file and its associated AppleDouble file is maintained by using file names that follow a simple pattern: When creating an AppleDouble file to store the Mac-specifics of the file "example," macOS will use "._example" as its name.

> TinkerTool System cannot prevent in advance that these files are created. (This would cause the Finder no longer to remember view settings, and would cause data loss in case of AppleDouble files.) The Finder contains an advanced preference setting however, which can be used to suppress the creation of new .DS_Store files when the Finder is opening folders located on network file servers. This setting is accessible via the sister application TinkerTool.

TinkerTool System can remove these two types of hidden files, cleaning a whole hierarchy of folders if desired. The user initiating the removal must have read permission for the files and folders affected. To delete hidden files, perform the following steps:

1. Open the sub-item **Hidden Support Files** on the pane **Clean Up**.
2. Drag the top folder that should be processed from the Finder to the field **Top folder**. You can also click the button [...] to navigate to the object, or click on the white area to enter the UNIX path of the object.
3. If you like to remove all Desktop Services Store files from that folder and all its subfolders, check the option **Remove per-folder view settings used by the Finder**.
4. If you like to remove all AppleDouble files associated with existing files from that folder and all its subfolders, check the option **Remove AppleDouble files**. If you like to include files which just look like AppleDouble files, no matter if their associated files exist or not, set an additional check mark at **Also include orphaned AppleDouble files**.

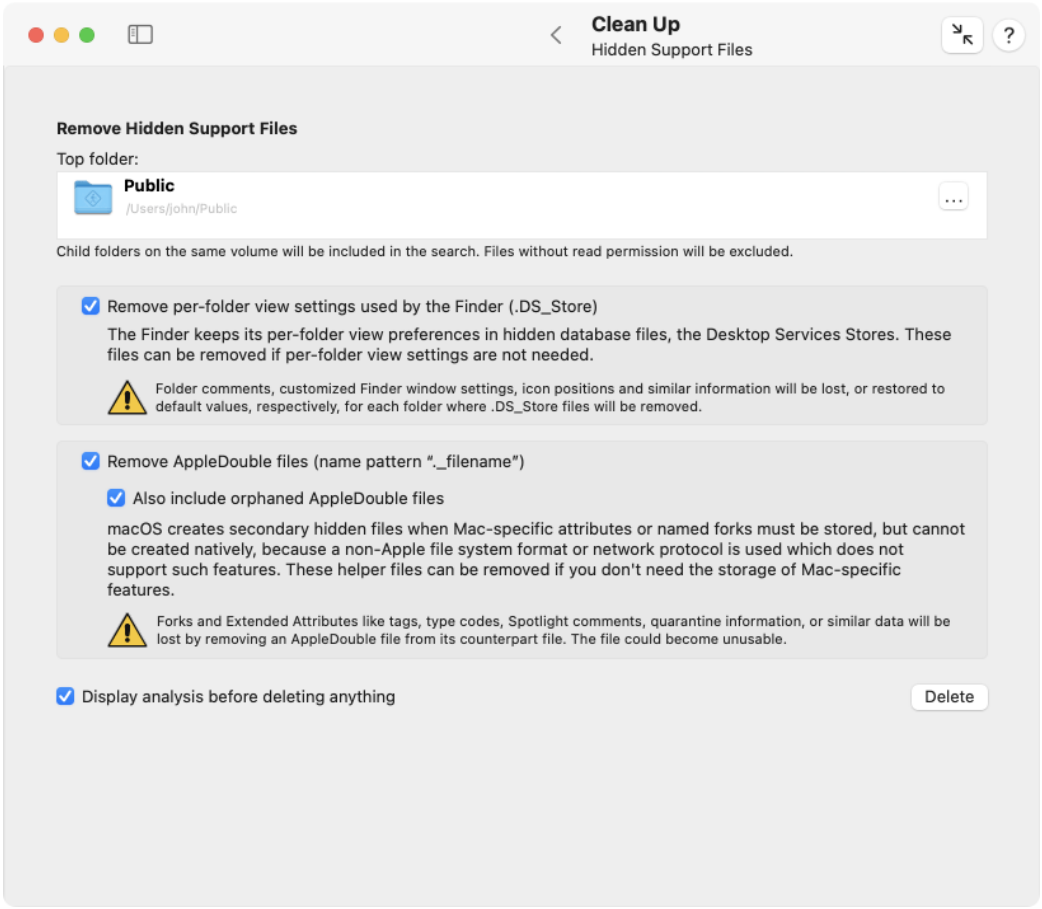


Figure 3.12: Hidden support files

5. Click the button **Delete**.


Only remove hidden files when you know for sure that their contents is really not important. Otherwise serious data loss could occur.

3.2.3 Log Archives

As outlined in the chapter The Pane Info (section 2.10 on page 121), macOS keeps a high number of log files which collect messages about events and error conditions that occurred during the operation of the computer. When log files have reached a certain age or size (depending on information category), macOS will automatically remove them, starting anew with clean files. Several log files are considered to be important, however, so the old copies are not simply deleted but are compressed and put to an archive area. Depending on importance of the log category in question, macOS will hold several generations of those archived copies until they will be finally deleted.

If your computer is very low on storage space, you may like to remove all archived log files immediately. The currently used generation of log files won't be touched during this operation. To delete archived log files, perform the following steps:

1. Open the sub-item **Log Archives** on the pane **Clean Up**.

2. Click the button **Delete**.

3.2.4 Crash Reports

Whenever an application crashes, macOS automatically creates a so-called *crash report* which can help software developers to determine the exact technical reason why the application had to be terminated immediately. Application crashes are usually caused by programming errors either in the application itself or in the operating system. When you report a crash incident to the application's publisher, the responsible software engineer will usually request the crash report to be submitted for analysis.

In case you no longer need specific crash reports for communication with the software vendor, you can delete them to reclaim storage space. TinkerTool System can automatically find crash reports that either apply to programs affecting the whole computer (usually system services), or that apply to applications which have been run in the current user account. (Crash reports owned by other users won't be displayed.) The list of crash reports may also include crashes which occurred on mobile Apple devices that could not send the report directly to Apple, e.g. an iPod touch.

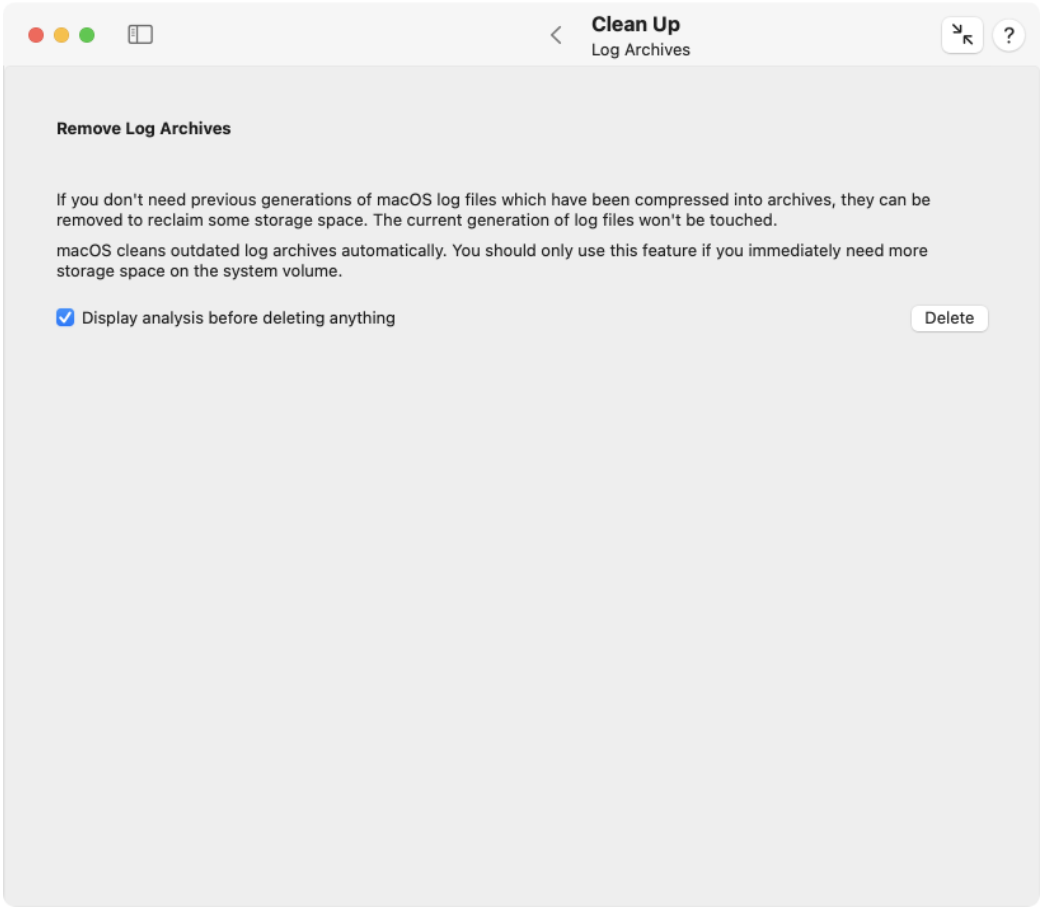


Figure 3.13: Log archives

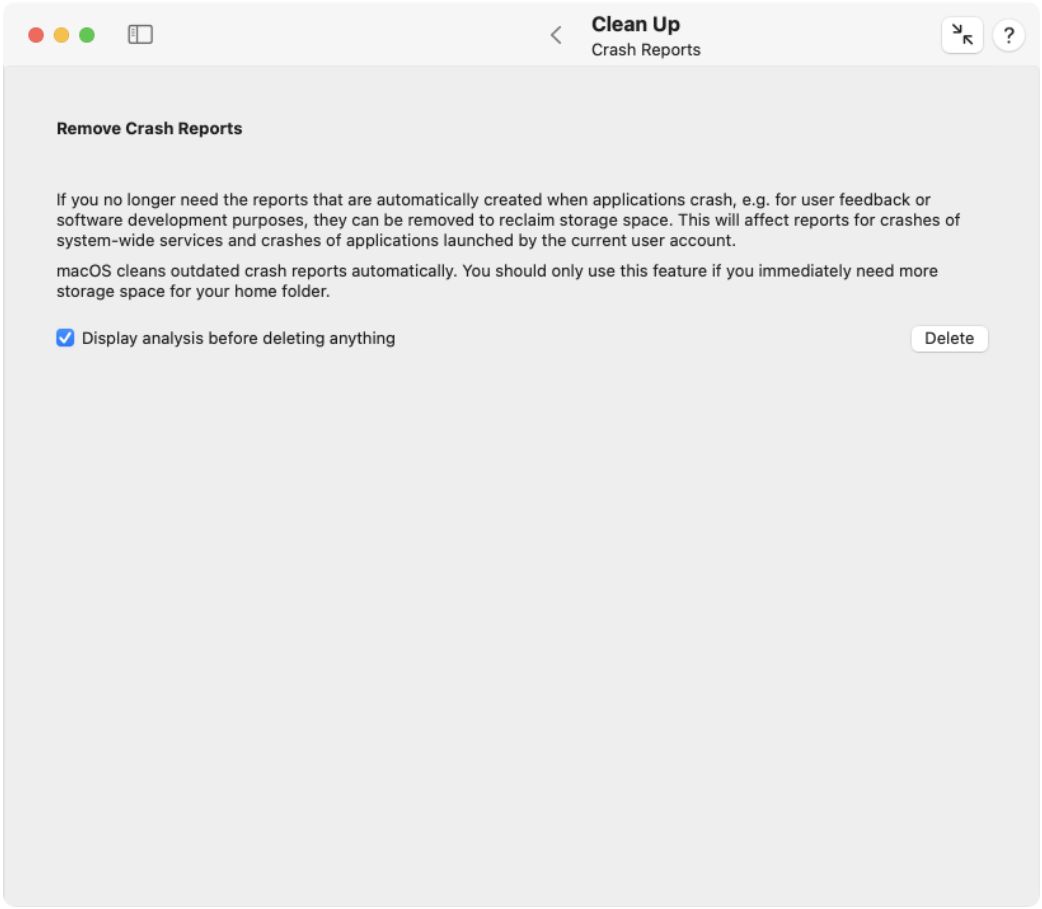


Figure 3.14: Crash reports

macOS automatically removes excessive and outdated crash reports, that is, repeating reports on the same type of incident which don't add any new information, and reports which have become so old that they no longer seem to be useful. Automatic removal of expired crash reports usually takes place after 30 days.

To delete unneeded crash reports manually, perform the following steps:

1. Open the sub-item **Crash Reports** on the pane **Clean Up**.

2. Click the button **Delete** and wait until the program has collected all reports.

3. If the setting **Display analysis before deleting anything** is on, a list of the available crash reports will appear. The table contains the following information: the name of the device on which the crash occurred, a marker if this was a mobile device, the process name of the crashed program, the exact time when the crash was recorded, and the file size of the report. By selecting or deselecting check marks in the column **Remove?** you can choose which reports to delete and which to keep.

4. Click the button **Delete** in the dialog sheet to remove the selected reports or click **Cancel** to perform no operation.

3.2.5 Orphaned Files

In environments where a computer is used by many people, it will happen from time to time that user accounts are deleted after they have been in use for a certain time. For a company computer for example, this will be the case when an employee is leaving, for a school computer after a student has completed her final exams. Typically, the application **System Settings** is used to delete the account, and the program offers to delete the affected user's home folder at the same time. This usually means that all files the user had created will be properly removed from the computer as well.

Problems can occur if users were granted permission to create files *outside* their home folder or to store applications there. In this case, *orphaned* files, folders and applications may remain stored on the computer, even after the user account and the user's home folder have been deleted. TinkerTool System can help you to find such objects and to delete them when desired. Alternatively, the objects can also be assigned to a new owner. This operation must be repeated for each single volume and is restricted to volumes capable of storing ownership information. A file system object is considered to be orphaned if it has an owner entry which can no longer be matched with available user accounts. The info panel of the Finder only shows the text **Loading**… as owner of such an object in this case. The pane **ACL Permissions** (section 3.4 on page 198) of TinkerTool System only lists **ID x** (i.e. no readable name) at the permissions table in the POSIX owner line where **x** is a numeric value.

Warning: If the computer is part of a managed network, user accounts are typically not only stored on the computer itself, but also on one or more other computers in the network. These network-wide accounts are records in *directory services*. Before you work with this feature, you should ensure that the computer is currently connected to all directory services relevant for your network and the directories are working correctly. Otherwise, there won't be a reliable way to determine which user accounts are available and which are not. Files owned by network users could so mistakenly considered to be orphaned.

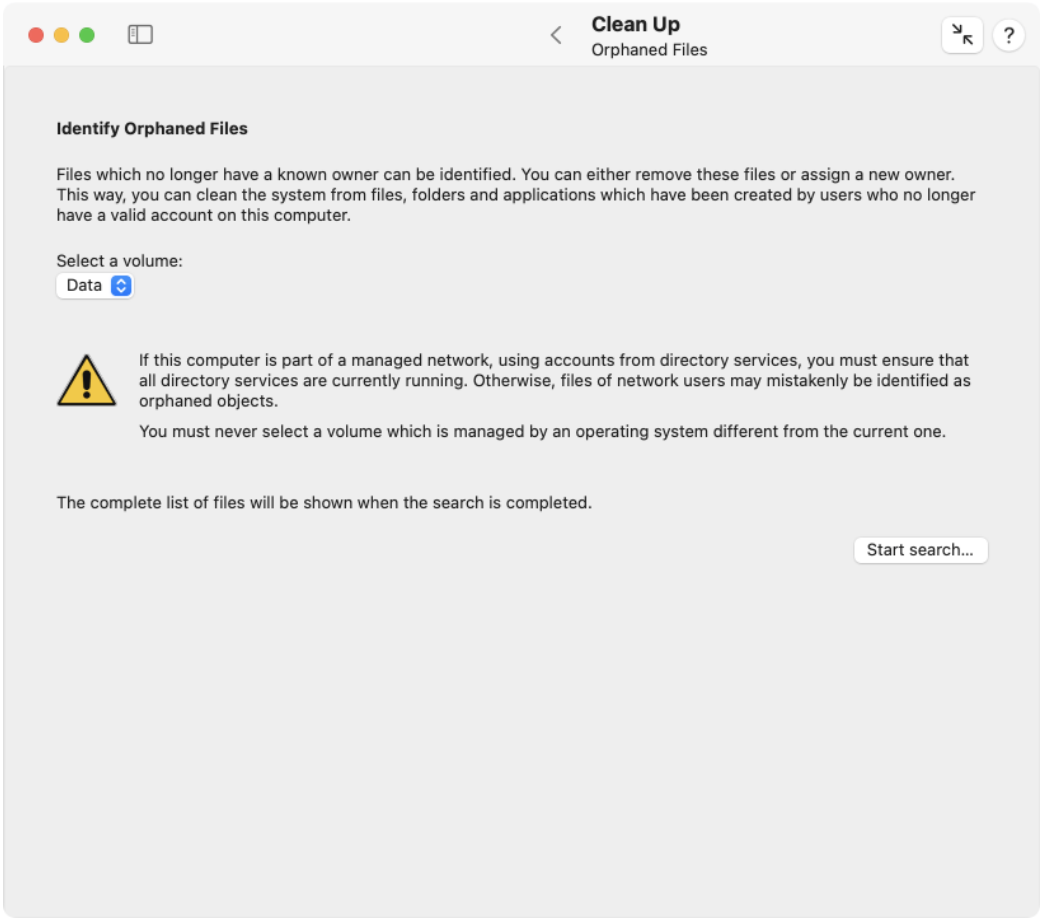


Figure 3.15: Orphaned files


Warning: You must not this feature on a volume which is managed by an operating system different from your current system. The other system might use a different user account database, so the information which users are still present and which ones have left could be very different.

To identify orphaned files, perform the following steps:

1. Open the sub-item **Orphaned Files** on the pane **Clean Up**.
2. Click the button **Start search**... and answer the questions of the application.
3. When a search for orphaned files is necessary, wait until the program has collected all matching files.
4. The list of all affected files and folders is shown. By making a corresponding selection in the column **Operation**, you can determine how each object is to be dealt with. You can also select multiple or all rows in the table by using the drop-down menu below the table, choosing the same operation for the selected items, then clicking **Set** to avoid single treatment.
5. Press the **Perform selected actions** button in the dialog sheet to initiate the appropriate handling of orphaned objects.

In detail, the different operations mean:

- **Ignore:** the object is left as it is
- **Delete:** the object is removed from the volume and will be lost
- **Reassign:** the object is “given away” to a new owner

You can only assign one new owner at a time. If you want to assign objects of a single volume to different users, you must first **ignore** the corresponding entries and then assign them to the next desired user in repeated runs.

Some orphaned objects may be marked with the note **wrong ownership setting likely**. In this case, the owner of the object is indeed unknown (so the file is orphaned), however there are some indications that this is just a wrong ownership setting, not an object which has been left by a deleted user account. Some software vendors (including Apple) sometimes deliver applications or other components with erroneous permission settings which can lead to such an effect. In this case you

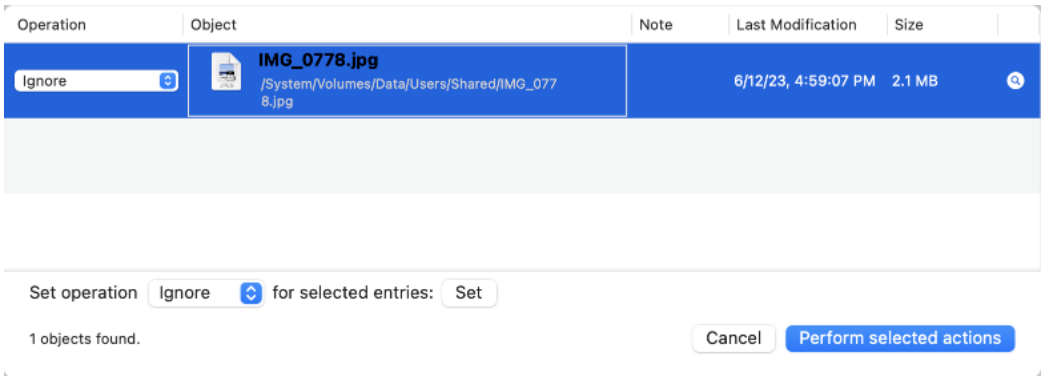


Figure 3.16: For each individual orphaned object, you can decide what to do.

should *not* delete the affected files but contact the vendors which distributed them, making them aware of the packaging errors.

Orphaned folders will only be offered for deletion if all of their contents is orphaned as well. In this case, the objects contained in such a folder won't be listed individually and TinkerTool System won't sum up the storage size of such objects. So the folder can be listed with a small size although it might enclose large file hierarchies.

3.2.6 Aliases

Aliases are a feature taken over from the classic Mac OS to macOS (see also the pane Files (section 3 on page 145)). They are file system objects which refer to other file system objects, making the original object accessible under a different name or in a different folder. When the original objects are moved or renamed, applications can still try to find the original object if they like to, tracking the objects by an educated guess, similar to a smart find operation. However, when the original objects have been deleted, aliases referring to them become outdated and will break. You can use TinkerTool System to find and remove such outdated aliases.

The operation to find the object to which an alias is referring to is known as *resolving* the alias. It is important to know that the current environment when an alias is being resolved plays a role in deciding whether the alias is outdated or not. An alias may refer to an object on a file system currently not mounted, e.g. a shared folder on a file server, an external disk drive, a CD-ROM, a pen drive, etc. It could also have been created by another user, referring to an object for which the current user has no access permission. In both cases, the original object does not appear to exist from the current user's point of view. However, the alias could still be valid for the other user, or after reconnecting the correct file system.

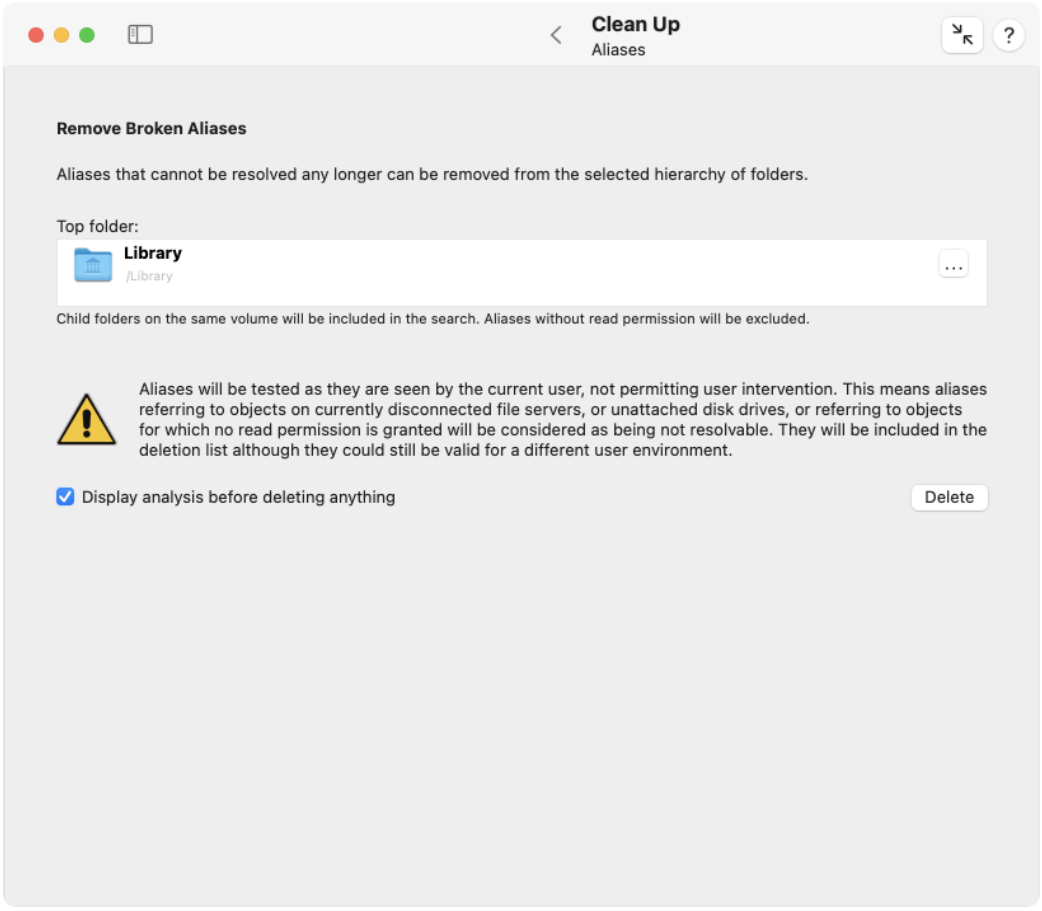


Figure 3.17: Aliases

> To decide whether an alias can be resolved, TinkerTool System uses the current user's access permissions and does not trigger any reconnect operations.

To delete unresolvable aliases from a hierarchy of folders, perform the following steps:

1. Open the sub-item **Aliases** on the pane **Clean Up**.
2. Drag the top folder that should be processed from the Finder to the field **Top folder**.
3. You can also click the button [...] to navigate to the object, or click on the white area to enter the UNIX path of the object. Click the button **Delete** and wait until the program has found all broken aliases.
4. If the setting **Display analysis before deleting anything** is on, a list of the available aliases will appear. By selecting or deselecting check marks in the column **Remove?** you can choose which aliases to delete and which to keep.
5. Click the button **Delete** in the dialog sheet to remove the selected aliases or click **Cancel** to perform no operation.

3.2.7 Removable Disks

The hidden files mentioned at the beginning of this chapter are not the only invisible components usually found on Macintosh disks. A disk typically contains additional hidden folders to store the Trash, the Spotlight index, and some other files needed to maintain full compatibility with the old Finder of the classic Mac OS. When you pass such a disk to users of a non-Mac operating system, e.g. Linux or Microsoft® Windows, and these users have configured their graphical file browsers to display hidden files, they may be confused. For some devices with embedded operating systems, like TV sets or car radios, the hidden files may even cause technical problems, for example when you like to play MP3 audio files copied by macOS onto a pen drive.

TinkerTool System can remove the complete set of Macintosh support files from an entire disk and then eject this disk to avoid that macOS will recreate the files. You can execute this procedure as the last step before passing the volume to users of a foreign operating system or to a non-Apple device. Perform the following steps:

1. Open the sub-item **Removable Disks** on the pane **Clean Up**.
2. Select the disk with the pop-up button **Removable disk volume**.
3. Click the button **Delete**.

> The list of removable disk volumes contains all disks for which you can perform an eject operation in the current situation. This can include internal disks which are not directly removable in the physical sense.

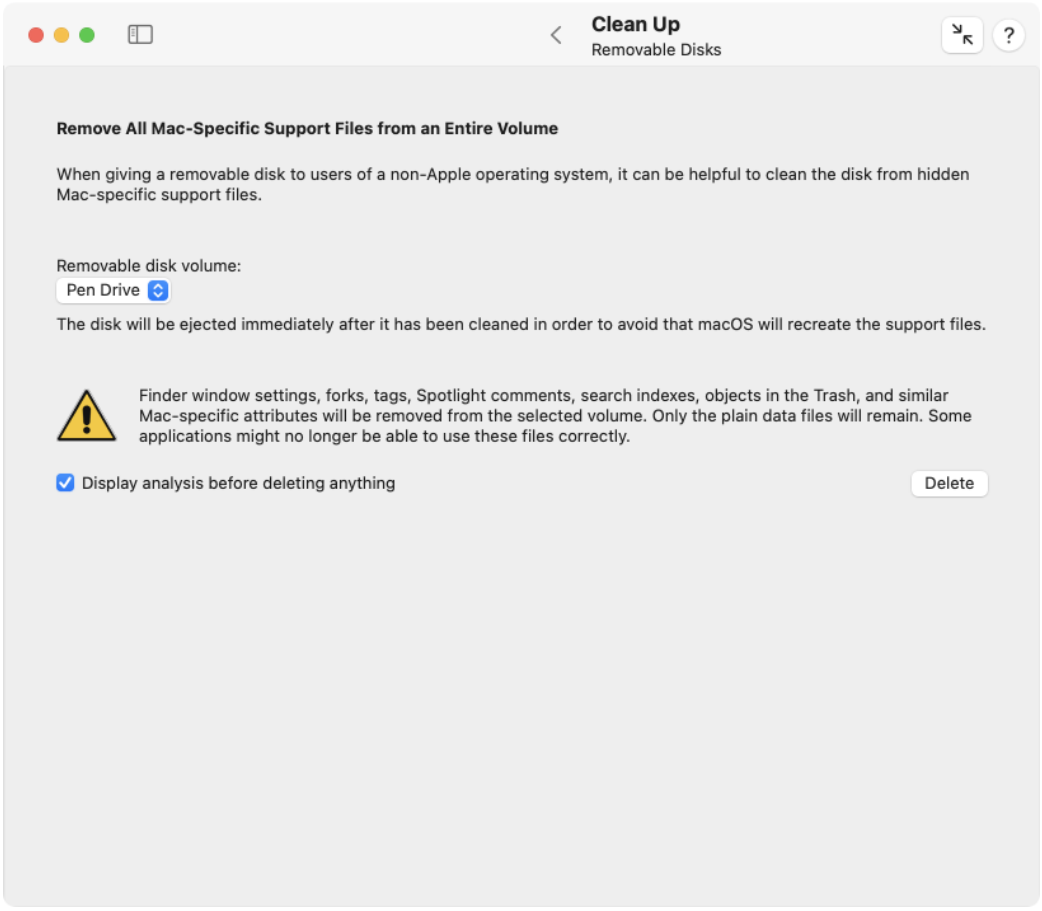


Figure 3.18: Removable disks

Remember that Macintosh-specific features will be removed from the files on the affected disk. Some files could become unusable from the point of view of the Mac. You should only use this feature on "transfer disks" passed to other non-Mac systems. The disk should only contain copies of original files you have still on your main disk or file server.

3.2.8 Slow-Motion Screen Savers

As of macOS 14 Sonoma, Apple introduced a new type of screen savers in macOS taken over from the Apple TV. They show slow-motion sceneries and can be combined with matching wallpapers. The resource files for these screen savers can use a large amount of storage space, typically between 500 MBytes and 1 GByte for each of them on the system volume group. With exception of a single specific default screen saver, which is a fixed component of the operating system, all other slow-motion screen savers are optional. They will only be downloaded and stored when the user expressly chooses them in the **Screen Saver** section of **System Settings**. In addition, these screen savers will automatically be deleted by macOS when the system is running low on storage space.

There can be situations where you like to remove a specific screen saver immediately, without waiting on macOS. TinkerTool System shows you how much storage is needed by the individual screen savers and allows you to delete them if you choose to do so.

1. Open the sub-item **Screen Savers** on the pane **Clean Up**.
2. Select one or more installed screen savers in the table by checking the respective entry in the **Remove?** column.
3. Click the button **Remove**.

- The built-in slow-motion screen saver which belongs to the operating system cannot be removed.
- The screen savers are presented in the default sort order defined by Apple. This order should match the corresponding items in System Settings.
- To navigate to the next or previous installed screen saver in the table, click the arrow buttons in the bottom left corner.
- TinkerTool System indicates the sum of all removable screen savers and the potential gain of storage when the selected savers would be removed.
- If screen savers have been added in System Settings while TinkerTool System is running, you can update the overview via the refresh button at the right below the table.

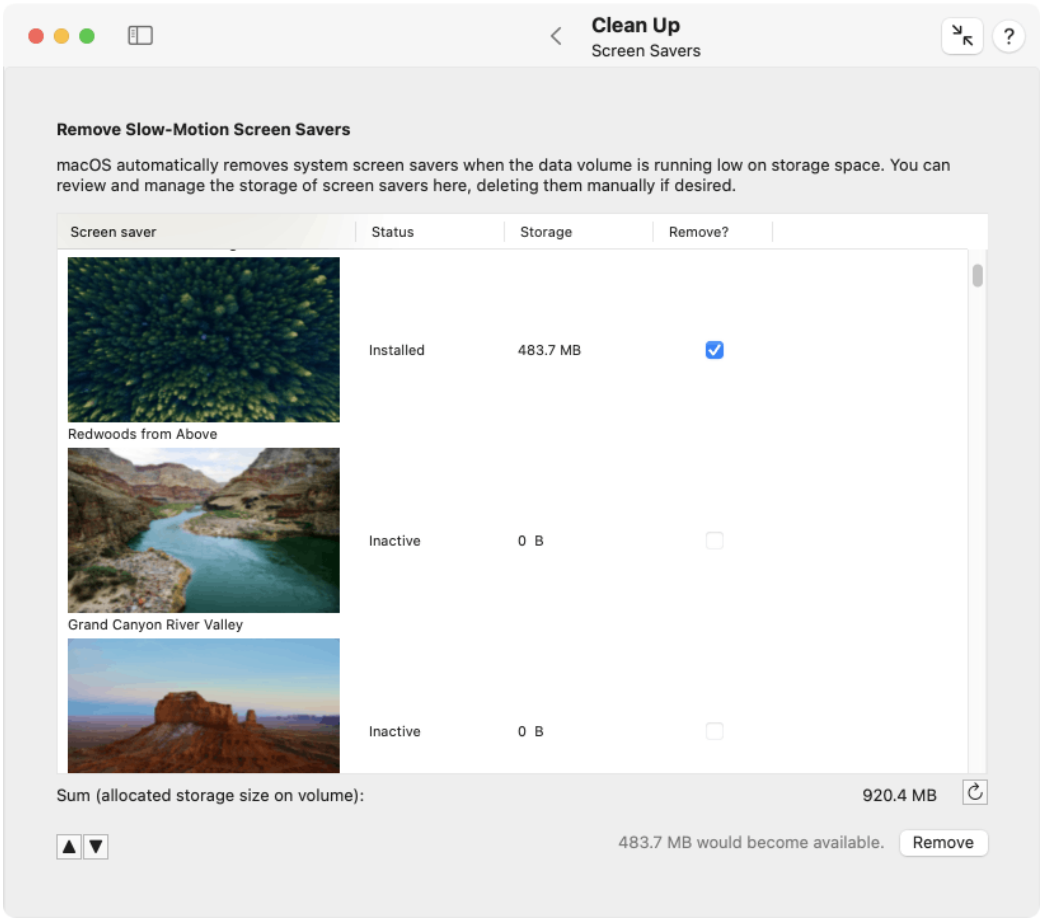


Figure 3.19: Slow-motion screen savers need a lot of storage space and can be removed if installed

It is not possible to check which of the screen savers are currently active for each of the user accounts on your Mac. TinkerTool System will delete the selected ones, regardless of whether they are currently preferred by some users.

Screen savers are stored on the system volume group, so their storage corresponds to the typical behavior of APFS files: The space of the deleted resource files becomes *available*, but not necessarily *free*. If you need free space, you may need to release the corresponding APFS snapshot additionally. Please see the chapters The Pane Operational Safety (section 3.6 on page 227) and The Pane APFS (section 3.7 on page 232) for more information.

3.2.9 Core Dumps

When using advanced software testing features of macOS, the operating system can be configured to produce so-called *post-mortem core dumps*. After a tested program – or in these special test situations usually the macOS kernel – has crashed, macOS will write the entire contents of the computer's main memory to a core dump file on the operating system disk. The core dump is basically a snapshot of the memory situation of the computer when the crash occurred, and can be analyzed further at a later time after the system has been restarted. Core dump files are typically as large as the available memory size, so they may consume a lot of space on the system disk. TinkerTool System can remove all available core dumps automatically if you don't need them. Perform the following steps:

1. Open the sub-item **Core Dumps** on the pane **Clean Up**.
2. Click the button **Delete**.

3.3 The Pane Applications

3.3.1 Uninstallation Assistant

Applications that strictly comply with Apple's software design guidelines for macOS and don't need to be deeply integrated into the operating system, are usually installed by a simple "drag and drop" operation. This means no actual installation is necessary, you just drag the application icon into one of your application folders and can launch it immediately.

However, macOS automatically creates additional files when you work with a new application, for example files to store the personal settings for each user, or cache folders for download files, when applications are accessing the Internet to search for automatic updates, etc. You can simply "uninstall" a drag-and-drop application by dragging its icon to the Trash. This won't remove all the aforementioned other support files, however. This is where the uninstallation assistant of TinkerTool System can help.

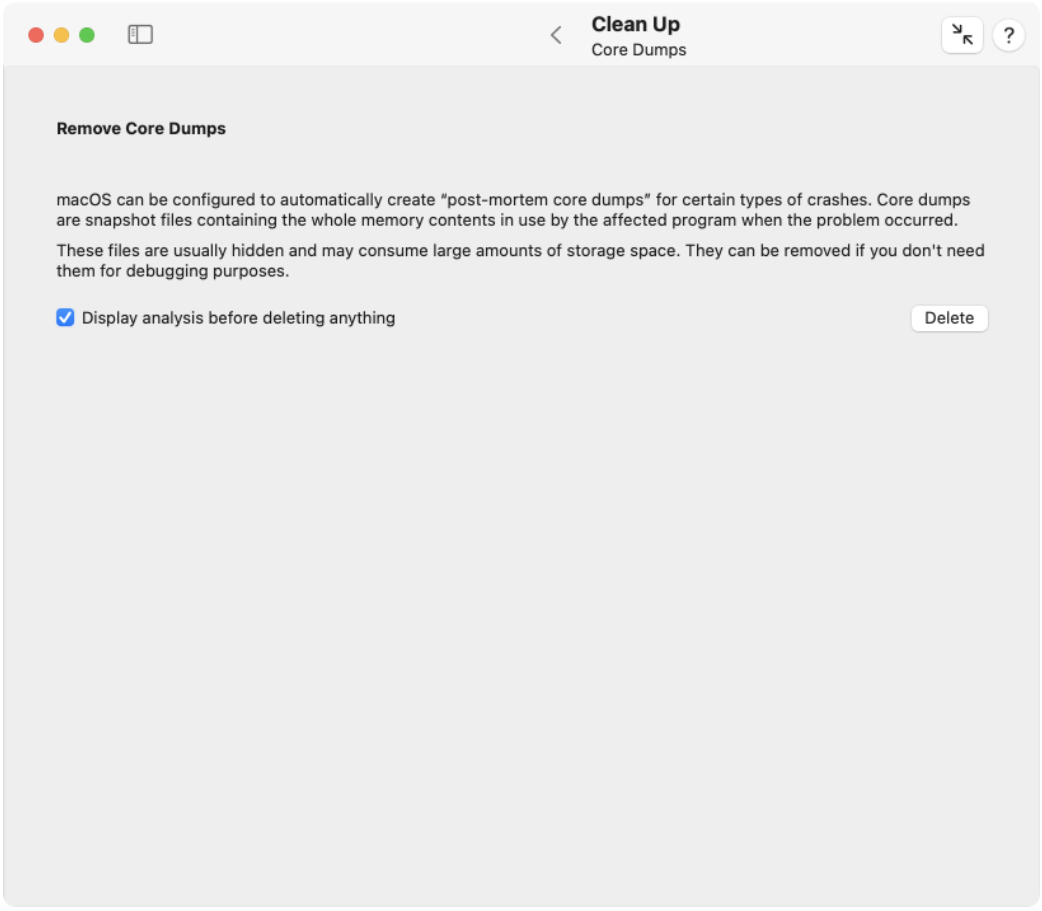


Figure 3.20: Core dumps

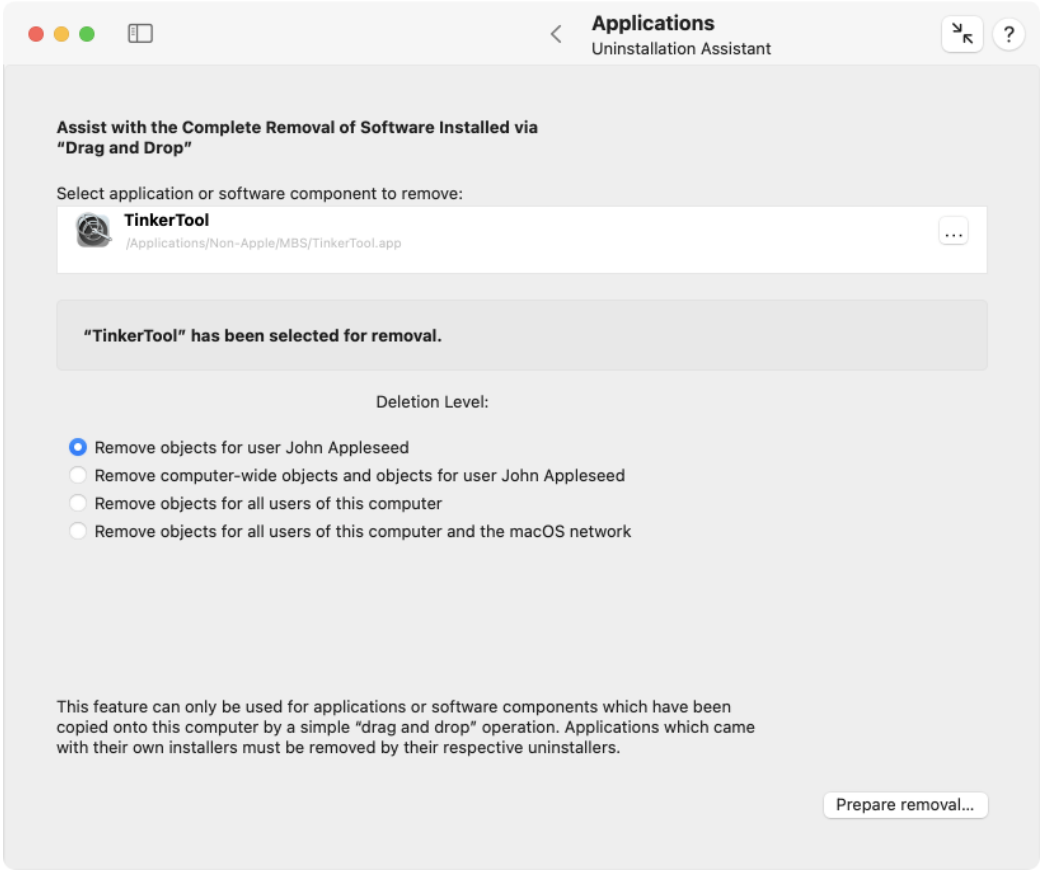


Figure 3.21: Uninstallation assistant

3.3.2 Removing software components and associated files

The job of the uninstallation assistant is to help you to identify all associated components that might have been created by the software component you want to remove. You can let TinkerTool System automatically remove the other files and folders as well, cleaning the entire computer. There are in fact four different levels of clean-up you can choose from:

1. You can restrict the search to components which have been created for your user account only.
2. You can search for components that have been installed for "computer-wide" usage by all users of the local computer and the personal items of your user account.
3. You can search for components which have been installed as personal items for all user accounts known to the local computer, including components which have been installed for computer-wide usage.
4. You can additionally include items which have been installed for "network-wide" usage. This is useful if you are using a central software distribution server and the management features of macOS which store information in the **/Network/Applications** and **/Network/Library** folders.

If you are using the search levels (3) or (4), TinkerTool System will allow you to delete files and folders which are owned by other users. This is a dangerous option which should be used by experienced system administrators only. Please verify each object carefully before you are actually going to delete it.

There are applications which completely hide where and how they store the data or documents you create when using that application ("shoebox apps"). Other applications may give you a choice to define individual file names for documents, but also use their own private area to store the files. Please keep in mind that the user documents created by such applications might be removed as well when you perform an uninstallation.

Before any object is removed, TinkerTool System will list each affected item. You can then decide for each single object whether you actually want to remove it. Perform the following steps:

1. Open the sub-item **Uninstallation Assistant** on the pane **Applications**.
2. Drag the icon of the program you like to remove from the Finder into the field **Select application or software component to remove**. You can also click the button [...] to navigate to the object, or click on the white area to enter the UNIX path of the object.

3. If an application was selected, you have to choose between one of the four possible search levels discussed above, using the buttons at **Deletion Level**. This step is not necessary if you have selected a component which is not an application.

4. Click the button **Prepare removal**....

Note that nothing is going to be removed yet. TinkerTool System will always analyze your selection first and display the items which would be affected. The program will begin to search for these objects after you have clicked the **Prepare removal**... button. You can interrupt and cancel the search at any time by clicking the **Stop** button which will appear while the search is running. Note that a search run can take several minutes if your computer or your network hosts a high number of user accounts and you have selected one of the search levels affecting each user.

After the search has ended, all candidates for possible removal will be listed in a table. The table contains the following columns:

- **Remove:** Set or deactivate the check mark to include or exclude the affected object from removal.
- **Object:** Icon, name and path of the object which is suggested for removal.
- **Type:** the role this object plays in respect to the software component you want to remove.
- **Owner:** the short name of the user who owns this object. Be very careful if you are going to delete personal items of other users.
- **Size:** the storage size of the object. This space will be freed when the object is going to be deleted.
- **Last change:** date and time when the object was modified last.
- **Show:** click the button in the **Show** column to display this object in the Finder.

The total number of selected objects and the total storage size is displayed right under the table. The two buttons in the lower left corner allow you to select

- if you want to put the items marked for removal into your Trash, or
- if you want to delete the marked items immediately.

> TinkerTool System does not allow you to bypass the security features of macOS. Although this feature allows you to delete objects owned by other users, you cannot use it to spy out the contents of private files. For this reason, it is *not* possible to display detail information of files which are neither owned by you or by the operating system, or to move items to the Trash for which you don't have access.

The selected objects will be removed when you click the **Remove** button. All objects remain untouched when clicking the **Cancel** button.

TinkerTool System automatically creates a detailed report on the components you are removing. It will be displayed after and while the removal takes place. After the operation has been completed, you can either save the report to a text file, or print it by clicking the respective buttons in the report sheet.

> The list of objects suggested for removal is computed according to Apple's software design guidelines for macOS. Please note that a few applications may not be fully compliant with these guidelines. **In this case, the list of removal candidates might not be complete.** This means there could be objects which have been created by the application in question, but have been omitted in the list. It could also occur (although this is very unlikely) that objects are included in the list but have actually not been created by the selected application, so they should not be deleted. Please verify each object carefully before using the removal function.
>
> If you are removing an application which is member of your list of login items, it will be removed from the list as well without reporting this in the table of deletion candidates. For technical reasons, this clean-up is limited to the current user, even if you had selected a search level including all users.

TinkerTool System contains several security features that prevent you from removing important parts of the system. You cannot remove components which are official part of macOS. You also cannot remove applications which are currently running on the local computer.

> 
>
> **You should never use this function for software components which have not been installed by a drag-and-drop operation.** Applications that came with their own installers or have been using the macOS Installer, usually had a technical reason to do so. In this case it is very likely that more than the usual components have been installed in the system, so they are not following the rules for self-contained applications. The Uninstallation Assistant cannot work as designed in that case. You should remove such applications following the instructions of their vendors.

3.3.3 Special Launch of Applications

You can use TinkerTool System to launch applications with non-standard options that are not the default when using Finder, Dock, or Launchpad. The following special settings are available:

- The system should not ensure that windows of the application are brought to the foreground and its main window gets the input focus. This means it does not be-

come the active program that listens to keyboard and mouse. Instead, TinkerTool System stays active.

- macOS should not add the program to the application section of the **Recent Items** menu.
- Even if the application is running already, a new copy should be started.
- The application should hide after launch, so it should not open with any visible windows.
- All other applications should hide. The launched application should become the only visible one.

> The last two options can be enabled at the same time. However, macOS will automatically try to resolve this conflict, making sure that at least one application stays visible. The detail behavior may depend on the operating system version you are using.

1. Open the sub-item **Special Launch** on the pane **Applications**.
2. Drag the icon of the program you like to launch from the Finder into the field **Application to launch**. You can also click the button [...] to navigate to the application, or click on the white area to enter the UNIX path of the object.
3. Set the options you would like to use.
4. Click the button **Launch**.

3.3.4 Privacy

In addition to user permissions, macOS supports other features to protect the privacy of users and to secure data. One of those mechanisms is based on privacy settings that prevent access to certain domains of a user's personal data in relation to applications. For example, access to the personal calendars of users can be configured in such a way that only the **Calendar** application of macOS has permission to process the calendar entries, but no other Apps, even if those Apps have been started by the user owning the calendar.

