Documentation 0688-1969/2

TinkerTool System 6

Reference Manual

Marcel Bresink
Software-Systeme

Version 6.995, June 7, 2022. US-English edition.
MBS Documentation 0688-1969/2

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 6?

TinkerTool System 6 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 Preferences,
- 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,
- 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 Preferences application.

In the remainder of this manual, we will use the designation "TinkerTool System" for simplicity, omitting the "6." However, there are in fact five 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 11.0 Big Sur

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. Administrators of large system installations can fine-tune the security policy of TinkerTool System, for example by giving different classes of administrator groups different permissions to perform certain operations. In order to do this, TinkerTool System integrates seamlessly into the authorization policy database of macOS.

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 6

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 6, you need an *Apple computer* which has the following operating system installed:

- macOS 10.14 Mojave
- macOS 10.15 Catalina

It is recommended to update macOS to the latest version which is available from Apple. This can be done using the **Automatic Software Update** 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 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:

The running user session must be owned by an administrator: 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 login session in which TinkerTool System is running must have been started by this user, or by a different user who has also been granted administrative rights. This means it won't be possible to initiate a privileged operation for a user account which has not logged in as administrator. You cannot act as a different user while your identity is being verified by entering that user's name and password.

> This is compliant with the classic security guidelines that were established for the first generations of macOS (called Mac OS X at that time), and is stricter than the guidelines usually in effect for graphical applications running with modern versions of macOS. The policy is similar to that used by macOS and other Unix systems for the *sudo* command on the command line, which is also responsible for unlocking privileged operations individually.

If you are currently working with a user account that has no administrative rights, you won't need to cancel your running login session in order to use TinkerTool System, however. By using **System Preferences** to activate the option **Users & Groups** > **Login Options** > **Show fast user switching menu as**, you can enable an item at the top right hand side in the graphical user interface of macOS which allows a direct re-registration, starting a second login as system administrator. This way you can work with multiple screen sessions for different users and switch back and forth between them.

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

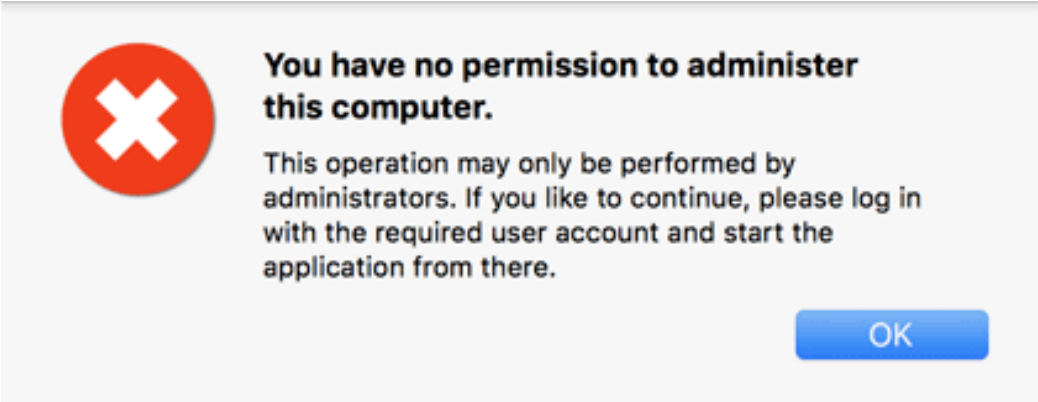


Figure 1.1: The login session must run for a user with administrator permissions.

> 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.

An administrator cannot have an empty password: Although it was possible with previous versions of macOS to create user accounts for administrators without a password (which actually means they have a password of zero length), up-to-date versions of the operating system consider this a configuration error. Affected administrator accounts cannot authenticate in all cases and several system features will fail for them. This includes the privileged operations which can be used under control of TinkerTool System. With default methods, accounts without passwords can no longer be created. If you still have such an account which was migrated from an older version of macOS, you must define a password for it before the account is permitted to use any features of TinkerTool System that require privileged operations.

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. To check the pending operation, there will also be an additional short description in the *Touch Bar* , like that in the depicted example. As usual in macOS, you can choose whether to identify by password or by fingerprint.

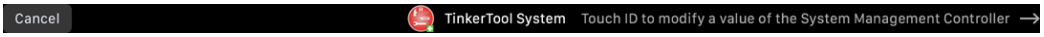


Figure 1.2: On computers with Touch ID, the confirmation is also possible by fingerprint. The Touch Bar shows a notification in this case.