The decisions which applications should have access to which areas are stored by macOS in a privacy database. All entries can be reviewed in the table at **System Settings** > **Privacy & Security**. TinkerTool System offers a user interface to perform Apple's official procedure to reset these permission entries. The decisions that have been made in the past regarding access to personal domains can be undone, returning to factory defaults. This causes the affected Apps to lose their access permissions and to ask the user again for a decision, the next time access to personal data is attempted.

1. Open the sub-item **Privacy** on the pane **Applications**.

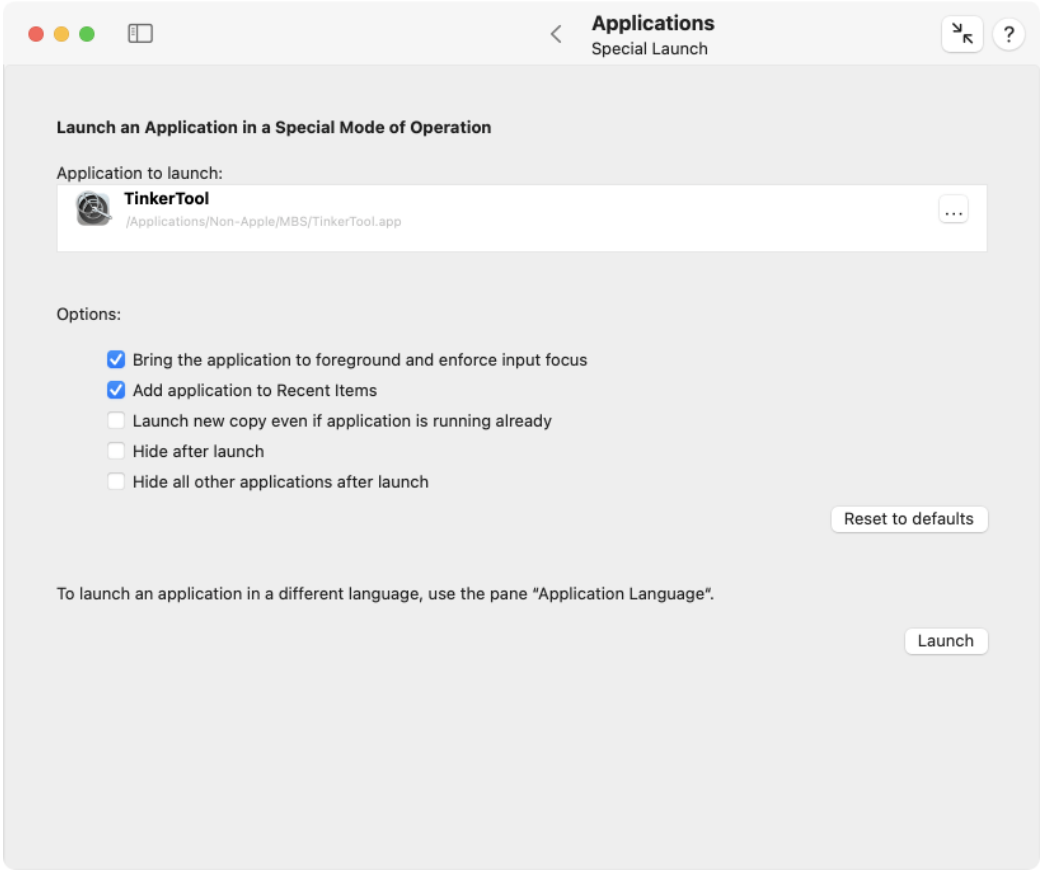


Figure 3.22: Applications can be launched with special options

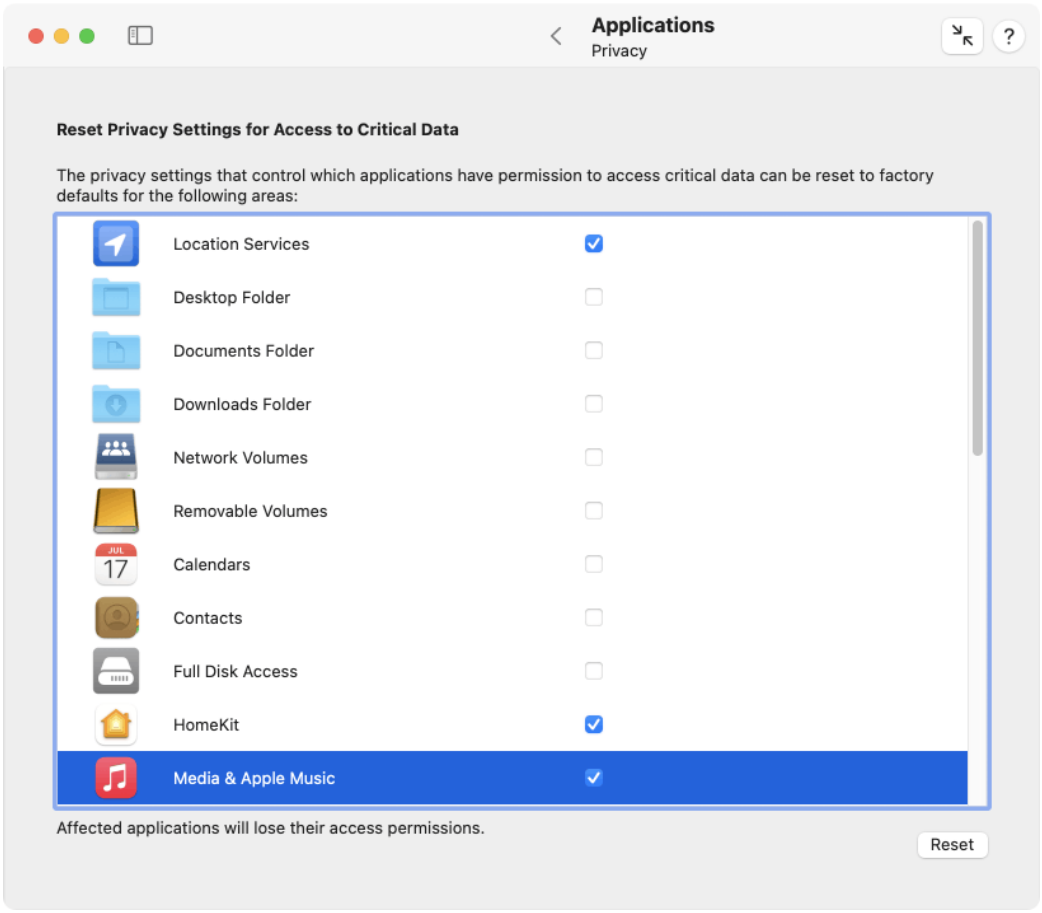


Figure 3.23: Reset application privacy settings

2. Set check marks for all access domains where the privacy settings should be reset.
3. Click the button **Reset**.

Note that these settings are system-wide and take effect for all user accounts.

> The number of items shown can be very different depending on your operating system version.

3.3.5 Security Check

To be protected against malicious software, macOS uses several different security techniques that complement each other:

- the *quarantine* feature that detects Internet downloads and tracks all files which are part of the download or have been indirectly created by the download,
- the *code-signing* technology which allows to recognize if a software component has been created by a known, trusted source, and which also detects possible subsequent modifications of files or memory pages by the use of digital seals,
- the *notarization by Apple* which certifies that the application had been submitted to Apple for review prior to its release to check for known viruses or similar malware,
- the *application sandbox* which ensures that a protected program cannot get access to specific system functions unless both Apple and the original software developer have explicitly granted such access. Each permitted type of access is called an *entitlement*. Programs protected in such a way come with an attached list of entitlements, digitally sealed in the application bundle. macOS launches such a program only after putting it into a sandbox first, enforcing compliance with Apple's restrictions of the sandbox and the specified entitlements. The entitlements are basically exceptions that give the application running in the sandbox a certain right it doesn't have by default.
- the *hardened runtime environment* which is basically an additional "light version" of the sandbox that applications can use to block themselves from using one or multiple of the following features of the operating system:
  - use of the just-in-time compiler for JavaScript code
  - generating code in memory at runtime
  - changing behavior of the dynamic code linker via environment variables
  - dynamically linking to code libraries of third parties
  - modifying code in memory at runtime
  - attaching to other applications in the role of a debugging tool
  - access to microphones or similar audio input

  - access to the built-in camera
  - access to Location Services
  - access to the user's Contacts database
  - access to the user's Calendar data
  - access to the user's Photos library
  - posting Apple events to other applications

- the *Gatekeeper* component, technically known as *security assessment policy subsystem* of macOS, which combines all functions and verification steps of the aforementioned features to eventually determine whether a given program should be considered "safe enough to execute," or not.

TinkerTool System can evaluate a given software component, such as an application, a code bundle, e.g. a plug-in, an executable file, or a signed software distribution disk image, against all mentioned security checks, showing all details. This allows you to verify the integrity, the source, and the overall security assessment of this software.

Checking a software product is very simple. Just perform the following steps:

1. Select the sub-item **Security Check** of the pane **Applications**.
2. Drag the icon of a software object from the Finder into the field **Object to check**. This can either be the bundle of a standard macOS application, a single executable file, or a signed software distribution disk image (DMG). You can also click the button [...] to navigate to the object, or click on the white area to enter the UNIX path of the object.

TinkerTool System and the security features of macOS will now analyze the selected software. This may take a few seconds, depending on the size of the bundle and the number of embedded subcomponents. The results will be displayed in the lower half of the window:

- **Unique identification:** the internal unique name used by macOS to identify this application. (Single executable files may not have such an identifier.)
- **Detected as download**: A **Yes** value indicates that quarantine markers are set for this application, so it has been detected that the selected program comes from a download.
- **Downloaded from**: If the application has been confirmed to come from a download, this entry will indicate the download source. It is usually specified as Internet address (URL) of the server which delivered the product.
- **Still under active quarantine:** Here, a **Yes** value confirms that the quarantine is still active, so a user opening the application must first confirm to be aware that the files come from the potentially unsafe Internet.

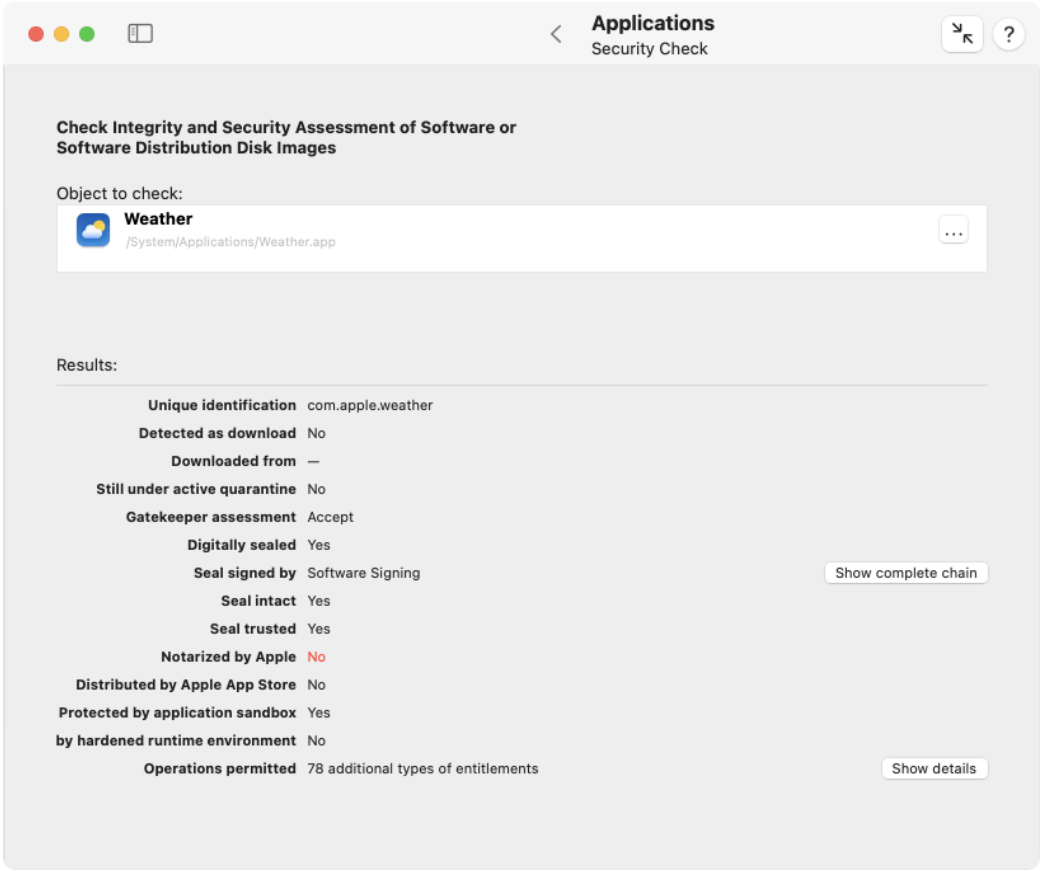


Figure 3.24: Security check

- **Gatekeeper assessment:** This line shows the official evaluation of the Gatekeeper component of your system, after having checked all mentioned security aspects and the policy you have currently set at **System Settings** > **Privacy & Security** > **Security** > **Allow apps downloaded from**…. The result can either be **Accept** or **Reject**.
- **Digitally sealed:** The value **Yes** indicates that the software has been signed and protected by a digital seal.
- **Seal signed by:** This line shows the name of the entity that code-signed the application. After clicking the button **Show complete chain**, TinkerTool System will show the entire chain of trust that confirms the validity of the digital signature. Entries are listed bottom-up in order of authority. The topmost entry repeats the name of the party who signed the software. The subsequent entries confirm (in compliance with each party's certification policies) that the signature of the preceding line is genuine. The entry at the end is usually a *CA*, a *Certificate Authority* which is the root of this chain of trust.
- **Seal intact:** The value **Yes** confirms that the selected application has not been modified (in a way which has not been explicitly permitted by the party signing the application) after it was signed.
- **Seal trusted:** This indicator reflects the most important aspect of the digital signature, namely whether the seal was signed by a party trusted by Apple. Because anybody who has the necessary technical knowledge could sign and seal an executable program, this is what makes the signature actually meaningful to assess whether it might be safe to run the program. The trust indicator also confirms that some additional checks have been passed successfully, e.g. that there are no contradicting signatures in an application which contains multiple code parts.
- **Notarized by Apple:** If the component is notarized, this will confirm that the software meets certain basic security requirements. Apple has additionally checked that this software was "virus-free" at the time it has been published.
- **Distributed by Apple App Store:** If this entry is set to **Yes**, you have selected an application which has been sold by Apple as App in the App Store. Such "Apps" are limited in the sense that they must not perform certain actions and are not permitted to use specific features of macOS. They are restricted by a set of *App Rules* specified by Apple. Compliance with these rules has additionally been verified by an *App review team* at Apple. In most cases, this review also guarantees a certain minimum of product quality.
- **Protected by application sandbox:** A **Yes** value confirms that the selected application is protected by the macOS Application Sandbox when the program is launched.
- … **by hardened runtime environment:** A **Yes** value indicates that the application is self-restricted by the macOS hardened runtime environment.
- **Operations permitted:** Three possible results can be listed here: The entry **Full sandbox protection without exceptions** indicates that the selected program cannot get

access to any "unusual" right. Apple's sandbox for applications will be in place with the highest possible security settings. The status **Only restricted by user permissions** is the opposite, indicating that no sandbox will be used at all. An entry of the pattern **xx additional types of entitlements** confirms that the program will be sandbox-protected, but it will need some exceptions from the default rules, specified by a list of additional rights the application must have in order to work correctly. *xx* is replaced by the actual number of entitlement types needed. To see the complete list, click the button **Show details**. The table in the detail sheet describes each entitlement and, if applicable, shows a variable aspect of the entitlement in the column **Object**. For example, if an application should be granted permission to read the contents of the known folders A and B in the user's home folder without informing the user first, there will be two entitlements of type **Read access to specified file in home folder without confirmation**, one referring to the object ∼**/A** and one referring to the object ∼**/B**.

Many applications that are part of macOS are shown with the Gatekeeper assessment **Reject**. This is not an error, but the correct result. Most of Apple's built-in applications indeed do not comply with Apple's own security guidelines. However, this won't matter because the affected programs have not been downloaded off the Internet and come from a source trusted by Apple.

All executable files which do not have the form of a macOS application bundle are always rejected by Gatekeeper. Examples are command-line utilities or plug-ins. This is the correct and intended behavior.

Code can be sealed anonymously, i.e. without specifying a valid signature. This is known as **ad-hoc signing** which will be indicated by a respective marker in the line **Seal signed by**….

A software distribution disk image can contain multiple applications. If you are testing such an image file, TinkerTool System will only show the security assessment for the container itself. Information exclusive to applications (like sandbox protection) will be missing. A sealed image file should guarantee that its checksummed contents is authentic as well. However, to see the actual results for the individual applications, you'll have to open the image and point TinkerTool System to one of the files inside.

Only modern disk images can be signed. This security feature is mainly used for software products targeting macOS 10.12 Sierra or later.

Apple has defined a high number of entitlements which are not documented, so they are not known to the general public. Only Apple, and in some cases a few selected developers who could not solve problems with the sandbox otherwise when using the known standard set of entitlements in their applications, have permission to use these undocumented "holes" in the sandbox. TinkerTool System lists these entitlements with the notice **Unofficial entitlement** and the internal name Apple uses for the related right.

Additional Checks for Software Developers

macOS and TinkerTool System offer two additional checks that are of interest to independent software developers. Different security and "packaging" rules apply to applications developed not for the Apple App Store, but for independent distribution. Developers can test whether an application's current security settings, signatures, and packaging are designed so that the application

- can be submitted to Apple's notarization service, or
- that it can be started on any end customer's computer, i.e. not just on the publisher's development Macs.

If the test fails, Apple will refuse to accept the application or Gatekeeper will prevent it from starting, respectively.

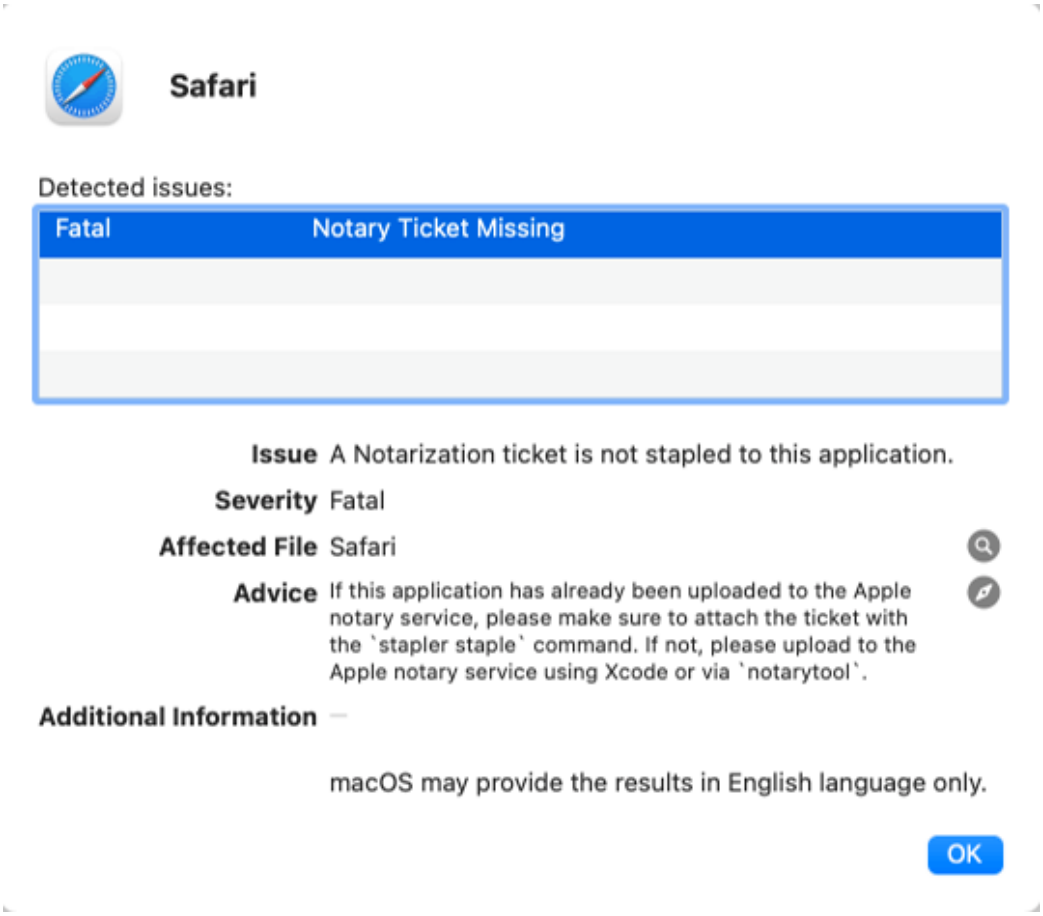


Figure 3.25: Example for the results of a check

If your system and the currently selected application meet the requirements, you can run the tests as follows:

1. Press the **Developer Check**… button that appears at the upper right of the results list.
2. In the dialog window, select which of the two tests you would like run.
3. Click **Run** or press the return key.

After waiting a while, the results will be displayed in another dialog window. All detected errors, problems, and notes are listed in a table. Details are shown in the lower area of the window after clicking on a line in the table. If a specific file in the application bundle is affected, you can reveal it in the Finder by clicking on the magnifying glass icon. If Apple provides manuals or similar documentation with more detailed information about this issue, you can access them on the Internet using your standard web browser by clicking the compass icon.

3.4 The Pane ACL Permissions

3.4.1 Introduction to Permissions

Every file and every folder accessed by your computer is associated with a specific set of rights that define which users are allowed to perform what operations with these objects, e.g. reading the contents of a file, or removing a file from a folder. This set of rights associated with a file system object is called *permissions*. macOS uses the classic permissions found on every UNIX system, the so-called *POSIX Permissions*, an extended set of permission-like markers, called *Special Permissions*, and an advanced set of right definitions used by Microsoft® Windows, most modern UNIX systems, and many other operating systems, the *Access Control Lists*, abbreviated *ACLs*. ACLs are also called *POSIX.1e permissions*, because they behave very similar to a draft document called POSIX.1e which was planned to become an industry-wide standard for permissions one day. However, the 1e documents have been officially withdrawn for various reasons, so actually no standard exists by that name. The 1e draft contained very good ideas, however, so permissions very similar to the intentions of 1e exist in most operating systems today. But you should keep in mind that the exact meaning of ACL permissions may differ slightly between different OS vendors.

3.4.2 POSIX Permissions

The minimum set of permission definitions used in all UNIX systems and many other operating systems which are compliant to the POSIX standard (IEEE 1003) is based on three predefined “parties” for which rights can be granted:

- the **owner** of the object: By default, the user who created the object automatically becomes its owner.

- the **group owner** of the object: a named group of users who are also considered to be special owners of the object. In a UNIX system, each user must be member of at least one user group. Although a user can be member of many different groups, she or he always has one preferred group, which is called *primary group*. By default, the primary group of the user who created the object automatically becomes its group owner.

- all **other** users: this access party is defined by the "rest," namely all remaining users who are neither owner, nor members of the group owner group, respectively. All unidentified users, e.g. users from other computers on the Internet, who have not been identified by their names and passwords yet (or cannot be identified at all), are automatically considered to be users of a special user account called **unknown**, which is also member of the primary group with the same name **unknown**. This means any other users, no matter if the operating system could identify them or not, will be included in the category **other**. This access party indeed refers to "the rest of the world."

> Apple identifies the third category by the term **everyone**. Unfortunately, this term is incorrect, because this category does explicitly not include the owner or any member of the primary group. If you grant or deny a right for "everyone" via the Finder, those users won't be included, which is not really what the word everyone suggests. For this reason, TinkerTool System uses the correct term **other** only.

For each of the three categories, the following permissions can be granted:

- **read:** the permission to open the object and to read its contents.

- **write:** the permission to write to this object which includes creating it, changing its contents, appending data, etc.

- **execute:** the permission to execute this object. For programs, this means that the respective party can actually launch and run the program, for folders, it means that the affected users are permitted to "pass" through that folder. Note that this right has also the characteristics of a marker which allows to differentiate between executable and non-executable files, i.e. programs as opposed to other data files.

If one of these rights is not explicitly granted for a user, this will mean that the user doesn't have permission to access. The right is denied, although there is no possibility to explicitly define denials in this model.

By default, most applications create files with the following permission settings:

- the current user is made owner and has read and write permissions,

- the current primary user group is made group owner and has read permission,

- others have read permission.

- If the object is a program or folder, the execute rights for user, group, and others will be granted additionally.

Applications can grant less rights for specific files if they have been programmed to do so. For example, an e-mail application is designed to "know" that a new mail folder should be kept confidential, so it won't grant any group and other permissions when creating it. Only the owner should have read/write permission in this case.

3.4.3 Additional Permission Markers

macOS supports some other special permission settings. They can be found on most other UNIX systems as well.

- the **SUID** setting: SUID is the abbreviation for "set user identification." Under normal circumstances, every program which is started by a certain user will have the rights of that user. (Actually, starting and running programs is what a user does when working with a computer, so, as a matter of fact, the sentence "user A has permission to do B" really means "all applications started by user A have permission to do B.") The SUID setting allows that certain marked programs break that rule. If a SUID marker is set for a program, this will mean "when running, the program should have the permissions of the file owner, not the permissions of the user who started the program." Such an exception rule is needed for very special cases where small, restricted programs need access to system resources which are normally protected. For example, when a user likes to change her own password, the program performing this operation must have temporary permission to modify the system file containing all encrypted passwords, although – in all other cases – no user ever has permission to read or even write the password file via "normal" programs. The use of the SUID marker should only be restricted to very special cases. Very serious security problems will arise if the SUID marker is misused.
- the **SGID** setting: SGID is the abbreviation for "set group identification." This is basically the same as the SUID marker, but does not apply to user and file owner, but to user group and the program's group owner.
- the **sticky** setting: This flag was originally used to mark *resident* programs, i.e. programs that should always "stick in RAM" and must not be removed from memory even when the program quits. For programs used very often, this could result in a speed gain, because on later starts, the program could just run from memory and did not need to be loaded from disk again. In today's computers, such mechanisms are usually counter-productive. For this reason it doesn't make sense to use this marker for program files any longer. However, the sticky bit has a different meaning when being applied to folders, and this aspect is in active use by macOS: A folder whose sticky marker is set becomes an "append-only" folder, or, more accurately, a folder in which the deletion of files is restricted. A file in a sticky folder may only be removed or renamed by a user if the user has write permission for the folder and the user is either owner of the file, or owner of the folder. The sticky setting is typically used for "public" folders where everyone should have write permission, but users should not have permission to delete each others files.

3.4.4 Access Control Lists

Introduction to Access Control Lists

Access Control Lists, or, in short, ACLs, are a supplement to the existing POSIX permissions, so you don't necessarily need to use ACLs. The conventional rules for access rights outlined above still apply, but some optional new rules can be added.

Technically seen, an ACL is a list of individual rights which can be attached to a file system object. The ACL can either be empty – in this case, the conventional POSIX permissions apply only –, or it can contain one or more objects called *Access Control Entries (ACEs)*. An Access Control Entry includes the following information:

- *to which users* does this entry apply (this can be an individual user or a user group)?
- does this entry *allow* or *deny* access?
- which *right* in particular is allowed or denied, respectively?
- how should this entry be *inherited* from a folder to the contents of this folder?

ACL Rights

ACLs allow the definition of **13 different rights** to access a file-system object:

- **read data/list folder contents:** the right to read data from a file, or to list the contents of a folder.
- **execute file/traverse folder:** the right to execute a file as a program, or –if the object is a folder– the right to traverse this folder to open an enclosed folder.
- **read attributes:** the right to read the attributes of a file or folder, e.g. its creation date.
- **read extended attributes:** the right to read extended attributes of a file or folder. Extended attributes are for example Spotlight comments or the quarantine info of a file.
- **read permissions:** the right to read the permission settings of a file or folder.
- **write data/create files:** the right to write data into a file, or –if the object is a folder– the right to create a new file in the folder.
- **append data/create folders:** the right to append additional data to a file, or –if the object is a folder– the right to create a new folder in this folder.
- **write attributes:** the right to write attributes of a file or folder, e.g. its creation date.
- **write extended attributes:** the right to write extended attributes of a file or folder. Extended attributes are for example Spotlight comments or the quarantine info of a file.

- **delete:** the right to delete this file or folder.
- **delete subfolders and files:** if this is a folder, the right to delete enclosed objects.
- **change permissions:** the right to change permission settings for this file or folder.
- **change owner:** the right to change the owner of this file or folder.

These rights can be joined in any possible combination.

ACL Inheritance Settings

Each Access Control Entry is allowed to contain additional information that specifies how this entry is inherited to objects located at deeper levels in the file system hierarchy, for example, a file in a folder which is enclosed in another folder. The top folder may have an ACL which is automatically inherited to objects inside this folder.

> Inheritance operations take only place in the moment when new objects are created. For example, when a file B is created in a folder A, the file B will inherit ACEs from A only at that time. When somebody changes the permissions of B later, the system will not automatically reinforce a new inheritance operation from A to B. Also, a change in the ACEs of folder A won't be "re-inherited" to the already existing object B.

There are four different settings which control how ACE permissions should be inherited from a certain folder onto the objects that will later be created in that folder. The settings basically control how "deep" the inheritance should take effect.

- **apply to this folder:** the ACL permission settings should take effect on the folder itself.
- **apply to subfolders:** The ACL permission settings should be inherited to folders inside the current folder.
- **apply to enclosed files:** The ACL permission settings should be inherited to files in the current folder.
- **apply to all subfolder levels:** The inheritance of ACL permission settings should not stop at the level of the current folder, it should also take effect on all deeper levels of nested folders.

There are 16 possible combinations of these four settings, but only 12 of them really make sense in practice.

Inherited and Explicit Entries

Because ACE settings can be inherited from folders to the objects they contain, the system has to keep track which ACEs in an ACL are inherited and which are not. Only ACEs which are not inherited can be changed. Non-inherited entries are called *explicit*. To change an inherited entry, it is either necessary to change the entry at the parent level (where this inherited entry came from), or to delete the ACL for this object (hereby breaking the inheritance), replacing the inherited entries by explicit entries.

The Evaluation Rules for Access Control Entries

As mentioned before, an Access Control List consists of several Access Control Entries. Certain rules define how macOS evaluates the entries when a specific user wants to access an object in the file system. Note that ACEs could contradict each other. For example, if user A is allowed to access the file B, but user A is also member of a user group which is denied access to file B, we have a contradiction which must be resolved. The following rules apply:

- The ACEs in the ACL are processed in top-down fashion. The first ACE rule that matches the particular user in question will "win" and take effect, either granting or denying access.
- The conventional POSIX permissions will be checked after the ACL has been processed. If a file system object has no ACL, the POSIX permissions will take effect only.

Important Recommendations

Access Control Lists are a powerful tool to define specific rights at a low level of granularity. However, you should keep in mind that ACLs are also very complex.

> There are 13 different permissions which can be granted or denied, and 12 possible ways to define inheritance. This results in a total of 2^13 * 12 = 98,304 different concepts of access rights you can define.

Each of these nearly 100,000 different access rights can be applied to a user or a user group to form an ACE, and a nearly unlimited number of ACEs can be combined into an ACL. Each file or folder in your system can be attached to a different ACL, so maintaining all these entries can easily become a nightmare. For this reason you should define ACL permissions with greatest care only.

- Use ACL permissions only when it is necessary, which means only when you have a permission problem which cannot be solved by using conventional POSIX settings.
- Use as few user groups as possible. Don't over-organize your users.
- Avoid to define Access Control Entries for users. Apply ACEs to user groups instead, whenever possible.
- If you want to protect certain files, use POSIX permissions to define very limited access rights, then use as few ACEs as possible to grant permissions to the user groups which should have access.
- Use inheritance whenever possible. If you inherit permissions, you only need to maintain ACLs for a small list of top folders.

- Avoid Access Control Entries of the deny type. Denials can easily create unexpected side effects. You might inadvertently lose the right to access some objects yourself, or worse, also lose the right to release this restriction.
- Never apply ACLs to parts of macOS, and never try to redefine the access permissions on system files. The computer might become unusable.

File Systems Supporting ACLs

Access Control Lists can only be used on file systems which are capable of storing them. macOS allows using ACLs when working with the following types of file systems, under the prerequisite that the computers hosting these file systems are using an operating system version generally capable of handling ACLs:

- disk volumes formatted with the Mac OS Extended file system (HFS+) or the Apple File System (APFS),
- network volumes accessed via the Apple Filing Protocol (AFP, AppleShare)
- network volumes accessed via the SMB/CIFS Protocol (Microsoft® Windows)
- network volumes accessed via the NFS version 4 protocol (modern UNIX systems; macOS can support NFSv4 as client but not as server).

Other file systems, e.g. disk volumes formatted using UFS, FAT, VFAT, FAT32, ExFAT, NTFS, or ZFS, and network volumes accessed via NFSv2, NFSv3, FTP, or WebDAV cannot support Access Control Lists. Not supporting ACLs over a file server connection means that the client computer cannot "see" or modify ACLs stored on the server. However, if the file server is capable of using ACLs, it will still respect them, no matter if the accessing computer may notice this or not.

3.4.5 Show or Set Permissions

Displaying Permissions

TinkerTool System can display the full set of POSIX and ACL permissions which are currently set for a specific file or folder. The settings are displayed in a clear table, sorted by the same order in which evaluation of effective rights takes place. The table can also be used to change permission settings.

> The Finder of macOS is not capable of displaying the "true" permission settings of a file system object. Due to several design flaws, the section **Sharing & Permissions** in the **Get Info** panel of the Finder may show a very simplified or even wrong summary of the permission settings. TinkerTool System, however, will display the true settings, as they are defined and stored by the core operating system. For this reason, some permission details shown can differ between the two applications. In such a case you should not trust the display of the Finder.

To display or change the current permission settings of a file system object, perform the following steps:

1. Open the sub-item **Show or Set Permissions** on the pane **ACL Permissions**.
2. Drag the file or folder from the Finder into the field **File or folder**. You can also click the button [...] to navigate to the object, or click on the white area to enter the UNIX path of the object.
3. The current settings will be shown in the table.

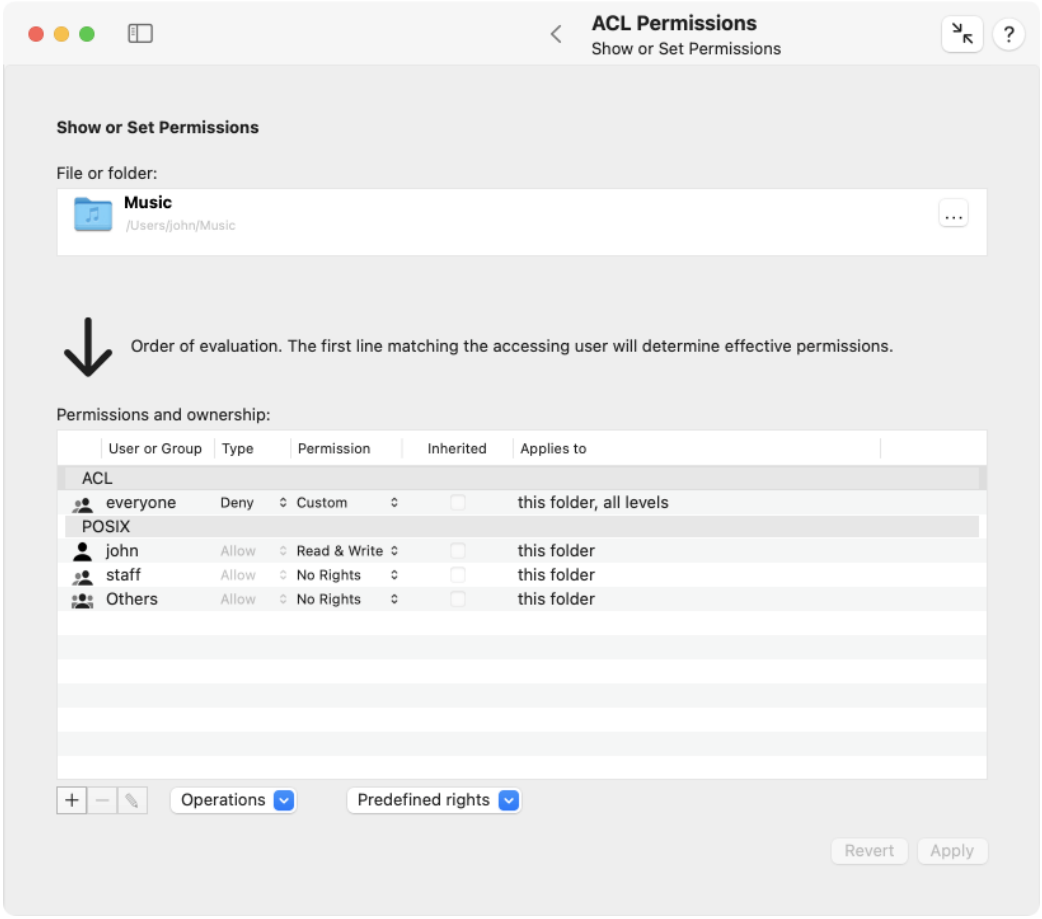


Figure 3.26: Show or set permissions

Header lines in the table show which rights are ACEs of an ACL, and which are based on the conventional POSIX settings. The columns specify the following information:

- the user or group for which an entry takes effect,

- the type of entry, namely to allow or deny permission,
- the permission setting, in simple terms,
- a marker if the entry has been inherited or is explicit,
- the inheritance settings.

> If a permission is being displayed as **Custom**, it will indicate that the rights cannot be described by simple terms, like **read only**. Remember that there are 98,304 different concepts of permissions which can be defined by combining ACL rights. To see the 13 detail rights and 4 inheritance settings (for folders) exactly, double-click a line of the table. Alternatively, you can click on the button with the pencil icon directly below the table.

In cases where ACLs or even permissions in general are not supported for the selected object, a red warning will appear below the **File or folder** box, together with a question mark help button. You can click the button to get detailed information why there could be issues when reviewing or editing permissions on the affected volume.

> There can never be any file system object without permission settings, so macOS will automatically convert rights of other systems to "plausible" permissions for the local system if this should be necessary, or it will completely synthesize artificial settings which aren't actually stored on the volume. TinkerTool System will show you the effective settings as macOS is simulating them for your current user account in such a case, but you should keep in mind that processes running for other users may receive different settings. It is also possible to edit and save such artificial permissions, but macOS will "re-translate" them back to the affected volume when applying them, so the results may not always be what you expect. We don't recommend to apply new permission settings in cases where TinkerTool System shows a support warning.

Changing permissions

After you have chosen an item and TinkerTool System is displaying its permission settings in the table, every aspect of the settings can be changed. After you have made all desired changes, you can click the button **Apply** in the lower right corner to save the current settings. The button **Revert** will discard all changes you have made and TinkerTool System will go back to the original settings currently stored for the object in question.

If you like to modify the **Type** of an entry, or want to change one of the **Permission** concepts to one of the simple standard terms, you can do so by using the pop-up buttons in the table.

To change user or group of an entry, perform the following steps:

1. Double click the respective line of the table, or select the line and click the pencil button.

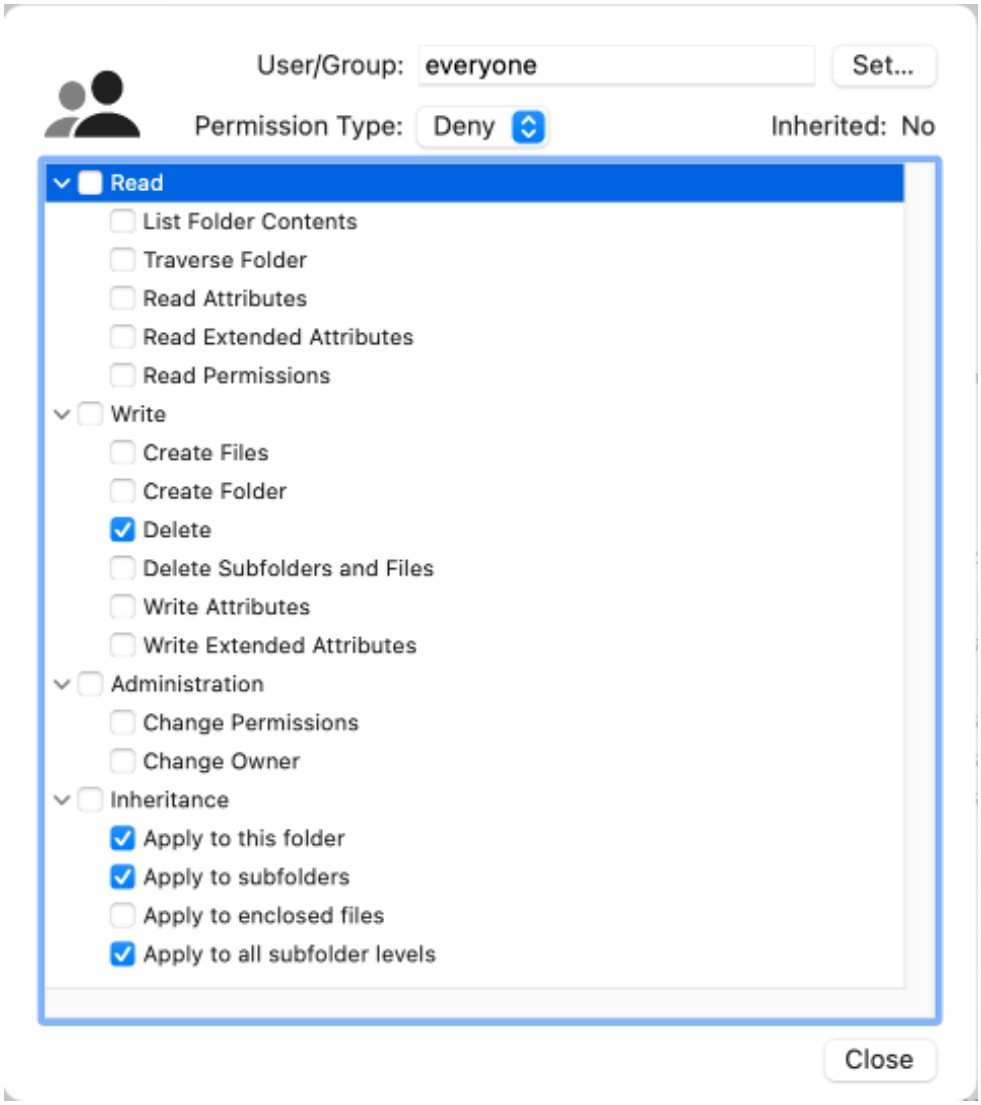


Figure 3.27: Set permission details

2. In the detail sheet, click the button **Set**... at the top of the panel.
3. In the new sheet, select either **Users** or **Groups** (if applicable).
4. Select a user or group in the table and click the **OK** button.
5. In the detail sheet, click the **Close** button.

The entry type and the detail rights can be changed in the same fashion. Note that the detail sheet is grouping the rights and inheritance settings into four categories. You can enable or disable all rights in a category by setting or removing the check mark in the respective group header. Enabling all rights of an ACE is also possible by selecting the item **Full Control** in the **Permission** pop-up. The inheritance settings will be set to appropriate defaults in this case.

To add an ACE, click the button **[+]** below the table. To remove one or more ACEs, use the **[—]** button. To reorder an ACL, drag a line in the ACE section of the table and drop it at its intended new position. Note that objects always have well-defined POSIX permissions and that POSIX permissions are always evaluated in the predefined user-group-others order, so it won't be possible to remove or reorder one of the lines below the POSIX headline.

Selecting users and groups

You may have to select a user or group account when making changes to access rights. TinkerTool System uses several dialog panels and sheets in this context which allow you to easily choose an entry from the list of all accounts available on your computer.

In large organizations, the list of available accounts can be very long. In some cases, it might not be stored on your local computer alone, but also on other computers *(directory servers)* in your network which need to be contacted. For efficiency, TinkerTool System may not show the complete list of accounts when you open a user or group dialog for the first time. The list can be restricted to accounts which have already been used somewhere in the operating system since the computer was started. In order to retrieve the full account list, click the button **Fetch all entries** in the lower left corner of the window. This makes sure the list of users or groups is complete.

> Fetching all entries may take a considerable time, especially in environments with directory servers.

Additional Operations

Additional operations can be performed by selecting one of the items in the pull-down menu **Operations** at the bottom of the window. The operations vary depending on whether you have selected a file or a folder.

If you have selected a folder, you can:

- **Sort Access Control List Canonically:** This means that the ACL will be brought into a recommended order which is considered to be "normal." The canonical sort order

is: explicit deny entries, explicit allow entries, inherited deny entries, inherited allow entries.

- **Remove Inherited Entries:** ACEs inherited from objects at higher levels in the folder hierarchy will be removed.
- **Make Inherited Entries Explicit:** all inherited ACEs will be replaced by explicit entries of the same contents.
- **Remove all ACLs in this folder:** all Access Control Lists will be removed from this folder and from all files and folders contained in it. Only the POSIX rights will be kept.
- **Propagate Permissions:** This feature can be used to transfer the permission settings of the current folder to all objects at deeper levels in the folder hierarchy. TinkerTool System will ask what categories of permissions you want to propagate in detail. You can propagate any combination of **owner entry, group owner entry, owner permissions, group permissions, permissions of others**, and **Access Control List**. This will completely reset all selected permission settings of all objects enclosed in the chosen folder. For security reasons, objects with special permissions settings (SUID/GUID) will be excluded from the operation automatically.

There is an additional option when propagating Access Control Lists: It is either possible to *copy* the existing Access Control List from the top folder to the entire hierarchy as it is, or to let TinkerTool System *simulate inheritance* in retrospect. In the latter case, the inheritance attributes of the top folder may cause the results to be different. For example, if the top folder does *not* have the option **apply to all subfolder levels** enabled for a particular ACE, inheritance of that ACE will stop at the first level.

Another option controls how TinkerTool System should handle objects which have the attribute "locked" set. The default behavior of macOS is to stop the propagation, cancelling the running operation with an error when such an object is found, because macOS does not permit that a permission setting of a locked object is changed. The policy to stop the operation makes sure there won't be any undetected security problems that could arise when the access rights for a locked object remain unchanged unexpectedly. However, you may like to ignore such cases, simply continuing the operation silently, which was the behavior of old versions of macOS Server.

> When propagating permissions in folders containing symbolic links, the program will operate on the links themselves. The objects referred by the links will remain unchanged. Folders referred by a link won't be traversed. Access Control Lists won't be propagated to symbolic links because macOS does not support this.
>
> If you like to ensure that no object is omitted during propagation of permissions, it is recommended to remove all protection attributes prior to the propagation. This can be done with the feature **Protection** on the Files pane (section 3 on page 145).
>
> A propagation is automatically limited to the volume where the top folder is located.

If you have selected a file, you can:

- **Sort Access Control List Canonically:** see above.
- **Remove Access Control List:** this will remove the entire ACL.
- **Get Inherited Access Control List:** TinkerTool System will load a new ACL based on the Access Control List macOS is creating for new files in that folder, based on the current inheritance settings effective in that folder.

With exception of the propagation feature, the operations will modify the permissions table first, not the actual settings on disk. The changes will take effect after clicking the **Apply** button.

Saving and reusing rights

In practice, it can happen that you want to apply a very specific assignment of rights to different objects multiple times, e.g. when specifying access rights for several network shares that are located on different volumes. In order to avoid having to enter all settings for users, groups, access control entries and their options again and again, you can save a set of rights once you have defined them in the program. Later, you can select them on the same computer again, reusing the permissions for a different entry in the file system. TinkerTool System refers to this as *Predefined Rights*. The associated features can be accessed via the pull-down menu **Predefined Rights**.

After you have set and applied all access rights for an object, you can save the associated set of permissions independent from that object on the same computer as follows:

1. Make sure TinkerTool System displays the desired set of permissions settings in the table of the sub-item **Show or Set Permissions**, and that the settings have already been applied (the **Apply** button is gray). You can load the rights of an existing object into the program any time by selecting the object via **File or Folder**.
2. Open the **Predefined rights** button to select the menu item **Save as predefined rights**....
3. In the dialog box that appears, specify a new name for this set of permissions that should be used to retrieve the entry later. Click **Save**.