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** > **Preferences**... 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.

The paragraphs below contain information for experienced system administrators. You can skip them during first reading.

1.2.2 Technical Details for Advanced Users

The security component will be installed into the folder **/Library/PrivilegedHelperTools** which is Apple's recommended folder to be used for such utility programs. The name of the component is **TinkerToolSystem-PrivilegedTool**. macOS will automatically launch and quit this program as needed, avoiding to let it run as a background service for an extended period of time.

You can choose to remove the security tool at any time without any traces. In this case TinkerTool System will lose its capability to access privileged system areas, so the program will be forced to shut down either. Perform the following steps to remove the component:

1. Launch TinkerTool System if it is not running yet.
2. Select the menu item **Reset** > **Remove Security Component**....
3. Follow the instructions the program is giving. The program will quit itself as last step of this operation.

1.2.3 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**....

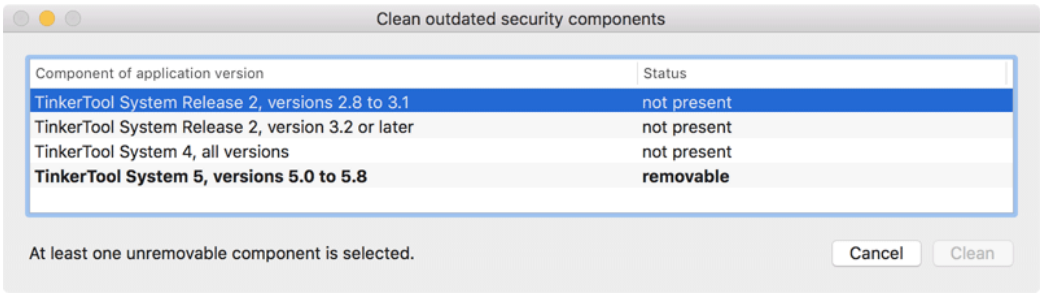


Figure 1.3: Outdated copies of the privileged helper can be removed if desired.

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.

1.3 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 1.4: The control window of TinkerTool System with TinkerTool integrated

The control window is divided into horizontal bars, representing the different functional areas of the application. Each bar contains a number of icons which can be clicked to open the control pane connected with the respective feature set. For example, clicking on the icon **Info** in the row **System Maintenance** will open the pane named **Info**, used to access detail information about the computer and operating system. The panes behave very similar to the items found in the System Preferences application of macOS.

As an alternative, you can select one of the items in the menu **View**. Jumping from one pane to the next or previous one is possible by clicking one of the two arrow buttons in the toolbar of the control window. Stepping through the panes is also possible by menu, selecting the items **View** > **Back** or **View** > **Forward**, respectively, or by pressing ⌘+← or ⌘+→. To go back to the overview of all pane icons, click the button with the little dots in the toolbar of the window, or select the menu item **View** > **Show All Panes** (⌘

+ L).

You can also use keyboard navigation to open the different panes. If you like to do that, you'll have to ensure that full keyboard access is enabled for your user account:

1. Open the **System Preferences** application.
2. Open the pane **Keyboard** and its tab item **Shortcuts**.
3. Verify that the button **All controls** is selected at **Full Keyboard Access**.

If full keyboard access is active, press the tab key ⇥ in the control window of TinkerTool System to display the keyboard focus ring in the pane overview. You can then move the focus using the arrow keys or tab keys. Press the space-bar to open a pane.

Panes can also be subdivided into different functional areas. Tab items are used to select between these features. TinkerTool System automatically remembers which tab was open the last time you used a pane. It will automatically go back to the previously selected item the next time you use the pane again.

1.3.2 Searching for features by keywords

TinkerTool System offers a high number of different features. You may not use all of them regularly and may forget on which pane and tab they are located. To help you in this case, you can search for functions and options by keywords: Ensure that the icons for all panes are visible, then type a word for the feature you are looking for into the search field in the upper right corner of the window. After having typed the first letters, TinkerTool System will additionally make suggestions based on your input. You can select one of the suggestions by clicking, or by using arrow keys and then pressing the ↵ key. This will automatically open the related pane and tab. While searching, TinkerTool System dims the overview of panes and highlights the items that relate to your keyword.

The entered keyword can be deleted by clicking on the button with the cross in the search field.