TinkerTool System saves these predefined rights as part of your personal preferences for this computer.

If you would like to apply a set of rights saved in this way to another object later, proceed as follows:

1. Open the sub-item **Show or Set Permissions** on the pane **ACL Permissions**.
2. Drag the file or folder from the Finder into the field **File or folder**. You can also click the button [...] to navigate to the object, or click on the white area to enter the UNIX path of the object.

3. Activate the desired predefined rights by selecting the corresponding menu item **Load xxx** via the **Predefined rights** button, where *xxx* is the name you assigned previously. The current permission settings are now overwritten with the predefined rights.

4. Save the rights to the selected object with the **Apply** button.

> Rights for folders and rights for files (or other non-folder objects) have slightly different meanings. They also provide different options for Access Control Entries. Because of this, you cannot apply permission settings for a file to a folder and vice versa.
>
> Settings for rights usually refer to accounts. Because accounts are unique, you cannot transfer predefined rights from one computer to another.

You can rename or delete a set of access permissions any time using the **Predefined Rights** button.

3.4.6 Effective Permissions

The combination of several Access Control Entries and the POSIX permissions can make it difficult to estimate how the final rights for a certain user will be. TinkerTool System can compute and display the effective permissions of a user. This feature is helpful if you don't have much experience with permission settings yet. To display effective permissions, perform the following steps:

1. Open the sub-item **Effective Permissions** on the pane **ACL Permissions**.

2. Drag a file or folder from the Finder into the field **File or folder**. You can also click the button [...] to navigate to the object, or click on the white area to enter the UNIX path of the object.

3. Click the button **Select**... to choose one of the known user accounts of the current computer.

4. TinkerTool System will display the results in the table at the bottom. Rights currently granted to this user will be displayed by a green marker, rights currently denied by a red marker.

3.4.7 Special Permissions

The set of POSIX permissions contains three special settings, named SUID, GUID, and sticky. For their individual meanings, please see the introductory sections earlier in this chapter. TinkerTool System can display and change any of the three settings. Perform the following steps:

1. Open the sub-item **Special Permissions** on the pane **ACL Permissions**.

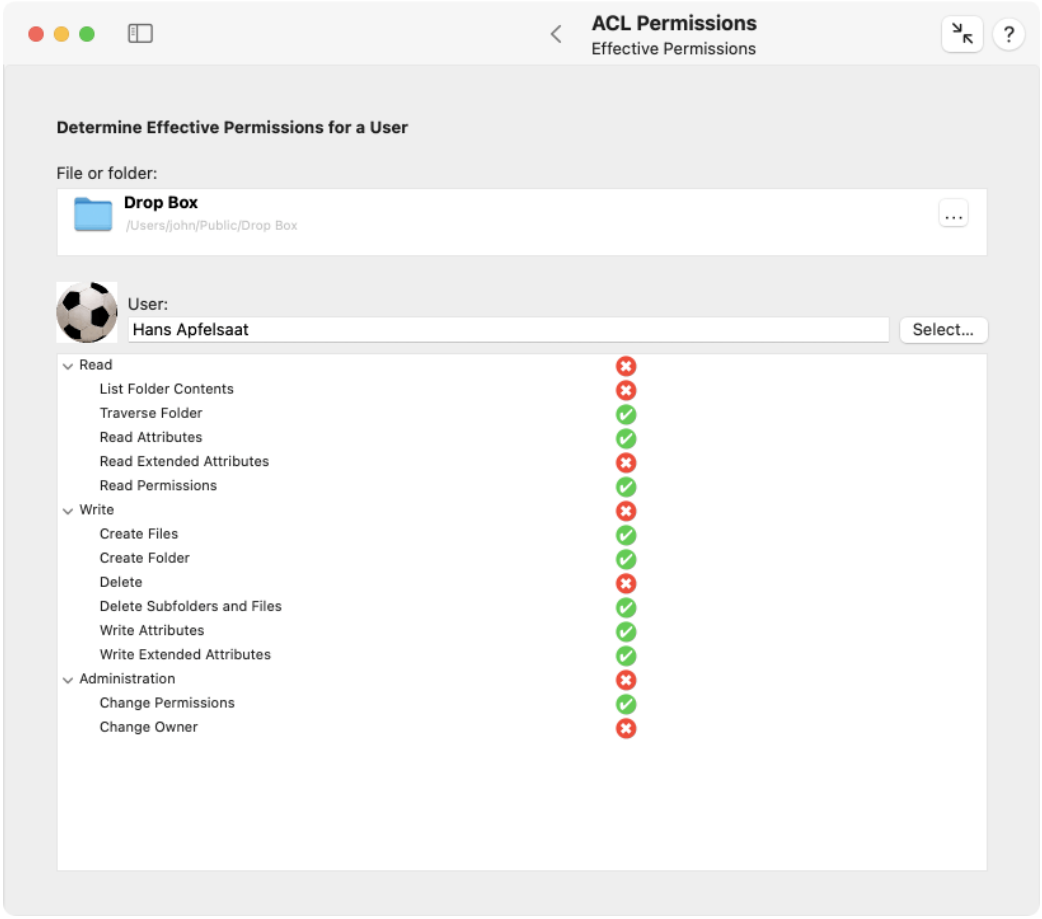


Figure 3.28: Effective permissions

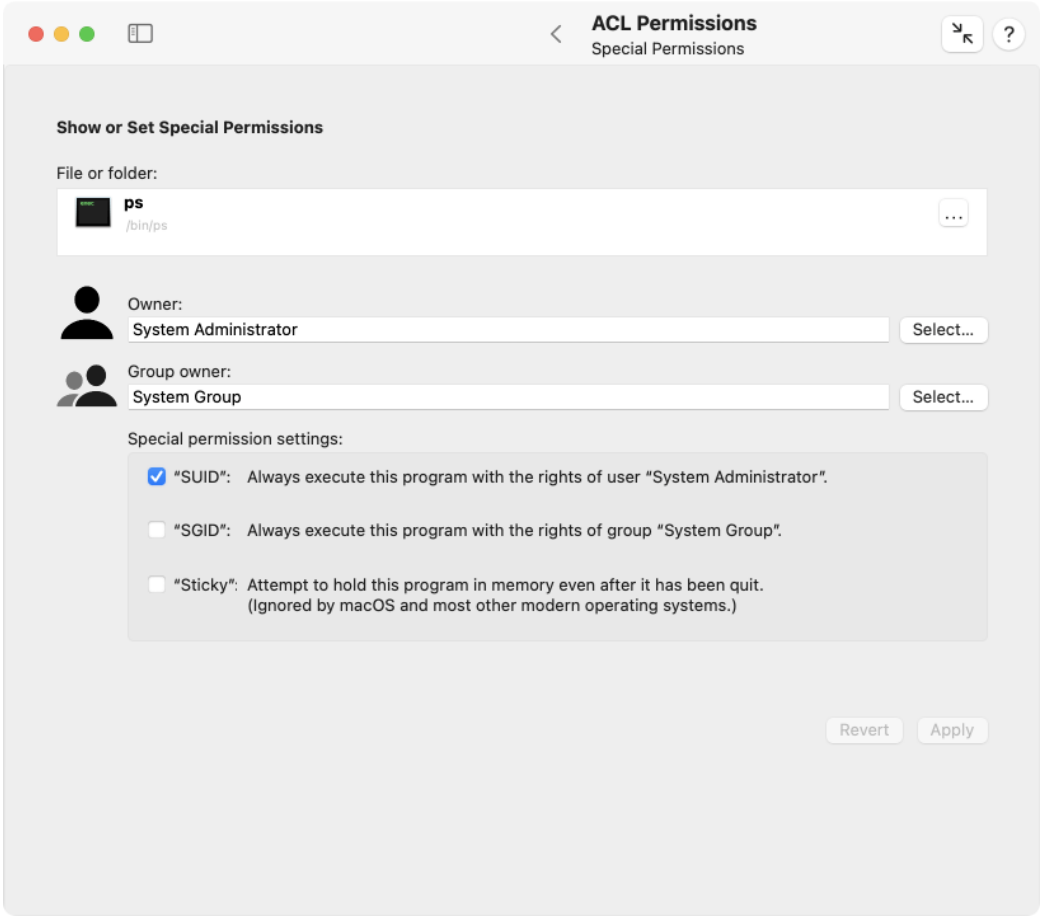


Figure 3.29: Special permissions

2. Drag a file or folder from the Finder into the field **File or folder**. You can also click the button [...] to navigate to the object, or click on the white area to enter the UNIX path of the object.

3. The current settings will be displayed. You can modify the fields **Owner, Group owner, SUID, GUID,** and **Sticky** as desired.

4. Click the button **Apply** to save the new settings.

Warning: As mentioned in the introduction, setting the SUID or GUID markers may cause very serious security problems affecting the whole operating system. It should never be necessary to set the SUID/GUID markers for programs when their installers have not set the flags already. Removing flags can cause the affected programs to malfunction. You should not use this feature if you don't know exactly what you are doing.

3.4.8 Remove Orphaned Access Control Lists

Entries in Access Control Lists contain references to the specific access parties to be granted or denied a specific combination of rights. If this party, i.e. either a user or a group account, is deleted, all entries that referred to this party no longer have any function. However, they still remain stored in a volume's file system, even though they are superfluous. We refer to such entries as *orphaned*. The Finder only displays the text **Loading...** for such entries. TinkerTool System uses the indicator **ID x**, where x is an alphanumeric identifier (see above).

TinkerTool System can determine if a volume contains orphaned ACEs. These can then be removed automatically.

Note that ACLs are just "additional rights" beyond the rights of the file owner. If even a *file owner's* account is deleted, the entire file is considered orphaned, which has other implications. You can also let TinkerTool System handle such cases. For more information, see **Orphaned Files** in the chapter The Pane Clean Up (section 3.2 on page 168).

Warning: If the computer is part of a managed network, accounts are typically not only stored on the computer itself, but also on one or more other computers in the network. These network-wide accounts are records in *directory services*. Before you work with this feature, you should ensure that the computer is currently connected to all directory services relevant for your network and the directories are

working correctly. Otherwise, there won't be a reliable way to determine which accounts are available and which are not. Entries owned by network users could so mistakenly considered to be orphaned.

Warning: You must not this feature on a volume which is managed by an operating system different from your current system. The other system might use a different account database, so the information which users are still present and which ones have left could be very different.

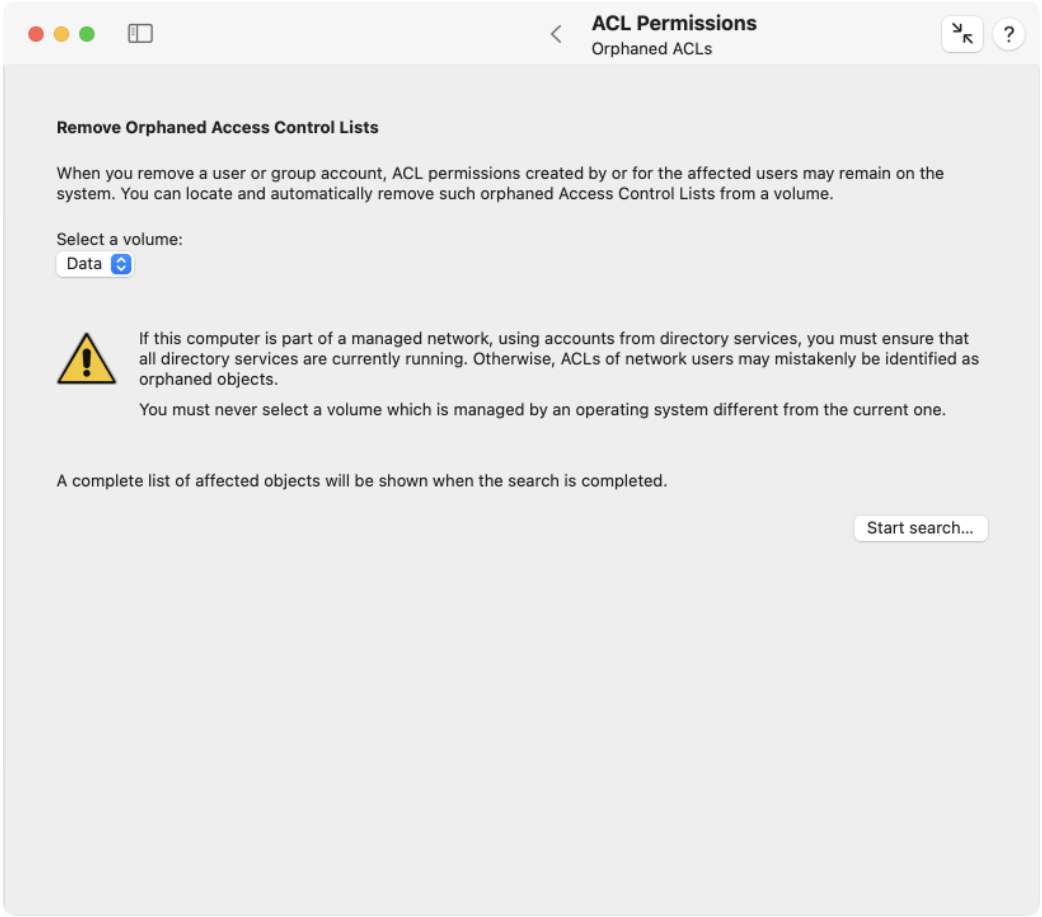


Figure 3.30: If invalid ACL entries remain on a volume after accounts have been deleted, they can be removed automatically

Perform the following steps to check for ACLs with orphaned entries:

1. Open the sub-item **Orphaned ACLs** on the pane **ACL Permissions**.
2. Use the pop-up menu **Select a volume** to specify where to search for orphaned rights.
3. Click the **Start Search**… button.

When the search is complete, you will receive a list of all affected file paths and all access party entries that refer to missing accounts. The names of these entries can no longer be determined since the corresponding accounts no longer exist. Instead, the identifiers (UUIDs) are shown. By clicking on **Delete**, you can have all displayed entries removed. This will only delete invalid Access Control List Entries. The file system objects themselves and their still valid ACEs remain untouched.

3.4.9 Set permissions in a user folder to defaults

If you have used the Finder or other means to change permissions for files in your home folder in such a way that programs no longer work correctly, cannot save settings any longer, or you lost access to your own data, TinkerTool System can reset the permission settings to suggested default values. This applies to all files and folders in the home folder of any local user.

For older versions of macOS, Apple had temporarily provided a Unix command-line program where a similar procedure could be executed in the recovery system of macOS. In addition, this was tied to resetting the affected user's password. This option is no longer available in current versions of macOS.

This procedure is sometimes incorrectly called "repairing permissions". This term is misleading, because permission settings can only ever be changed by a program or user, but they cannot be damaged.

Warning: You should never use this feature when it isn't necessary, and never regularly. The default rights are a clean suggestion that guarantees affected users can work with their own files without any problems. However, these default values could also make files readable by other users, even though the application that created the data may have originally saved them with a "readable only by this user" setting. Neither macOS nor TinkerTool System can "know" the meaning of each individual file and folder and whether it should be classified as confidential or public from the owner's point-of-view. This is unmanaged user data where any setting could make sense. In other words: The standard settings could be too insecure for confidential data in some cases. The affected user has to make sure that no unauthorized persons can read or delete the data, by subsequently checking and possibly tightening the rights after the defaults have been set. Some (not all) applications may

automatically correct insecure permission settings the next time they automatically save data for this user.

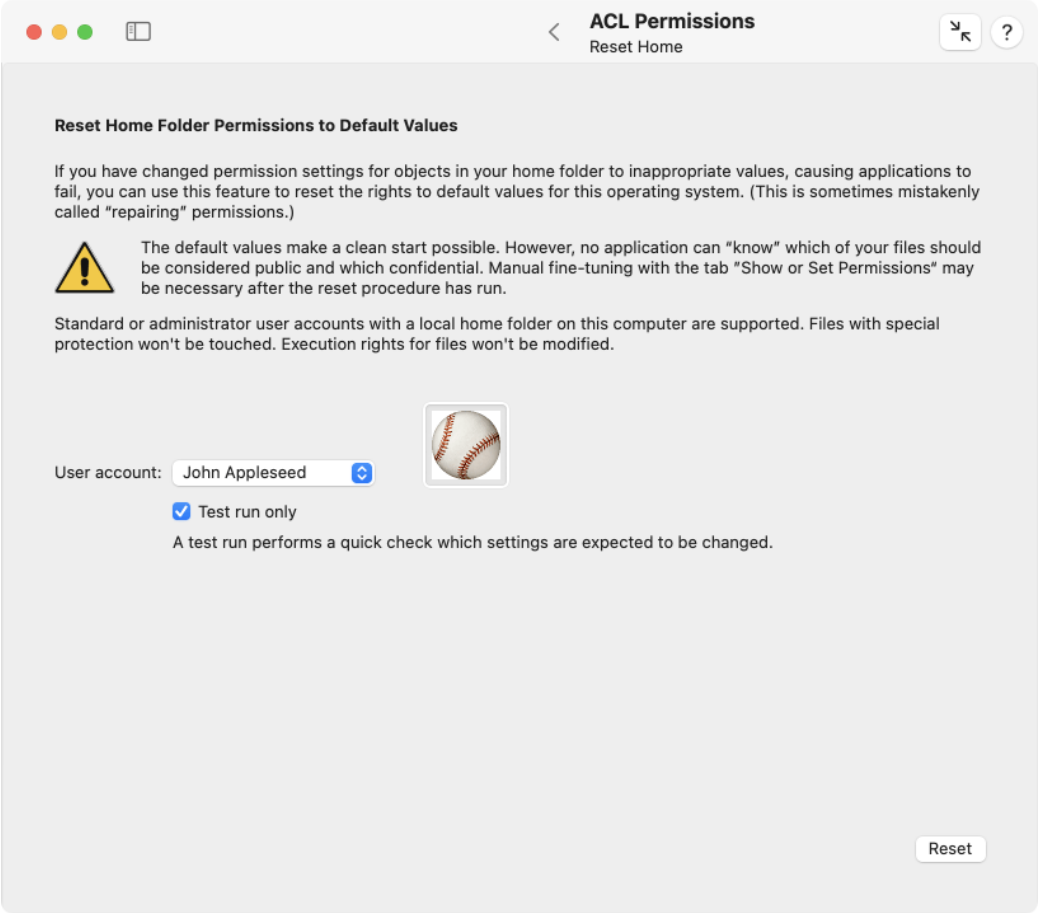


Figure 3.31: Incorrect permission settings in a home folder can be set to default values

The following basic rules apply:

- The affected user must have a local home folder on this computer.
- If the user folder contains data with *Special Permissions* (see previous section), those objects will always remain untouched for security reasons.
- The same policy applies to objects that are marked as *dataless files* which are automatically synchronized by iCloud or other cloud solutions. Changing the permissions of such a file would otherwise trigger an automatic download of the file's contents by macOS.

- Rights related to the executability or non-executability of programs will never be changed.
- Default values for permissions are based on the settings Apple chooses on the currently running operating system version when creating a new home folder for a new user account. This means the results can be different for each system version. If the user folder was originally created by control of an older operating system, then upgraded to a later version of macOS, it will be possible that many rights will change.

If you like, a test run can be performed to check all files and folders in a user folder without actually modifying any permission setting. You get a report how many settings would change or would remain unchanged, and which files would be affected.

Due to the particular nature of ACL inheritance, there are cases where the results of a test run won't exactly match the results of an actual run. Changing an Access Control List can indirectly trigger future changes to other objects, which is not always predicted in detail.

To reset rights in a local user's home folder to working default settings, perform the following steps:

1. Open the sub-item **Reset Home** on the pane **ACL Permissions**.
2. At **User account**, select the user whose folder should be processed.
3. Use the **Test run** option to choose whether permissions should actually be modified, or you only like to get a preliminary preview.
4. Click the button **Reset**.

The selected procedure will be executed, ending with a detailed report which can also be saved to a text file. While the operation is running, a preview of the report is shown as scrolling text.

Depending on individual case, the report may contain several millions of lines. In order not to overload macOS with this amount of data, the text won't be shown in a scrollable text editor box exceptionally.

3.4.10 Finding internal identifications of user and group accounts

Each user and group account is a record maintained by macOS to hold the data of individuals who have permission to access certain information. Depending on circumstances, the operating system can use different representations to identify each account:

- the **account name**, sometimes also called *short name*, usually written with lower case letters only and without a blanks in it
- the **full name,** as you would normally write it, usually longer as the account name, with blanks and capital letters. This item is sometimes called the *GECOS name*, a traditional reference to the time of very early Unix operating systems in the 1960s, where Unix stored the short names of users only, but other systems from that era, like *GECOS* from *General Electric (GE Comprehensive Operating Supervisor)* already stored more information for a user account, like the users' full names, room numbers, telephone numbers, etc.
- a **numeric identifier** in form of an integer value. This is compliant with the *POSIX* industry standard for operating systems.
- an alphanumeric identifier which follows the industry standard for **Universal Unique Identifiers** (UUIDs). UUIDs use mathematical techniques to guarantee they exist only once in the world. They are not only used to identify user and group accounts, but can refer to anything which needs an individual label.

If you specify one of these four identifications, TinkerTool System can help you to find the remaining three items for you. This can be helpful, for example, when the operating system refers to "an issue with user 502" in an internal log message and you need to find out which user account is actually affected.

A matching identification can sometimes be used for both a user and a group, even if they are completely different objects, so you also need to specify which type of account you are searching for. This is not necessary for UUIDs however, because they are always unique. Accounts may not only be stored on your Mac, but your network may keep one or more databases for accounts which are valid for all computers of the network. A server which hosts such a central account database provides a so-called *directory service*.

1. Open the sub-item **ID Finder** on the pane **ACL Permissions**.
2. Enter data into the field **Specify either account name, full name, POSIX identifier or UUID.**
3. Select either **User** or **Group** if you did not specify a UUID.
4. If your Mac is configured to access a network directory service, searching for items may affect thousands of accounts and may cause a high amount of network traffic. You can choose whether you like to permit an **Exhaustive search** through all records on all directory servers, or whether you like to limit the search on accounts which have actively been in use on your local Mac. (A non-exhaustive search may still consider accounts from remote directory services if the OS referred to these accounts recently.)
5. Press the return key.

The result of the search will be shown in the box **Result.**

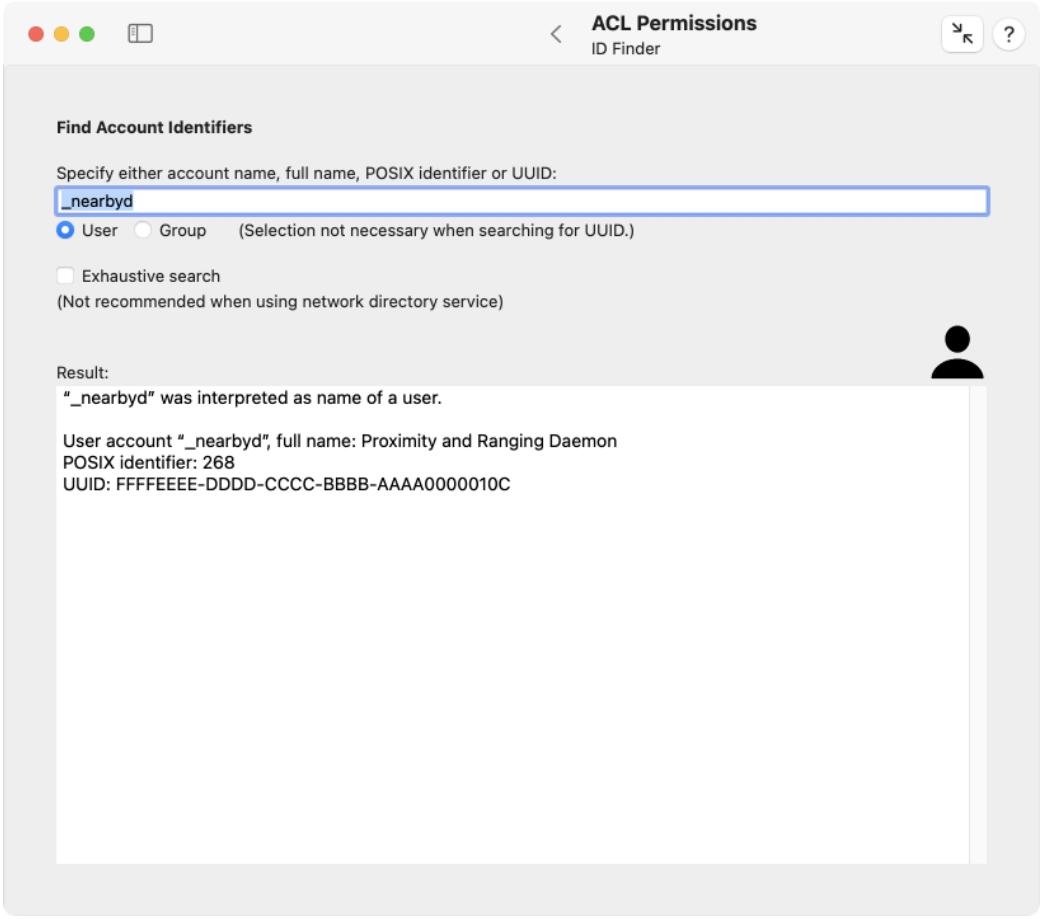


Figure 3.32: ID Finder

3.5 The Pane Install Media

3.5.1 Operating System Installation

As of summer 2011, Apple distributes operating systems only as downloads of installer Apps from the Mac App Store, or together with new Macs. This means there is no longer a tangible medium holding a copy of the operating system which could be used in case of emergency when the running copy of the OS on your computer was damaged or erased. There is only a small mini operating system for emergency cases stored in a *recovery volume*, which is installed in parallel for each macOS installation on your Mac and for each Time Machine destination disk. New Macs with Apple Silicon also contain an additional fallback recovery system which is stored in a usually inaccessible part of flash memory and behaves like firmware. Each recovery system allows you to download a copy of the full operating system from the Internet again when you have lost it. Depending on the speed of your Internet line, a full download may take more than 4 hours, however. In cases where all disk drives of your Mac have been erased or have become unusable, you can also start the recovery system by a NetBoot feature, so the emergency system is directly loaded from an Apple-provided Internet server.

All these emergency procedures won't help if you need to install a new operating system on a Mac which has no Internet connection, or which should not have such a connection for security reasons. For such cases, all Mac operating systems as of OS X 10.9 or later support a feature to create standalone install media. Such a medium behaves like a classic operating system DVD: The computer can be started from it, and you can install a full copy of the operating system without the need for an Internet connection. The medium can also fully replace a recovery system: It contains all components of the recovery OS, so you can, for example, use Disk Utility, Terminal, or Time Machine for maintenance purposes if the main OS is no longer working correctly.

TinkerTool System can guide you through the process of creating macOS install media. A bootable installer can be created by a few mouse clicks.

3.5.2 Requirements

You need additional software and hardware to create macOS install media. The following items are required:

- an installer application for the operating system you like to use, downloaded from the Mac App Store. Any operating system installer for OS X or macOS, version 10.9 or later can be used. If you had downloaded an OS installer between version 10.9 and 10.11 from the App Store in the past, you can download it again as often as you like via the **Purchased** section when you let the App Store application show you the data of your Apple Account. As of macOS 10.12.4, installers have become freely available and are no longer shown as previous purchase, but it is not possible to search other than the up-to-date version in the App Store. If you are interested in an installer between macOS 10.12.4 and the latest version, go to Apple's *support web page* and search for the name of the operating system, e.g. "How to upgrade to macOS High Sierra". You should find a web page that contains a link to a hidden entry in the App

Store, or Apple's Software Update Server, respectively, which offers the associated installation App. For specific Macintosh models however, Apple may reject a download request when they detect that your Mac could run an operating system with a higher version number. In addition, you can try to download installation apps directly within TinkerTool System (see below).

- any disk-like mass storage device supported by macOS which has a capacity of 8 GibiByte or higher. (Up-to-date versions of macOS need more than 8 GibiBytes. TinkerTool System will inform you accordingly if necessary.) A USB flash drive ("pen drive") is typically used for that purpose. You could also use an external disk drive or SSD, for example. Note that this disk will be completely erased when creating the installer.

> Although the destination volume is erased and reformatted as HFS+ during the media creation process, the latest versions of Apple's installers generally reject storage devices where partitions or file systems don't follow specific rules in advance. TinkerTool System has been modified accordingly and will only suggest HFS+ volumes as possible destination disks.

If macOS or TinkerTool System have problems detecting an external storage device which should be used to create install media, erase the device first, creating an empty HFS+ file system:

1. Launch **Disk Utility**.
2. Ensure that the option **View** > **Show All Devices** is switched on.
3. Select the device in the sidebar of Disk Utility.
4. Press the button **Erase** in the toolbar.
5. Specify **Format: Mac OS Extended (Journaled)** and **Scheme: GUID Partition Map**, enter a **Name** by your choice.
6. Press the button **Erase**.

After the device has been erased, macOS and TinkerTool System will accept it as destination medium.

> A few operating system installers downloaded from the App Store may be incomplete. In such a case, the installer app is a "stub" only which does not contain the actual operating system, but only information how to internally download the missing parts from Apple in case they are needed. You can recognize such an app by its size of only between 20 and 30 MB. Unfortunately, it won't be possible to create install media with such an incomplete installer. TinkerTool System will correctly detect this, giving you a respective warning in this case. The App Store may decide per customer and per OS version when to offer a complete or an incomplete operating system installer package.

3.5.3 Downloading Installer Apps without the App Store

If you have problems getting the right installer from the App Store, you can instruct macOS to automatically find a specific installer and to perform the download:

1. Open the pane **Install Media**.
2. Click the button **Download installer app from Apple**….
3. In the request sheet, choose an installer from the table of available Apps currently offered by Apple, and click the **Start download** button.
4. TinkerTool System will send a request to Apple to locate and download the installer. You will see status messages in a download sheet. The procedure can be stopped any time by clicking the **Stop** button.

> Usually, you will not be offered any system versions that would not run on your Mac. So, with a new Mac, you cannot download an operating system that is too old and incompatible with it. Depending on the model of Macintosh you are currently using, you will get different results in the list.
>
> We cannot predict which installer versions Apple will offer in your region and for your specific Mac. The available versions may change any minute without further notice.

Depending on the speed of your Internet line, the download may take several hours. After the download has been completed successfully, you will find the installer in the main **Applications** folder which is opened automatically by TinkerTool System. If you stop the download procedure, macOS may decide to continue the operation in the background. TinkerTool System has no influence on this.

3.5.4 Downloading IPSW files

In addition to the installer applications, Apple provides another type of file for Macintosh with Apple Silicon that can be used to reinstall the computer. For historical reasons, this technique is called *IPSW file (iPhone Software)*. A single file contains both the operating system and the firmware of the Mac. Such a file can be used for two different purposes:

- You can use it to erase a Macintosh with Apple Silicon completely and restore it to a well-defined, “empty factory condition”. User data is removed, firmware and operating system are replaced. A Mac with corrupted firmware or a device that has lost all of its recovery systems can be repaired this way. To import the IPSW file, the Mac must be put into the so-called *DFU mode (Device Firmware Update)*. To do this, you need a second Mac, a suitable connection cable and the software *Apple Configurator* version 2 or higher, which is available free of charge from Apple.
- You can populate a completely empty virtual machine with the necessary firmware and operating system software during its initial setup. The hypervisor software for operating the virtual machine must provide the function of enabling installations via IPSW.

Click the button **Download IPSW file from Apple**... to get the list of IPSW files currently offered by Apple via Internet. This list is subject to change at any time without notice. You will find in the table

- the Macintosh series for which an IPSW file is offered,
- the version number of the operating system,
- the build number of the operating system.

After selecting a table row and clicking **Download selected restore file** the download will start. The process can take some time since over 12 GB of data have to be transferred. After downloading, the file is automatically placed into your personal Downloads folder.

> Even if there are several entries for different Macintosh series in the list of IPSW files, this will not mean that you actually need a different file for each model. In many cases, a single file can also be used for other or even all model series.
>
> Using Apple Configurator or a hypervisor goes beyond the functionality of TinkerTool System. The further handling of IPSW files is therefore not described in this manual.

3.5.5 Creating Install Media

To create the standalone installation disk, perform the following steps:

1. Open the pane **Install Media**.
2. Drag the icon of the installer App for OS X or macOS from the Finder into the field **Installer App**. You can also click the button [...] to navigate to the App, or click on the white area to enter the UNIX path of the App.
3. Use the pop-up button **Storage medium** to select the destination device.
4. Press the button **Start**....

> 
> Warning: The volume selected as install medium will be erased completely. You should not assume that other volumes or partitions on the same disk remain untouched. In the worst case, they could be removed as well if Apple's installer has to make changes to the partitioning scheme. To avoid misunderstandings, it is recommended to use install media that contains one single volume only.

If TinkerTool System doesn't list a device you like to use, please read the instructions in the previous section.

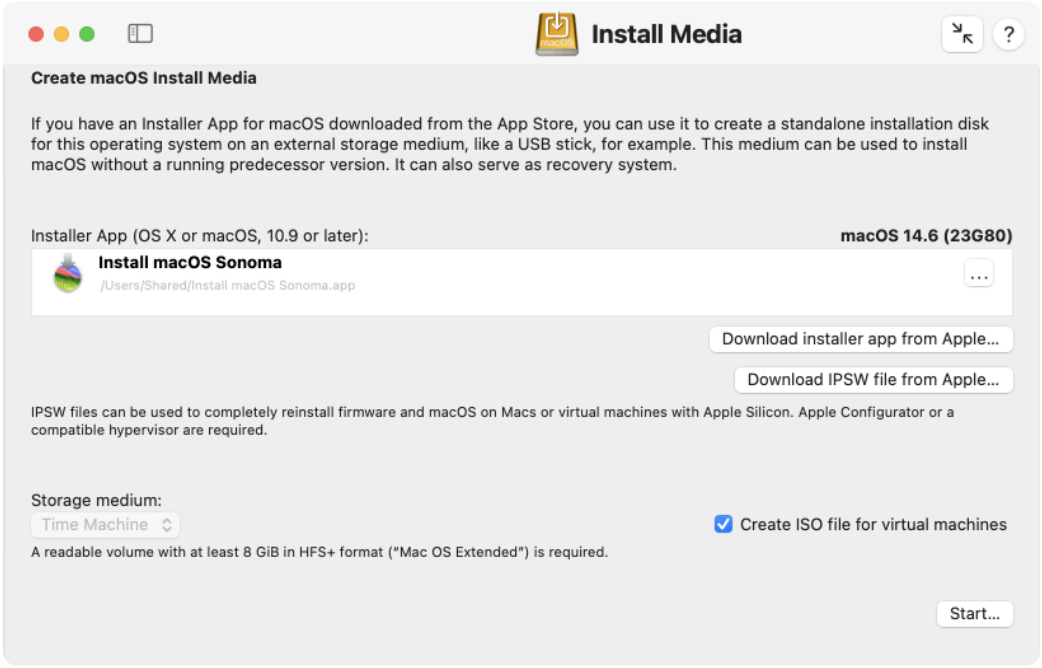


Figure 3.33: A standalone OS installation disk can be created with a few mouse clicks

Creating the installer disk is not directly managed by TinkerTool System, but by the installer App you downloaded from the App Store. For this reason, the procedure might slightly vary depending on what operating system version you are using.

When you start the first media-creation process based on a freshly downloaded installer App, macOS may sometimes launch its internal antivirus software *XProtect* automatically to check the contents of the program. This can cause a delay of several minutes at the beginning of the media creation process where neither macOS nor TinkerTool System will show any messages.

Not all versions of macOS permit the creation of install media across different processor architectures. For example, it might not always work to create an installation disk for an Intel-only operating system on a Mac with an Apple Silicon processor. TinkerTool System automatically informs you if you are trying to perform such a "cross-creation" operation with a macOS version where Apple does not allow this.

As part of the creation process, macOS might open parts of the created system in a new Finder window which might appear at the end of the procedure. The window can be used to check successful creation of the disk. You can safely close the window and eject the disk.

3.5.6 Creating Install Media as ISO file

If you need installation media to install macOS in a Virtual Machine, the process can often be simplified by not using a separate storage disk, but a disk image instead. All virtual machine hypervisors usually accept an ISO file, a disk image which follows the industry standards for creating CD-ROM or DVD masters.

To create such a disk image, check the option **Create ISO file for virtual machines** in addition to the aforementioned steps to create install media, and set a destination for the output file when the applications asks for it.

> TinkerTool System temporarily needs twice the recommended storage space while creating the ISO file. This will be 16 GiB for older versions of macOS, and 32 GiB for the latest versions. The final output file will automatically be optimized to use as little storage space as necessary.

3.5.7 Repairing the October 2019 edition of the Sierra installer

Apple released an updated copy of the installation App for macOS 10.12.6 on October 23, 2019. This particular version of the application has internal errors, however, that usually prevent the automatic creation of install media. Apple has officially declared this App as not being suitable for this purpose.

TinkerTool System is capable of detecting and repairing this App, so that you can indeed use it to create install media. In this case, an additional **Repair**… button will automatically appear on the pane. You can click the button and follow the instructions to perform the repair operation. Afterwards, it will be possible to use the repaired copy in normal fashion to create install media, as outlined before.

3.5.8 Defects and limitations of the running operating system

As of macOS 13.3, Apple added new security features to the operating system. Some of these functions are not particularly well thought out and accordingly immature. Apple's own installers can be incorrectly flagged by macOS as being unsafe or damaged. TinkerTool System is aware of this design flaw and includes several additional features that can work around the problems associated with it. The program precisely analyzes the situation and, if necessary, displays additional steps when creating installation media. Please note the following in this context:

- If the installer app you are using is *not* located on the system volume, TinkerTool System may temporarily need additional storage space on that volume. The additional space requirement corresponds to the size of the respective installer.
- When creating installation media, the antivirus scanner of macOS may put TinkerTool System on hold up to twice to scan Apple's installer for possible malware. To the outside, each of these steps appears as a longer pause during which the program does not seem to be working. If you use functions to display running processes during this pause, it can happen that TinkerTool System is shown with the status **not**

responding. *This is normal and not an error.* After macOS has checked the installer for viruses, the entire procedure will resume its work normally.

- With certain versions of the installer, macOS may indicate that the app is allegedly damaged and should be thrown into the trash. If you know you downloaded the installer directly from Apple, you should ignore this.
- If you want to create installation media for a version of macOS 10 on a Mac with Apple Silicon, the additional component **Rosetta** will be required to be able to process the Intel code of the installer. macOS recognizes this situation automatically and guides you through any necessary installation.

3.6 The Pane Operational Safety

3.6.1 Storage Space

With the latest versions of macOS, users are regularly confused as to how much storage space on a given volume is actually free and allocated. This confusion has several causes:

1. Applications may use different definitions of memory units when referring to storage space without correctly labeling it. 1 kilo byte may represent 1,024 bytes or 1,000 bytes, depending on definition. Apple has changed the guidelines for presenting storage space multiple times in the last years. Detailed information on this topic can be found in chapter Basic Operations (section 1.3 on page 8), section *Display of Memory Sizes*.
2. Applications may show storage space from a user's point-of-view (Finder) or from a technical point-of-view (Disk Utility) . For example, the Finder considers storage space allocated for local Time Machine snapshots to be free. This should signal to the user that the storage space used for that purpose could be freed automatically by the operating system when it is needed for something else. Some applications explicitly differentiate between "free" and "available" space, where "available" is defined to be "free plus purgeable". For further information, please see the chapter The pane Time Machine (section 2.5 on page 55).
3. Modern file systems can use special management technologies for the administration of storage where capacity may be counted several times although it exists only once in reality.

Apple's *APFS* is one of these modern file systems. Among others, it supports the following technologies used today, which can lead to confusion regarding storage space specifications:

- APFS no longer needs partitioning. Within an APFS zone on a disk drive, multiple volumes can be created without the need to divide them into partitions. (A zone administered by APFS is however a partition itself, the *APFS container,* in order to separate it from the areas not maintained by APFS.) Volumes in the same container

can share their storage space, i.e. free blocks don't need to be permanently assigned to a single volume, but are potentially available to each of the volumes. Consider an APFS container with 250 GB, containing 4 volumes: We have 4 volumes of 250 GB, so apparently 1,000 GB of space, although 250 GB are available in reality only. To capacity is *overbooked,* which would only become an issue when each of the volumes actually tries to allocate its registered maximum storage.

- APFS supports a snapshot feature. If desired, a file system can "remember" its state at any given time across the entire volume. At the touch of a button, this condition can be restored within seconds. Any number of these "frozen" states can be created as long as there is still free capacity to store the old and current version of all data. Technically, the snapshot feature works by no longer discarding deleted or overwritten data blocks, but keeping their former contents. Note that the storage space used for this does not become visible at the file level. The volume will need more storage space than the sum of all currently stored files, however. Modern backup systems typically use snapshots.

So if a volume is using APFS, the question for free space may not be easy to answer.

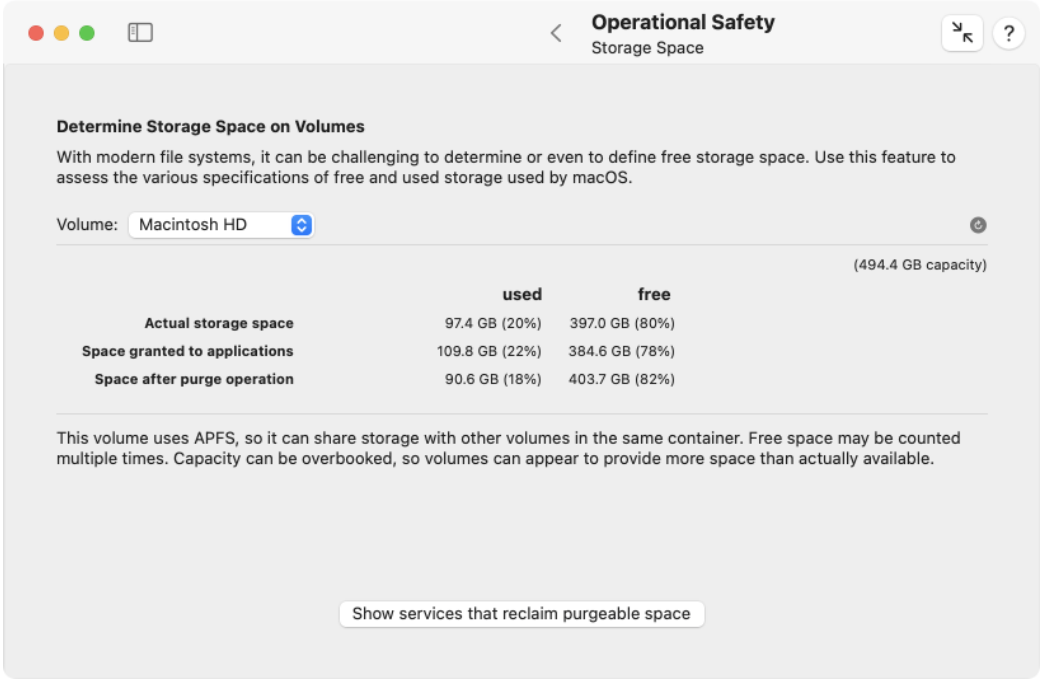


Figure 3.34: With modern operating systems, free storage space can have multiple definitions

TinkerTool System can show the different views on storage space supported by macOS for each volume:

1. Select the sub-item **Storage Space** of the pane **Operational Safety**.
2. Choose the desired volume with the pop-up button **Volume**.

> The system volume is internally split into a read-only system part, a read/write part for data, and a running sealed volume snapshot. However, this is usually hidden by macOS, and all three volumes share the same storage space, so they are presented as single volume in the pop-up button.

The different definitions of used and free storage space will be presented in a table also listing total physical capacity. When APFS is in use, a corresponding warning will be shown below the table. When comparing the results with other applications, please remember to set the correct unit for measuring memory in TinkerTool System as intended. See Basic Operations (section 1.3 on page 8), section *Display of Memory Sizes*.

- **Actual storage space:** the physical space allocated on the volume for use.
- **Space granted to applications:** the space available to applications without any restrictions. For safety reasons, a certain reserve is taken into account for the operating system itself.
- **Space after purge operation:** the storage which will become available when the operating system is forced to delete "unimportant" data automatically to regain more actual space. This difference between the true free space and the potentially free space is called **purgeable storage** by Apple. The actual meaning of this can vary depending on the system version. For example, this could be media files of rental movies already played, which could be downloaded again from the cloud at any time, or it could be local APFS snapshots created by Time Machine.

> What Apple actually means by a purge operation to reclaim storage space is not exactly defined.

However, you can press the button **Show services that reclaim purgeable space** to show the list of all system services that have currently registered with macOS to free storage space when necessary.

3.6.2 Application Integrity

On the pane Applications (section 3.3 on page 183) you may have used the feature **Security Check** already, which is designed to examine different aspects of an application under security considerations.

The pane **Operational Safety** allows you to run a specific part of this check, namely the one based on protecting executable code by digital seals *(codesigning),* for a large number of applications at the same time, e.g. for the entire system volume. This makes it possible to quickly assess the overall security situation of a computer.

The check considers the following items:

- Is each application digitally sealed and does each seal meet the security requirements of the currently running operating system?
- Has any application been changed after it was sealed?
- Is each seal trustworthy?

> The bulk check is limited to applications for the graphical user interface. As part of such a test run, you cannot check code for the command line, or other sealed components, like disk images, for example.

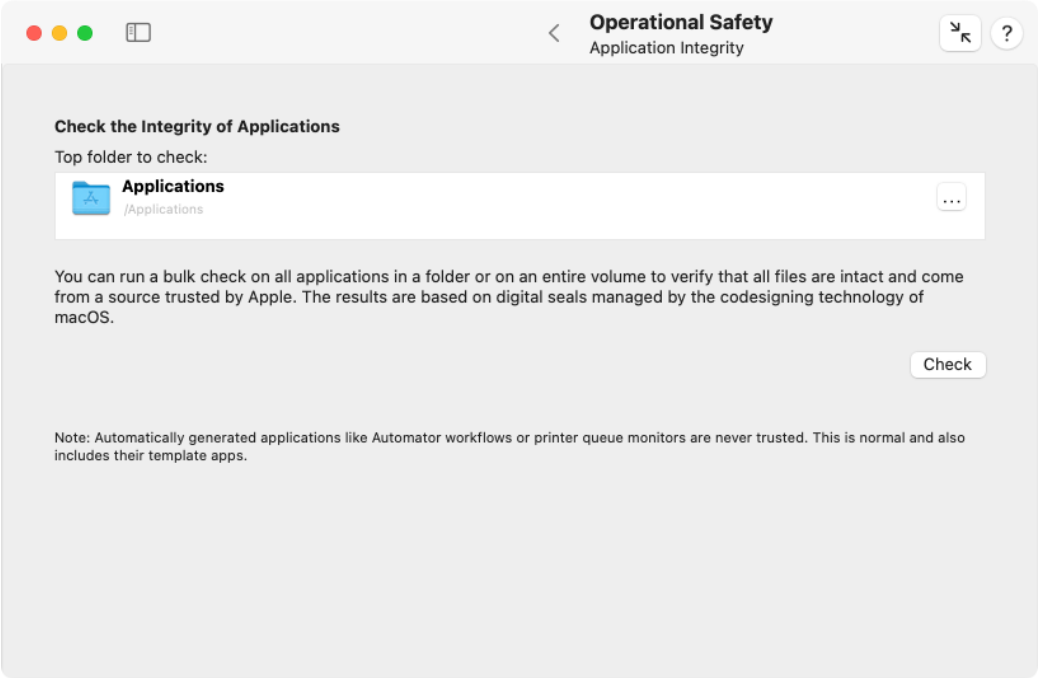


Figure 3.35: All applications of the system can be checked if necessary

1. Select the sub-item **Application Integrity** of the pane **Operational Safety**.
2. Drag the folder with the applications you like to check from the Finder into the field **Top folder to check**. You can also click the button [...] to navigate to the folder, or click on the white area to enter the UNIX path of the folder.
3. Click the button **Check**.

It is possible to choose not only a folder, but an entire volume for the check. The bulk check is automatically limited to one volume even if it contains links to other volumes.

The check can take a long time, depending on how many applications are contained, and how large they are. Particularly large applications, like Xcode or complex computer games, for example, can greatly lengthen the test. During the test run, the button **Stop** on the wait panel can be clicked to cancel the check.

> For technical reasons, test runs that have been started already may not be interrupted immediately when clicking the **Stop** button. TinkerTool System may continue running some of the test jobs in the background (which still can put load on your Mac) but will then discard the results. To cancel all running checks immediately, you must quit the application after clicking the **Stop** button.

After all test procedures have been completed, the final results will be shown in a table. It lists all applications with their names and marks the aforementioned aspects of the check in the last three columns, using icons:

- **Sealed:** the application is digitally sealed using Apple's codesigning technology.
- **Intact:** the seal is not broken, i.e. all components of the application are still unchanged, and nothing has been added or removed. The requirements of the running operating system in respect to the seal are met.
- **Trusted:** the seal was signed by a party currently trusted by Apple.

The following icons are used:

- **green dot:** the test was passed
- **red cross:** the test was not passed
- **empty field:** the test could not be performed

After selecting a line in the results table, details about the application and its check will be shown. The button with the magnifying glass can be used to reveal the respective application in the Finder. If there was a failure, the line **Detected issue** indicates the reason why the test was not passed.

You can also click the button **Close and run full security check on selected application** in order to open the program on the pane Applications (section 3.3 on page 183), letting it perform a complete security test.

By clicking the button **Text Report** you can create a copy of the result table in text form. This report can either be printed or you can export it in Rich Text Format to a text file.

> Programs created automatically by the operating system and not by a software developer are *not* classified as trustworthy in general. This includes, among other things, workflows that were created with Automator , programs for displaying printer queues, but also their associated template applications that macOS uses on demand to create the specific programs. This behavior is normal and not a cause for concern.

3.6.3 Check the system log for suspicious user activity

To ensure the security of a Mac that is open to the public, it can be helpful to automatically scan the system log for entries related to user authentication or the authorization of privileged operations. If there is an accumulation of an unusually large number of failures (e.g. entering incorrect passwords), it can be assumed that intrusion attempts have taken place. Publicly accessible can hereby mean that the keyboard and screen (called *console* in classical data processing) are not in a monitored location, e.g. in a school workroom. However, it can also mean that protected services that require a user to log in can be accessed from the local network or from the Internet.

TinkerTool System can evaluate the existing system log regarding the following operations:

- successful and failed logins at the macOS login screen,
- successful and failed logins on the lock screen, i.e. after exiting the screen saver or after waking from sleep mode,
- all unsuccessful attempts to authorize a privileged operation, both locally and when accessed through a network service.

> This list does not claim to be complete. It is not possible to predict how long entries will remain in the system log. This depends on the respective operating system version, individual settings, use of maintenance functions and available disk space. FileVault logins occur outside of macOS and are therefore typically not included in the log.

To start the evaluation, select the desired item under **Search for** and then click the **Check** button. The search may take some time depending on available log size. The results will be shown on a separate sheet window.

- When evaluating the console and lock screen data, successful logins are highlighted in green, failed ones in red.
- When evaluating the authorization of privileged operations, *all* listed entries refer to failures.

The overviews are computed based on original excerpts from the system log. Therefore, they usually contain quotes which depend on the respective macOS version.

3.7 The Pane APFS

3.7.1 Overview on APFS Volumes

As explained in the previous chapter (section 3.6 on page 227), Apple's File System *APFS* uses modern techniques for storage organization that can be confusing upon first look.

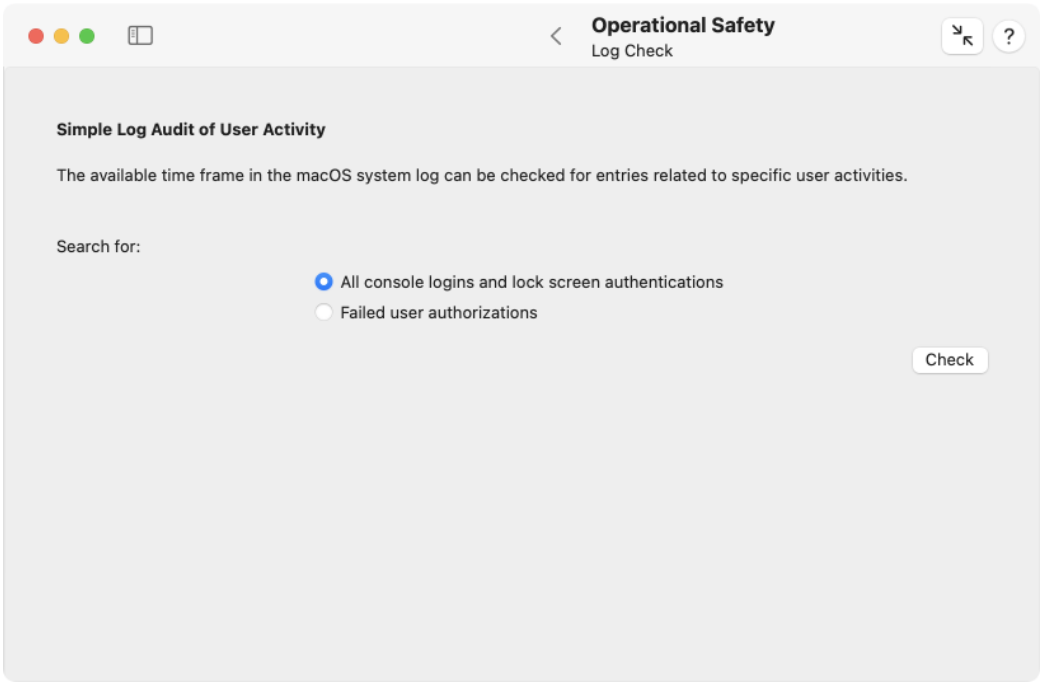


Figure 3.36: The system log can be evaluated to detect possible intrusion attempts

The sub-item **Overview** on the pane **APFS** tries to present the individual objects that have been created as part of APFS technology on the available hard disks, focusing on their hierarchical relationships. It shows the complete list of all APFS data structures on all disks currently attached to your Mac. By using the disclosure triangles in the column **Object**, the individual elements can be expanded and their parts can be reviewed. The following technical terms are used:

- **APFS containers** are the physical sections on disk drives or SSDs that mark the "zones" on storage media where APFS is active.
- **Physical disks** are one level below in the hierarchy, because an APFS container can be spread onto multiple physical storage units. In the default case, an APFS container is located on a single disk. However, it may also use multiple disks of a software RAID system, or it could be placed onto a Fusion drive, a composite of an SSD with a mechanical disk.
- **APFS volume groups** are an option to collect multiple volumes within the same container into a single unit. APFS volume groups are capable of providing a feature called *firmlink* which means that a file can appear multiple times on volumes of the same group, but it is actually only stored once.
- **APFS volumes** appear as separate entities that simulate classic disk drives. APFS volumes don't need partitions. They can be added or removed at runtime, without stopping the operating system. Volumes within the same container share the same physical storage space, so each volume has virtually its entire container available. This means however, that the same used or free space may be counted multiple times. So a container of 1 TB that hosts 4 volumes provides virtually 4 TB, although only 1 TB is actually available. To avoid concurrency between volumes of the same container, it is possible for a volume to define a *reserved space*, a minimum of physical storage that is guaranteed to always be available for that volume, or a *quota*, a maximum of physical space that may be consumed even if more is available in the container.

When you click on a line in the table, details about identification and size will be shown in a box at the lower part of the window. The table is updated automatically when connecting or disconnecting APFS disks. This also happens when you alter the APFS configuration, e.g. with Disk Utility. APFS volumes still appear in the table even when they are currently not mounted.

Please note that an APFS container can be spread onto multiple physical devices. This can be the case, for example, if a container is stored on an *Apple Fusion Drive,* a composite disk made by software, comprised of an SSD and a mechanical hard drive. For a Fusion Drive, the disk considered "faster" is shown with the type **Main**, the slower but bigger disk is marked as **Secondary**.

APFS volumes may have a special label that assigns this volume a particular task. This additional entry is called *APFS role*. At the moment, Apple uses the following types of roles:

- **System:** volume for storing the operating system

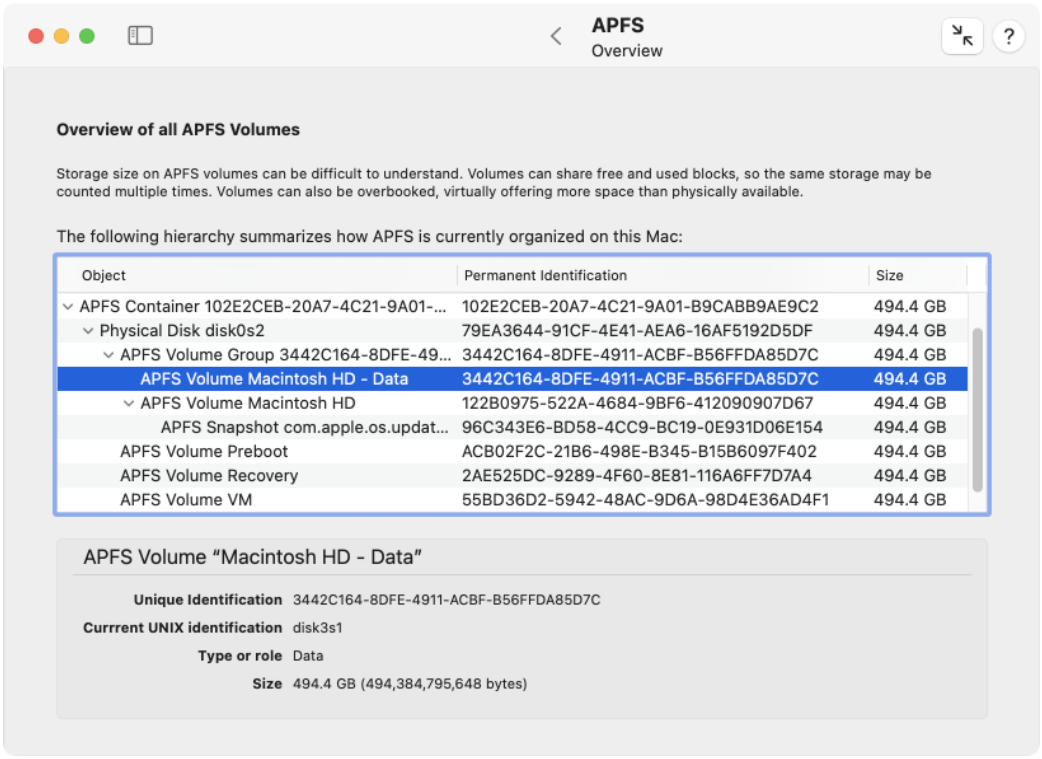


Figure 3.37: The relationship between the different APFS object can be visualized as hierarchy

- **Data:** all mutable data of users and the operating system
- **Recovery:** mini operating system for recovery
- **VM:** swap space as part of the virtual memory management
- **Preboot:** the boot loader for the operating system
- **Installer:** temporary storage of data that is needed during the installation of the operating system
- **Baseband:** firmware for operating the radio hardware of mobile devices, only used by iOS or iPadOS
- **Update:** an auxiliary volume which is used during processing of operating system updates
- **XART:** an auxiliary volume which is used for transferring data to and from the secure enclave, e.g. fingerprint information
- **Hardware:** an auxiliary volume that stores firmware for hardware components
- **Backups:** a volume used as destination for Time Machine data
- **Enterprise:** a volume used to store device data if the computer is enrolled in the remote management system of an organization
- **Sidecar:** reserved for future features of Time Machine

3.7.2 APFS Keys and Volume Ownership

APFS volumes can be encrypted. On modern Macintosh model series, the built-in flash memory is always encrypted by hardware, even if users aren't aware of that and do not even know the actual key. In this case, the hardware must manage the associated keys or key parts and regulate access to this data in a secure manner. The *Secure Enclave* is used for this, a cryptographically protected high-security area within the processor, which is unique for each Mac and for which even Apple does not know all parts of the keys.

For each encrypted APFS volume, there is a list of users who are able to access the data needed to decrypt the volume. This is unrelated to file permissions. In addition to actual persons, institutional roles can also be registered in the list of accounts. For example, if FileVault is used on the macOS startup volume, not only local users can decrypt the volume. Alternatively, decryption is also possible using a *recovery key*, which was either given to an administrator as a text code during setup, or stored in Apple's iCloud if desired. In this case, the FileVault recovery role is also listed as an apparent user in the key management list of an APFS volume.

TinkerTool System can retrieve a list of users or key access roles capable of decrypting a given APFS volume. To do this, perform the following steps:

1. Open the sub-item **Keys & Ownership** on the pane **APFS**.

2. Click **List Volume Key Access Parties**….
3. Select the desired APFS volume.

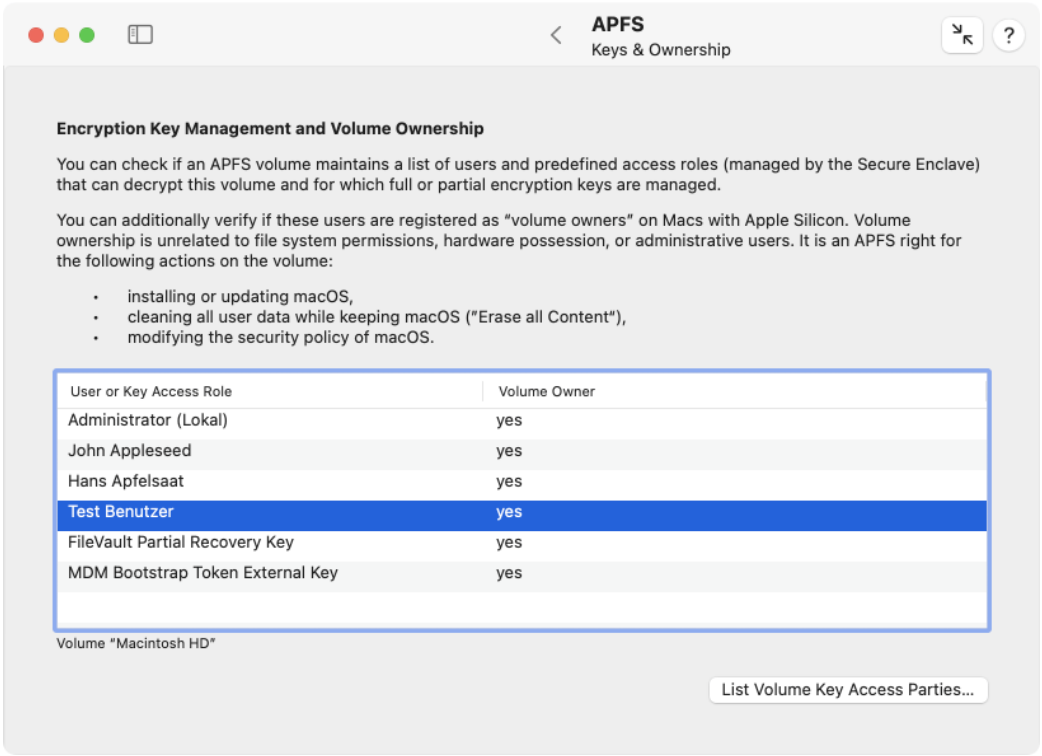


Figure 3.38: For each encrypted APFS volume, a list of users with key access is managed. Macs with Apple Silicon additionally maintain a volume ownership property.

As mentioned previously, the flash memory of modern Macs is always encrypted. For Macs with Apple Silicon, this fact is also used for further security measures. For such models, the notion of **volume ownership** is introduced. This term has nothing to do with file permissions or legal possession of the Mac. Among others, the following operations are blocked for all users who are not considered volume owners of the volume on which the affected macOS system is stored:

- installing or updating macOS,
- removing all user data while keeping the operating system, i.e. using the function **Erase all content and settings**,
- changing the startup security policy.

This property appears in the column **Volume Owner** for each user who can decrypt the volume. Macs with Intel processors do not have this security measure.

3.7.3 Automatic Defragmentation

macOS is able to automatically defragment disks. *Defragment* means that the memory blocks that make up a single file are stored as close together as possible on the medium. They should not be in separate parts *(fragments)* that are far apart from each other. This way, the read/write heads of a magnetic hard drive have to move as little as possible when a file is read. This increases the perceived speed of hard disk access. The computer works faster. Fragments occur when files have to be enlarged and the necessary storage is already occupied by other files "behind" the occupied blocks. The defragmentation moves all blocks to a different location on the hard disk where there is just enough free space available at the moment to store all blocks one after the other, if possible.

With modern SSD storage media or flash memory, there are no read/write heads any longer. Each block can be addressed directly and be read at the same speed, no matter how far apart the parts of a file are scattered on the storage medium. Therefore it does not make sense to use defragmentation on such storage media. On the contrary: Since many or all blocks of a file have to be copied to another location during defragmentation and each memory block of a flash memory can only tolerate a limited number of write operations, wear and tear increases. The lifetime of the storage medium decreases.

Defragmentation may therefore only be used on conventional magnetic hard drives with read/write heads, not on SSDs.

Since Apple has stopped using magnetic disks in Macs for several years, automatic defragmentation is switched off for the APFS format by default in macOS. However, it can make sense to enable automatic defragmentation for external magnetic disks. The files are not defragmented at specific times, but only when necessary, namely when a file is large enough to make defragmenting worthwhile and only when this file has to be changed during an ongoing write process anyway.

TinkerTool System allows you to verify on which APFS volumes automatic defragmentation is active. You can turn this feature on or off if you like. Perform the following steps to do so:

1. Open the sub-item **Defragmentation** on the pane **APFS**.

2. Click the button **Update** below the table.

> Volumes located on SSDs or flash memory are automatically omitted from the table if this property could be detected reliably. However, there may be storage media for which, for technical reasons, it won't be possible to determine whether storage is magnetic or using solid-state technology. You should be able to tell for yourself based on the volume name on which medium a volume is stored, ensuring defragmentation is only enabled for magnetic disks.

You can activate automatic defragmentation for a volume or container by setting the check mark in the respective table row. The changes will take effect as soon as you click **Apply**. If you enable defragmentation for an APFS container, it will only affect *future* volumes that will be created later on that container, not existing volumes.

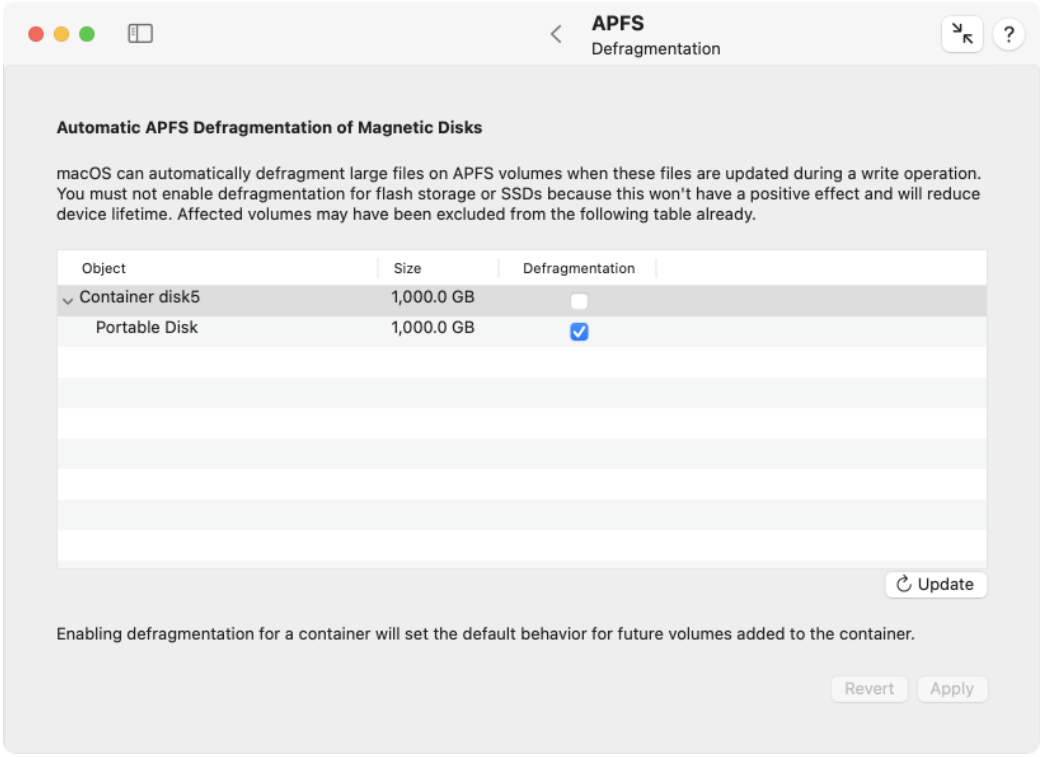


Figure 3.39: Automatic defragmentation can be activated for APFS volumes and containers stored on magnetic disks

3.7.4 Working with APFS Snapshots

The purpose of snapshots has been discussed in detail in the chapter for the pane Time Machine (section 2.5 on page 55) already. Each *Local Snapshot* of Time Machine is implemented technically by an *APFS snapshot*. However, the operating system is free to use these snapshots for purposes other than Time Machine as well. The sub-item **Snapshots** on the pane **APFS** gives you the opportunity to work with *all* snapshots, not only the ones in use by Time Machine.

> However, Apple does not grant users the right to create new APFS snapshots on a volume at their own discretion. There is no official feature to initiate this process for a selected volume, unless this is performed by backup software which has explicit approval by Apple to do so. *The user can produce new APFS snapshots only indirectly, by sending a maintenance command to Time Machine to create a Local Snapshot.* However, this is naturally associated with the restriction that snapshots will be created on those APFS volumes only which are part of a Time Machine backup, and that snapshots will be created on all those volumes simultaneously.

If you like to create APFS snapshots in this indirect way, click the button **Create new snapshots via Time Machine**… in the lower left corner of the window.

To review the current snapshots stored for a specific APFS volume, perform the following steps:

1. Open the sub-item **Snapshots** on the pane **APFS**.
2. Choose the desired volume with the pop-up button **Select APFS volume:**.

The complete list of snapshots will then be shown in the table. When you click on a line in the table, more detailed information will also be shown in the box at the bottom of the window. You will see the name of the snapshot as it was assigned by macOS, a short numerical identification, also known as *XID* , and a unique identification in form of a UUID. The field **private size** indicates how much storage space the corresponding snapshot is actually consuming for itself. Virtually, each snapshot contains a copy of the entire volume for a particular point in time of the past, which is much more storage. However, the snapshot shares this storage with the current volume content or other snapshots. Such multiply counted storage is not actually used additionally, so it does not become part of the private size of a snapshot.

The notice **Limiter** is an indicator that macOS is also using this snapshot as additional marker to define the minimum size of the respective APFS container. The operating system is capable of changing the size of partitions in hindsight, without requiring to erase and to re-partition the entire disk. When using APFS, reducing the size of a partition means shrinking the APFS container included in that partition. Because multiple volumes and multiple snapshots may share the storage space of a container, shrinking can be a complex procedure. The “rearmost” APFS snapshot of the container determines the minimum size to which the container can be reduced. The detail box lists this furthest limit for each snapshot as **tide mark** .

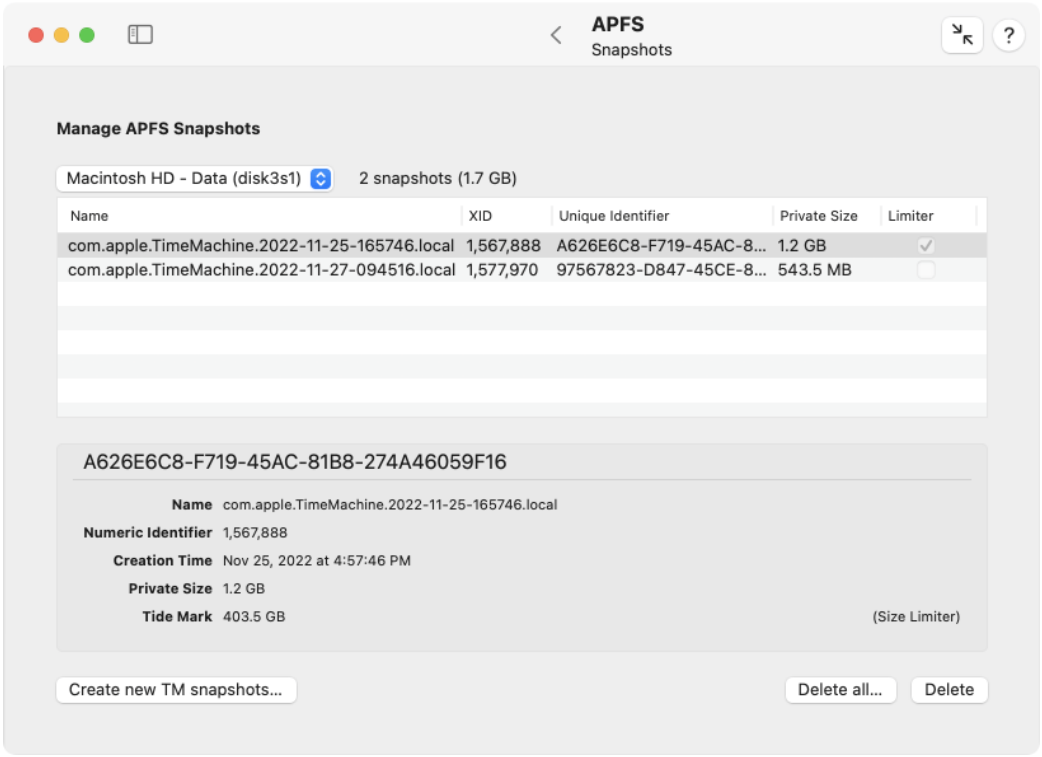


Figure 3.40: APFS snapshots can be listed and deleted

When you have selected one or more snapshots in the table, the button **Delete** can be clicked to remove the respective snapshots immediately. The visible data on the APFS volume won't change in any way. Only the possibility to travel back in time at the push of a button to an earlier state of the volume will be eliminated. The button **Delete all**… will remove all APFS snapshots from the volume after you have expressly confirmed this.

3.7.5 Copying APFS Data

macOS offers system features that make it possible to copy parts of an APFS hierarchy, i.e. containers, volume groups, or volumes, very rapidly. This quick-copy function is known as *replication* in this context. The resulting copies will match the originals with high fidelity. Each copy is an identical clone of the original and will also retain volume names. The unique identifiers won't match, of course.

In detail, you can clone the following APFS objects:

- an APFS container to another APFS container: the destination container is erased completely. However, this copy operation will only be possible if all volumes in the source container have individual APFS roles (see also the introductory section).
- a volume group or a volume into a different APFS container: the affected volumes will be added to the destination container. This means no data will be erased.
- a volume group into an existing volume: The destination volume will be erased. It must not be part of a different volume group already.
- a snapshot of a volume into a different volume: here, the destination volume will also be erased. It is additionally necessary that the source volume is currently mounted.

It is possible to clone an entire installation of macOS. The operating system and your user data are stored in a volume group consisting of a volume with the role *System* and a volume with the role *Data*. If that system is currently running, there will also be a sealed snapshot volume for the system volume. At least two additional volumes with the roles *Preboot* and *Recovery* also need to be copied. TinkerTool System and macOS automatically detect whether you intend to replicate a macOS installation and automatically add the minimum set of volumes required. This is only guaranteed to work correctly if the following conditions are met:

- If you like to clone the running system, select the *snapshot of the System volume* as source, and an empty APFS volume as destination.
- If you like to clone another system, select its *volume group* as source, and an empty APFS volume as destination.

Unfortunately, a successful replication of all required macOS volumes does not always mean that the copy can launch correctly, or could launch on any computer. In particular, Macs with security chips may refuse to start up unless the operating system copy has not been activated once again via an Internet connection with Apple.

- If the hardware is protected by an Apple security chip or an Apple Silicon processor, an additional authentication by a user account of the copied system may be required for startup.
- If the hardware is protected by an Apple Silicon processor, it can be necessary to "over-install" the operating system with a matching version to re-bind OS and hardware. Your user data will remain intact.
- If such a re-installation of macOS is required, Apple may not support this yet for all types of disk drives, firmware versions, and Macintosh models.

In all cases, source and destination must belong to different APFS containers. This means it won't be possible to duplicate a volume within its container.

Perform the following steps to copy an APFS object:

1. Open the sub-item **Copy** on the pane **APFS**.
2. Choose the object that should be copied in the table **Source**. If desired, set a check mark at **Copy snapshot instead of live volume** additionally.
3. Select the destination where the object should be copied in the table **Destination**.
4. Click the button **Copy**….

While selecting source and destination, TinkerTool System will already show a message at the lower edge of the window that gives a preview which operation would be executed if you started the procedure. If data will be lost in the target container (because one or more volumes replace already existing volumes), you will be informed in a separate dialog and will have to confirm this. When copying a snapshot, you will also be asked about the snapshot's name.

When the copying has begun, a dialog sheet will be shown which is filled with a report of the ongoing operations. After the copy procedure has completed, the report can be saved or be printed.

By clicking the **Stop** button, TinkerTool System can be forced to cancel the running copy operation. This is not recommended however, and should only be used in emergency cases. At the moment, macOS is not mature enough yet to handle an APFS

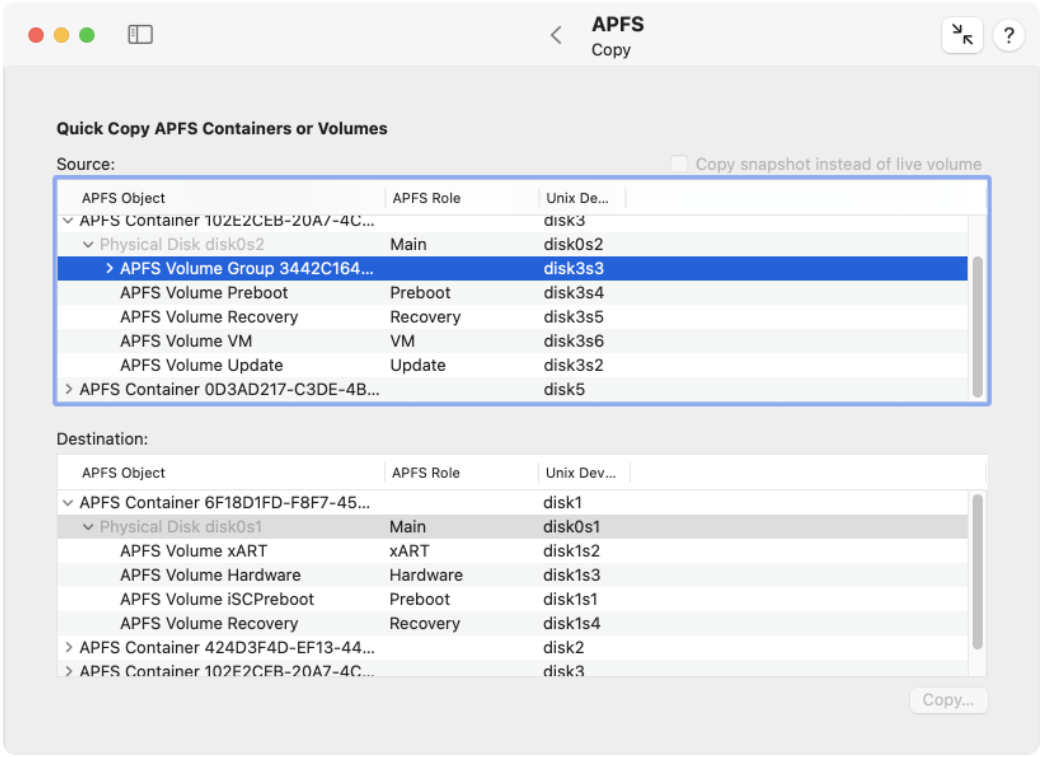


Figure 3.41: APFS objects can be copied quickly

volume copied “halfway”. In the destination container, the volume will appear as damaged item with a temporary name. In such a case it is recommended to restart the computer, and then to remove the affected volume from the destination container with Disk Utility.

Chapter 4

System Settings

4.1 The Pane System

4.1.1 Drives

Hard Disk Sleep Timer

Nearly all hard drives contain a built-in sleep timer which is designed to power down the spindle motor, saving energy when the drive has not been in use for some specified time. macOS supports a simple yes/no setting to manage this sleep feature of hard drives. It can be controlled by the option **Put hard disks to sleep when possible** on the pane **Energy Saver** (or **Battery**, respectively) of the **System Settings** application. Enabling this option corresponds to setting the sleep timer of disk drives to a value of 10 minutes of inactivity.

With TinkerTool System, you can control the sleep timers of hard disks more precisely, by specifying the exact value for the timer. Time intervals between 1 minute and 2 hours 59 minutes can be selected. To change the sleep timer of all disk drives, perform the following steps:

1. Open the sub-item **Drives** on the pane **System**.
2. Drag the slider **Put hard disks to sleep when not in use after**... to the desired value.

Throttling of Low-Priority Operations

The kernel of the operating system uses priorities to organize its *Input/Output Jobs*, mainly disk and network operations that must be executed as service for the applications currently running. Work carried out for invisible background applications (like Time Machine, for example) has lower priority than operations performed for interactive applications (like a text-processing program). Operations with low priority are *throttled* which means they are artificially slowed down, by letting them pause for certain small time intervals.

In some situations, this performance penalty can become tedious, e.g. when you are waiting for an extensive Time Machine backup run to complete. Time Machine jobs are

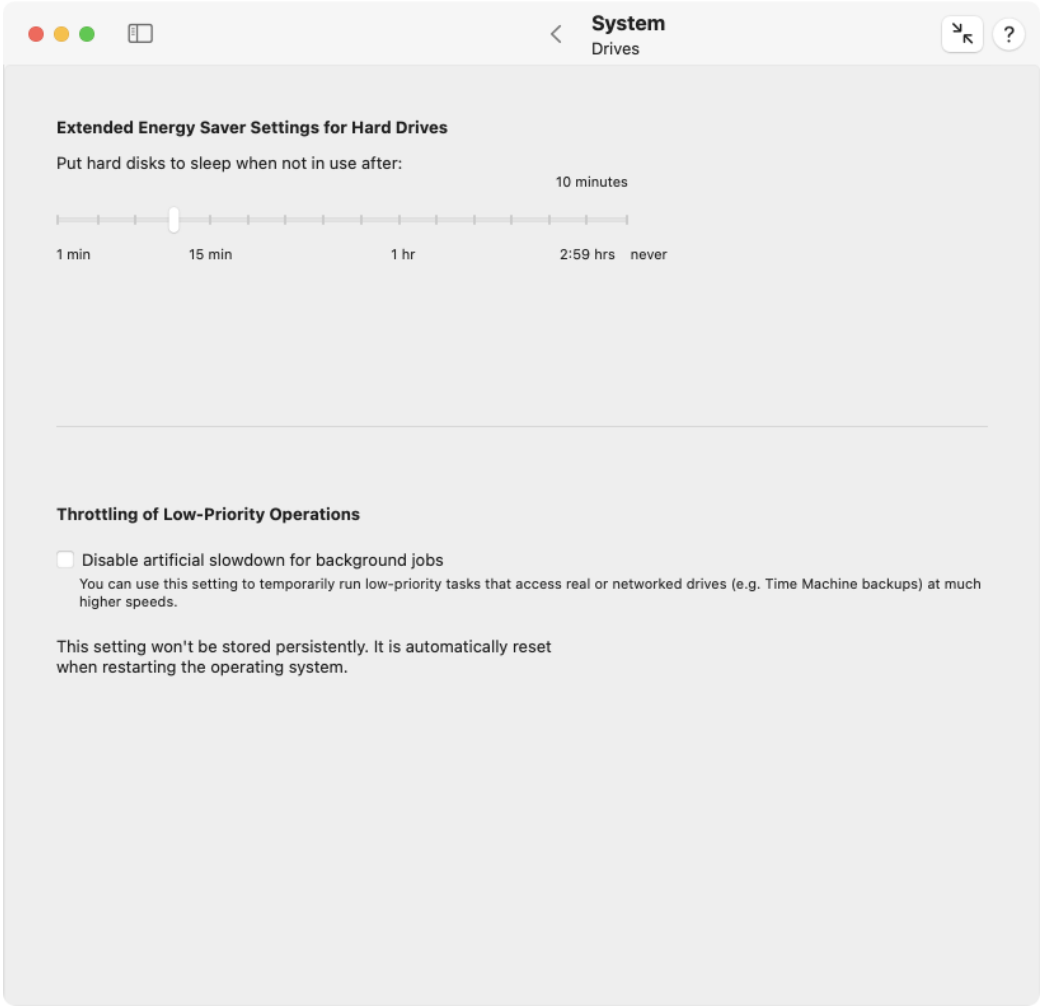


Figure 4.1: Drives

mainly made up of input/output operations on disks or network, so they are significantly affected by this slow-down.

You can temporarily disable throttling of input/output operations for background applications, giving them the same priority as other tasks. The change becomes effective immediately, but is not permanently stored as a preference. The setting will only be retained until you either shut down the operating system or change the setting again.

To disable low-priority throttling for I/O operations in the kernel perform the following steps:

1. Open the sub-item **Drives** on the pane **System**.
2. Set a check mark at **Disable artificial slowdown for background jobs**.

> Under very rare circumstances, running jobs could block each other while throttling is disabled, causing the system to freeze. Because all I/O operations run with the same priority in this case, the system can no longer reschedule important jobs to run before low-priority ones. High-priority operations may need to wait for a large number of low-priority ones, increasing the likelihood that jobs that depend on each other start waiting in circular fashion, causing a mutual blockage.

4.1.2 Volumes

macOS follows the strategy to automatically detect all disk drives and all their volumes currently connected to the computer, making them active and visible on the user interface. This might not be useful in certain situations, for example when you have a Windows partition on your computer which you don't need when working with macOS, or when you keep a backup copy of your system volume in reserve on a secondary disk drive. With the help of TinkerTool System, you can tell macOS not to activate *("mount")* specific volumes automatically.

> This setting only takes effect for purely automatic mount operations. If you are using an encrypted disk, macOS will always try to determine whether this disk contains volumes, and this disk has no readable identification (because it is encrypted). When you enter the password for unlocking, or the Keychain provides it, the corresponding volumes will be mounted, because this is a manual activation of this disk.

Another independent option allows you to choose whether the system should allow the execution of programs which are stored on specific volumes. This feature can be useful if you connect "foreign" drives to your system that contain applications written for other operating systems, incompatible with macOS. You can no longer mistakenly try to open programs on such drives.

Finally, a third option allows a volume to be automatically activated while suppressing its display on the graphical user interface. The volume is usable but hidden. This can be practical if you only want to use certain volumes in conjunction with specific applications that inherently "know" they should work with data on the corresponding drive,

but manual user access to the data isn't required, or should even be explicitly avoided. Suppressing the display affects:

- Finder windows,
- the Finder's **Desktop** feature, and
- dialogs for opening or saving files.

The volume remains visible

- in Disk Utility,
- on the non-graphical interface, such as in Terminal,
- in indirect references, for example through aliases or through the Finder sidebar.

In all cases, macOS must have a way of reliably referring to each drive and volume. This is done by so-called *Universal Unique Identifiers (UUIDs)*, a sequence of characters like 7F176A72–72B2–3D69–19FC–27ABBEFA662D which are guaranteed to be unique for every volume of every disk drive in the world. You don't need to enter these UUIDs by hand. TinkerTool System automatically finds out the UUIDs and helps you to identify the drives by specifying their current volume names and file systems.

> As mentioned before, all volumes mounted manually or by a user program remain unaffected by the settings in the table. Either such volumes are directly excluded by TinkerTool System because they are detected as not being compatible, or adding such volumes wouldn't have any technical effect, because macOS only indirectly processes the mount operation. An example for mounting by user applications is Apple's technology *LIFS (Live File Provider File System)* or the third-party software *macFUSE (Macintosh File System in User Space)*. In some versions of macOS, LIFS is used by default to process foreign file systems such as ExFAT or NTFS . Apple's usage of LIFS may vary in each version of macOS.

Perform the following steps when you like to exclude certain disk volumes from automatic mounting, execution of programs, or presentation on the graphical user interface:

1. Open the sub-item **Volumes** on the pane **System**.
2. Click the **[+]** button below the table.
3. In the dialog sheet, select one or more disk volumes that should be operated with custom settings and click **OK**.
4. Check or uncheck all options that should be enabled or disabled, respectively.
5. After all volumes have been set as intended, click the button **Apply** in the lower right corner of the window.

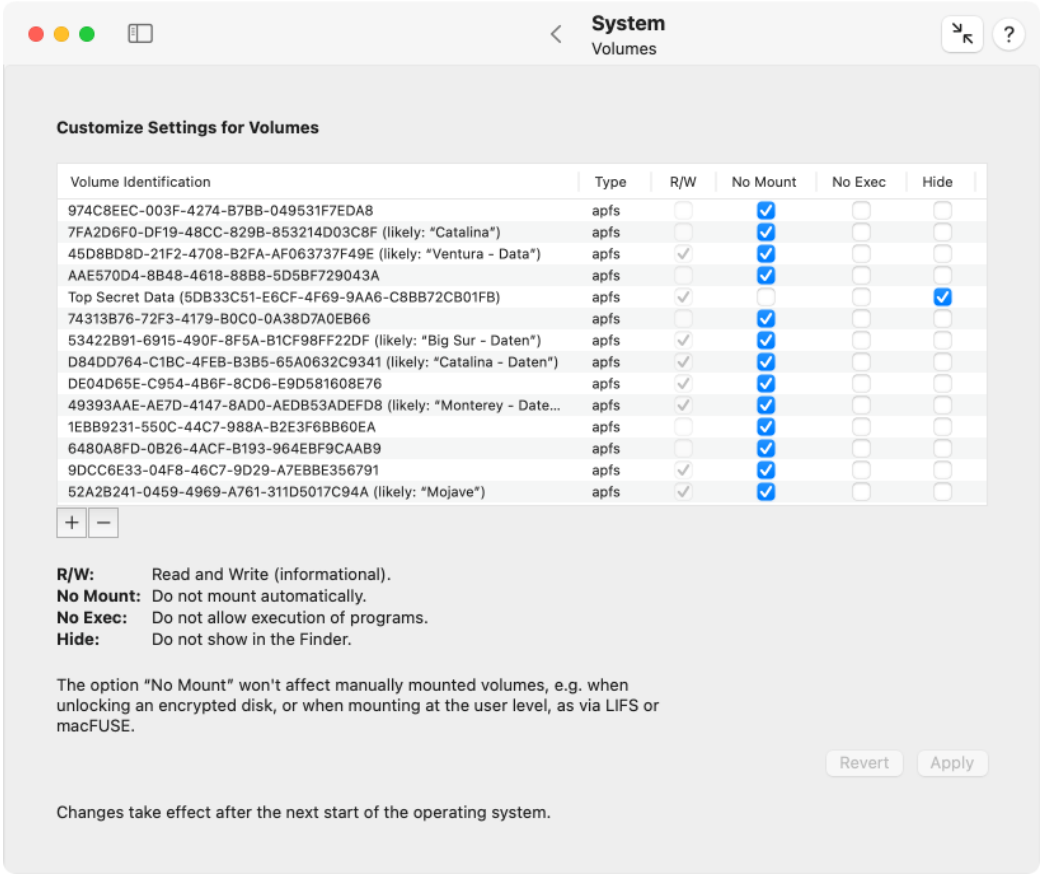


Figure 4.2: Customized settings for volumes

Volumes without any customized settings are automatically removed from the table when applying the changes.

It is also possible to drag volumes from the Desktop or the Finder's computer folder directly into the tables. You can remove one or more volumes by clicking the **[—]** button below the respective table, and saving your modifications. To discard your changes and return the tables to the state currently established in macOS, click the **Revert** button.

When you excluded volumes from automatic mounting, TinkerTool System will ask you whether you like to eject the affected volumes immediately after applying the changes.

If you have additional copies of macOS installed on your Mac, and you added one or more system volumes containing macOS 11 or later to an exclusion table of the system you are currently running, you may notice that the table entries for these volumes no longer take effect after you have performed an update or upgrade on the related system volumes. This is the correct and expected behavior because a modern macOS update *deletes* the previous system volume and *adds a new one* with the same name.

TinkerTool System can assist here: When the application detects this specific situation, the additional button **Update system volumes**… will automatically appear below the table. Click this button to review the affected entries. After clicking **Update table**, the identifications of the affected system volumes will be updated automatically to reflect the new configuration. The update button won't be available when you begin to edit the table manually.

4.1.3 Spotlight

Spotlight Operation

Spotlight is the built-in search technology of macOS which is designed to find files very rapidly after the user has specified key words or other search criteria. The technical implementation is based on several system services which operate silently in the background. However, Spotlight can sometimes be affected by technical problems, so administrators may need to fine-tune Spotlight operations in certain situations.

Spotlight is designed to operate as one of the basic core components of macOS. For this reason, other system services and many applications developed for macOS depend on the correct operation of Spotlight and will fail when Spotlight has been shut down. This includes the Time Machine backup service and the App Store application. For this reason, TinkerTool System does not support any operation to disable Spotlight completely. However, you can shut down Spotlight indexing on selected disk volumes.

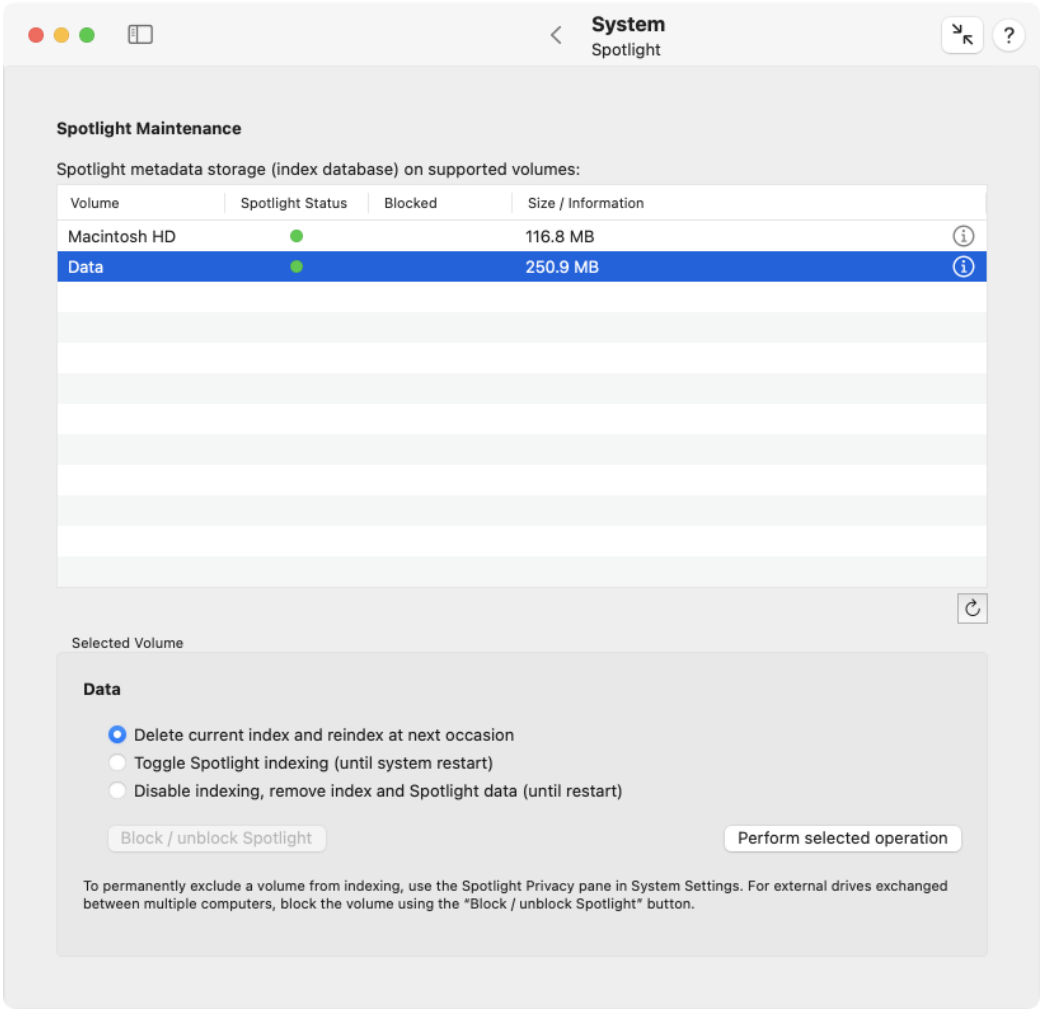


Figure 4.3: Spotlight

Spotlight Index Databases

When Spotlight is active, it automatically creates a hidden index database and some preference files on each volume currently connected with your computer. The database and the preference settings are needed to quickly find the contents you are searching for. These hidden components are called *Metadata Stores*.