1.3.3 Using the Touch Bar

If you have a Mac with a Touch Bar, you can also use the bar as an alternative for navigating between panes or searching for features. The controls to switch to the previous or next pane, to the icon overview, or to enter a search keyword can also be found in the Touch Bar.

Figure 1.5: The elements of the toolbar are also available on the Touch Bar

1.3.4 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 tab 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.

1.3.5 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 tab item, so you will have the chance to review settings and to adjust them before anything will happen.

1.3.6 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 1.6: 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.

1.3.7 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.

1.3.8 General Preferences

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

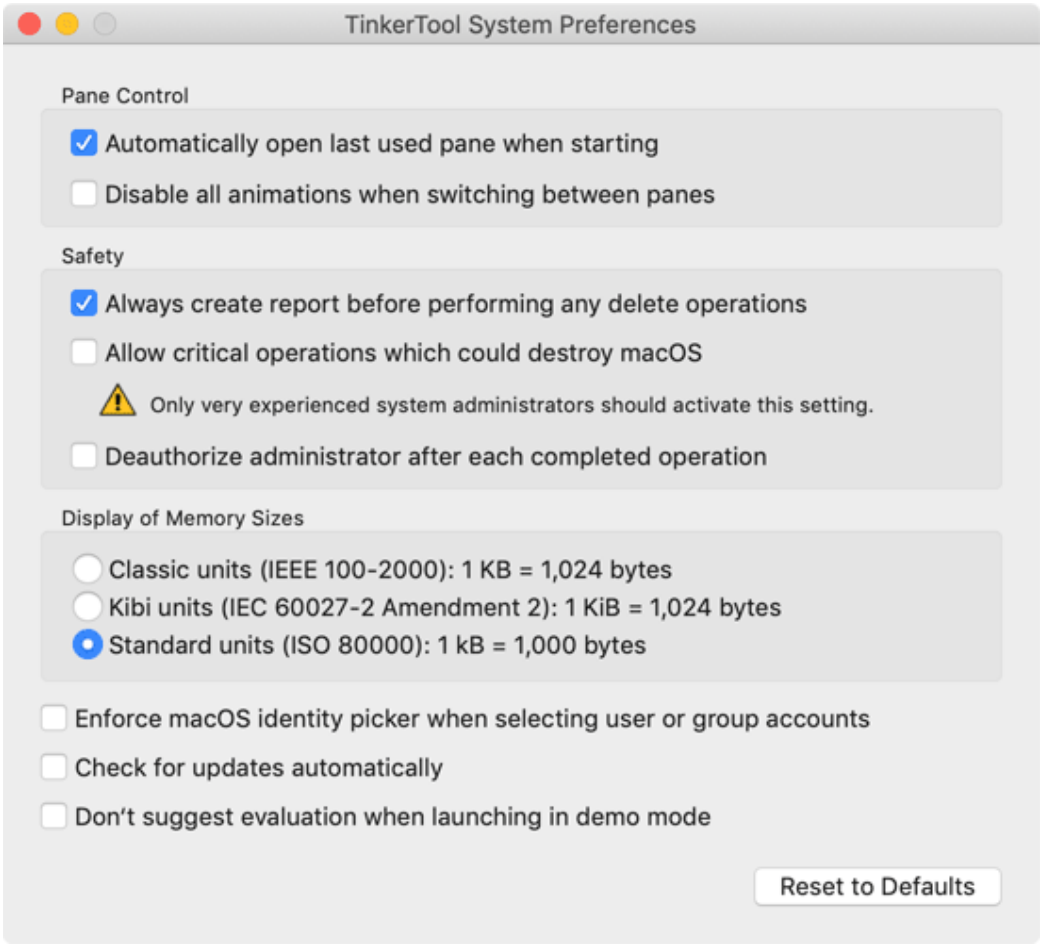


Figure 1.7: The preferences window

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 control tab the next time it is started.

In case you don't like the short animation sequences that are shown when switching from icon overview to a pane, or when switching between different panes, you can disable all animations setting a check mark at **Disable all animations when switching between panes**

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 or when removing language support packages from applications, 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 253).

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.

1.3.9 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 Preferences** after TinkerTool System has switched the respective option to off.