For each of the volumes, TinkerTool System allows you to display whether Spotlight is activated on that volume (column **Spotlight Status** with indicator in green or red), whether Spotlight is generally disabled (column **Blocked**) and how much storage space is currently needed by the Metadata Stores. This information is displayed in the table **Spotlight Metadata Storage**. Only volumes which are technically capable of supporting Spotlight are listed in the table. A refresh button right below the table will update the contents of the table. This step is necessary to let macOS allow TinkerTool System (after authentication) to compute the size of the index databases. Access to the databases is protected because they contain potentially confidential information, namely all words of all documents all users have stored on the current computer.

After selecting a line in the table, you can activate several operations that should be performed:

- You can **delete** the metadata store on the selected volume. This will reset the privacy settings for this volume and enforces complete reindexing of all documents stored on the volume. This feature is helpful when the metadata appears to have been damaged. You would typically use this function when you detect that Spotlight finds less documents than it actually should.
- You can **toggle Spotlight indexing**, which means all indexing operations on the selected volumes will either be stopped, or be re-enabled for the currently running session of macOS. If you re-enable indexing, macOS will resume the background index operations at its own discretion at a later time.
- You can **remove** the metadata stores on the selected volume and **disable indexing** at the same time. The search database will be removed and Spotlight will no longer touch the affected volumes in the currently running macOS session.

To activate one of these functions, click the button **Perform selected operation**.

> Note that the deactivation of index operations is only in effect until you restart macOS. Unless Spotlight isn't blocked on affected volumes by using the setting **Siri & Spotlight** > **Spotlight Privacy**… in **System Settings**, macOS will recommence its indexing services upon next startup.

When you click the info symbol at the end of a table line, you can get further details about Spotlight for the corresponding volume. The application will open an additional panel with the following data:

- the current position in the UNIX file system where the volume is actually located
- a detailed presentation of status, memory usage, and possible blocking

- the information whether blocking is generally possible at the technical level and also not discouraged by TinkerTool System
- the operating system version used to configure Spotlight originally on this volume, together with the time specification
- the operating system version used the last time to modify the configuration of Spotlight, together with the time specification
- a list of UNIX file paths locked out expressly by one or more users for search operations

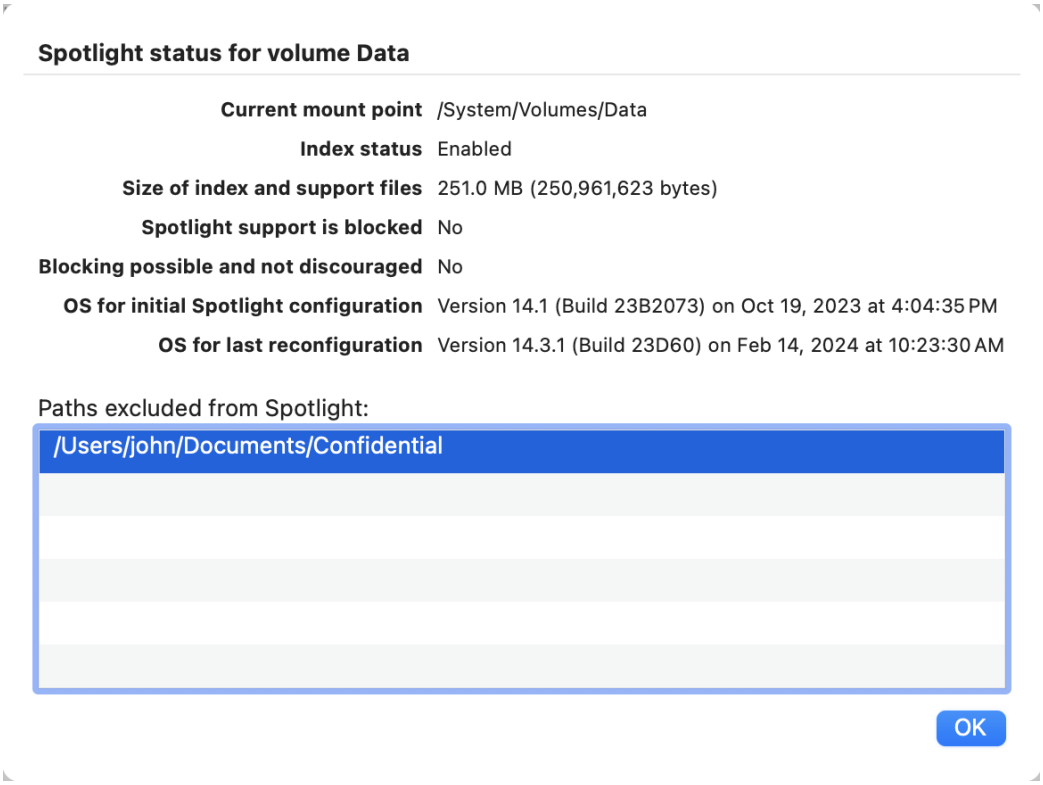


Figure 4.4: Further details for an indexed volume can be shown

Under specific circumstances, it might be helpful to disable Spotlight operations on a disk volume "forever," e.g. on a slow pen drive which you only use to transport data to other computers. This can be done by a special marker which works independently of the Spotlight privacy settings. Setting such a marker is particularly helpful on external drives which are used with different macOS computers, because all systems will automatically respect this setting after it has been established. To set or remove this marker, perform the following steps:

1. Open the sub-item **Spotlight** on the pane **System**.
2. Click the refresh arrow at the right hand side below the table to ensure the program had the chance to analyze all volumes completely.
3. Select the desired volume in the table.
4. Click the button **Block/unblock Spotlight** in the lower left corner.

Actions that could cause severe damage to the normal operation of macOS, e.g. removing the Spotlight index of Time Machine, are disabled automatically.

You should avoid to send Spotlight commands that contradict each other within short time frames, e.g. switching the index off, on, then off again. Spotlight works asynchronously in the background and may need several minutes to complete a command successfully. If an incomplete operation is still running in the background, the status display can be temporarily inconsistent, or a volume might even disappear completely from the table.

If you have triggered a command to have a search index be recreated, you can check as follows whether the indexing operating has actually been completed in the background:

1. Open a Spotlight search inquiry via the Spotlight icon (magnifying glass) at the right hand side of the menu bar and enter a file name that you know exists on the affected volume.
2. Leave the dialog open for a few seconds.

If the Spotlight index is *not* ready yet, macOS will show a progress bar after a few seconds, to indicate how much time it needs until the index will be complete. When the Spotlight index is ready, the search results will be shown without an additional progress indicator.

4.1.4 Network

Options for Connecting to File Servers

When you attempt to connect to a file server manually, a password entry panel will appear. TinkerTool System can modify the system setting that controls which name macOS should suggest in this panel. You can select between the **short name** of the current user, **another preconfigured name**, or the option not to suggest any name **(No name)**. Perform the following steps:

1. Open the sub-item **Network** on the pane **System**.
2. Choose the desired option at **Suggested name in panel**.

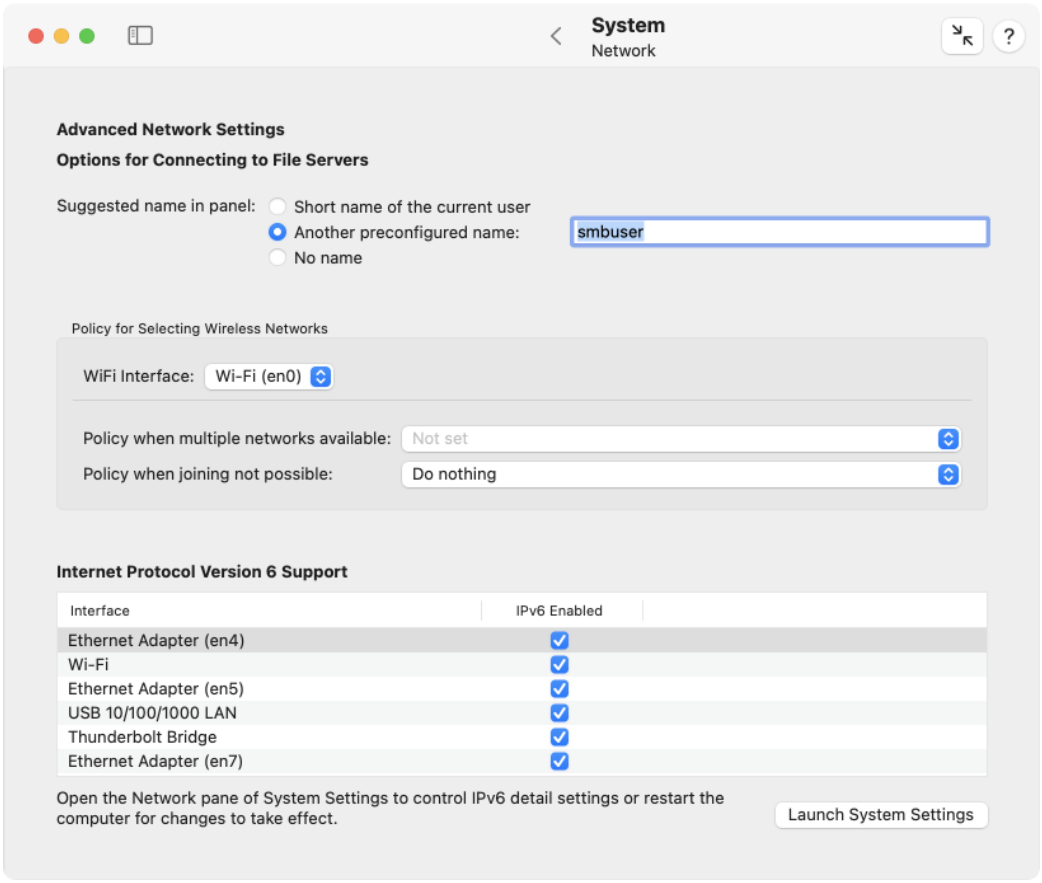


Figure 4.5: Network

Policy for Selecting Wireless Networks

Each WiFi unit attached to your Mac is supporting two settings which are normally invisible at the graphical user interface: These preference settings control which strategy macOS should use when joining one of the available wireless networks. The setting **Policy when multiple networks available** controls which network should be chosen if more than one is accessible in the current environment. Accessible means that signal reception is good enough and the credentials for a possible encryption of the network are known. The following settings are possible:

- **Automatic:** macOS should choose the "best" network at its own discretion.
- **Select preferred network:** The network which this Mac joined most frequently in the past should be chosen.
- **Select by ranking:** By using the current configuration in **System Settings** and the observed connections in the past, the system should create a ranking and choose the first network in this list.
- **Select recent network:** The network to which the Mac was last connected should be used.
- **Select strongest network:** The network that is best receivable at the moment should be selected.

The special menu item **Not set** indicates that macOS has not set a specific policy since the operating system has been installed. This entry cannot be selected.

If connecting to the network that was chosen by this policy is not possible or was not successful, the second setting **Policy when joining not possible** takes effect. Here, the following values can be set:

- **Ask user:** A dialog is shown that asks the user how to proceed.
- **Join next open network:** The first best network without encryption is chosen, even if it is not known from the past.
- **Keep looking:** The search should continue until a connection succeeds.
- **Do nothing:** After a failure to join the network, the search should be canceled. In this case, no wireless connection is made.

Internet Protocol Version 6 Support

By default, the pane **Network** of the application **System Settings** does not show a menu item to disable the support of IPv6 on specific network interfaces. The feature to switch **IPv6** to **Off** is present in the operating system, however. You can use TinkerTool System to control this option.

1. Open the sub-item **Network** on the pane **System** of TinkerTool System.

2. Locate the network service you like to modify in the table **Internet Protocol Version 6 Support**.

3. Remove the check mark in the column **IPv6 Enabled** to disable IPv6 for the network interface in that line.

When you have disabled IPv6 support for an active network service, System Settings will correctly reflect this, adding an **Off** menu item to the **Configure IPv6** option. You can either use System Settings or TinkerTool System to re-enable this feature later. If you use TinkerTool System to do this, your configuration setting automatically switches back to the mode previously defined in System Settings.

> If you change your network location or the IPv6 mode in **System Settings** while TinkerTool System is running, it is recommended to restart TinkerTool System to ensure that the application shows the updated status.

4.1.5 Permission Filter for New File System Objects

> Note: This feature will not be available or visible if you are using macOS 15.0 (including 15.0.x subversions). This particular operating system version does not run stable enough to provide this feature reliably.

In the permission system of macOS, which is explained in detail in the chapter The Pane ACL Permissions (section 3.4 on page 198), each application decides for itself what rights it will grant for a new a file or folder when that file system object is being created. This also includes the Finder which is the typical application to create new folders.

Security problems could arise if you are using badly written or very old applications which don't care about permission settings. Such applications could grant write permission to the category "other users" which means that nearly everyone – no matter if the user is even "known" by the current computer – could access, overwrite, and delete each and every document created by that program. In environments where users cannot be considered to behave cooperatively, like schools or large companies, such a lax policy of granting permissions can make a system unusable. For this reason, macOS and every other UNIX system is using a *permission filter*: Whenever an application creates a new file or folder and has to set the initial permission settings, the permissions will be sent through a filter first which decides if applications are allowed to grant a specific right or not. The filter corresponds directly with the three POSIX rights **read**, **write**, **execute**, and the access parties **owner**, **group owner**, and **others**. See the chapter The Pane ACL Permissions (section 3.4 on page 198) for details.

By default, macOS uses a permission filter which is preconfigured with the following policy:

- don't allow applications to grant initial write permission for the group owner of a new object

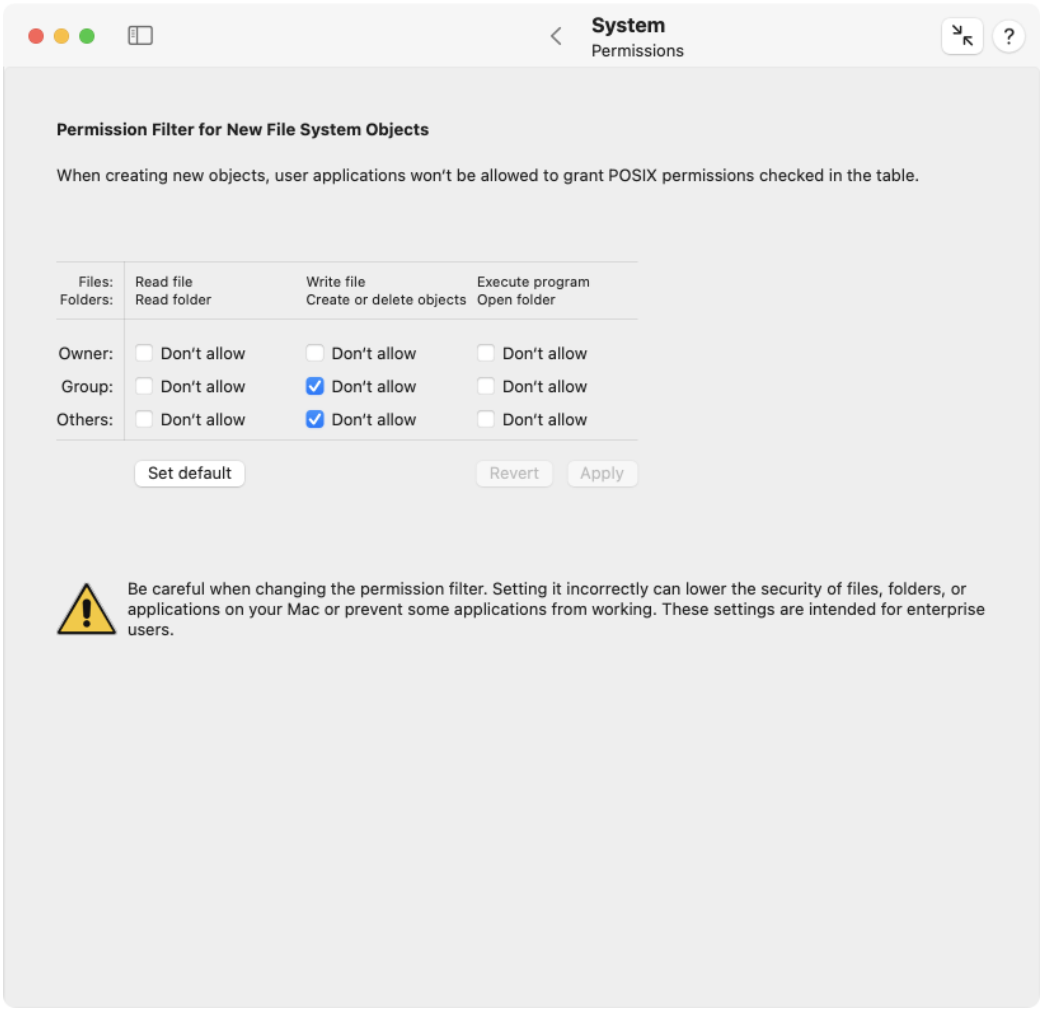


Figure 4.6: Permission Filter

- don't allow applications to grant initial write permission for other users, who are neither owner nor group owner of the new object.

Administrators can change this policy, modifying the permission filter so that the initial permissions are either relaxed or become even stricter. To modify the permission filter of macOS, perform the following steps:

1. Open the sub-item **Permissions** on the pane **System**.

2. Set or remove check marks in the table **Permission Filter for New File Systems Objects**. The lines of the table represent the three access parties **Owner, Group,** and **Others**, the columns represent the rights which should be blocked when creating new objects, namely **read**, **write** and **execute**. Remember that write permission for a folder means the right to create, rename and delete objects in the folder, and that execute permission for a folder means to browse the contents of a folder.

3. Click the button **Apply** below the table.

The change will take effect the next time you start the computer. The button **Set Default** can be clicked to return to the recommended standard filter. Clicking the button **Revert** will cause TinkerTool System to discard your changes and to display the settings currently established in the system.

Warning: It is very dangerous to set check marks in the line **Owner**. Enabling a filter option in this section means that applications will no longer have the right to access the files they just have created.

The setting only affects programs started in user sessions. Background programs of the operating system won't be affected (unless they are started as part of a user session).

There are specific circumstances where TinkerTool System detects that it won't be possible to modify the permission filter. In this case, the table is disabled and an error message appears below. The following situations can cause such a problem:

- A pending operation to change the filter is currently in progress. New values have been set to be established but the computer has not been restarted yet.

- Some third-party application is manipulating the permission filter. This could be intended by the other application but it could also indicate a defect. It won't be possible to change the filter settings until this problem has been resolved.

4.1.6 Miscellaneous

Screen Sharing

If a remote administrator uses the screen sharing feature of macOS to receive the current contents of the computer screen on her own computer across a network connection, macOS automatically tries to protect the privacy of the user currently working on the local screen: If the remote administrator connects with a user account which is *different* from the one of the local user, the screen session won't begin immediately. Instead, the accessing user is asked whether he likes to work on his own, separate screen, or if the local user should be asked to grant permission that the remote user can see and take over the current screen. The local user could have private or confidential information on screen, so this behavior will protect the displayed data.

In some cases, this policy may not be useful. You can disable this privacy feature as follows:

1. Open the sub-item **Miscellaneous** on the pane **System**.
2. Click on the item **Permit clients to take over frontmost screen session**.

> You should check if this policy is compliant with local laws and the guidelines of your organization, if applicable.

FileVault Options

If you enabled FileVault on your computer, the entire system volume will be encrypted by a secure key and a password will be necessary to unlock and decrypt the disk. When the computer is switched on, the operating system cannot start immediately, because the Mac cannot read the encrypted disk. Instead, the computer's firmware and some parts of the unencrypted preboot volume present a special login screen (which resembles the login screen of macOS). Users have to log in here first, and for entitled users, the secret decryption key will be unlocked, which is then used to decrypt the operating system volume and to launch macOS.

At this stage, it is known that the user who unlocked the disk must also be a valid user of macOS, so the firmware *passes* the name and password of this user to the operating system, performing an automatic login, hereby avoiding to ask for credentials a second time. For this reason, the activation of FileVault automatically enables the automatic login feature of macOS, too.

In some cases, this behavior might not be intended. macOS supports a special feature to uncouple the decryption of the FileVault disk from the initial login upon start of the operating system:

1. Open the sub-item **Miscellaneous** on the pane **System**.
2. Click on the item **Use separate logins for disk decryption and first user session**.

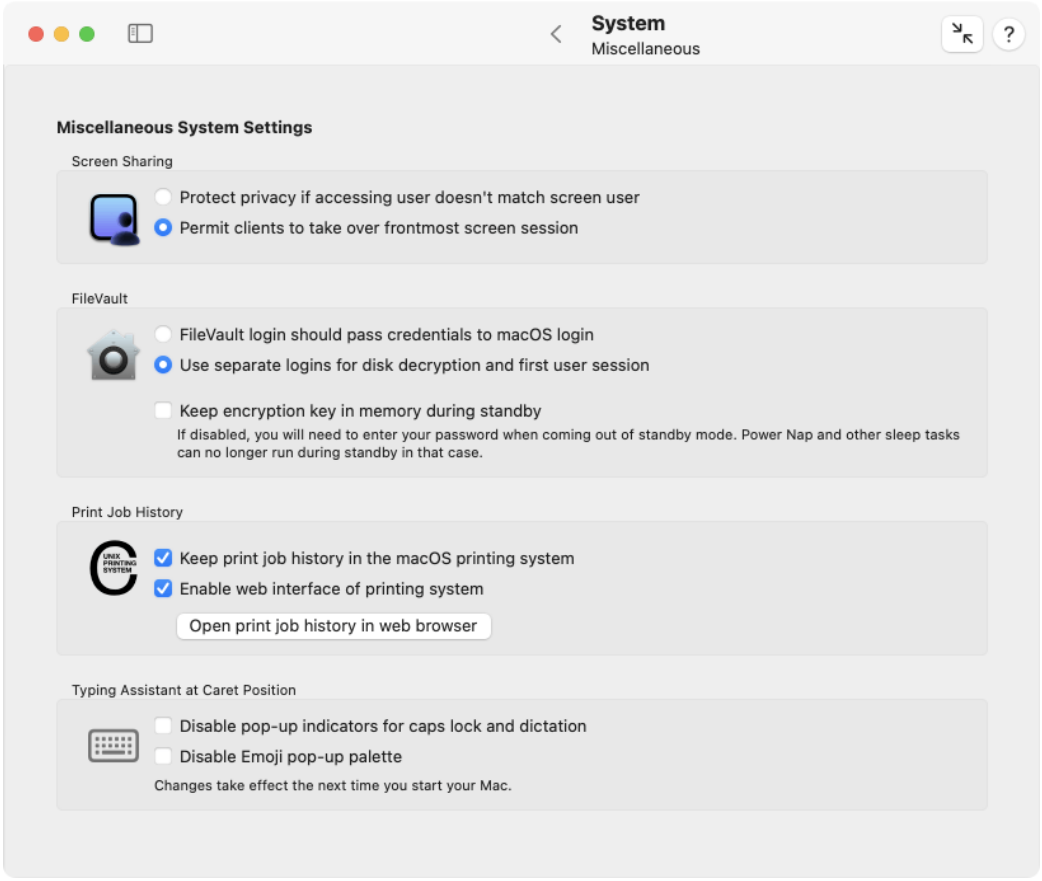


Figure 4.7: Miscellaneous System Settings

You can also enable an advanced security feature of FileVault for cases where this is needed. To guarantee continued access to storage media, your Mac must always keep the key for disk encryption in memory in order to successfully process any block on the disk the operating system needs to read or write. That includes time periods where your Mac enters sleep and standby modes. This is necessary to ensure that the Mac can still perform regular maintenance tasks when not being fully switched on and to execute Power Nap functions.

This policy maintains a certain comfort level, but can become an issue should your Mac be stolen, when an attacker tries to get direct memory access by connecting special hardware devices to the sleeping Mac. In theory, the disk encryption key could be disclosed this way.

By removing the check mark **Keep encryption key in memory during standby** you can avoid this possible method of attack. If this option is not checked, macOS will destroy the FileVault key in RAM when the system enters standby mode. In this configuration, your Mac will no longer have disk access during standby, so Power Nap and similar maintenance features will no longer be active regardless how you have configured them.

Print Job History

The printing features of macOS are implemented by *CUPS*, the *Common Unix Printing System*. By default, macOS keeps a log of all print jobs ever processed by the local computer, the *print job history*. TinkerTool System can disable the log if desired, and it can show you the records currently in the log. To change the system setting for keeping print job records, perform the following steps:

1. Open the sub-item **Miscellaneous** on the pane **System**.
2. Set or remove the check mark **Keep print job history in the macOS printing system**.

The log can be reviewed by clicking the button **Open print job history in web browser**. TinkerTool System will delegate this task to your preferred web browser. Web access to the printing subsystem is inactive by default in several versions of macOS. By using the option **Enable web interface of printing system** you can control whether web access should be possible or not.

Typing Assistant at Caret Position

As of macOS 14, Apple introduced new pop-ups when typing text, which are displayed right next to the cursor, at the insert position of the text. Many users find these pop-ups annoying. You can turn them off with TinkerTool System, which is done system-wide (for all users of the computer). Two system settings are available:

- the pop-up for the Caps Lock key (capital letters) and for text dictation
- the pop-up of a palette with suggestions for emojis when you have entered appropriate text and open the menu item **Edit** > **Emoji & Symbols** or press the corresponding keyboard shortcut.

Perform the following steps to change these system settings:

1. Open the sub-item **Miscellaneous** on the pane **System**.
2. Set or remove check marks at **Typing Assistant at Caret Position**.
3. Restart your Mac if you like the change to take effect immediately.

4.2 The Pane “Always On” Mobiles

The pane **“Always On” Mobiles** is only visible if you are using TinkerTool System on a mobile Mac with “always on” behavior and an Intel processor. On mobile Macs with Apple Silicon, please use the following chapter The Pane Portables (section 4.3 on page 265).

4.2.1 Automatic Power-On (Intel)

Some of the portable computers introduced by Apple at the end of 2016 no longer have a dedicated power key. They simulate to be “always on” and have no control lights on the case or on the power connector. The system starts up as soon as you open the display lid. Some users prefer the classic behavior, however. TinkerTool System gives you access to a hardware setting that controls this. Instead of sending a “power on” signal, opening the lid or connecting a power adapter can alternatively trigger to briefly show a battery status indicator on the display screen.

Perform the following steps:

1. Open the pane **“Always On” Mobiles**.
2. Choose one of the items at **Auto Power On**.

The battery indicator is shown by the firmware. When automatic power control is off, the Touch ID button will work as a power key. Press it briefly to switch the system on.

4.3 The Pane Portables

The pane **Portables** is only visible if you are using TinkerTool System on a portable Mac with Apple Silicon running macOS 15.3 or higher. On older Mac laptops with Intel processors, please use the preceding chapter The Pane “Always On” Mobiles (section 4.2 on page 265) instead.

4.3.1 Automatic Power-On

Modern portable Macs no longer require a power button. These devices are designed to remain powered on at all times. If they happen to be shut down or turned off, they will automatically restart and turn on again when either the display lid is opened or an external power source is connected.

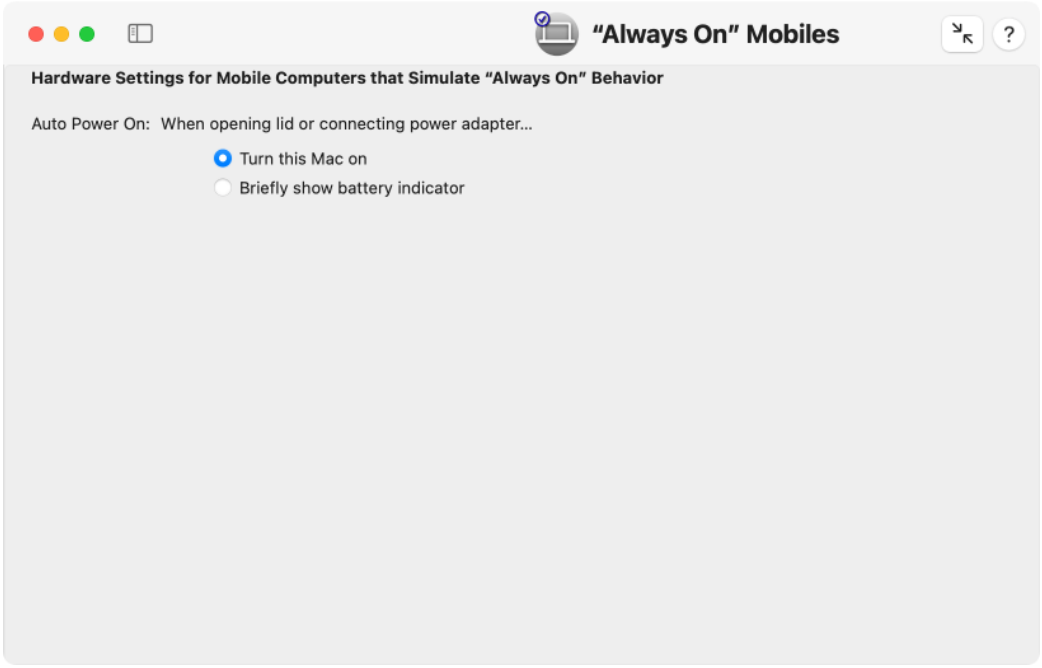


Figure 4.8: Settings for the automatic power-on feature

In some situations, this behavior may not be desirable, for instance, if you want to clean your computer. TinkerTool System provides the option to modify the startup behavior with a simple mouse click.

Perform the following steps:

1. Open the pane **Portables**.
2. Enable or disable the checkboxes of the options **Turn on and start this Mac when** as desired.

The device will also turn on if any key is pressed. This behavior *cannot* be disabled.

4.4 The Pane Startup

The pane **Startup** is designed to manage special settings of the operating system or of the computer's firmware, which won't affect normal operations, but only the startup phase of macOS.

4.4.1 Notes on Macs with Apple Silicon

Macs with Apple Silicon use a different startup sequence and technical design as Macs with Intel processors. The following options won't be available if you are using a Mac

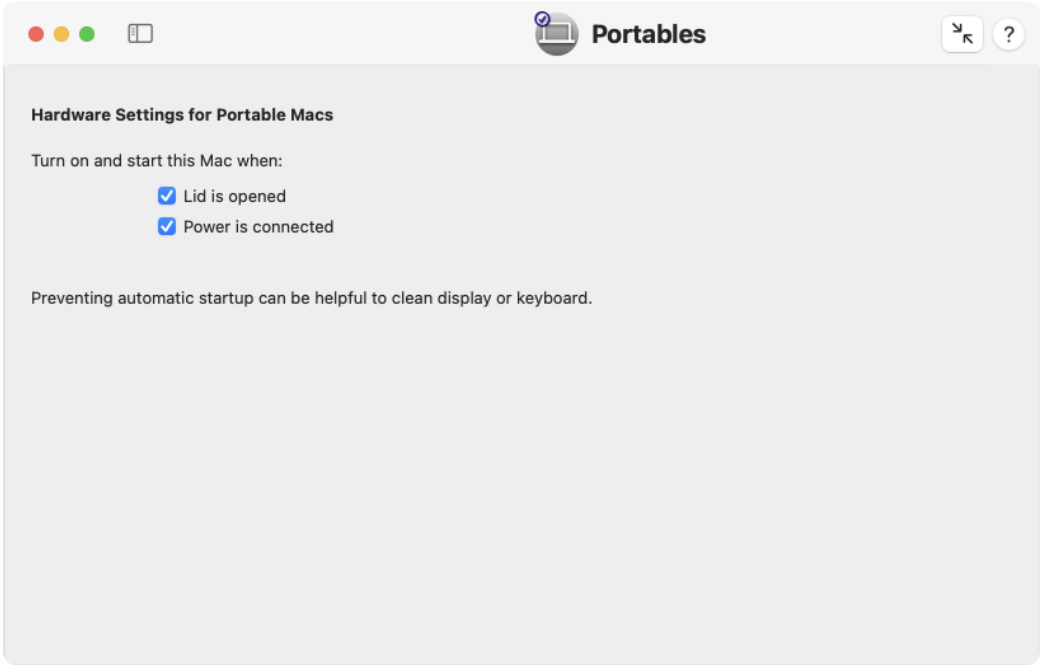


Figure 4.9: Settings for automatic startup

with Apple Silicon:

- Startup Mode
- Use special OS for next start
- Optimize system for server operations
- Diagnostic options

4.4.2 Options

macOS is supporting different startup modes that can be preconfigured with TinkerTool System:

- **Normal start:** the default setting. The operating system will start with graphics mode and all features enabled.
- **Verbose mode:** macOS will display text messages when executing the first phase of the startup, the start procedure of the kernel. After that phase, the system will switch back to graphics mode and continue normal operations. Shutting down the system will also be accompanied by diagnostic messages in text mode.

> macOS can also start in *Safe Mode* which means that it will start normally, but only with a minimum set of features enabled. All third-party startup components like drivers, kernel extensions, or background services will remain inactive. This mode is helpful if you installed bad system software or drivers which prevent macOS from starting up correctly. In addition, nearly all system and user caches will be cleared. Safe mode can be activated temporarily by holding down the shift key (⇧) during startup. It does not make sense to enable Safe Mode permanently.

In addition to these startup modes for the launch of the main operating system, you can instruct your Mac not to choose the main system for the next restart, but to select a special operating system for maintenance purposes. This selection takes effect only once, for the following startup. Available options are:

- **Not enabled:** The normal operating system will be started.
- **Recovery system:** The mini operating system to recover the main operating system will be started from the disk of the local computer. If multiple operating systems are available, the Mac will select the recovery system associated with the current startup volume.
- **Recovery system via Internet:** as before, but the system will be loaded from Apple's servers in the Internet. A working Internet connection is required. With this setting, it will be possible to even conduct maintenance operations if the built-in disk of the Mac is defective or it should be erased completely.
- **Apple Diagnostics:** The application for testing the hardware of the individual Macintosh model will be launched from the disk of the local computer. This program allows a quick assessment whether all components of the Mac are working correctly.
- **Apple Diagnostics via Internet:** as before, but the application will be loaded from Apple's servers in the Internet. This way you can check the hardware even in cases where the diagnostic program on the local disk has been damaged.

Power Control Options

Modern versions of macOS are optimized to detect whether a real user or another external event is waking a Mac from sleep mode. If not an actual person sitting in front of the screen is responsible for the wake-up, the screen can remain dark. This saves energy and avoids unwanted light effects. Such a "dark wake" happens if, for example, a client in the network accesses a service of the sleeping Mac, or a mobile device is attached to one of the Mac's USB ports to charge it.

For some use-cases however, it might be desired to wake the Mac "fully", i.e. together with its screen, and keeping it active for a longer period of time. One example would be a Mac working as a multimedia player, mounted together with a TV at a poorly accessible place, and configured to be activated remotely via network. It should be possible to wake

the Mac without the keyboard to play a movie and keeping it switched on for some time. To achieve such a behavior, set a check mark at **Don't leave screen dark if woken by network request or mobile device**.

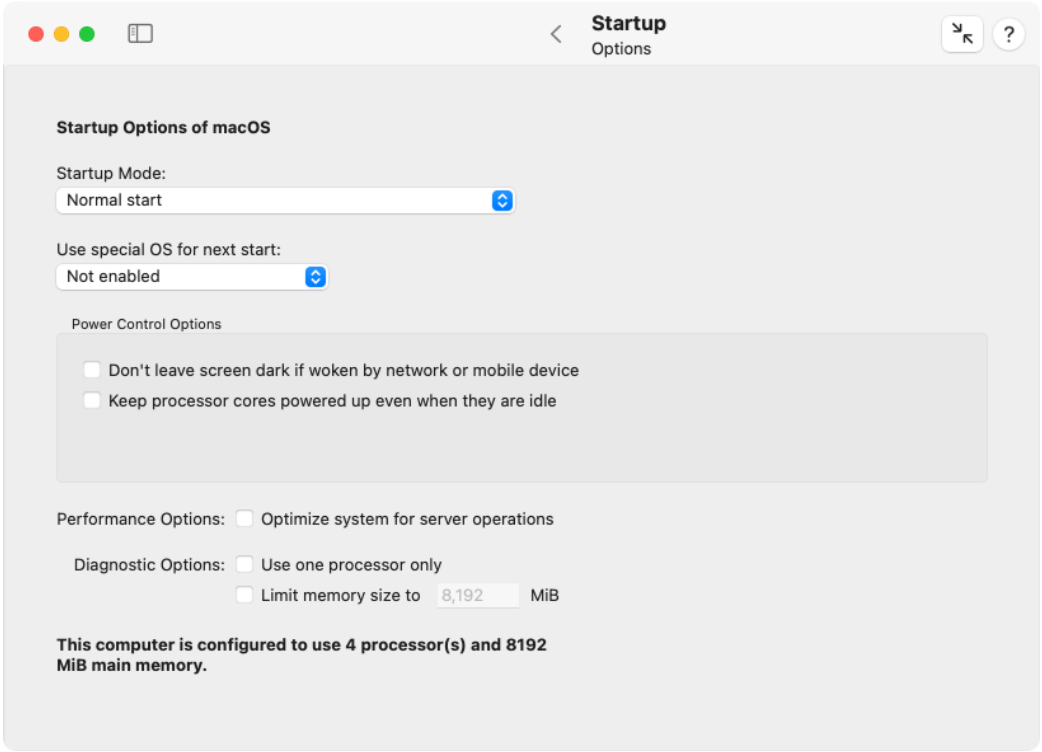


Figure 4.10: Startup options

Keep processor cores powered up even when they are idle: By default, modern computers shut all processor cores down which are currently not in use. "Not in use" means that the process scheduler has not enough jobs to keep all cores busy for a complete scheduling time slice, which usually lasts 10 milliseconds. For the time period where there is nothing to do (processor load per core is less than 100%), the affected cores will be powered down into sleep mode. Keeping the cores always powered up is mainly useful for diagnostic purposes only. It has no positive effect on system performance. The system might consume significantly more energy and produce more heat when this feature is activated.

Performance Options

macOS can reconfigure its kernel to optimize itself for working as a server. This means certain system parameters, like the strategy for reserving network and file caches, or the multi-threading characteristics will by modified in a way so that typical server applica-

tions gain better performance. Such server applications typically run without a visible user interface in the background and use many threads mainly doing network and file operations. On the other hand, a standard installation of macOS is usually optimized to give the frontmost application running on the graphical user interface the best speed behavior.

If you like to change the default and give typical server jobs better performance, set a check mark at **Optimize system for server operations**. After restarting the computer, the kernel will respect the new setting.

> Apple may change the exact meaning of this setting any time without further notice.

Diagnostic Options

Additional options are available for diagnostic purposes:

- **Use one processor only:** causes the operating system to only use one CPU core in case more than one processor (or core) is available in the system.
- **Limit memory size to:** macOS can be forced to use less RAM than is available in the system. Using this feature can be helpful for software developers to simulate the effects of low memory situations. It can also help to diagnose problems with defective memory modules.

Changing Options

To use one of the listed options, perform the following steps:

1. Open the sub-item **Options** of the pane **Startup**.
2. Activate or deactivate the listed options as desired.

4.4.3 Job Overview

When the operating system is starting and the user logs in, a high number of system services and user applications is started automatically. TinkerTool System can help you to get an overview of all automatically starting components which become effective for your personal user account. It will also analyze all auto-starting jobs, comparing their configuration entries with their current status. If a mismatch is found, the application will warn you. This way, you can easily detect invalid or outdated configuration entries. Additionally, you can see whether specific jobs have failed due to technical problems, or if the operating system was forced to stop system services due to temporary lack of memory.

To let TinkerTool System create a report of all automatically starting jobs, perform the following steps:

1. Open the sub-item **Job Overview** of the pane **Startup**.
2. Click the button **Create report**.

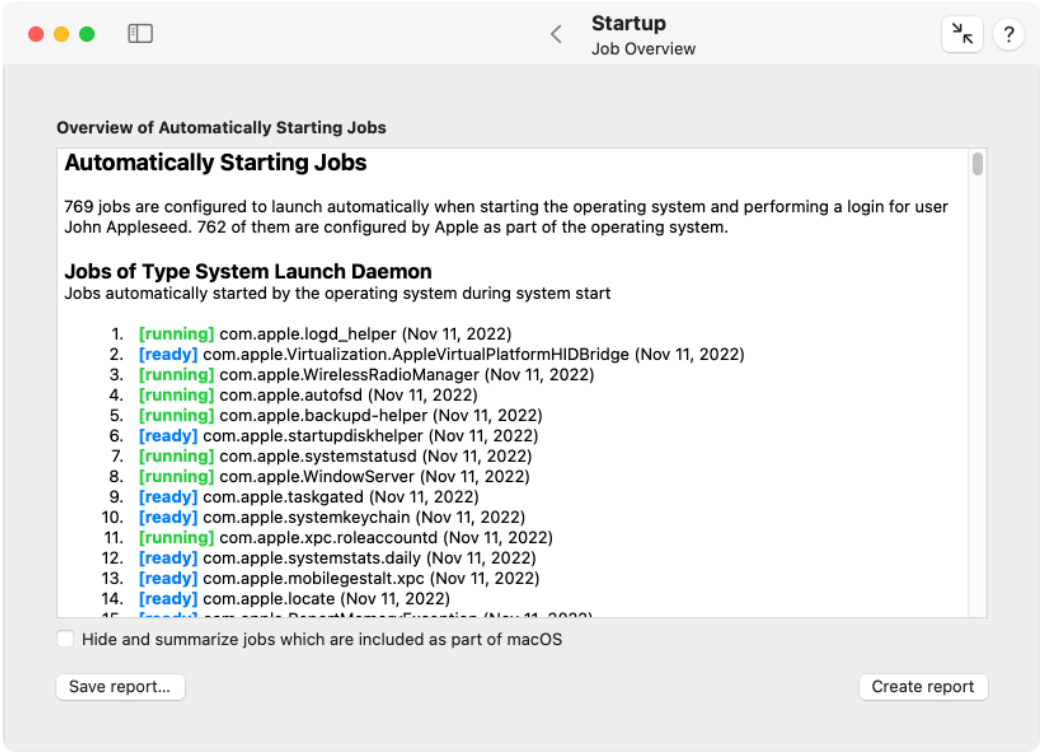


Figure 4.11: Overview of all automatically starting jobs

After a few seconds, the report will appear in the text view. By using copy/paste, you can transfer it into other applications if necessary. To filter out all "normal" jobs which are preconfigured by Apple and are a standard part of the operating system, set a check mark at **Hide and summarize jobs which are included as part of macOS**. You can save the report currently shown in the window by clicking the **Save report**… button.

The configuration of auto-starting jobs is part of different launch behaviors and different realms: So-called *daemons* are services running in the background which can launch as soon as the operating system is running, even when no user is logged in yet. So-called *agents* are background services that run for each user session. They can launch as soon as a user has logged in, and are automatically quit when that user logs out. If multiple users are logged in, multiple sets of agents run simultaneously for each session. Daemons and agents can be defined by the operating system itself *(system)*, or as third-party entries for all users of the computer *(computer)*, or for a particular user *(user)*, a case which is then of course limited to agents.

A user can also add and remove auto-starting applications herself, using the setting **Login Items** in the **General** pane of **System Settings**, or via the context menu of the Dock.

Apps sold in the Mac App Store have no permission to touch any of the daemon, agent, or login item settings. This is monitored by Apple and additionally enforced by technical means built into macOS. However, if a feature of such an App needs to control whether the App or parts of it should launch automatically after the user has logged in, it first has to ask the user for explicit permission (e.g. by changing a preference setting within that App), and then has to send a specific request to macOS to register the auto-starting component. If the request is OK, macOS will store the auto-start wish in an internal database, hidden from the user, only visible to the App that requested it. TinkerTool System uses the term *Service Login Item* to refer to such special configuration entries for Apps.

> If macOS or the managing application modifies the configuration of a service login item for a user account, the change will not become visible in TinkerTool System until this user logs out.

For each job that is currently configured to launch automatically, TinkerTool System shows the following entries:

- a sequence number, which makes it easy to count all entries and to refer to them,
- the current status of the job when the report was created,
- the identification name macOS uses internally to manage the configuration entry,
- the date the automatically starting program has been modified the last time.

The different status entries, which are shown with color markings and between square brackets, have the following meaning:

- **user-controlled:** this entry has been created by the user. The user also controls when to quit the auto-started component.

- **canceled:** the operating system auto-launched the job, but stopped the running process later, because the computer experienced very high memory pressure due to lack of RAM, and the affected job is not absolutely necessary for the computer's operation. When this happens, the system may run slower than normal, and some features may be limited. It is recommended to use the function **Diagnostics > Evaluate RAM size** of TinkerTool System to find out whether you should purchase more RAM to let your computer cope better with your typical workload.
- **failed:** the operating system auto-launch the job, but the associated program stopped with an error code. There appears to have been a technical problem which caused the job to fail.
- **running:** the job was started automatically and is currently running.
- **ready:** the job is correctly configured to start automatically, but is currently not running. This is normal for jobs that only run it certain situations, at specific times, when specific events occur, when specific hardware devices are connected, etc.
- **switched off:** the job is generally preconfigured to be started automatically, but a setting in the operating system explicitly deactivates this job. This is normal for services that should only run in specific cases, for example after certain features have been switched on.
- **inactive:** the job has a configuration entry for automatic start, but the operating system has rejected to register this entry for some reason. This is usually uncritical and the exact reason has not been determined by TinkerTool System.
- **finished (single run):** the job is configured to be started automatically, but it fulfills a certain task which needs to be done only once at startup, so the process can quit as soon as its work has been completed. Everything was executed correctly and the job is no longer running at the moment.
- **invalid (no executable):** the job is configured for automatic start, but could not run because the associated program is missing. TinkerTool System has determined that this configuration entry is invalid. In most cases, such a problem is caused by deleting an application without uninstalling it correctly.

> Unfortunately, it has become a habit that Apple ships the operating system with some incorrect configuration entries. If TinkerTool System detects a job with abnormal status which relates to one of these known issues (which are usually uncritical), it will indicate this by the additional message line **Note: This is a known defect of the running operating system and thus "normal"**.

Removing invalid auto-start entries

TinkerTool System can automatically remove invalid entries for automatically starting jobs in cases where its analysis has confirmed that it will be absolutely safe to do so. If one

or more of such entries have been found, the additional button **Resolve problems**... will become visible at the bottom of the window. These are usually cases where an outdated entry had been left on the system because its associated application had been deleted without correctly uninstalling it first.

After clicking the button **Resolve problems**..., TinkerTool System will show a table with all invalid entries that can be safely removed. When clicking on lines in the table, detail information will be shown. Click either the button **Clean selected entry** to fix a problem with the job currently selected, or the button **Clean all entries** for all entries currently shown in the table.

> When cleaning invalid entries of type *service login item*, special conditions apply: Apple has specifically designed these entries in a way to ensure that they should only be accessible by the Apps that created them. It is possible for TinkerTool System to override this protection, but this is not recommended and should only be used as a last resort. To remove a bad entry for a service login item, it is recommended to reinstall the App shown as "managed by..." at the entry in the job overview report, and then to use the preference settings within that App to disable its autostart features.

If invalid entries of type *service login item* are in the list, TinkerTool System will ask you whether they should be considered during the clean-up procedure or not.

> To remove invalid login items, use the respective feature of the pane User (section 5 on page 293).

4.4.4 NVRAM

> This feature is only available for Macs with Apple Silicon processors. It is not necessary on Intel-based Macs.

The *NVRAM (Non-Volatile Random Access Memory)* is used on each Mac to store settings permanently that should become effective for the entire computer and all installed operating systems. The part of the memory visible to the user is sometimes also called *Parameter RAM (PRAM)*.

Settings that can be stored in NVRAM include sound volume, display resolution, startup-disk selection, time zone, and information on recent system crashes. The settings stored in NVRAM depend on your Mac and the devices that you are using with your Mac. If you experience issues related to these settings or others, resetting NVRAM might help.

On classic Macs, NVRAM can be reset directly when switching on the computer by holding down a specific key combination. Modern Macs with Apple Silicon no longer have this feature. TinkerTool System can help here, by deleting as many settings from the NVRAM as possible. Which exact settings this will be in a specific case will depend on the current security settings of the Mac, in particular for System Integrity Protection. Perform the following steps to execute the procedure to erase the NVRAM:

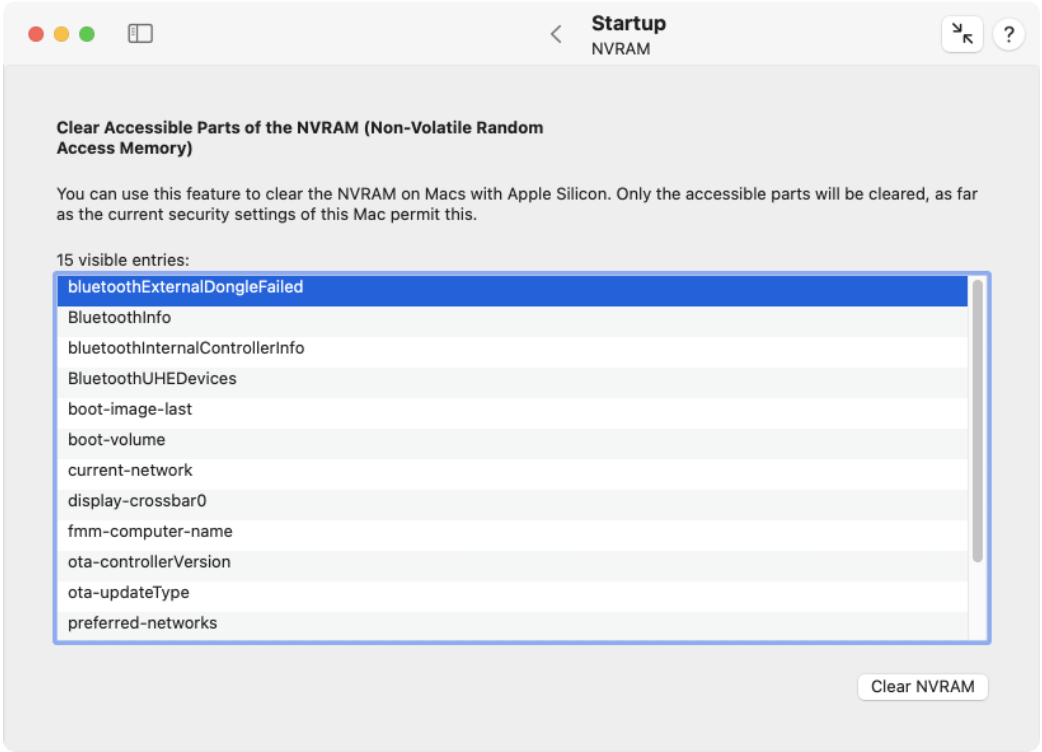


Figure 4.12: Clear the NVRAM

1. Open the sub-item **NVRAM** of the pane **Startup**.
2. Click the button **Clear NVRAM**.

You can review the visible parameter settings of the NVRAM in a table before and after the delete operation.

4.4.5 FileVault

FileVault, more precisely *FileVault 2*, is the name of Apple's technology of being able to encrypt the startup volume of a Macintosh, although the operating system is stored at that location together with the user data. At startup, macOS is not yet available, since it is on the encrypted volume at that point in time, so a second login with a second administration of users must be set up, which is only connected to the macOS user administration after its decryption and its launch.

In modern Macintosh model series, the built-in flash memory is always encrypted, even if FileVault is switched off (see also the chapter The pane APFS (section 3.7 on page 232), section APFS Keys). FileVault only has to take care of the encryption process on older Macs. The actual capability of FileVault is to manage a user login before macOS even starts, hereby granting access to the keys needed for decryption. FileVault can therefore be viewed as an upstream mini operating system that controls which users can decrypt and start the actual operating system.

TinkerTool System indicates these two aspects separately in the upper half of the window of the **FileVault** feature:

- **Encrypted startup volume**: indicates whether the volume group containing the running macOS and user data is encrypted
- **User management for startup decryption**: specifies whether FileVault login precedes the startup of macOS

Access to FileVault data in the lower half of the window is protected by macOS and only becomes active after an administrator has enabled it by clicking **Fetch user list**. It is also necessary that FileVault is enabled.

The table **FileVault User Accounts** lists all macOS users that should be included in the FileVault login. The item **Personal recovery key** indicates whether a special key was stored when FileVault was enabled, which allows the start volume to be decrypted by entering a text code in case of an emergency, even if all registered user accounts are failing.

A personal recovery key is a readable code based on the pattern

```
ABCD-EFGH-IJKL-MNOP-QRST-UVWX
```

which can be archived permanently in a text file or on paper for emergencies. Alternatively, the recovery key can also be stored in Apple's iCloud. In this case, however, it will be bound to an Apple Account.

Another alternative especially for large organizations is to create a master key for FileVault that fits all Macs, instead of maintaining a separate key for each individual device.

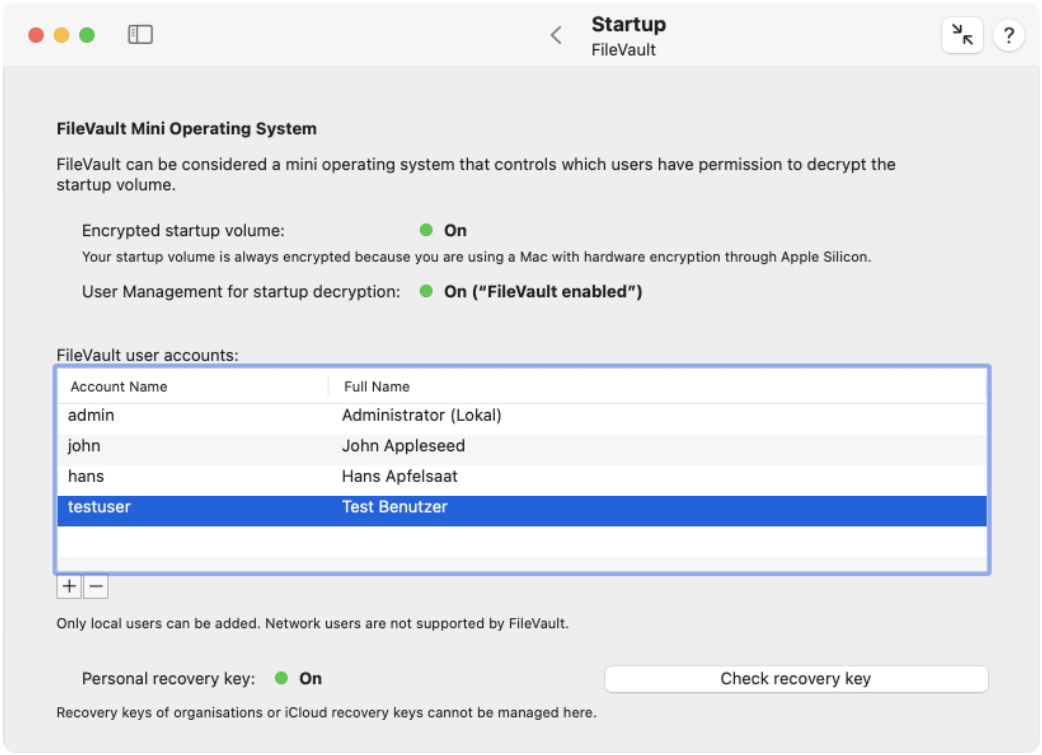


Figure 4.13: TinkerTool System indicates the status and user management of FileVault. If available, a personal recovery key can also be tested.

> Such institutional keys or iCloud keys are not shown by TinkerTool System.

Managing FileVault users

As mentioned, FileVault user management must be separate from macOS user management for technical reasons. You can add or delete accounts to FileVault with the two buttons + and – below the user table.

To delete users from FileVault, select one or more of the affected rows in the table and click –.

To add users to FileVault, several prerequisites must be met:

- You need to know which user account is currently considered the primary FileVault account. This is usually the account that initially set up FileVault and is shown at the top of the table. However, this could have changed later when user accounts have been erased.
- You need to know the macOS password for the primary FileVault account.
- You must also know the macOS passwords for any user accounts that you subsequently add to FileVault.

If the prerequisites are met, perform the following steps:

1. Press the + button below the user table.
2. From the list of local macOS users, select the ones that should be added to FileVault and click **Continue**.
3. Enter the name and password of the primary FileVault account and click **Continue**.
4. Enter the appropriate password for each user that will be added and click **Continue**.

If adding users was successful, the results will be shown in the table.

> The FileVault mini operating system is not capable of working with directory servers. Therefore, only local users of this Mac can be added, not network accounts.

Checking a personal recovery key

If you use multiple Macs or have managed multiple Macs over the years, you may have kept a lot of notes about personal FileVault recovery keys. In practice, uncertainties can easily arise here as to whether an archived key actually fits a specific Mac. This can be checked quickly with TinkerTool System:

1. Click **Check recovery key**.
2. Enter the text code of the key when the program asks for it.

You will then be informed whether the key fits this Mac or not. As mentioned, institutional master keys or iCloud keys cannot be validated this way.

4.5 The Pane Login

The pane **Login** controls system preference settings for the login screen that shows the entry fields for name and password before an actual user session can begin. macOS will only use a login if you haven't configured it to perform an automatic login with a predefined user account. You can enable the login by using the sequence **Users & Groups** > **Automatically log in as**... > **Off** in System Settings.

> macOS also uses automatic login if you have enabled the *FileVault* feature to encrypt the system disk. In this case, the firmware uses its own built-in login screen, asking for the password, which is then used to decrypt and start the operating system. The password is hereby passed from the firmware to the system, avoiding that it has to be entered twice. You cannot disable automatic login in this case, so the login screen won't be used. The alternative login screen is not part of macOS and cannot be customized via TinkerTool System.

Options you modify on the **Login** pane of TinkerTool System will take effect immediately. To return the login screen settings to the factory settings defined by Apple, click the button **Reset all to defaults** at the lower right corner of the window. Note that clicking this button will affect the options on all tab items offered by the **Login** pane, not only the options visible in the front item. The only exception are the "hide" settings for local user accounts, because resetting them requires a special type of login. More details can be found in the following sections.

4.5.1 Settings

The first tab controls the basic style and advanced features of the login screen. You can switch between using

- **Name and password text fields** and
- **List of users able to use this computer**.

If the latter option is selected, you will be able to further influence which users should be included in the list:

- **Show local users:** the "normal" user accounts configured on the current computer.
- **Show mobile accounts:** these are special users, managed by a directory service, which are using both a home folder on a central file server, and an automatically synchronized home folder on a mobile notebook computer.
- **Show network users:** the user accounts known in your network. Your computer must be configured to use a network directory service with a search path for user accounts in order to use this feature.
- **Show computer's administrators:** the user accounts configured on the current computer which have administrative permission.

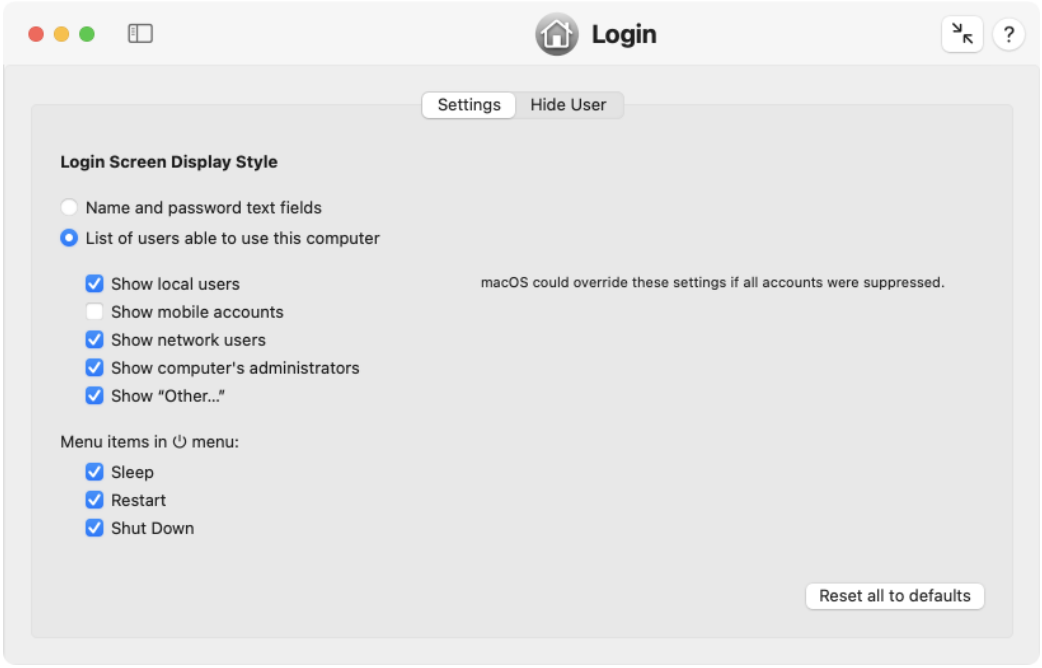


Figure 4.14: Login screen settings

- **Show "Other...":** a special button with the label "Other" which can be used to manually switch to name and password text fields.

Depending on the list of user accounts found on the local system and in network directory services, the login screen may choose to ignore one or all of the above settings. This is necessary to guarantee that at least one user can successfully log in. Otherwise, it could happen that the list is empty and the login screen would become unusable.

However, you should not rely on this safety feature. Depending on operating system version and the user accounts available on your computer, disabling too many user categories could cause the system to no longer offer "useful" logins. In case of emergency, you can use the utility TinkerTool System for Recovery Mode (section 2.8 on page 104) to reset the login screen to factory defaults.

Power control settings

Additional options allow the control which menu item should be shown in the power menu in the upper right corner of the login screen:

- **Sleep:** the menu item used to manually switch to sleep mode,
- **Restart:** the menu item used to restart the operating system,
- **Shut Down:** the menu item used to switch the computer off.

4.5.2 Hide User

macOS supports a feature to hide selected user accounts in case you had activated the display style **List of users** for the login screen. This can make sense to keep the list clean, offering "real" users in the list only, not some special accounts which might have been created for administrators, technicians, or other service tasks. Such role accounts can still log in via the **Other** button in the list.

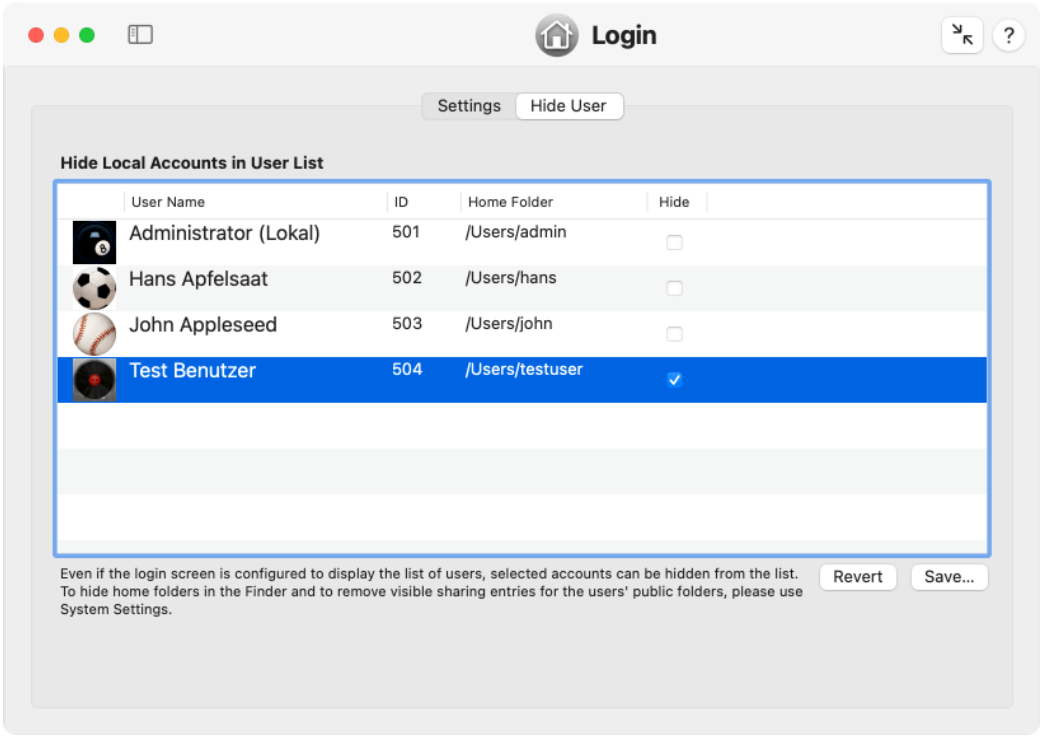


Figure 4.15: Hide accounts in the login list of users

TinkerTool System shows all local user accounts which belong to standard users that have permission to log in, on the tab item **Hide User**. The accounts are sorted by their

numerical identification codes which usually match the order in which they have been created. To hide a user, set a check mark in the column **Hide** and click the button **Save**… to store your settings.

After clicking the save button, TinkerTool System will ask for name and password to authenticate with the Open Directory account database on the local computer. Although you can use the same names and passwords of administrative users as in standard login situations, this type of login is technically different.

> In this particular case, it is actually TinkerTool System, **not macOS,** asking for the password. The credentials are then verified by the Open Directory subsystem which will grant or deny permission, depending on the results.

To undo changes which have not been saved yet, click the button **Revert**. TinkerTool System only offers local user accounts in the list, not network users which might be stored on other directory services.

The hidden user accounts may still be visible indirectly, e.g. by their private home folders at **/Users** and by their individual entries for file sharing. To hide these items as well, experienced administrators can additionally do the following:

1. Move the affected home folder of the hidden user to an invisible Unix folder, for example inside **/var**. Then open **System Settings** > **Users & Groups**, right-click the affected account, and select **Advanced options** in the context menu. Set **Home directory** to the new location of the user's private folder.

2. Open **System Settings** > **General** > **Sharing** > **File Sharing** > **i** and remove all entries in the list **Shared Folders** which should no longer be active.

4.6 The Pane Application Language

All parts of macOS and many applications of third-party vendors are multi-lingual. This means the user interface of an application can be switched between different languages without having to install special language-specific versions of the program. Under normal circumstances, the language that will be used by an application is determined when launching it. macOS checks the available language support packages embedded in the application and compares it to the user's priority list of preferred languages. The first language in the list which matches a language package available in the application will "win" and will be chosen to become the active language for running the program. Each user can modify her personal priority list at **System Settings** > **General** > **Language & Region** > **Preferred languages**. You can add all languages you like to use with the **[+]** below the language table, and the drag the languages into your preferred order of priority. The first language in the table will become your primary language.

TinkerTool System allows you to temporarily ignore your personal language priority list, forcing an application to launch in a specific language, different from your usual preferred one. Neither your language settings, nor the language packages within the application will be touched. This can be very helpful if you are working in a multi-lingual

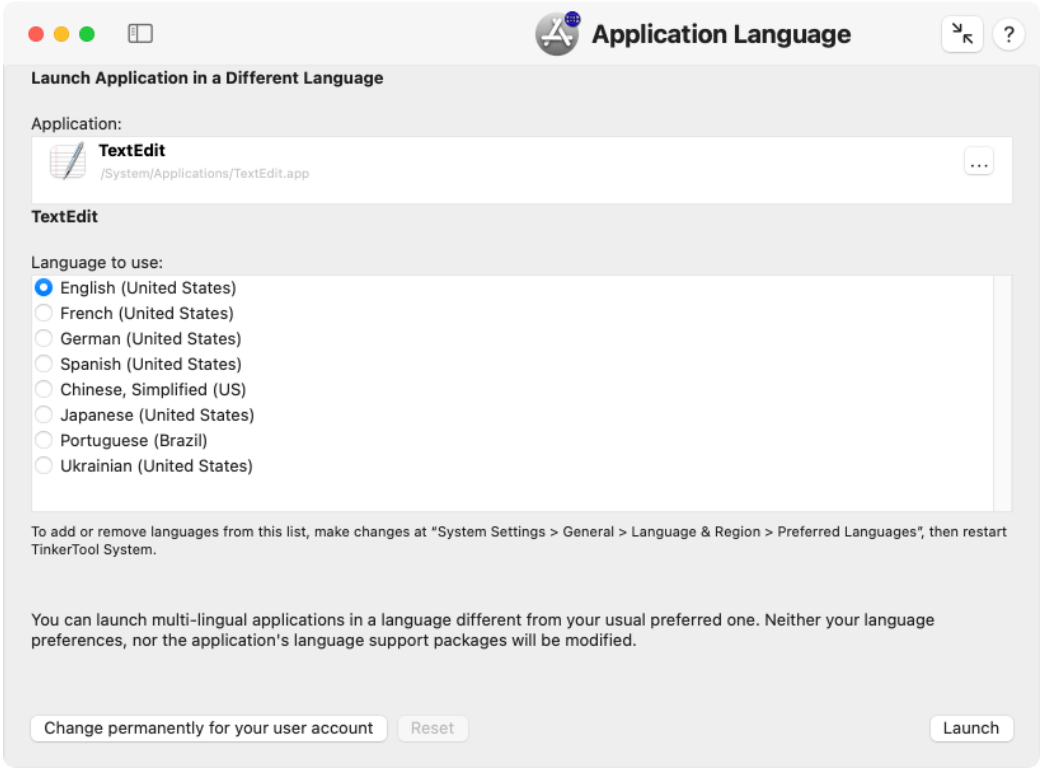


Figure 4.16: Application language

country or organization. This is also helpful to give remote support to a user which has configured his macOS setup for a language different from yours. You can even run the same application multiple times, using different languages in each instance.

> Some applications might not be prepared to run concurrently in the same user session. Conflicts can arise when the multiple instances modify the same configuration files, so you should be careful when changing data. Please check the documentation of the applications for possible information.

Perform the following steps to launch an application in a specific language:

1. Ensure that all languages you like to work with are shown in the table **Preferred languages** of **System Settings** as mentioned above. If not, edit the table and relaunch TinkerTool System.

2. Open the pane **Application Language**.

3. Drag the application from the Finder into the field **Application**. You can also click the button [...] to navigate to the object, or click on the white area to enter the UNIX path of the object.

4. Select the language, clicking on one of the buttons in the list **Language to use**.

5. Click the button **Launch**.

> If the application you are launching does not provide support for the language you have selected, the application's standard language will be chosen. This is usually the language the application was originally developed for.

Known limitations

As of macOS 14, Apple established a security feature called *Launch Environment Constraints*. This function makes it possible that applications can restrict which other applications can launch it. Depending on the current safety policies of Apple, the environment constraints for the operating system itself may be set up in an extremely strict fashion: In some cases, macOS may not allow that TinkerTool System can launch applications that are made by Apple and are a built-in part of the operating system, like TextEdit, for example. In such a case, macOS will immediately cause an intended crash of the Apple application as soon as you have launched it via TinkerTool System.

If you are affected by this, you will not be able to use the respective Apple application with a temporary language setting. Alternatively, you can briefly change the language for all applications using **System Settings**, over override the language for that application permanently.

4.6.1 Permanently overriding the launch language for a specific application

The feature outlined in the previous section requires that you are using TinkerTool System to launch an application. In some cases, you might like to *always* start a specific application in a different language, for example if the translation for this application in your default language is bad, so you want to use an alternative language each time you run the program.

TinkerTool System can store preferred language settings for specific applications in your user account. After such a preference has been set, macOS will automatically launch the selected application in your personally preferred language, independent of your default language priority settings. You won't need TinkerTool System to launch the application. Perform the following steps to store such a preference:

1. Ensure that all languages you like to work with are shown in the table **Preferred languages** of **System Settings** as mentioned above. If not, edit the table and relaunch TinkerTool System.
2. Open the pane **Application Language**.
3. Drag the application from the Finder into the field **Application**. You can also click the button [...] to navigate to the object, or click on the white area to enter the UNIX path of the object.
4. Select the language, clicking on one of the buttons in the list **Language to use**.
5. Click the button **Change permanently for your user account**.

You can remove such a language override any time. Just drag the application into the pane again and click the button **Reset**.

> Although the override button is shown on a pane of the category **System Settings**, it is actually a user preference. The override takes effect for your user account only, not for the entire system.

4.7 The Pane Cloud Protection

Apple offers a range of services under the name *iCloud* that make it possible, among other things, to synchronize data stored on one computer automatically via Internet with other Apple devices of the same user. So when saving a file on one of the participating devices "into the cloud", a copy of that file will then appear on all other devices.

If you store data about other individuals on your computer for more than just private purposes, e.g. the dates of birth of members of a sports club, you must observe special legal rules and due diligence when handling this data, depending on the country in which you are located. In general, personal data may not be passed on to third parties unless you have the express consent of each person concerned. The processing of such data by a third-party service provider may also be permitted if

- you have concluded an individual contract with that provider, in this case called *processor*, which ensures that the legal person, public authority, agency or other body which processes personal data on behalf of you complies with the necessary data protection regulation and due diligence obligations on their computers as well, and
- you have the opportunity to check for compliance with these protective measures yourself, e.g. in the form of an on-site audit.

Apple does not offer either of these two items for iCloud, so the use of iCloud may be unlawful, depending on the type of data stored and the legal situation. You can find out about the rules applicable in your country by consulting a legal advisor. In many regions, Apple also transfers the data to other cloud service providers, so they don't store the information themselves. These providers include AIPO Cloud (Guizhou) Technology Co. Ltd in mainland China, IXcellerate in Russia, as well as Amazon Web Services, Google Cloud Storage, or Microsoft Azure in other countries.

TinkerTool System can ensure that specific components of iCloud cannot become accidentally activated on your computer. This way, you can secure your computer against inadvertent transfer of data to Apple in order to guarantee data protection.

For the general synchronization of files (e.g. iCloud Drive or using the feature "Optimize Mac Storage", among others) and synchronization of the user folders **Documents** and **Desktop**, TinkerTool System can deactivate the related services and then block them against being switched on again.

Other selected functions of iCloud can be locked by TinkerTool System as well. *For technical reasons, the current states (on/off) of the respective features will be kept at first and can no longer be modified via System Settings by the user, however.* Due to security mechanisms in macOS, TinkerTool System can neither verify which states the current settings are in, nor can it disable the respective functions itself. But macOS still assumes that the default value for a locked iCloud feature is "off". If macOS validates the settings for internal reasons later, it may automatically disable the locked iCloud functions in the future, at a time unknown in advance.

> This means, if iCloud functions (except file synchronization) are mistakenly active when you lock them via TinkerTool System, it will be unknown if and when macOS will switch them off later.

For this reason you should avoid this unsafe transitional state and always perform these steps:

1. Click the button **Show state in System Settings**. The current iCloud settings will open.
2. In System Settings, click onto **See All** at **Saved to iCloud** to review the current states of all iCloud functions.
3. Ensure that all detail functions you like to block with TinkerTool System are in the **Off** position.

4. Click on **Done** in System Settings.
5. Now check all switches in TinkerTool System in the table **Lock the following iCloud features in their current state** where iCloud functions should remain permanently disabled.

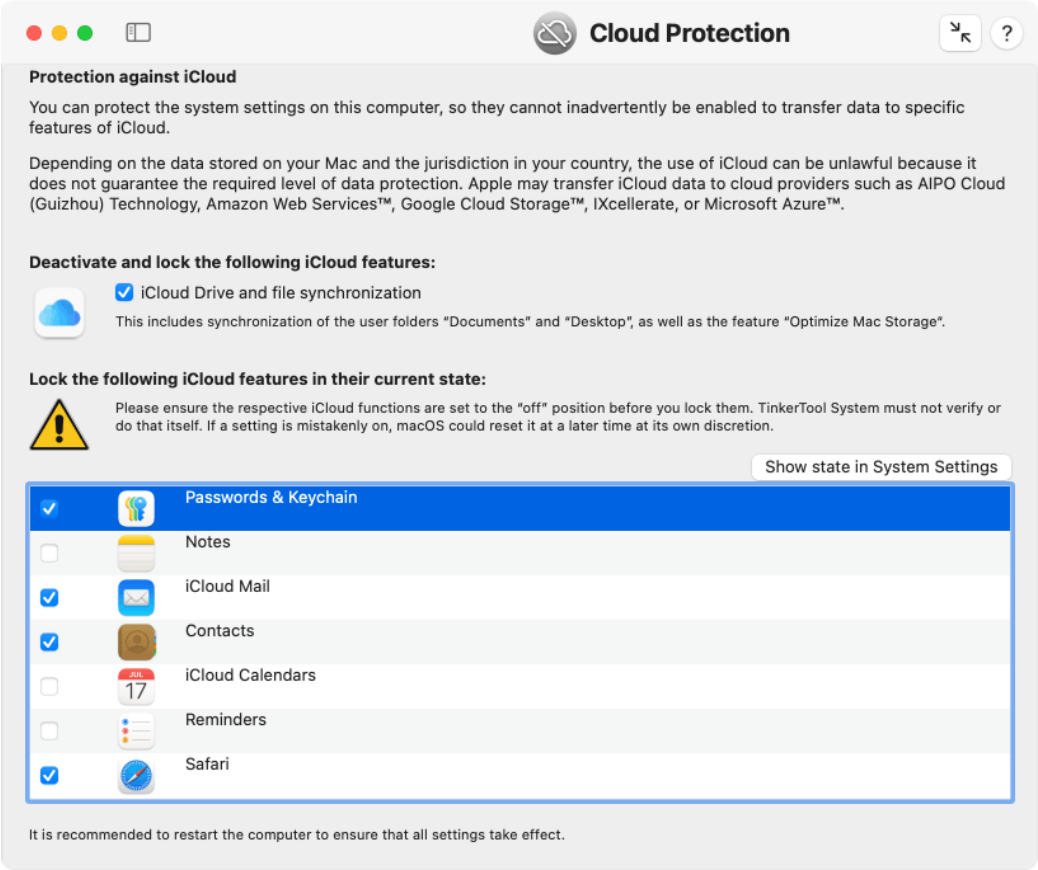


Figure 4.17: Cloud Protection

> Please note that not every operating system from Apple supports every iCloud service. In the same way, not every version of macOS is capable of locking every iCloud service. The services listed by TinkerTool System on the pane **Cloud Protection** are the only ones that can be blocked in the current situation.

You can unlock a service any time later by removing the respective check marks. The new setting will be sent to macOS immediately. However, depending on the current system state and the background tasks executed by iCloud at the moment, a setting might take effect after some delay only.

To ensure that a changed setting has indeed taken effect, it is recommended to wait a short time and then to restart the computer.

Locks take effect for all users of the respective computer.

If file synchronization has been deactivated and locked by TinkerTool System, macOS may move affected iCloud files automatically into an archive folder in the respective user's home folder.

Depending on the version of macOS, it can happen that **System Settings** mistakenly indicates that an iCloud function has been locked by a configuration profile, although TinkerTool System never uses such profiles.

4.8 The Pane Power Schedule

The Power Schedule pane can be used as a substitute to replace the discontinued features of the previous panes **Energy Saver**, or **Battery** respectively, which had been part of the System Preferences application of older versions of macOS. TinkerTool System provides a widely identical range of functions and also allows access to additional settings for scheduling one-time power events.

4.8.1 Dates for Repeating Events

A constantly running clock with an alarm function enables a Mac to turn itself on when it is off. If the Mac is already switched on at that time, but is in sleep or standby mode, a wake-up event is triggered instead, so that macOS is always ready for use at the chosen time. The reverse function, namely

- going to sleep,
- a restart, or
- shutting down the computer

can also be programmed as part of the schedule. Either a single event or a pair of an activating and a deactivating event can be set up for a selected time, which is then repeated daily. In addition, these events can be defined not to really take place every day, but only on certain days of the week. TinkerTool System allows you to set up repeating power events

- every day,
- at weekends,
- every day except on weekends, or
- on a specific day of the week,
- for arbitrary combinations of weekdays (via the menu item **Custom**...).

You can define such regularly repeating events for the power control of your Mac as follows:

1. Open the pane **Power Schedule**.
2. Set a check mark at one or both lines in the box **Repeating Events**. Use the pop-up buttons to select the appropriate days of the week and the desired times. The upper line is used to define an activating event, the lower line for a deactivating event, whose type can be chosen exactly via an additional pop-up button.
3. Click the **Save** button at the bottom right.

Unless you receive an error message, the schedule will become active and be in effect without further notice. You can delete all repeating events by clicking the button **Clear all**. This change takes effect immediately without having to click the **Save** button.

> The UNIX command line of macOS additionally allows you to set up schedules with relative times. Apple advises against this as such a schedule cannot be implemented accurately for technical reasons. Such a configuration cannot be edited with TinkerTool System. If this case is detected, an error message will appear in the box in red. You can click the **Clear all** button to delete the schedule, and then replace it by a simpler one.

4.8.2 Dates for One-Time Events

In addition to the events repeating on a weekly or daily basis, you can also set up one-time events, specified by a fixed date and time. All of the power control event types mentioned so far can be used, either with an enabling or disabling character. Apple recommends to add a comment to each of such events, stating which application or user "owns" the entry.

macOS also uses the schedule of one-time events for itself, to enforce a wake from sleep at specific times. This can trigger maintenance work or send reminders to the user. You can usually identify such entries by an owner remark beginning with **com.apple**.... Dates set up by macOS itself are automatically cleaned up.

You can define one-time power events as follows:

1. Open the pane **Power Schedule**.
2. Click the **+** button to add a new line at the end of the table.
3. In the new row, choose date, time and the type of power event. You can also add a short text as comment.
4. Click the **Save** button at the bottom right.

If you don't enter a comment for the event, the internal identification of TinkerTool System will be specified automatically as "owner" of the entry.

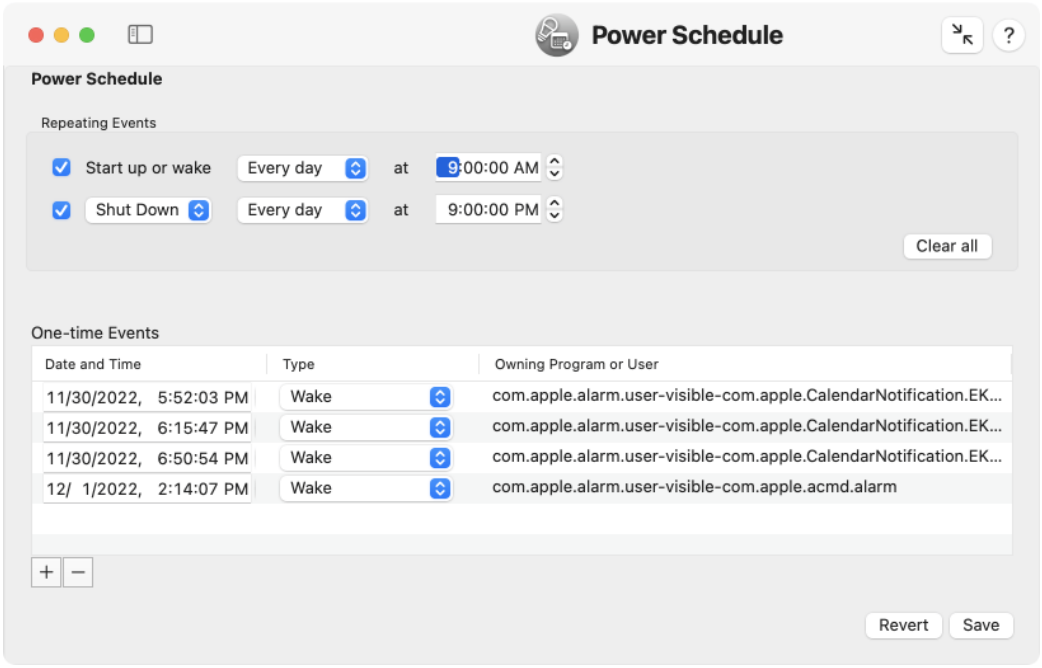


Figure 4.18: Repeating power schedule events and one-time events can be reviewed and edited.

> When saving, macOS may decide to sort the table in a different order at its own discretion. This cannot be prevented.

You can also select one or more lines of the table and delete the associated events by clicking the – button.

4.8.3 General Notes on the Power Schedule

If you have made changes, but not saved them yet, you can use the button **Revert** to return all settings to their previous states. This includes both repeating and one-time events.

> Neither TinkerTool System nor macOS are responsible for implementing the power control events. They are implemented *by the Macintosh hardware*. This means if you are running macOS in a Virtual Machine or are not using a genuine Apple computer, the schedule may not take effect.

Please also note that the power schedule has unexpected limitations: An automatic shutdown is only possible if the Mac is *not* in sleep mode at the specified time and at least one user is logged on locally. If older software is currently running which has unsaved documents open, sleep mode, restart or shutdown can be prevented. If the computer is secured by FileVault, it can be turned on automatically, but it cannot start the operating system because a user must enter a password to decrypt the system volume first.

> If you are logged in as a user with administrative rights, you are allowed to change the power schedule settings without additionally entering a password. This corresponds to the simplified security policy that Apple used in previous versions of the System Settings application.

Chapter 5

User Settings

5.1 The Pane User

All operations available on the pane **User** affect a single user account only, namely the user who started TinkerTool System. Detail information about the selected user account can also be found on the sub-item **Info** of this pane.

5.1.1 Preferences

Motivation

Macintosh software is usually designed after very high usability standards. Technical problems are solved by the applications on their own, in most cases silently, without needing to interact with the user. There is one type of technical problem however, which can often not be handled by affected applications, namely cases where the applications' preference settings have been damaged. TinkerTool System offers features to automatically find and eliminate bad preference files.

The Preferences System of macOS

Applications send messages to the operating system to store and retrieve user settings, e.g. color preferences, the last position of windows on screen, the last saved document, etc. macOS uses a core technology of the system called *property lists* to organize all preference settings in a kind of database. The database is distributed onto a large number of files which have the name extension **plist**. Each of these property lists contains settings which apply to a certain area of the system only, i.e. it forms a subset of the total preferences collection. Such a subset is called a *preference domain*. A preference domain usually corresponds closely with an application you have used, e.g. the preferences of the application **Mail** are stored by the preference domain called **com.apple.mail**. However, there is not always a one-to-one relationship. Apple's Mail program also makes use of the additional preference domain **com.apple.mail-shared**, for example.

According to Apple's software design guidelines, the identifiers of the preference domains must be structured based on a hierarchical list of descriptive names, written from left to right in top-down order, separated by dots. The first part of the hierarchy must be the Internet domain name (DNS name) of the application's vendor, so two different software companies can never create the same identification for a domain, even if their products should happen to have identical names.

Example: The unique identifier for Apple's web browser Safari is **com.apple.Safari**, because it is published by the company with the Internet domain name **apple.com** and **Safari** is the descriptive name to identify this program in Apple's software portfolio. Note how **com.apple.Safari** is written in top-down order, with the most important part at the beginning, while Internet domain names like **www.apple.com** are written in reverse order, with the most significant part at the end.

Software companies are free to use more than one descriptive name components to identify a particular application or aspect of an application. Examples for this are **com.apple.airport.airportutility** and **com.apple.airport.clientmonitor** to identify two different applications which are both part of the subject area "Airport." The naming scheme guarantees that each application will have a unique preference domain.

Verifying the Integrity of Preference Files

If the property list file for a preferences domain has been damaged for some reason, macOS will feed the application belonging to the file with invalid preference settings, a situation which is not handled correctly by many programs, because they don't expect that such a thing could happen. The application could crash or behave erratically.

To avoid this, you can verify the integrity of all preference files effective for the current user. This includes all settings of all applications ever launched by this user. To do this, perform the following steps:

1. Open the sub-item **Preferences** on the pane **User**.
2. Click on the button **Check Files**.

> Legacy applications which have not been correctly ported to the macOS platform use preference files they have created on their own. These files cannot be tested because they don't follow any standards.

While the verification process is running, you can stop it any time clicking the **Stop** button. After all tests have been completed, TinkerTool System will display a report table, listing all problems found. The problems are categorized by severity which is visualized by different colors:

- **Yellow:** a negligible warning. The preference file is not fully compliant with macOS standards but doesn't seem to cause problems.
- **Orange:** a warning. A problem with the preference file has been detected and it is recommended that you make further checks on this file or the application it belongs

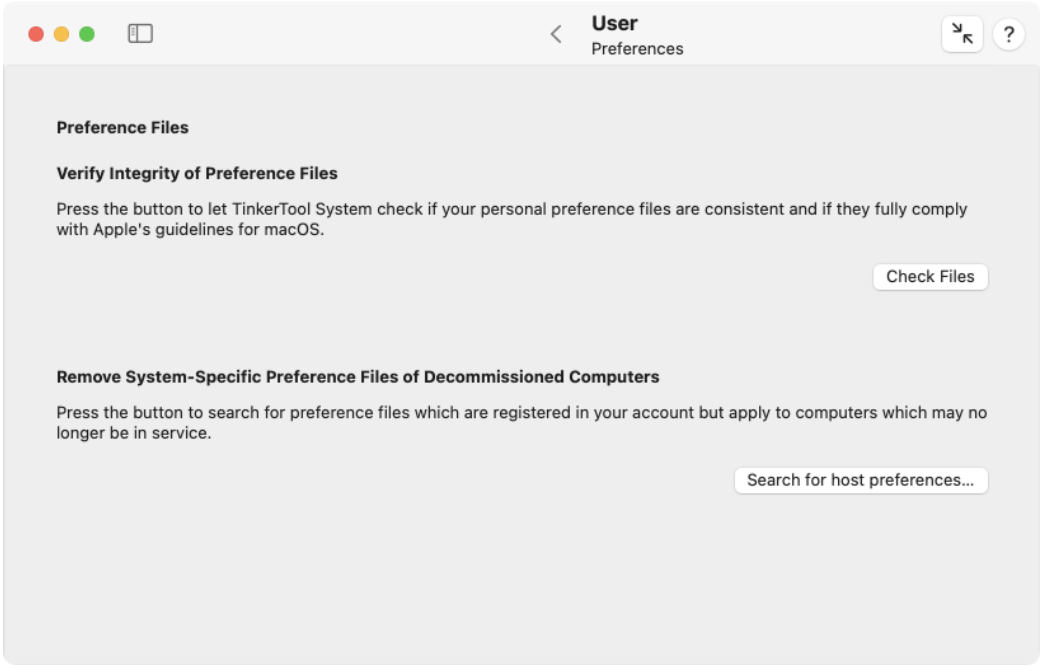


Figure 5.1: Preferences

to. In some cases, only the software developer of the application can fully resolve the problem because the application may use operations on the preference files which don't comply with macOS software design guidelines.

- **Red:** the file is definitively causing problems. It's structure is corrupt, so the application it belongs to will be fed with no or invalid preference settings.

The report table will contain a line for each of the problems found. Preference settings that are free of errors will not be listed. Each entry consists of a short problem description and the name of the preference domain.

To display detail information about a problem found, select an entry in the table. The full path to the affected property list file and a detailed error description will be displayed below the table. You can make the Finder navigate to the file by clicking the symbol with the magnifying glass. In cases where it could make sense, you can either deactivate or delete the problematic preference file by clicking one of the buttons.

- **Deactivate:** renames the file to the effect that macOS will no longer use it. The affected application will use clean preference settings the next time it is launched. Deactivation of a file gives you the possibility to retrieve all application settings in cases where you find out later that the preference file did not cause the actual problem, but something else. In this case you should quit the application, delete the new preference file that was created, and rename the deactivated preference

file to its former name. When you the relaunch the affected application it will use its previous preference settings. TinkerTool System deactivates preference files by renaming them with the extension **INACTIVE-plist**. If you change the extension back to **plist**, the file will become active again.

- **Delete:** deletes the preference file. You will lose all preference settings for the application it belongs to. The next time the application is launched, macOS will automatically create a new clean preference file for it.

> You should not delete or deactivate preference settings of applications currently running because this won't have any effect. Quit affected applications and rerun the test before you decide to remove a corrupt preference file.

Removing System-Specific Preference Files of Decommissioned Computers

In professional networks, the users' private home folders won't be stored on the local hard disks of the computers, but on a central file server. In this case, it will no longer matter which particular computer a certain user is working with. The user's personal documents and all her preferences seem to automatically move with her when she is using a different computer. The account always uses the same data although no form of synchronization is necessary. macOS automatically keeps track which of the preference settings of a user should be valid for all computers in the network, and which of them are computer-specific. For example, the trackpad and mouse settings should be stored individually for each computer, because each model might use a different type of mouse, or trackpad, respectively. Similar rules apply to Bluetooth, Airport, printer, screen saver, and many other settings, which are individual per user, but also per computer, because they will depend on the particular hardware equipment.

A similar situation can occur for computers of private persons, too: If you have migrated your personal home folder from an old computer to a new one —perhaps even across several generations of computers— you will have the same scenario. After a computer has reached a certain age, it will usually be removed from the network or your personal access, so storing computer-specific user preferences for that system will no longer make sense.

To use this feature, you will have to identify the computer which is no longer in operation. This might need to be done manually, because no program can get information about a computer which is no longer accessible. To identify a computer, old versions of Mac OS X used the MAC address of the system's built-in primary network interface, modern versions of macOS use the hardware UUID code (Universal Unique Identifier).

On modern versions of macOS using UUID codes, TinkerTool System shows the identification at **Info** > **Mac** > **Computer** > **Unique hardware identifier**. In case TinkerTool System is not available on the computer in question, you can also use the **System Information** application, selecting the category **Hardware**, looking for the line **Hardware UUID**.

After you have identified the decommissioned computer, perform the following steps:

1. Open the sub-item **Preferences** on the pane **User**.

2. Click the button **Search for host preferences**….

While the search is running, you can stop it any time clicking the **Stop** button. After the scan of preferences has finished, TinkerTool System will display a report table, listing the computer-specific preference sets known by the current user account. Next to the computer identification code, you will find the date of last use, and the number of preference files available for the respective computer. By checking the buttons in the column **Remove?** you can mark preference files for deletion. Clicking the buttons **Select all** or **Deselect all** causes all check marks to be set or removed, respectively. When you click the **OK** button, all files for all computers that had the **Remove?** check mark set will be deleted. If you click the **Cancel** button, no file will be touched.

The radio buttons in the lower left corner of the report panel control how the removal should take place. You can either **Delete files immediately**, put the files into the **Trash**, or move the files into an **archive folder** which you have to specify additionally.

5.1.2 Recent Items

Among a lot of other settings, each application keeps track what documents have been opened the last time you have used the program. The entries are listed in the submenu **File** > **Recent Items** of each application. Additionally, there is a central list of recently used documents and applications in the Apple menu, and the Finder maintains a list of servers to which manual network connections have been made.

To protect your privacy, you may like to remove these entries because they allow to keep track how you used the computer in the past. The server list may also contain passwords in the clear that should be protected. TinkerTool System can automatically clear the following entries for you:

- all recent document items in the Apple menu
- all recent application items in the Apple menu
- all recent servers in the Apple menu
- all recent servers in the Finder

To remove the entries for Recent Items, perform the following steps:

1. Open the sub-item **Recent Items** on the pane **User**.
2. Check each category for which the entries for **Recent Items** should be removed.
3. Click the button **Remove selected entries**.

This will delete the entries, of course not the documents these entries refer to. We strongly recommend that you log out immediately after you have cleared Recent Items. Otherwise, it cannot always be guaranteed that macOS won't just restore the items.

The **Go** > **Go to Folder** dialog offered by the Finder also remembers a large number of folders that you last used with this function. These entries can also be removed, but this additionally requires restarting the Finder. To do this, click the button **Remove entries and restart Finder**.

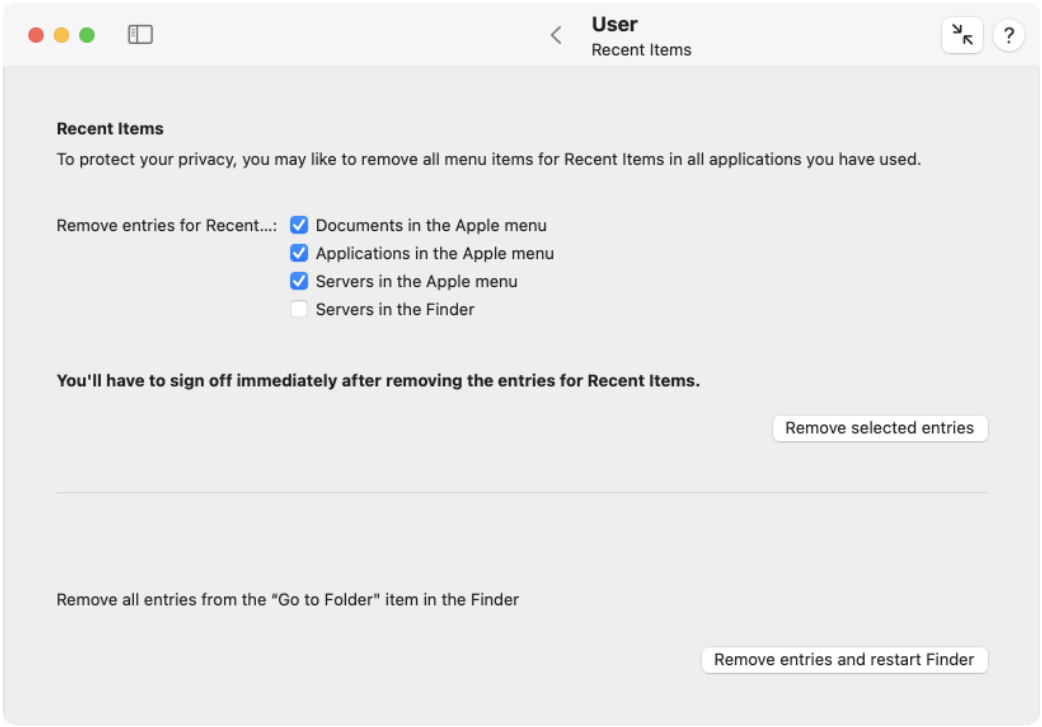


Figure 5.2: Recent items

5.1.3 Dictionaries

macOS contains a system-wide spell checker service supporting the core languages which are part of macOS. The spell checker can be controlled via the menu item **Edit** > **Spelling and Grammar** in all applications which use its services. When the spell checker is processing text of a document, the user can add unknown but correct words to her or his personal spell checking dictionary. There can be one dictionary per language and all added words are shared by all applications which use the macOS spell checker.

> Some applications come with their own spell checkers. They don't participate in the mechanism described here.

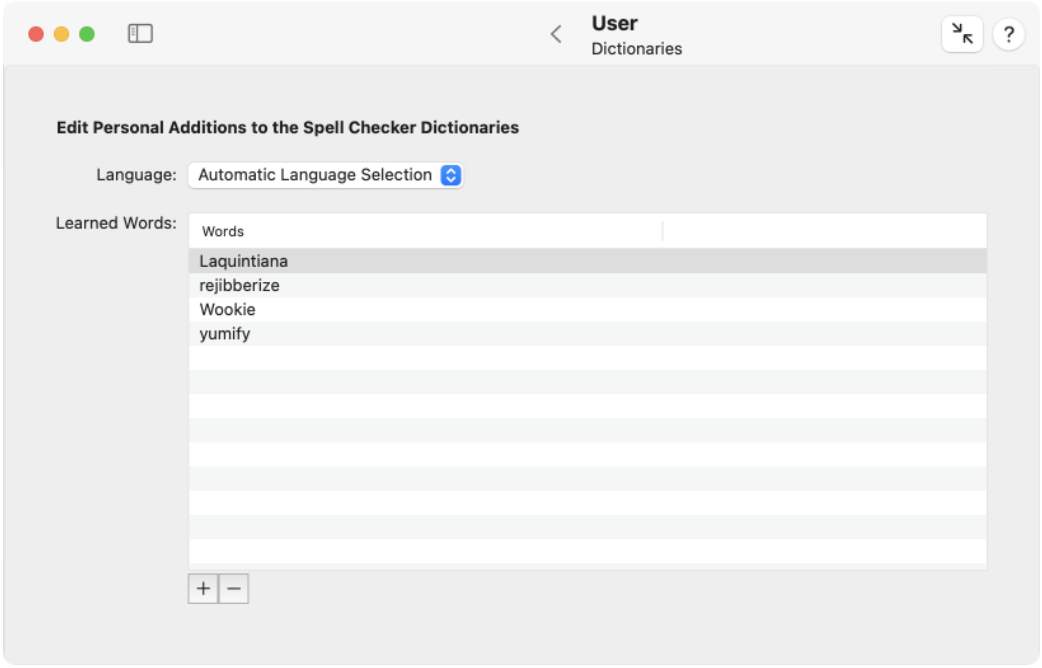


Figure 5.3: Spelling dictionaries

TinkerTool System can give you access to your personal dictionary of words you have added to the system's spell checker. You can change, add, or remove words if necessary. Perform the following steps:

1. Open the sub-item **Dictionaries** on the pane **User**.
2. Use the pop-up button **Language** to select the dictionary you like to work with.
3. Edit a word in the table **Learned Words** by double-clicking it, or click the button **[+]** to add a new word, or select one or more words and click the button **[–]** to remove them.

In addition to the dictionaries for the languages you are using normally, macOS provides another dictionary which is listed by TinkerTool System by the name **Automatic Language Selection**. This is a multi-lingual dictionary accessed whenever the spell checker is not set to use a fixed language.

Current versions of macOS may have technical problems to inform all open applications that changes have been made to your personal spell checker dictionaries. To ensure that all applications learn the changes you have made to your spell checker word list, log out and log in. You should avoid changing the word list from multiple running applications simultaneously. Some or all of your changes might be ignored.

5.1.4 Repair

Reset Launchpad

The **Launchpad,** designed to mimic the application starter of Apple's mobile devices has no settings directly accessible to users. It continuously recognizes all applications with graphical user interface available on the Mac and creates the respective launch icons for them. The user can only control the assignment to groups and the placement on different screen pages. In practice, this fully automatic setup can have problems, e.g. when wrong or duplicate icons are shown or applications are missing. The internal database maintained by Launchpad might by damaged in this case. If such an issue occurs, Launchpad can be factory-reset for the current user account. Please note that any arrangement of icons you may have adjusted and their distribution to groups and screens will be lost.

If you like to reset Launchpad for user account, perform the following steps:

1. Open the sub-item **Repair** on the pane **User**.
2. Click the button **Reset now** in the section **Reset Launchpad**.

TinkerTool System will guide you through the reset process.

Repair "Help Viewer"

Some versions of macOS have internal defects which can cause the Help Viewer application built into macOS to fail. Help Viewer acts like an invisible application and will be used each time you open an application's online manual via its menu **Help**. A floating help window will appear, pretending it would be part of the running application. As a matter of fact, the window is displayed by the Help Viewer application, although the viewer does not appear with a Dock icon or a separate menu bar.

If you have trouble with the online help window, no matter if you are using Apple or third-party applications, this will usually be caused by defects of the Help Viewer application. Typical symptoms are:

- No help window appears at all.

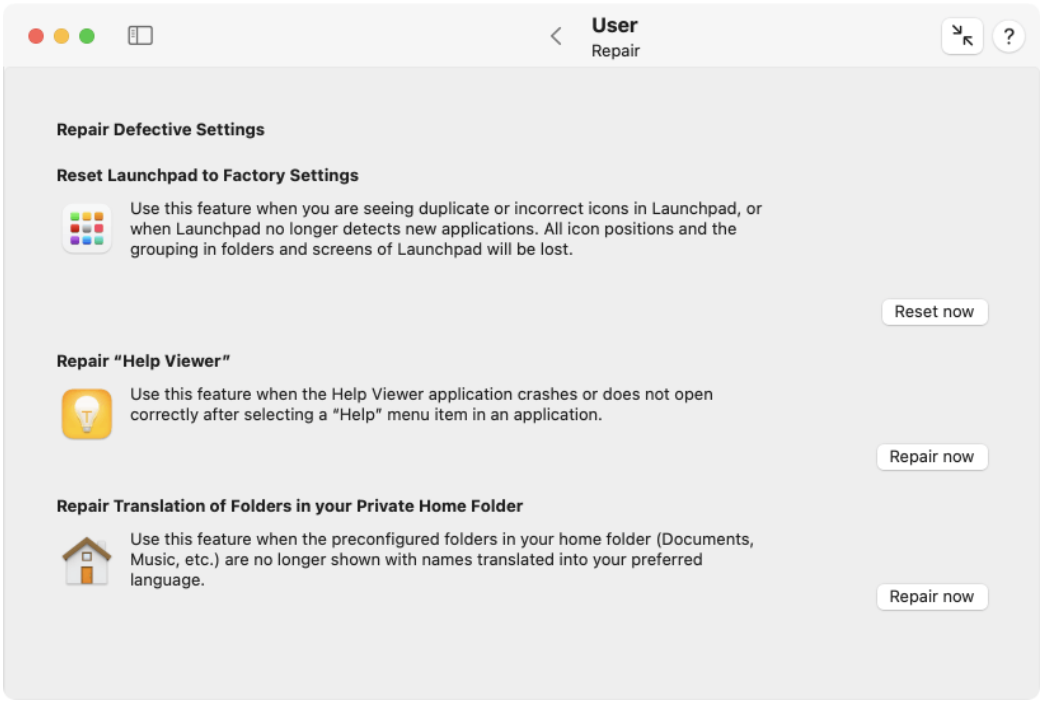


Figure 5.4: Repair features

- It takes a very long time until the help window appears.
- The help window can be seen shortly, but then the application Help Viewer crashes.
- Help Viewer does not respond on search requests.

TinkerTool System can temporarily repair Help Viewer, so that it will work for some time. Perform the following steps:

1. Open the sub-item **Repair** on the pane **User**.
2. Click the button **Repair Now** in the section **Repair "Help Viewer"**.

Repair Translation of Folders in your Private Home Folder

If your personal preferences for languages are set to use a language different from English, the Finder will show translated names for most system folders and the preconfigured folders in your home folder. For example, the folder **Desktop** will be displayed as **Bureau** if French is your preferred primary language.

When you have removed, then recreated some of the preconfigured folders, or if you have upgraded a user account which was created under control of Mac OS X Puma (10.1), this automatic translation feature might not work correctly. To repair this, perform the following steps:

1. Open the sub-item **Repair** on the pane **User**.
2. Click the button **Repair Now** in the section **Repair Translation of Folders in your Private Home Folder**.

> This will only affect folders in your own home folder, not system folders or folders of other user accounts.

5.1.5 Deleting the index database of Apple Mail

In some cases it happens that search functions within the macOS Mail program no longer work properly, or no longer deliver the complete search results. Certain messages are no longer found. If this is the case, this usually also affects the search for emails using the Spotlight function outside of the application.

Corruption of the index database of Apple Mail is almost always the cause of such issues. Wiping the data and rebuilding the index can fix such a problem. TinkerTool System provides a corresponding delete feature. Mail automatically rebuilds its index database the next time it is started. A message appears that all emails must be re-imported. After confirmation, all further steps will be carried out fully automatically.

> Please note that this import process can take several hours, depending on how many mailboxes and messages you manage with the Mail application. You cannot work with the Mail program during the import. However, you can still access the email server and its messages via a second device (e.g. an iPhone) if the server is using the IMAP protocol.

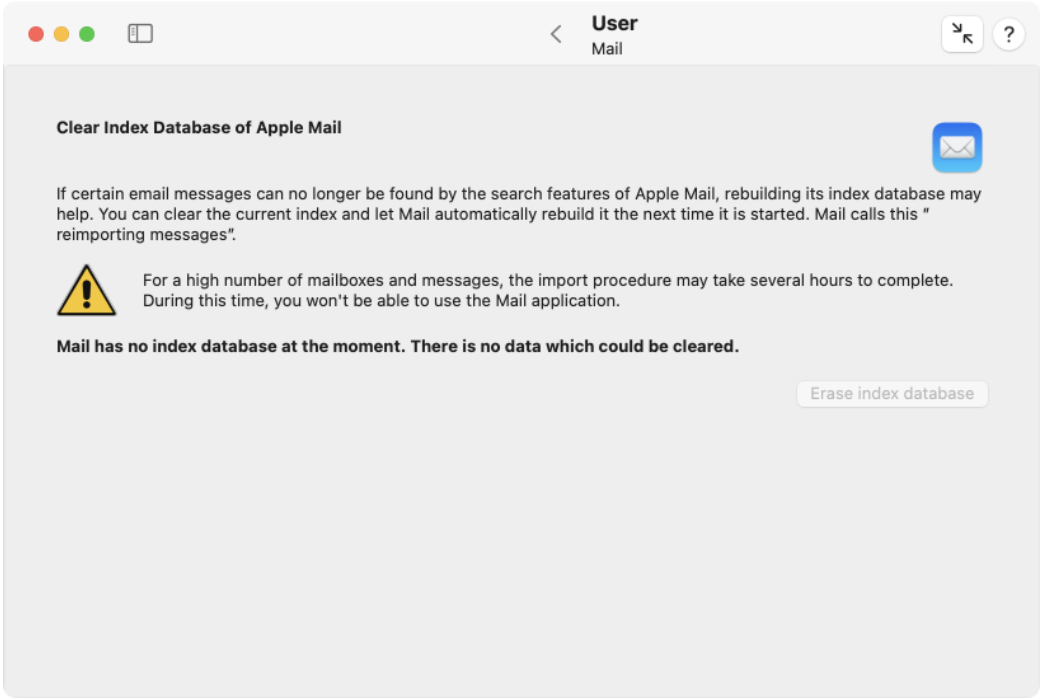


Figure 5.5: Clear index database of Apple Mail

TinkerTool System indicates by a status message in bold whether an index database is available for your user account and how large it is. If the index database is present, you can quit Mail and have the data deleted. To do this, click on the **Erase index database** button. Rebuilding the index will be done automatically as import operation the next time you start Mail.

5.1.6 Info

The sub-item **Info** can be used to display advanced information about the current user account, not visible in the System Settings application. Note that the panel is designed for information purposes only. You cannot use it to change any of the data. The following items are listed:

- The user's short name.

- The user identification number. This number is used in all parts of the core operating system to uniquely identify this account.
- Membership in the primary group. The group is listed with its full name and its group identification number.
- A photo associated with the account. In professional environments, this will usually be a passport photo of the user. It is used on the login screen and applications like Contacts, Mail, Messages, or others when referring to this user graphically.
- The UNIX path of the home folder. This is the folder where all personal information and documents of the user are stored. You can make the Finder open this folder by clicking the symbol with the magnifying glass.
- The initial *shell*, configured to be used as the default for this account. The shell is the program controlling the user session when the user opens a session in text mode, for example by opening a Terminal window.
- The information whether the user has administrative permissions or not.
- The complete list of user groups this user is direct member of. Group identification number, short name of the group, long name of the group, and the group's unique identification code are listed for each membership. Indirect memberships (a group is defined to be a nested member of another group) won't be listed.

> If the user is member of a user group which no longer exists, the column entries for name and full name repeat the numeric ID in the form <**GID: ID**>.

5.2 Working with Panes from TinkerTool

After you have integrated a copy of TinkerTool into TinkerTool System, (section 1.6 on page 22) you can work with any of the panes of TinkerTool directly from the System application, so you no longer have to start both programs separately to access their full feature set.

Panes of TinkerTool give you access to advanced preference settings built into macOS which are not visible in the standard System Settings application or in the settings windows of applications, like Safari. To change one of these advanced settings, perform the following steps:

1. Select one of the additional panes shown in the section **User Settings** in the sidebar of TinkerTool System.
2. Change the settings using the buttons in the pane that has opened.
3. Read the line in the lower left corner of the pane to learn when the changes will take effect.

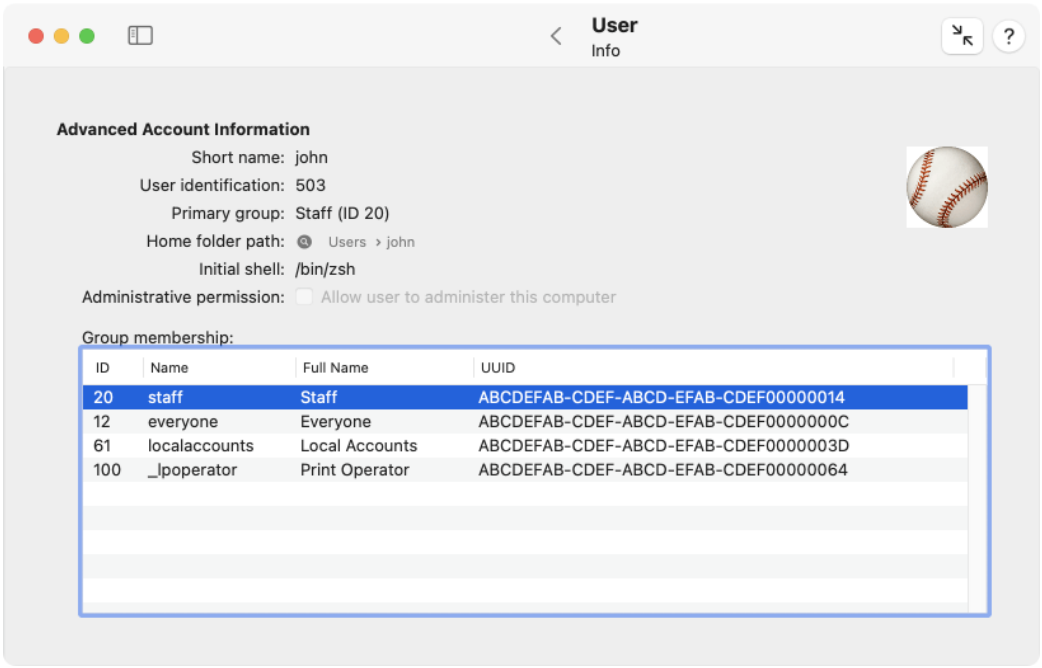


Figure 5.6: Info

Chapter 6

Working in macOS Recovery Mode

6.1 General Information

To work with the program **TinkerTool System for Recovery Mode** , you'll have to start the recovery version of macOS that belongs to your respective operating system, and then call the emergency tool by entering a command in Terminal. Further information can be found in the the chapter The Pane Emergency Tool (section 2.8 on page 104).

> If you click on the question mark button in that pane, you will find an Internet link among other things, where Apple has collected the latest information on how to work with macOS Recovery Mode.

If TinkerTool System is located on the same volume as the operating system, you will generally be able to use the emergency tool. No special installation steps or other precautions have to be taken.

6.1.1 The Main Menu of the Application

After launching via Terminal, the main window of **TinkerTool System for Recovery Mode** will appear. It is comprised of three parts:

- a clock indicating world time,
- a menu that offers the different features via buttons,
- a status line that confirms on which volume the application is currently working.

If your Mac has multiple operating systems, it is recommended to check the status line, verifying before running any feature that the intended operating system volume is selected. Please remember the interdependencies between storage location and operating system mentioned in the chapter The Pane Emergency Tool (section 2.8 on page 104).

To select a function, simply click onto the respective icon or its label. The functions of each of the different menu items are described further in the following sections:

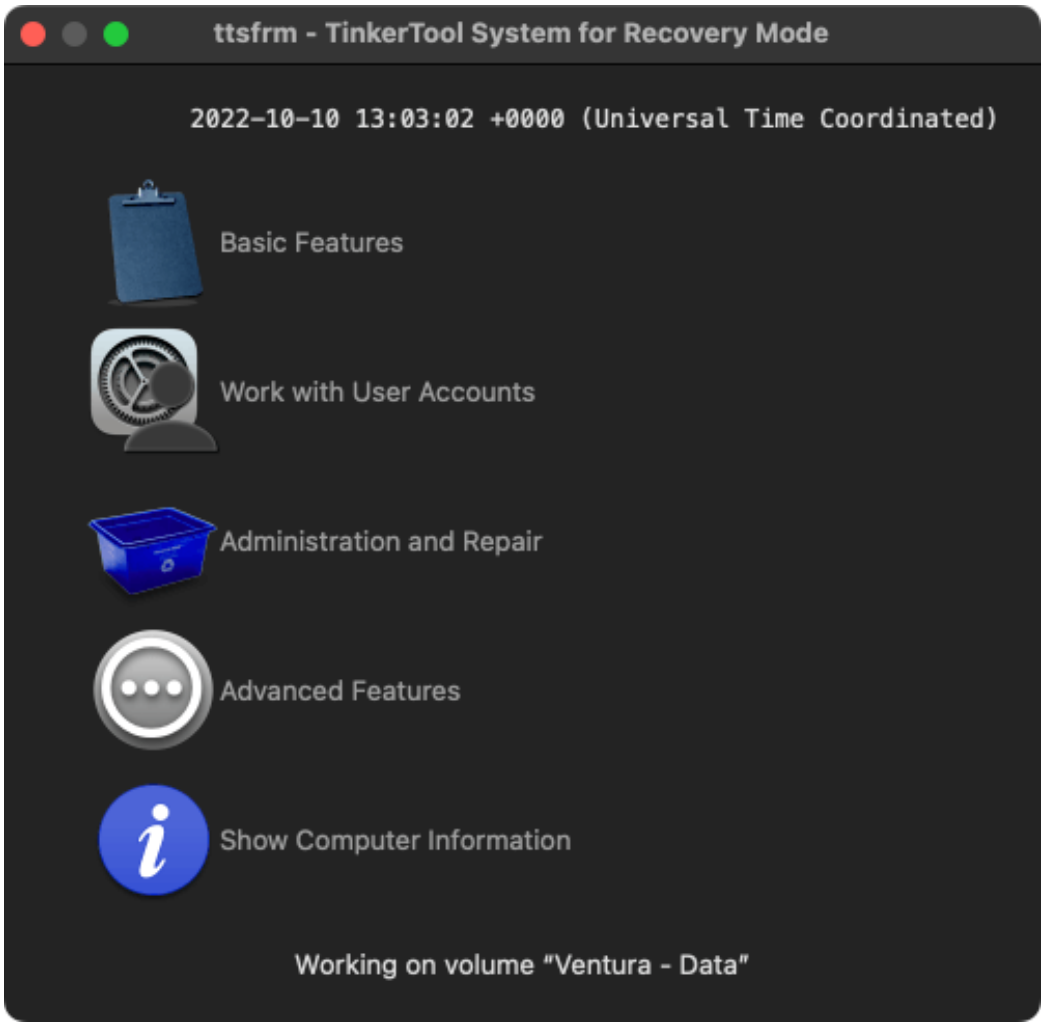


Figure 6.1: The main menu of TinkerTool System for Recovery Mode (ttsfrm

6.1.2 Quitting the Application

To quit the application, select the menu item **ttsfrm** > **Quit ttsfrm**. You can also press the key combination ⌘ + Q as in the normal version of macOS. The computer can be restarted or be shut down via the Apple menu.

6.2 RecoveryMode: Basic Features

The dialog **Basic Features** opens after clicking the corresponding item in the main menu. The sheet can be closed by clicking the button **Close**.

6.2.1 Repairing the System's Temporary Folder

This feature is designed for cases where the operating system's main folder for temporary objects has been deleted. If this folder is missing, many parts of the system will no longer work. Some applications may show the error message that the folder named **/tmp** cannot be found. In that case you should recreate or repair the folder.

Simply click the button **Repair**. The button can only be clicked when a repair is necessary and possible.

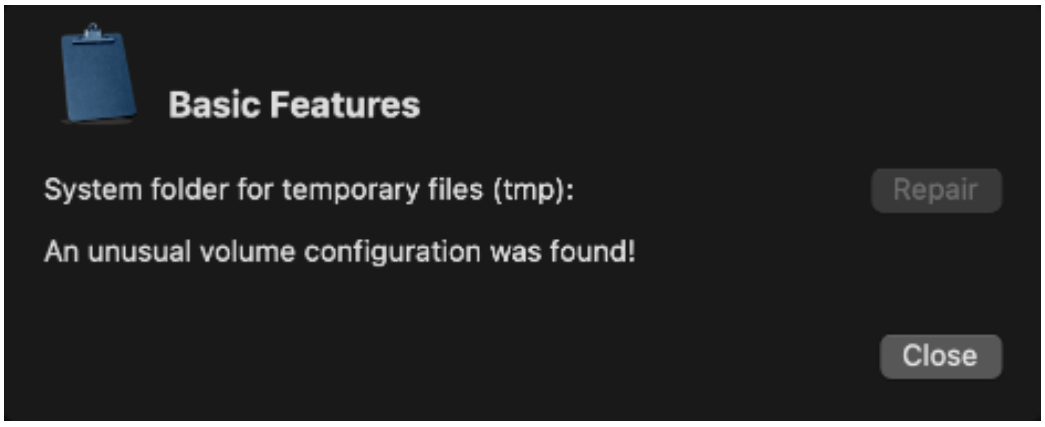


Figure 6.2: Basic Features

6.3 Recovery Mode: Working with User Accounts

6.3.1 Selecting the User Account to be Processed

The first step of all features listed under the title **Work with User Accounts** in the main menu must be to choose the account on which the operation should be conducted. After selecting the menu item, a dialog sheet appears that contains the pop-up button **Users**. Choose a user by his or her short account name.

> The pop-up button **User** contains only those users who have their home folders at the usual place, i.e. the folder **Users** *(/Users)* of the operating system. Other users or their files, respectively, are not available in macOS Recovery Mode in the general case.

The dialog sheet can be closed by clicking the button **Close**.

6.3.2 Deactivating Corrupt Preference Files

You can instruct **TinkerTool System for Recovery Mode** to verify all preference files of a user, and deactivate all files which are detected from the outside as being corrupt. Nothing will be deleted during this step. The damaged files will be deactivated by renaming them, so that they can no longer have any effect on macOS and applications which use the affected preferences. This is equivalent to a strongly simplified version of the feature **User** > **Preferences** > **Check Files** of TinkerTool System.

1. In the main menu, click on **Work with User Accounts**.
2. Choose a user account via the pop-up button **User**.
3. Select the item **Deactivate Corrupt Preference Files** in the pop-up button **Function**.
4. Click on **Run**.
5. Wait until the final results of the verification or repair steps are shown on screen.

6.3.3 Deactivating All Caches of a User

As described in the chapter Caches (section 2.2 on page 32), damaged cache contents can lead to errors during the execution of programs in individual cases. The standalone program can completely deactivate the personal standard caches of a user account if desired. Nothing is deleted, so the valuable cache contents can be restored in case of doubt to maintain a high operation speed of the system. Perform the following steps to deactivate the personal standard caches of a user temporarily or permanently:

1. In the main menu, click on **Work with User Accounts**.
2. Choose a user account via the pop-up button **User**.

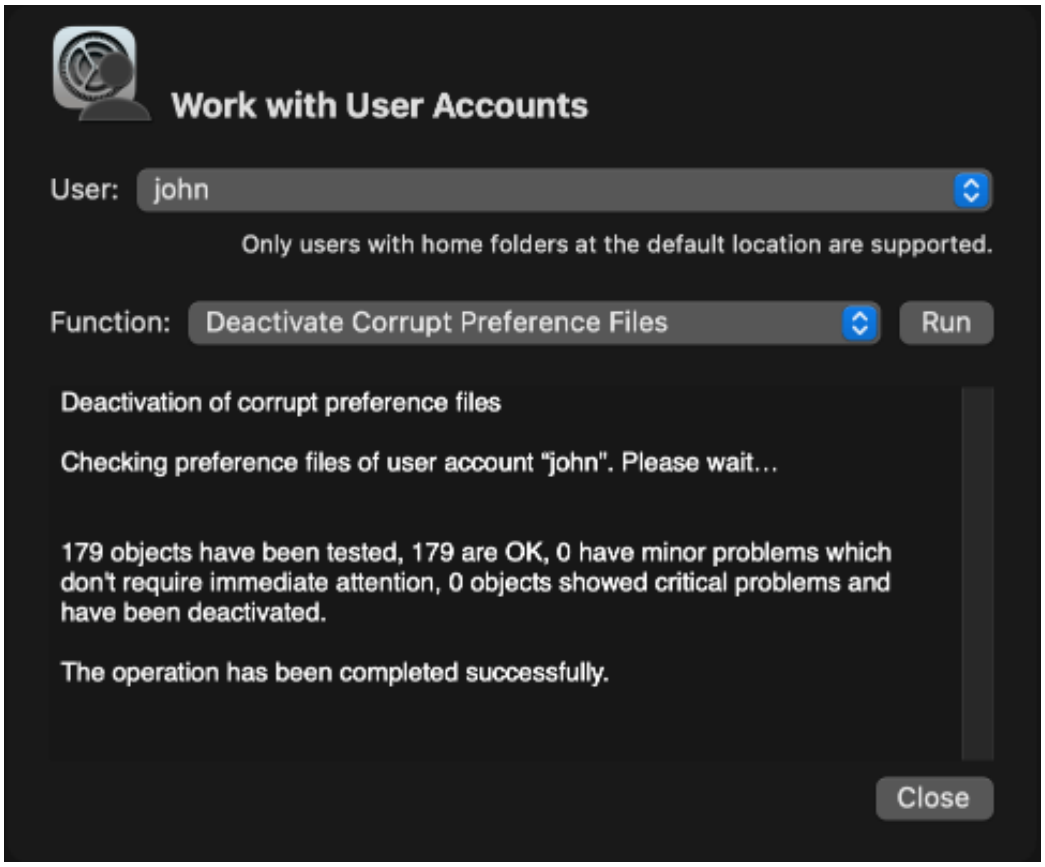


Figure 6.3: Working with user accounts

3. Select the item **Deactivate All Caches of a User** in the pop-up button **Function**.

4. Click on **Run**.

5. Wait until the final results of deactivation are shown on screen.

6.3.4 Reactivating All Caches of a User

After removing the contents of caches, macOS and many applications will run slower because the caches must be rebuilt internally. If deactivation of caches (from the previous section) did not have the expected success, the affected data can be restored completely by a simple key press, avoiding loss of performance.

1. In the main menu, click on **Work with User Accounts**.

2. Choose a user account via the pop-up button **User**.

3. Select the item **Reactivate All Caches of a User** in the pop-up button **Function**.

4. Click on **Run**.

5. Wait until the final results of reactivation are shown on screen.

6.3.5 Deactivating All Preferences of a User

Preference settings of users can be damaged in such a way that their outer appearance is still correct, however the internal meaning of the stored information might be inconsistent. In rare cases, this can cause applications to behave erratically or not to launch at all. If such a problem cannot be isolated to a specific application, a last resort to troubleshoot the error might be to temporarily deactivate all preference settings of a user. All applications started by this user will run with “fresh” manufacturer defaults afterwards. When deactivating preferences, the settings will not really be deleted, so that they can be restored in case of doubt later.

1. In the main menu, click on **Work with User Accounts**.

2. Choose a user account via the pop-up button **User**.

3. Select the item **Deactivate All Preferences of a User** in the pop-up button **Function**.

4. Click on **Run**.

5. Wait until the final results of deactivation are shown on screen.

6.3.6 Reactivating All Preferences of a User

In case you find out that deactivating all preferences (from the previous section) did not have the expected effect, all preferences can be restored completely (to the status of the time the deactivation procedure occurred). Perform the following steps:

1. In the main menu, click on **Work with User Accounts**.
2. Choose a user account via the pop-up button **User**.
3. Select the item **Reactivate All Preferences of a User** in the pop-up button **Function**.
4. Click on **Run**.
5. Wait until the final results of reactivation are shown on screen.

6.4 Recovery Mode: Administration and Repair

6.4.1 Deactivating Corrupt System Preference Files

You can instruct **TinkerTool System for Recovery Mode** to verify all system-wide preference files which affect all user accounts, and deactivate all files which are detected from the outside to be corrupt. Nothing will be deleted during this step. The damaged files will be deactivated by renaming them, so that they can no longer have any effect on macOS and applications which use the affected preferences. This is equivalent to a strongly simplified version of the feature **User** > **Preferences** > **Check Files** of TinkerTool System, limited to system-wide settings.

1. In the main menu, click on **Administration and Repair**.
2. Select the item **Deactivate Corrupt Preference Files** in the pop-up button **Function**.
3. Click on **Run**.
4. Wait until the final results of the verification or repair steps are shown on screen.

6.4.2 Deactivating System-Related Caches

This function is equivalent to the item **Deactivate User-Related Caches** of the menu **Work with User Accounts**. Here, all caches will be deactivated which are active system-wide for all users. Perform the following steps to annul all system-wide caches temporarily or permanently:

1. In the main menu, click on **Administration and Repair**.
2. Select the item **Deactivate System-Related Caches** in the pop-up button **Function**.
3. Click on **Run**.

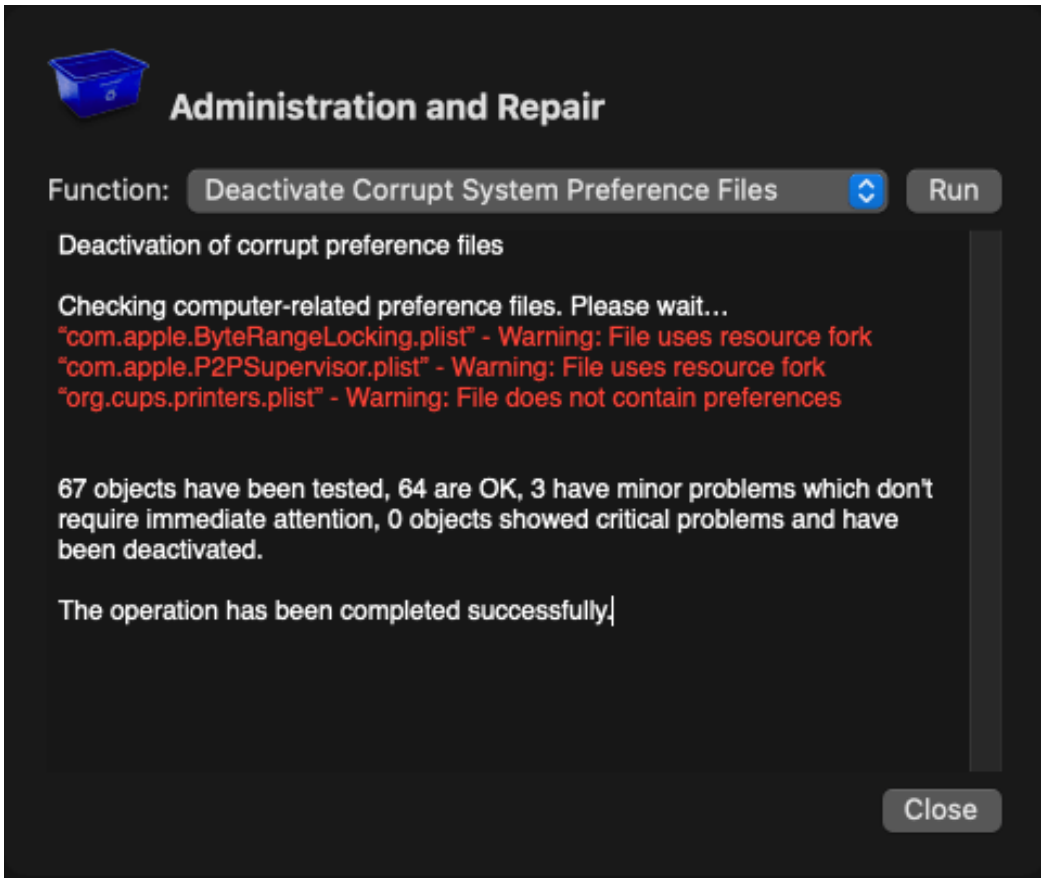


Figure 6.4: Administration and Repair

4. Wait until the final results of the deactivation are shown on screen.

Detailed notes on the function of caches can be found in the equally named chapter (section 2.2 on page 32).

6.4.3 Reactivating System-Related Caches

After removing the contents of system-wide caches, macOS will run slower because the caches must be rebuilt internally. If deactivation of caches (from the previous section) did not have the expected success, the affected data can be restored completely by a simple key press, avoiding loss of performance.

1. In the main menu, click on **Administration and Repair**.
2. Select the item **Reactivate System-Related Caches** in the pop-up button **Function**.
3. Click on **Run**.
4. Wait until the final results of the reactivation are shown on screen.

6.4.4 Resetting Managed Preferences

If your computer is part of a macOS network where management features are used, situations can arise where the management is not working as expected. A restriction which is defined via management might not become active on a computer, or, the other way around, a limitation which is no longer predefined by management is still blocked on a certain computer. Such problems can be resolved by resetting all managed preferences. If the system is still connected with the managed network, the computer will learn the managed settings anew, and will activate them again with an up-to-date state. If the system is no longer connected with the network, the managed settings will be released and can then be modified locally again. Perform the following steps to reset the managed preferences:

1. In the main menu, click on **Administration and Repair**.
2. Select the item **Reset Managed Preferences** in the pop-up button **Function**.
3. Click on **Run**.
4. Wait until the final results of the reset procedure are shown on screen.

6.4.5 Resetting the Login Screen

Technical issues with the reliability of the login screen can occur. It is possible that invalid preference settings for this screen create a situation where successful logins at the graphical user interface become impossible. This can make the system basically inoperable. You can resolve such a problem by resetting all preferences of the login screen to clean factory settings. To do this, perform the following steps:

1. In the main menu, click on **Administration and Repair**.
2. Select the item **Reset Login Screen** in the pop-up button **Function**.
3. Click on **Run**.
4. Wait until the final results of the reset procedure are shown on screen.

6.4.6 Removing Custom Startup Objects

Many user applications which provide services at the system or hardware level often install additional programs in the operating system which become active automatically in the background during each startup. We use the term *Custom Startup Objects* for such services. Has such an application been removed "improperly," i.e. without using the official uninstaller of its vendor, obsolete startup objects may remain in the system which are no longer of real use. These objects may consume resources or can even cause problems. When using the macOS Migration Assistant, it could also happen that inappropriate startup objects are unintentionally taken over from an old onto a new computer.

TinkerTool System for Recovery Mode can be used to display all common types of system-wide custom startup objects, removing them if required.

> The term "custom" should indicate that we are speaking about a startup object which is not part of the official installation of macOS, but has been installed by a third-party application. The utility intentionally does not support any operations on built-in startup objects which are part of macOS.
>
> 
> The manual removal of startup objects should be used in cases of emergency only, if you know that a certain object is causing technical problems and cannot be removed by other means (e.g. by an uninstaller of its vendor). For technical reasons, the standalone application cannot detect any interdependencies between startup objects, or assess if a startup object is fulfilling an important service.

Perform the following steps to remove custom startup objects manually:

1. In the main menu, click on **Administration and Repair**.
2. Select the item **Remove Custom Startup Objects** in the pop-up button **Function**.
3. Click on **Run**.
4. Another dialog sheet appears, showing three tables with different type of startup objects.

The first section shows objects stored in a technical form which can be used by Mac OS X 10.4 Tiger and by later versions of macOS. These objects are usually described by clear

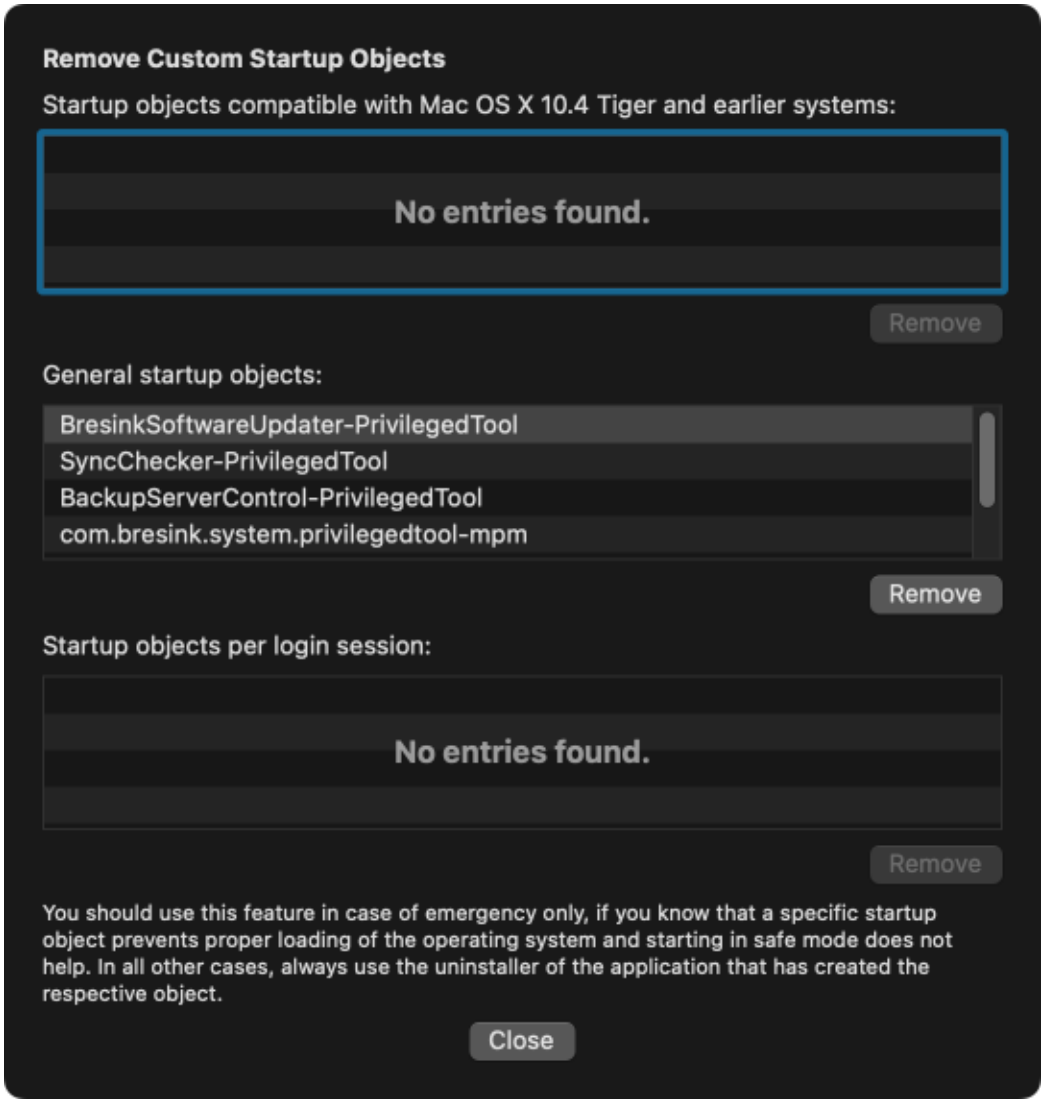


Figure 6.5: Remove Custom Startup Objects

text, based on the descriptions provided by their vendors. The second section contains "more up-to-date" objects which are incompatible with Tiger and become active during each startup of macOS. The third section lists objects also running in the background, but becoming active not at startup time but for each new login session. Note that the third section does not refer to login items of users, but to system-wide services per user which cannot be modified by these users. The second and third section use unique identification names for each of the objects, complying with a naming scheme defined by Apple. Some of the tables might be empty, in case no associated objects are installed on your computer.

You can select one or more start objects and press the button **Remove** below the respective table. The objects will be removed immediately. The dialog sheet can be closed with the **Close** button.

6.5 Recovery Mode: Advanced Features

6.5.1 Disabling Automatic Login

In some cases, a program which cannot be quit during normal operation (like the Finder or the Dock) could cause a technical problem with your computer. Such a problem becomes even more severe if automatic login of a user is active, so the erroneous application is becoming active by itself after each startup. To resolve such a problem by using a second user account, the automatic login of a user after startup can be switched off by **TinkerTool System for Recovery Mode**.

1. In the main menu, click on **Advanced Features**.
2. Select the item **Disable Automatic Login** in the pop-up button **Function**.
3. Click on **Run**.
4. Wait until the final results of this operation are shown on screen.

Automatic login can be reenabled later if desired, by selecting **System Settings** > **Users & Groups** > **Automatically log in as**... in macOS.

6.6 Recovery Mode: Retrieving Information

Sometimes it is useful to retrieve internal technical data about computer, operating system, or application version in recovery mode. This is possible by using the menus **Show Computer Information** and **About TinkerTool System for Recovery Mode**.

6.6.1 Hardware and OS Information

Hardware data about computer, processor, and memory equipment, as well as the currently running recovery operating system can be displayed as follows:

1. In the main menu, click on **Show Computer Information**.

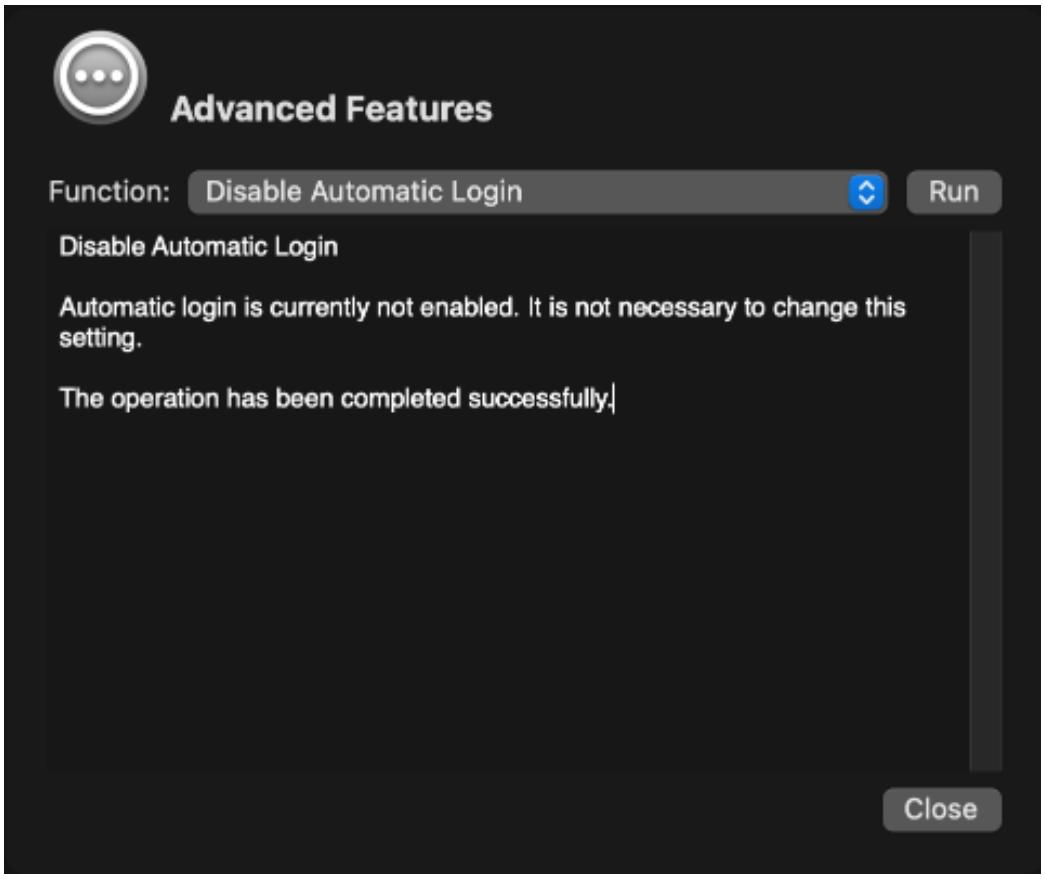


Figure 6.6: Advanced Features

2. Make sure the tab item **Hardware Overview** is selected.

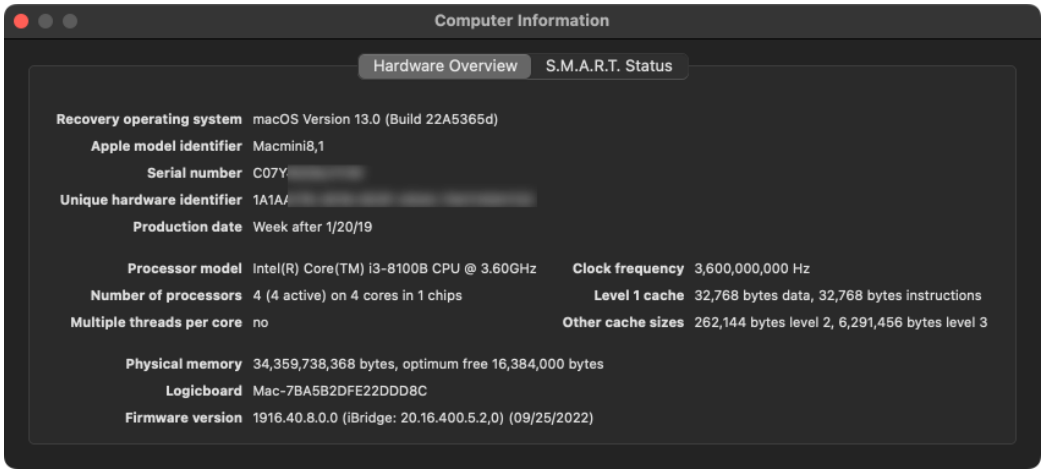


Figure 6.7: Hardware Overview

This corresponds with a simplified version of the feature **Info** > **Mac** in TinkerTool System.

6.6.2 S.M.A.R.T. Status of Hard Drives

All modern hard drives use a diagnostics technique complying with an industry standard which is called *S.M.A.R.T. (Self Monitoring, Analysis, and Reporting Technology)*. This standard has been introduced in 1992 to react earlier on hard disk failures. A hard drive supporting the S.M.A.R.T. standard monitors itself with its own micro processor and allows the operating system to request readouts that indicate whether operational parameters have changed in such a way that the hard disk might become defective in the near future. In this case, the hard disk can be replaced before any data is lost. The diagnostic processor of the hard drive summarizes the internal readouts into a simple yes/no value, the so-called *S.M.A.R.T. Status*. It can have the following two values:

- **Verified:** Based on the observed data, the diagnostic processor in the drive assesses that the drive will survive the near future.
- **Failing:** The measured values indicate that the drive has exceeded its expected lifetime. It should be replaced as soon as possible to avoid loss of data.

> Note that the S.M.A.R.T. Status does not indicate whether the drive is currently OK, or has a defect. It is not a test result in the strict sense. The S.M.A.R.T. Status is a recommendation only which assesses how the hard drive might behave in the near future. This assessment is based on the monitored technical data and the experience of the respective hard drive manufacturer.

Use the following steps to show the S.M.A.R.T. Status values of the attached hard drives:

1. In the main menu, click on **Show Computer Information**.
2. Make sure the tab item **S.M.A.R.T. Status** is selected.

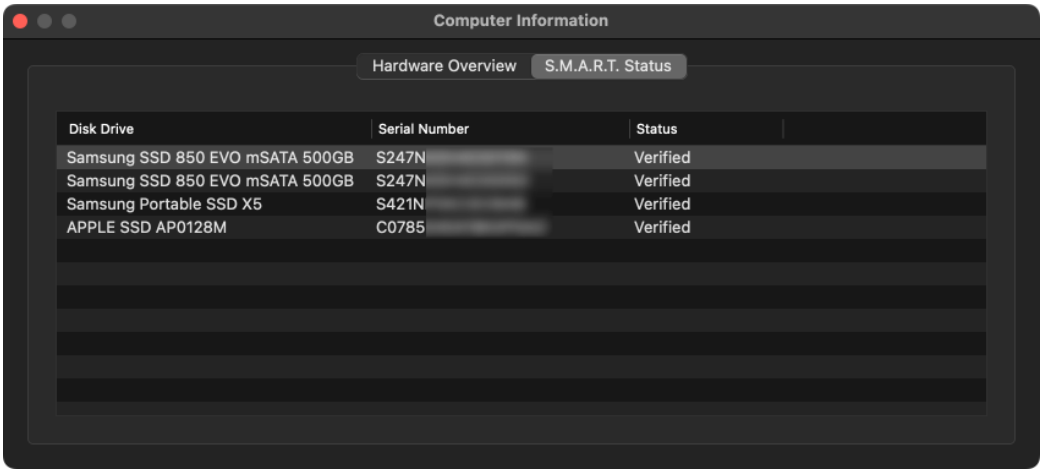


Figure 6.8: S.M.A.R.T. Status

> Most external hard drives are connected via a bridge chip which "translates" all transferred data between the SATA standard and the standard of the connection being used (e.g. USB or FireWire). Due to technical limitations, these bridge chips are not capable of transferring S.M.A.R.T. data. For this reason, the S.M.A.R.T. Status of hard disks can only be retrieved from drives which are directly connected to the computer by a SATA bus or via NVMe. A Thunderbolt connection can link these components neutrally in between. It does not block the transfer of diagnostic data.

6.6.3 Version Information of TinkerTool System for Recovery Mode

The version number of the utility and legal notes can be shown by selecting the menu item **ttsfrm** > **About TinkerTool System for Recovery Mode**.

Chapter 7

General Notes

7.1 Registering and Unlocking the Software

TinkerTool System 9 is electronically distributed software which is offered following a "First try, then buy" principle. You can download the application free of charge and test whether it fits your needs. You can select between two different modes of testing the program, named **Evaluation Mode** and **Demo Mode**.

7.1.1 Evaluation Mode

Evaluation mode allows you to use the software **without any limitations**, no matter if you own a registration or not. Only the following restriction applies:

> You can launch the application six (6) times per computer only. After six launches, evaluation mode will end and can no longer be enabled for any copy of this application having the version number you have evaluated. After the evaluation period has ended, the program will fall back to demo mode.

Certain conditions must be met to activate evaluation mode, however. To check whether your computer is eligible to test the current version of the application, it has to request permission from us via Internet. This permission is also known as *evaluation ticket*. Such a ticket is usually issued immediately, after a few seconds. To receive a ticket, the following conditions must be met:

- In order to save the ticket, you must have administrative permission for this computer. macOS may ask for administrator credentials.
- The computer must be connected to the Internet while requesting the ticket. For evaluation and operation of the program, an Internet connection will no longer be necessary.

- The Internet connection must not filter https traffic (encrypted web communication).
- You must grant the application permission to send us data containing
  - type and version number of the application,
  - an identification of your computer (e.g. a serial number of the hardware),
  - an identification of your Internet connection (e.g. the IP address), giving us permission to record these items.

The program will explicitly ask for this permission before any data will be sent and a ticket will be requested. After a valid ticket has been received, it will be stored on your computer and the application will be unlocked for evaluation.

7.1.2 Demo Mode

Without a valid registration (and after the free evaluation period has ended), the application will operate in demo mode only.

- A window with the note **Running in Demo Mode** appears each time the application is started.
- The window **Running in Demo Mode** also appears whenever you attempt to use a feature which is not included in the following list. This feature will be blocked, so it cannot be used.

The following features of TinkerTool System can be used in demo mode:

- Repairing the shared user folder
- Evaluate RAM size in relation to typical workload
- Removal of old versions of the emergency tool (Standalone Utility)
- Displaying system information
- Displaying processor information
- Displaying system management information
- Displaying the Safe Downloads List (malware protection)
- Displaying the deny lists for App Nap, HiDPI, and application launch
- Accessing classic logs and reports
- Analysis of file contents
- Display of Spotlight metadata for files
- Analysis of the security assessment for applications

- Computation of effective permissions
- Setting user preferences to override the language for specific applications
- Overview and analysis of all jobs auto-started for the current user
- Displaying different definitions of free storage space on volumes
- Display of advanced user account information
- Resetting all system settings which might have been changed to factory defaults

7.1.3 Unrestricted Usage

If you like to use the software permanently, you'll have to place an order for the required number of usage licenses. For each license you will receive a so-called *registration* which will allow you to switch the application from demo mode to normal operation.

Distributing or leasing the application or its license to third parties is prohibited without prior written permission. In particular, you have no permission to transfer the registration to somebody else. The exact contractual obligations for licensing the software are shown and can be printed after you have opened the downloaded software package.

7.1.4 Ordering Registration Files

Placing an order for registrations of TinkerTool System 9 is possible via our distribution partner and is usually done via Internet. Delivery is possible worldwide. Payments are accepted in more than 130 different international currencies, with common payment options supported for the respective regions.

To learn more about placing orders, please use the following Internet page of TinkerTool System 9:

`https://www.bresink.com/osx/301031383-2/order.html`

For first written information, you can alternatively select the menu item **Help** > **Purchase Registration**... in the application.

7.1.5 Different Types of Registrations

The registration info needed to fully unlock the application can have been delivered to you in three different forms:

- as a **registration key**, i.e. a sequence of letters and digits which can be easily saved or noted down. Informally, many users often refer to this as a "serial number", although the term does not really apply.
- as a **registration file**, usually presented by an entry ticket icon on macOS. Activation occurs by double-clicking or loading the file.
- as a pair of **registration name** and **registration key**: Instead of being delivered as a single character sequence, the registration is provided as a two-part text. Name and key belong together and must both be entered.

Which one applies to you should be easy to recognize. The different types of registration are due to the long historical development of the software. In many cases, the type of delivery depends on the date of your order:

- from December 1, 2024 onwards, simple registration keys are usually delivered.
- from June 1, 2016 to October 24, 2024, registration files were delivered.
- from May 1, 2001 to May 31, 2016, or in special license situations (such as press copies), and during the transition period in autumn 2024, pairs of name and key are delivered.

The necessary unlock procedures differ slightly, depending on what type of registration you have received. The following sections describe all unlocking procedures in detail. Only one procedure will apply to you.

7.1.6 Unlocking the Software with a Simple Registration Key

> If a key has been sent to you together with a readable registration name, this won't be the correct section for you. In this case, please look further down at "Unlocking the Software with a Name/Key Pair".

Unlocking the software by a simple registration key requires that your computer is connected to the Internet. (If you don't have an Internet connection, an alternative solution might be possible, but only in specific cases. Contact us for more information.) You should have received your registration key from the software reseller after your order had been processed successfully. Note that the key code represents a value, so it should be archived at a safe place, e.g. by printing it on paper or saving it into a password manager. If you had ordered multiple licenses for the same application, you will have received separate keys for each copy.

To unlock the application, perform the following steps:

1. Launch the application. The window **Demonstration Mode** will appear. Click the button **Unlock**…. (If the application was running already and the demo window had been closed, you can also select the menu item **TinkerTool System** > **Unlock TinkerTool System**….) The window **Registration and Activation** will appear.
2. Upon the question which type of registration you have received, click the button **Registration Key**.
3. Transfer the registration key exactly as you have received it into the field **Registration Key**. You can type the data manually. However, if you currently have the registration data on the order web page or the delivery email on the same computer, it will be easier to transfer the data by the features **Edit** > **Copy** (⌘ + C) and **Edit** > **Paste** (⌘ + V).

4. The application will be unlocked via Internet, and you'll eventually see a window which confirms your successful registration. In case of multiple licenses, the window will also inform you which key out of which order you have used.

If your Internet connection is not working correctly, or in the rare case that all licensing servers have technical problems, you will receive a related error message. In that case, please follow the instructions given in that message.

> The registration becomes valid for all user accounts of that computer.

7.1.7 Unlocking the Software with a Registration File

> This section describes how to use a *registration file* you have received from the software reseller. If you have received a readable key, possibly with an additional name, please look for more information in either the previous or next section at "Unlocking the Software with a Simple Registration Key", or "Unlocking the Software with a Name/Key Pair", respectively.

Unlocking the software by registration file requires that your computer is connected to the Internet. (If you don't have an Internet connection, an alternative solution might be possible, but only in specific cases. Contact us for more information.) You should have received your registration file from the software reseller after your order had been processed successfully. Note that this file represents a value, so it should be archived at a safe place, e.g. by copying it onto a USB pen drive reserved for that purpose.

If you had ordered multiple licenses for the same application, each registration will be represented by a separate registration file. The reseller has packed them into a single "zip" file. You can unpack this zip file by double-clicking it in the Finder.

A registration file is presented with the icon of an "MBS key card" and has a name ending with the marker "mbsreg." We assume that you had tested the application before placing the order for a permanent license, so both the program and the registration file should now be onto your computer. To unlock the application, perform the following steps:

1. Double-click the registration file in the Finder.

2. The application will be started if it is not running yet, it will be unlocked via Internet, and you'll eventually see a window which confirms your successful registration. That's all.

If your operating system is affected by technical problems, so it cannot locate the downloaded application for some reason, you can also load the registration file manually in the program:

1. Launch the application. The window **Demonstration Mode** will appear. Click the button **Unlock**.... (If the application was running already and the demo window had been closed, you can also select the menu item **TinkerTool System** > **Unlock TinkerTool System**....) The window **Registration and Activation** will appear.
2. Click the button **Load from file**... at the bottom of the window.
3. In the navigation sheet, locate the registration file and click the **Open** button to load it.
4. The application will be unlocked via Internet, and you'll eventually see a window which confirms your successful registration. This window also contains a confirmation code. *Note: This code is not a key which could be entered.*

If your Internet connection is not working correctly, or in the rare case that all licensing servers have technical problems, you will receive a related error message. In that case, please follow the instructions given in that message.

> The registration becomes valid for all user accounts of that computer.

7.1.8 Unlocking the Software with a Name/Key Pair

> This section describes how to use a delivery that contains a pair of *Registration Name* and *Registration Key*. If you have received a *single key* or a *registration file* from the software reseller instead, please see one of the two preceding sections.

Please note that the data pair you have received represents a value and should be archived at a safe place for future reference, e.g. by printing it on paper. The code consists of two parts, the **Registration Name** and the **Registration Key**.

Entering a Data Pair Manually

Perform the following steps to unlock the application for unrestricted usage:

1. Launch the application. The window **Demonstration Mode** will appear. Click the button **Unlock**.... (If the application was running already and the demo window had been closed, you can also select the menu item **TinkerTool System** > **Unlock TinkerTool System**....) The window **Registration and Activation** will appear.
2. Click the button **Name and Key** when you are asked for the type of registration you have received. Fields for the entry of the data pair will appear.
3. Transfer the registration name exactly as you have received it into the field **Registration Name**. You can type the data manually. However, if you currently have the registration on file on the same computer, it will be easier to transfer the data by the

features **Edit** > **Copy** (⌘ + C) and **Edit** > **Paste** (⌘ + V). Please pay attention not to transfer any additional blanks or empty lines. Also note that the contents of this field is case-sensitive.

4. With the same method, transfer the registration key into the field **Registration Key**.
5. Use the buttons at **Activate for** to select whether you like the registration to become active for the current user account only or for all users of this computer.
6. Click the button **Save**.

After both parts have been entered correctly, the window **Registration and Activation** will show your Certificate of Registration, with details about your license. You can close the window. If some part of the code has been entered incorrectly, an error message will be displayed. In this case, please check both parts of the code for exact match with the data that had been sent to you.

7.1.9 Entering a Crossgrade or Upgrade Registration

We may offer special licenses that permit to switch from a different product to the current version of TinkerTool System. In this particular case, it could happen that two registrations must be entered to unlock the program: one for the current application, and one for the application you previously used. The steps are the same as outlined in the previous sections, you only have to perform them twice. Please take care not to confuse the two different registrations.

- If you received a simple registration key for the previous product, enter it into the corresponding field in the Upgrade section of the window and leave the name field blank.
- If you received a registration file for the previous product, drag the file from the Finder onto the window.
- If you received a pair of name and key for the previous product, enter the data into the two fields in the Upgrade section of the window.

> If the previous product is still on your computer and fully unlocked, you will not be asked to provide a proof of purchase for the previous product.

7.1.10 Deactivate the Registration

You can deactivate the registration any time. Please perform the following steps:

1. Select the menu item **TinkerTool System** > **Manage registration**….
2. Click the button **Remove registration** in the product registration panel.

7.1.11 Handling Updates and Migrations

You usually don't need to care about your registration if you replace your copy of the application by a free update. Just drag the icon of the new version into the same folder where you have stored the previous version. The Finder will ask you if the old copy should be replaced. After the new version has been copied, you can simply launch it, and your registration will still be intact.

When migrating to a new computer, the situation could be different: If the application was unlocked by a personalized registration (with a Registration Name), you can simply use Apple's Migration Assistant to transfer all files of your system. Your registration will still be preserved and you won't need to re-enter it.

However, if the application was unlocked by use of a *registration file* or a *single key*, you will need to activate your registration once again, using the instructions given previously in this chapter.

7.1.12 Creating a Combined Ticket for Upgrade Licenses

As outlined in the previous section, you may need to re-register the application in some cases when moving to a new computer. This usually requires that you provide your registration data, and in case of an upgrade, a second key (or registration file, or name/key pair) for a previous product that proves that you are eligible to use the upgrade.

To avoid these tedious two steps, you can combine the two registrations into one single file. This file can then easily be loaded in a single step whenever it should become necessary to re-register the software. To create such a *one-step upgrade ticket,* perform the following steps:

1. Ensure that the application has been unlocked successfully by an upgrade license.
2. Select the menu item **TinkerTool System** > **Manage registration**….
3. Click the button **Create single-step upgrade ticket** in the product registration panel.
4. Follow the instructions to select the folder where the new file should be stored.

You should archive the file at a safe place. You can easily double-click the file later to re-activate your upgrade license on this or another computer. You will no longer need two separate registrations.

7.1.13 Working with Volume Licenses

If you need software licenses for an organization with a large number of computers, a single volume license can be used more efficiently than having separate licenses for each system. We may offer *site* licenses (for use on all computers of an organization located at one contiguous geographical site), and *global* licenses (for use on all computers of an organization worldwide), depending on product.

Please note the following guidelines if you are working with a volume license that was delivered after June 2016:

1. Customers with Volume Licenses can download the latest standard version of the software from the official web site.
2. One copy of the application must be registered with the Volume License registration file, using the normal method outlined in this chapter.
3. For that copy, the administrator enables a special feature of the application to generate an *Automatic Registration Request File for Volume Licensing*.
4. When copying the application onto a different computer of the organization, the request file must additionally be copied into a specific folder.
5. The first time the additional copy is launched, it will automatically register and activate the license.

So instead of just copying the application package only, a single additional file must be copied onto the destination computer. Note that each computer requires a working Internet connection when launching the application for the first time.

Generating Request Files for Automatic Volume Licensing

Ensure that you have already registered the application on one computer. Then perform the following steps:

1. Launch the application and open the menu **TinkerTool System**.
2. Hold down the option (⌥) key and select the menu item **Show Advanced Registration Features**. A window with a list of options will open.
3. Choose the option **Create auto-registration request for site license or global license** and click the **Start** button.
4. A navigation sheet will open, asking for a destination folder to save the file. Select a folder of your choice.
5. The application creates the request file in that folder. The file name ends with the marker **mbsalicreq**. *You must not rename the file.* Archive the file at a safe place, so you can distribute it to other computers of your organization later.

Using the Automatic Registration Request File

Each time you need to install the software on a new computer of your organization, you can have the application automatically register itself:

1. Copy the application bundle to the target computer.
2. Copy the auto-registration request file into the folder **/Users/Shared** of the target computer.

That's all. The application will auto-register as soon as it is launched. When the volume license could be confirmed via Internet, the auto-registration request file is automatically removed, so it cannot fall into wrong hands.

7.2 Important Release Notes

7.2.1 Workarounds for specific issues

Apple's approval feature for integrating security components is very immature: With macOS 13 Ventura, Apple introduced a new procedure that requires administrators to use System Settings to control whether to allow an application to install login items on the system or to let a program launch a privilege separation utility at the same time when the main application starts. These functions are immature and are affected by numerous technical defects. This can have influence on TinkerTool System 9, since for security reasons, it always uses the most modern form of privilege separation that a macOS version dictates. Among other things, there are the following issues:

(A) Apple incorrectly suggests that TinkerTool System would add an always-running background service: In the System Settings application, Apple states that Login Item permissions are required for background items that apps add *"to perform tasks when the application isn't open."* This description is incorrect or incomplete. Permission is also required for programs like TinkerTool System 9 that increase security through privilege separation by running a helper program *only when the main program is open*.

Workaround: We have notified Apple of this bug and hope it will be fixed in future versions of macOS.

(B) Network administrators cannot grant the necessary permission at the start of the program, but only via System Settings: When starting TinkerTool System 9 for the first time, macOS shows a notification that allows administrators to permit TinkerTool System 9 to run a privilege separation utility. This must be confirmed with an administrator's password. However, password entry only works for locally set up administrator accounts, not for network administrator accounts.

Workaround: We have notified Apple of this bug and hope it will be fixed in future versions of macOS. As a workaround, grant permission via **System Settings** > **Login Items** > **Allow in the Background** and not via the notification.

(C) If you store multiple copies of TinkerTool System on your computer in an unusual way, macOS service management may be overwhelmed: Current versions of macOS are not designed to handle situations where multiple copies of TinkerTool System can be found on your computer. (Copies in Time Machine backups do not count.)

Workaround: Only store one copy of TinkerTool System on your computer.

The privacy feature of macOS that grants TinkerTool System access to the full disk may fail if you have multiple copies of TinkerTool System on your computer: As noted in the chapter Basic Operations: Privacy Policy Settings of your Mac (section 1.3 on page 8), you have to approve that TinkerTool System has permission for Full Disk Access before you can use all features of the application. When you store multiple copies of TinkerTool System on your Mac however, this approval may fail unexpectedly. TinkerTool System may indicate that it does not have the necessary approval although it was given previously.

Workaround: This is a known design flaw of the Privacy feature of macOS. The protection feature can be confused when working with multiple copies of the same application.

Use the following steps to ensure that macOS grants permission to the intended copy of the software:

1. Identify all copies of TinkerTool System of your computer, e.g. by using Spotlight.
2. Delete all superfluous copies, keeping the correct one.
3. In System Settings, go to **Privacy & Security** > **Full Disk Access**, authorize as administrator, and remove the entry for TinkerTool System if available.
4. Re-add the entry for TinkerTool System.

Note that you can always keep backup copies of TinkerTool System on your Time Machine disks. This may not work when using third-party backup applications, however.

The size values for APFS snapshots on inactive operating system volumes can be wrong: Current versions of macOS are unable to determine the private size of APFS snapshots correctly if the snapshots belong to a volume of another macOS installation on your computer. In this case, you may receive a private size of zero and a tide mark at the 4.61 exabyte position.

Workaround: There is no known workaround. Apple's Disk Utility is also affected by this issue.

If you specify a time interval while querying the system log, specific versions of macOS may return incorrect data in case the time interval is a few seconds around the startup time of a Mac with Apple Silicon: If you use the feature **Info** > **Logs** to get an excerpt from the system log and you specify a time interval targeting the first boot phase of an Apple Silicon processor exactly, macOS will often return an incomplete or empty log as result.

Workaround: This is a defect in current versions of macOS. It is currently unknown when and if Apple will fix this issue. As a workaround, you can try to shift the time interval by a small amount, e.g. by 10 seconds after the startup time. In most cases, macOS will then provide the correct excerpt from the logs. Macs with Intel processors are generally not affected by this problem.

7.3 Version History

7.3.1 Release 9.41 (Build 250310)

- Added new feature to hide disk volumes on the graphical user interface. The Volumes part of the System pane was redesigned completely to integrate this option.

7.3.2 Release 9.4 (Build 250203)

- Adds new pane to control the automatic power-on feature of portable Macs with Apple Silicon. Autostart by opening the lid or connecting power can be prevented (macOS 15.3 or higher required).
- The layout of panes that don't have submenus has been modified slightly.

7.3.3 Release 9.3 (Build 250121)

- The list of Macintosh model series shown when downloading components to create macOS installation media has been updated.
- The interface of the control pane to protect user data against iCloud access has been slightly redesigned. This should prevent users from mistakenly locking iCloud features in the active ("on") state.
- This versions adds a workaround for an issue in some versions of macOS where flash storage and SSD health supervision mistakenly monitor the magnetic disk parts of Fusion Drives.
- Some technical details have been updated in the reference manuals.

7.3.4 Release 9.2 (Build 241119)

- Added new feature to show the current operational status and version of the XProtect antivirus software which is part of macOS. (The functions are located on the pane Maintenance.)
- Added new feature to retrieve the status info of the latest version of XProtect currently offered by Apple.
- Added new feature to update XProtect immediately.
- Added new feature to retrieve the activity log of XProtect.
- The feature to check whether an installed application has been published via the App Store (which had to be removed in July 2024) was completely rewritten using different technology, so it could be reinstated.
- The feature to retrieve the activity log of Time Machine backup sessions (which had to be removed for macOS Sequoia) was completely rewritten using different technology, so it could be reinstated. This feature is available for APFS backup media only.
- The feature to download IPSW files for macOS installation media now shows updated info for Macs with M4 processors released in November 2024.
- Added new user interface for simplified license registration and activation features which will become available in the near future.

7.3.5 Release 9.1 (Build 241014)

- As Apple has now released the official manuals and support documentation for macOS Sequoia, all links in the quick-help feature could be updated and adjusted accordingly.
- The Uninstallation Assistant now also deletes the user's corresponding list of recent documents when removing an application.
- Added a workaround for an internal issue of macOS Sequoia which could prevent the Logs feature from opening archived copies of the macOS log database.
- The feature to modify the user's POSIX permission filter is now supported again when the application detects an operating system version which is capable of providing this feature reliably.
- The term "Apple Account" has been updated in the reference manuals.
- Fixed a problem where the feature to delete a selected Time Machine snapshot from APFS media confirmed a successful removal when actually no operation was performed.

7.3.6 Release 9.0 (Build 240916)

- Added full support for macOS 15 Sequoia.
- More than 1,000 internal changes to optimize for macOS 15.
- The timing behavior when accessing values from the Open Directory database has been changed. The ensures better performance and avoids possible deadlocks with slow database connections.
- Fixed a problem where some state designations for certain configuration settings could be shown in English instead of the language selected by the user.
- Fixed a problem where changing the default user name for network logins did not work as expected.
- The features to modify the permissions filter for new file system objects and to rebuild the Launch Services database have been made invisible at the moment, because the first versions of macOS Sequoia don't run stable enough to support this. These items can hopefully re-appear at a later time.
- The features to compute change statistics, local file deletion and log retrieval for old Time Machine backups created on HFS+ volumes have been removed, because they are no longer supported by macOS 15.
- The diagnostic feature to test for specific defects of copy operations via the macOS Finder have been removed because new defects can have an impact on old ones, making the results less meaningful. Apple did not fix these issues in the last 14 years.

- The feature to reset a hanging macOS software update request had to be removed because it was blocked by Apple.
- The following features have been removed because they no longer make sense with macOS 15, or the necessary system components are no longer present in Sequoia:
  - Removing invalid keychain entries created by Xcode
  - Repairing the color tags feature for objects on network file servers
  - Firmware integrity checks for EFI and for Broadcom Ethernet chips
  - Unlocking outdated AFP authentication methods for old AppleShare servers
  - Catalina security guidelines for execution of Remote Apple Events
  - Resetting or repairing the startup language setting
  - Showing computer-related info on the login screen
  - Enforcing rerun of the macOS Setup Assistant via TinkerTool System for Recovery Mode.

7.3.7 Release 8.95 (Build 240731)

- Added support for alternative preview versions of upcoming operating systems.
- Added new feature to add color tags to file system objects stored on network servers (see Issues > Tags). This can be used as workaround for defective versions of the macOS Finder which can no longer do this.
- When showing undocumented Spotlight attributes for files, TinkerTool System will now handle cases where Spotlight has intentionally stored invalid date and time values more transparently.

7.3.8 Release 8.94 (Build 240712)

- Added new feature to disable the indicators for caps lock and dictation next to the text caret (see System Miscellaneous settings, macOS Sonoma and later only)
- Added new feature to disable the Emoji suggestion assistant next to the text caret (macOS Sonoma and later only)
- Added new features to describe more undocumented Spotlight attributes when analyzing the contents of files. More than 20 attributes have been added (see File Contents pane).
- Added new features to describe more Sandbox exceptions when analyzing the security of applications. More than 80 entitlement entries have been added (see Applications Security Check).
- Added the detection of new types of temporary files when checking and cleaning preference settings (User pane). This also affects TinkerTool System for Recovery Mode.

- The entry to assess whether an application was licensed via the App Store was removed from the Applications Security Check pane. Due to changes in the App Store, a reliable analysis is no longer possible.
- The policy not to allow the removal of Apps purchased from the App Store via the Uninstallation Assistant is no longer in effect.

7.3.9 Release 8.93 (Build 240612)

This release adds preliminary support for future versions of macOS.

7.3.10 Release 8.92 (Build 240515)

- Added new feature to reset the macOS time synchronization service (on the pane Issues). This can repair the operating system in cases where it continuously sets wrong time and date.
- The filtering options when retrieving log entries from the macOS log database now permit to use identifiers and names containing spaces.
- The general icons indicating successful or failing operations have been modernized throughout the application. They will now better match the design of up-to-date macOS versions.
- Internal modifications and updates necessary to adapt to changes in recent versions of macOS.
- Fixes a problem where it was possible to leave the pane for Power Schedule settings without saving changes.
- Fixes a problem especially with slow computers where retrieving entries from the macOS log database could sometimes fail with an error message indicating a possible syntax error.

7.3.11 Release 8.91 (Build 240417)

- Added new feature to separate or extract logs for specific process instances after a query has been made in the macOS log database.
- The user interface to work with the macOS database has been slightly redesigned.
- Fixed a problem where the options to retrieve source program and “signpost” information from the macOS log database did not work as expected.
- Changed error handling for cases where Apple blocks maintenance access to the macOS Software Update Service in operating systems published after March 2024.
- Several changes in the internal application architecture.

7.3.12 Release 8.9 (Build 240214)

- The feature to work with Spotlight was completely rewritten to supported the latest operating system versions. The corresponding user interface was redesigned.
- Added new detail panel when reviewing the Spotlight index of a volume.
- Added progress display when discarding or restoring unprotected user caches.
- Added new diagnostic features to determine whether and why macOS is slow when processing inactive user caches.
- All tables where bullets are used to indicate yes/no status information now use larger bullet characters for better readability.

7.3.13 Release 8.89 (Build 240111)

- Added new features for authorization of privileged operations. The application will now allow authentication of administrative users in additional special cases previously not permitted:
  - authorization within a running login session of a non-administrator
  - authorization by administrators with empty passwords in operating system versions that don't block this generally
  - authorization in cases where multiple users are logged in, but the affected user is not on the frontmost console session
- Administrators can return to the previous stricter authorization policies if needed.
- Added features on the Power Schedule pane that allow the definition of repeating events with more complex configurations. It is now possible to define arbitrary combinations of weekdays to trigger power events.
- Added a refresh button on the pane to remove slow-motion screen savers (macOS Sonoma only).
- Updated list of system services that perform automatic cleanup of storage space.
- Small changes in data presentation on the pane for RAM size evaluation.
- Fixed a problem where the layout of integrated TinkerTool panes was not as intended with specific operating system versions and languages.

7.3.14 Release 8.88 (Build 231116)

- Added new feature to remove the large files of optional Apple slow-motion screen savers immediately if necessary (macOS 14 or later only).
- Added support for new Background Item technology in upcoming versions of macOS.

- Added support for testing fans on Macs with M3 processors.
- All features that search or modify files selected by the user have been revised to avoid conflicts with iCloud or cloud solutions of other vendors. Opening affected folders will no longer trigger automatic synchronization downloads executed by macOS.
- Updated support for cleaning kernel core dump files.

7.3.15 Release 8.87 (Build 231024)

- Added new feature to remove history entries from the user's "Go to folder" panel of the Finder.
- The feature to reset home folder permissions for a user account was rewritten completely:
  - The accuracy when recreating the recommended permission settings of a fresh macOS user account has become even higher.
  - The folder modification dates will now only be changed if necessary.
  - Files owned by the operating system will now be included in the reset procedure.
  - A new reminder dialog makes the user aware that cloud synchronization should be avoided while the reset operation is running.
- Added support for new authentication situations available in macOS Sonoma.
- The quick help feature was updated to consider Apple's latest additions to macOS reference manuals.
- Many small changes and optimizations in the user interface.
- Fixed a problem where TinkerTool System for Recovery Mode (ttsfrm) could show a misleading error message on Macs with Apple Silicon.

Note: Users who like to integrate TinkerTool into TinkerTool System need to update TinkerTool to version 9.6 or later for technical reasons.

7.3.16 Release 8.86 (Build 230925)

- Added full support for macOS 14 Sonoma.
- Added new options to reset the privacy settings for Location Services, Motion & Fitness (macOS 14 or later only), and Passkeys Access for Web Browsers.
- Added new features for software developers when performing a security check on a single application that is not planned to be distributed through the App Store: It can be validated whether an application is ready either to be submitted to Apple's notary service, or to be executed on customer computers. This feature is only available for macOS 14 or later.

- Users can now also go back to the overview menu of a pane with subitems by clicking onto the pane in the sidebar.
- Due to architectural changes in recent Macintosh models and macOS versions, the feature to disable System Integrity Protection by mouse click via the emergency utility (ttsfrm) had to be removed.
- Fixed a problem where the current status of System Integrity Protection may not have been shown correctly on Macs with Apple Silicon.

7.3.17 Release 8.85 (Build 230816)

- Added new feature to the monitor test. It is now possible to add a moving black raster overlay with a grid size of 1 or 2 physical pixels to the color screens. This can make it even easier to detect hanging or dead pixels on high resolution displays.
- Added a workaround for a design flaw in macOS Ventura which could prevent the creation of install media for older versions of OS X and macOS.
- Added further support for future versions of macOS.
- Some workflows on the Install Media pane have been modified to work more efficiently.
- The instructions on the Emergency Tool pane for working with TinkerTool System on macOS Recovery systems now use special markers to identify spaces in the necessary Terminal command more clearly.

7.3.18 Release 8.8 (Build 230712)

- Added new feature to change the time specifications for file system objects. This includes, if available, time of last modification, last access, last backup, and the creation time. The time of last status change is shown additionally.
- Added new feature to support the revised beta test procedures of macOS. On the Info pane, the indicator Release Status on the Operation Environment page was replaced by a System Update Source field.
- Added new field for idle latency in the results of the macOS network responsiveness test.
- Added further support for future operating systems.
- Many small changes in the user interface reflecting new developments in macOS.
- Fixed a problem where the Finder copy operation checks could not be run, because macOS prevented it.

7.3.19 Release 8.7 (Build 230614)

- Added new feature to detect and clear orphaned Access Control List permissions from a local volume. Orphaned ACLs refer to accounts no longer present on the system.
- Added new feature to indicate the true type of file system objects presented by the Finder as alias.
- Added new feature to transfer orphaned files which no longer have a known owner to other user accounts. This is an alternative option for the feature known for years to automatically remove such files.
- Added new feature to repair the operating system in cases where macOS does not allow TinkerTool System to launch successfully due to corrupt settings for Background Items. The corresponding situation is detected automatically.
- Added preliminary support for future operating systems.
- Fixes a compatibility issue with specific versions of macOS where deleting a Time Machine snapshot was always rejected with error code 2 if the backup destination was an APFS volume.

7.3.20 Release 8.6 (Build 230515)

- Added new feature to check, enable, or disable automatic defragmentation for APFS volumes on magnetic disks.
- Added new features to guide users through the limitations of macOS 13 that affect the application's approval for Background Items and Full Disk Access.
- The Info pane now also shows the version number of Apple's XProtect antivirus software in addition to the version of the malware definition files.
- The security policy for access to the Power Schedule settings has changed: As in former versions of System Settings, separate administrator authentication is no longer necessary.
- The features to check integrity of the EFI firmware and Broadcom Ethernet firmware on Intel-based Macs have to be removed until further notice. Current versions of macOS 13 are no longer capable of performing such checks correctly.

7.3.21 Release 8.5 (Build 230418)

- Due to new limitations in macOS developer tools, the internal architecture of the application has changed. Users who like to use TinkerTool from within TinkerTool System have to update to TinkerTool 9.3 or later for technical reasons.

- Support for the new architecture of macOS 13 to control privileged operations has been reinstated. Due to limitations of macOS 13, some operating system versions may require a restart of the computer during the very first launch of TinkerTool System.
- Support for cleaning outdated installations of automatically starting jobs has been reinstated.
- Main categories in the application sidebar are now emphasized more clearly.
- Added new feature to show system XPC services, application-embedded daemons and application-embedded agents in the list of automatically starting jobs.
- Added new feature to show the build numbers of available macOS versions when presenting the list of installer applications offered by Apple for download.
- Added new feature to detect if the size specifications advertised by Apple in the list of installer applications available for download are plausible. If not, the storage size will automatically be corrected.
- Added new feature to detect why the creation of installation media may be refused by Macs with Apple Silicon.
- Added new feature to detect if volumes are handled by Apple's LIFS technology (Live File Provider File System) to indicate that they are not compatible with the macOS volume exclusion tables shown on the System pane.
- Several small changes and clarifications in the GUI and the reference manual.
- Fixed a problem where the repaired version of the macOS 10.12 installer was rejected as invalid software when creating install media.

7.3.22 Release 8.4 (Build 230315)

- Added new feature to manage the user accounts of FileVault.
- Added new feature to check the personal recovery key of FileVault.
- Added new feature to list the user accounts which are capable of decrypting a given APFS volume.
- Added new feature to determine which user accounts are defined as owners of an APFS volume (only on Macs with Apple Silicon). "APFS volume ownership" is required to manage the startup security policy for a macOS installation, to perform macOS installations and updates, or to run the "erase all contents" procedure.
- Added support for future versions of macOS 13.
- The preference setting to automatically show the sub-feature overview menus when switching between application panes is now enabled by default. Experienced users can disable this option any time via the settings window.

- The feature to analyze Ventura “Background Items” has been extended to support very complex setups.
- The wording to describe the different types of recovery systems on Macs with Apple Silicon has changed for clarification.
- If the installation of the security component is damaged, the application will now determine the exact technical reason together with individual instructions how to resolve the problem.
- Fixed a problem where clicking the button to analyze Ventura “Background Items” appeared to have no effect in some cases.

7.3.23 Release 8.3 (Build 230215)

- Added new feature to detect and to remotely analyze a Content Caching server in the local network. Such servers can cause issues during macOS software updates.
- Added new feature to reset the macOS service management of Background Items. This is helpful for users who are flooded with repeated notifications of added Background Items, or who see incorrect entries for these items in System Settings.
- Added new and unique feature to analyze the list of Background Items maintained by macOS. The allows the confusing and often erroneous entries in System Settings to be better understood.
- The list of model series for the download of IPSW files was updated.
- The list of Apple-provided system jobs was updated.
- The item to repair features of the macOS network user interface which could be damaged by the 11.2 update was removed. It is no longer needed in macOS 13 Ventura.

7.3.24 Release 8.2 (Build 230123)

- Added new feature to download IPSW files from Apple. IPSW files can be used to perform a full restore with factory reset in DFU mode on Macs with Apple Silicon.
- Added new feature to clear the message index database of Apple Mail. This is helpful to resolve issues when searching for email messages no longer works correctly and produces incomplete results.
- The currently selected Time Machine backup time interval and encryption mode are no shown on the Time Machine pane.
- The user interface for the Flash Drive status has been redesigned. This allows the Diagnostics pane to be shown with reduced height and resolves issues where some controls were difficult to access on small screens.

- Fixed a layout problem on the pane "User > Repair Defective Settings" for cases where the pane was resized to its minimum.
- Internal changes for features with Internet access, enhancing compatibility with third-party firewalls.

7.3.25 Release 8.14 (Build 221220)

- Because many users are confused by the bad quality of macOS 13.1, this version adds more protection against operating system defects and provides additional user guidance.
- Adds protection against cases where the application is configured for automatic software update checks, but is operated with a network firewall that doesn't allow the necessary Internet connections. In specific cases, this could result in intermittent program termination instead of an error message.

7.3.26 Release 8.12 (Build 221214)

This version adds additional workarounds for defects of macOS 13.1.

7.3.27 Release 8.11 (Build 221212)

This is an emergency update which has become necessary because Apple released a build of macOS 13.1 with several critical defects. These defects can prevent TinkerTool System 8 from launching successfully under specific circumstances.

We are downgrading the security component of TinkerTool System 8 to technology of macOS 10.12 Sierra to avoid specific new features of macOS 13 which are not ready to be used at the moment. Over the last 6 months, Apple has not been capable of providing system services that comply with the specifications of Ventura.

7.3.28 Release 8.1 (Build 221205)

- Added new pane to regain access to the power schedule of macOS. As in older versions of the System Preferences application, the Mac's features to schedule power-on, shutdown, sleep or restart events in regular time intervals during the week can be controlled by a few mouse-clicks.
- In addition, the power schedule of macOS for one-time events can be reviewed and fully edited.
- A toolbar was added to the main control window. It will cause macOS to show the titlebar of the window with a more aesthetically pleasant look.
- Optional control items have been moved from the sidebar to the toolbar.
- The items in the sidebar now automatically respect the user's general preference setting for sidebar display size.

- The items in the sidebar now maintain their status information for expanded or collapsed sub-items when relaunching the application.
- A new preference setting was added to allow the user to always prefer the feature overview of a pane instead of having the last used sub-feature opened.
- All Internet links in the Quick Context Help feature have been updated because Apple has finally published the user manual for macOS Ventura.
- This version fixes a problem where the general reset feature may not have worked as expected for the Cloud Protection pane.

7.3.29 Release 8.0 (Build 221019)

- Added full support for macOS 13 Ventura. TinkerTool System 8 can only be used with macOS 13 or later. It allows the integration of TinkerTool 9.
- The application uses a completely new user interface, based on the style specifications for the program “System Settings”. This also includes searching for features by keyword.
- The application window can now be resized. When showing tables with many columns, previous additional functions to “show in separate window” are no longer necessary.
- A new button has been added to optimize the currently shown pane in size, automatically selecting the smallest possible size to control all user interface objects.
- The auxiliary program for privileged operations now uses the latest Ventura technologies. It is no longer necessary to install it upon first start, it only needs an approval to run.
- If you integrate TinkerTool into TinkerTool System, its panes will also become accessible by keyword search.
- The feature to scan open network ports had to be removed. The necessary components are no longer available in macOS 13.
- The feature to automatically clear erroneous background services is blocked temporarily. Ventura uses new technologies to control such services, but they are currently not mature enough. It is planned to re-enable this feature later when macOS 13 has reached the necessary level of reliability.

TinkerTool System 8 begins a new product line. The section above lists changes in comparison to TinkerTool System 7, version 7.91. For more information about the version history of TinkerTool System 7, please see the respective application.

Appendix A

Tasks and Solutions

A.1 Where is this function now?

Information for users who moved from TinkerTool System 8

If you have performed an upgrade from macOS 13 Ventura or macOS 14 Sonoma to macOS 15 Sequoia or later, and you are searching for missing features in TinkerTool System 9, please use the table below to learn why specific functions can no longer be supported, or whether they are now located at a different location or under a different name, respectively.

All items not listed have kept their original locations and names.

A.2 Should I do any regular maintenance?

The short answer is: No.

macOS is designed not to need any form of regular —i.e. scheduled— maintenance. All housekeeping jobs are already performed automatically by the operating system. Under normal circumstances, you won't have to care about technical details, which follows the usual philosophy of Apple products. Recurring tasks, like monitoring printers, or removing expired crash logs, are automatically handled by service programs running in the background. Other tasks, like defragmenting hard drives, are carried out as a side effect of normal operations, or are avoided altogether by using up-to-date technology.

For this reason, **you won't need to use any of the features of TinkerTool System on a regular basis**. By intention, the tool does not contain any scheduler, "autopilot," or similar functions.

In some cases, scheduled maintenance could even be harmful to your computer. In particular, this is true for most cache-cleaning features. Cleaning caches can be an important troubleshooting procedure in case your computer is indeed suffering from a software problem, but it always has bad side effects, because the system and applications have to rebuild their caches, which can take days, depending on case. During this period, the

Table A.1: Comparison of feature locations

Previous Location	Current Status
Time Machine X (macOS 10 mode) > Compute Statistics on Changes	*removed*, because no longer supported by macOS 15
Time Machine X (macOS 10 mode) > Delete Data on any Local TM Disk	*removed*, because no longer supported by macOS 15
Time Machine X (macOS 10 mode) > Logs	*removed*, because no longer supported by macOS 15
Issues > Software Update > Reset Hanging Search	*removed*, because blocked by Apple as of March 2024
Issues > Xcode Keychains	*removed*, because no longer necessary with macOS 15 and Xcode 16
Issues > Tags	*removed*, because no longer necessary with macOS 15
Diagnostics > Finder Copy	*removed*, because no longer useful and meaningful
Info > Classic Logs & Reports > Other > Output of … maintenance script	*removed*, because no longer supported by macOS 15
Operational Safety > EFI Firmware	*removed*, because no longer supported by macOS 15
Operational Safety > Broadcom® Ethernet	*removed*, because no longer supported by macOS 15
System > Network > Allow outdated AFP authentication methods	*removed*, because no longer supported by macOS 15
System > Remote Apple Events	replaced by *System Settings* > *General* > *Sharing* > *Remote Application Scripting*
Startup > Language	*removed*, because no longer needed in modern OS versions
Login > Settings > Special Features > Show … when clicking the clock	*removed*, because no longer supported by macOS 15
User > Launch Services	*invisible* at the moment, because macOS 15 not stable enough to run this
ttsfrm > Advanced Features > Re-run Setup Assistant upon next OS start	*removed*, because no longer supported by macOS 15

system will run slower than usual, because cache information has to be refetched or recomputed. In summary, cleaning caches without a specific technical reason does not make any sense. It will cause the computer to run worse. For this reason, TinkerTool System introduced new features which can troubleshoot caches, but avoids cache-cleaning unless it is absolutely necessary.

> This does not mean that macOS would not need any maintenance at all. But you won't need to do it on a regular basis. Maintenance should only be done when there is actually something to repair.

There can be several causes for technical problems with a computer running macOS, which make maintenance necessary:

- Early versions of the operating system may contain defects ("bugs") which have not been fixed yet.
- The operating system can contain general design flaws which are not planned to be fixed, but are causing problems nevertheless.
- Badly written installation software of third-party vendors has damaged parts of the system.
- While working with administrative permissions, you have made a mistake in operating the machine.
- You like to use advanced features of the system, but don't have the necessary skills to activate them on the UNIX command-line.

In all these cases, TinkerTool System can assist you.

> If you are unsure when to use a specific maintenance feature of TinkerTool System, click the help button at the upper right of each control pane.

A.3 How can I repair the system if macOS displays garbled text when using certain fonts?

In nearly all cases, this problem is caused by technical problems with Apple's font registration server. It can be fixed by forcing this subsystem to rebuild its caches. Perform the following steps:

1. Verify if only a particular user account, or all user accounts are affected by this problem. Make sure you are logged in as the user who experiences the problem.
2. Open the pane **Caches**.
3. Select the sub-item **Font Caches**.

4. If only the current account is affected, select the item **Clean font caches of the user**…. If all users are affected, select the item **Clean font caches of the user and the operating system**.

5. Press the button **Clean font caches**.

Further information: The Pane Caches (section 2.2 on page 32).

A.4 How can I display the actual permission settings for a file or folder?

Because the display of permission settings in the Finder is very confusing or even wrong, TinkerTool System can help you to retrieve the true permission settings for a file or folder. Perform the following steps:

1. Open the pane **ACL Permissions**.

2. Select the sub-item **Show or Set Permissions**.

3. Drag the object in question from the Finder into the field **File or folder**.

The permission settings will be displayed in the table **Permissions and Ownership**.
Further information: The Pane ACL Permissions (section 3.4 on page 198).

A.5 Unlocking the Application

If you like to use TinkerTool System 9 without restrictions you'll have to purchase a registration that confirms that you have licensed the software for permanent usage.

1. Select the menu item **TinkerTool System** > **Unlock TinkerTool System**…. The window **Registration and Activation** appears.

2. Choose which type of registration you have received. Since the end of 2024, this should usually be **Registration Key**.

3. Transfer the key code you have received into the field **Registration Key**.

4. Click on **Save**.

5. Confirm your approval to let the application connect to the Internet.

6. Wait a few seconds until your registration has been confirmed.

The confirmation will be displayed. You can close the window now.
Further Information: Registering and Unlocking the Software (section 7 on page 323)

Index

T