1.3.10 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** > **Delete** > **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:

1. Restart your computer and hold down ⌘ + R to select the Recovery System.
2. Wait until the screen **macOS Utilities** appears, then select the menu item **Utilities** > **Terminal** to launch the Terminal application.
3. 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
```

> Switching System Integrity Protection on or off can also be controlled by mouse click, using **TinkerTool System for Recovery Mode**. Further information is available in the sections The Pane Emergency Tool (section 2.6 on page 77) and RecoveryMode: Basic Features (section 6.2 on page 239).

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 **Privacy** will appear in the toolbar 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 **Privacy** button in the toolbar 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 sections. 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 (macOS Mojave only)

> If you are using macOS 10.15 Catalina or later, please see the next section.

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

- **Full Disk Access** for the privileged component of TinkerTool System
- **Full Disk Access** for TinkerTool System itself
- **Automation** between TinkerTool System and the Finder if you like to use the feature **Test Finder Copy** on the **Diagnostics** pane (section 2.5 on page 59).

> At the moment, macOS is not capable of accepting an automation approval before it has observed that a failed attempt for automation between two specific applications occurred. This means if you like to use the **Test Finder Copy** feature, you'll have to try using this feature, let this fail, grant approval to use this feature, restart TinkerTool System, and call the feature once again. Apple may or may not modify this unfriendly behavior in future versions of macOS. Applications (except Apple's own) cannot circumvent this.

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

1. Launch **System Preferences**.
2. Open the pane **Security & Privacy**.
3. Go the tab item **Privacy**.
4. Click the lock and identify yourself as user with administrative permissions.
5. Select the item **Full Disk Access**.
6. Click the button **+** below the list of apps.
7. Navigate to the folder **Library** > **PrivilegedHelperTools** on your system volume.
8. Select the file **TinkerToolSystem-PrivilegedTool** and click the **Open** button.
9. If you like to work with Time Machine features in TinkerTool System, also add **TinkerTool System** itself to the table.
10. Relaunch TinkerTool System.

> This complex procedure has been under a lot of criticism by third-party software companies, but Apple was not willing to change or simplify it.

1.5.4 Changing the privacy settings (macOS Catalina or later only)

> If you are using macOS 10.14 Mojave, please see the previous section.

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

- **Full Disk Access**
- **Automation** between TinkerTool System and the Finder if you like to use the feature **Test Finder Copy** on the **Diagnostics** pane (section 2.5 on page 59).

macOS will automatically ask for your approval for automation when you are attempting to use the feature **Test Finder Copy** for the first time. If you like to approve full disk access for TinkerTool System, perform the following steps:

1. Launch **System Preferences**.
2. Open the pane **Security & Privacy**.
3. Go the tab item **Privacy**.
4. Click the lock and identify yourself as user with administrative permissions.
5. Select the item **Full Disk Access**.
6. 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.
7. Relaunch TinkerTool System.

1.6 Integrating TinkerTool into TinkerTool System 6

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 for** …. 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 6.51* and later can integrate copies of *TinkerTool 7.4* 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 Preferences** and go to **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 System Optimization

All applications you launch are dependent on services of the operating system: The programs are using features of the system, for example to receive click messages from the mouse, or to open windows on screen. Technically speaking, this means that each application has to link its own program code with the code libraries of the operating system. Programs typically use several thousand functions available in the system which have to be "located" while the application is starting. These locations, namely the file paths where the code libraries are stored, and the exact byte positions within the libraries are not necessarily fixed: They may change from OS version to OS version, so the applications have to do a lot of work checking and locating all these OS functions at launch time.

Applications try to accelerate this link process at start time by assuming that the code locations remain constant as long as no new operating system updates have been installed since the last launch. They store the required code locations of operating system functions in a cache area in their own program code. So the next time the application is launched, it can simply reuse this saved information and does not need to repeat the whole search process of locating the OS functions. The cache only needs to be rebuilt if the application detects that new system libraries have been installed.

This optimization technique is called *prebinding*. It speeds up the launch time of programs, but does not accelerate the programs themselves. This technique is not restricted to applications only. It is even more important for the system libraries themselves, because they are also using each other's functions. For example, the library drawing windows on screen uses features of the graphics library, and the graphics library uses functions of the system kernel. For this reason, code libraries and similar software components, like plug-ins, make use of prebinding, too, although they don't really have a "startup phase."

As mentioned in the previous paragraphs, each application "re-prebinds" itself to the available libraries when it detects that new libraries have been installed, for example as part of an OS update. In order to anticipate this step, it is a good idea for an upgrade

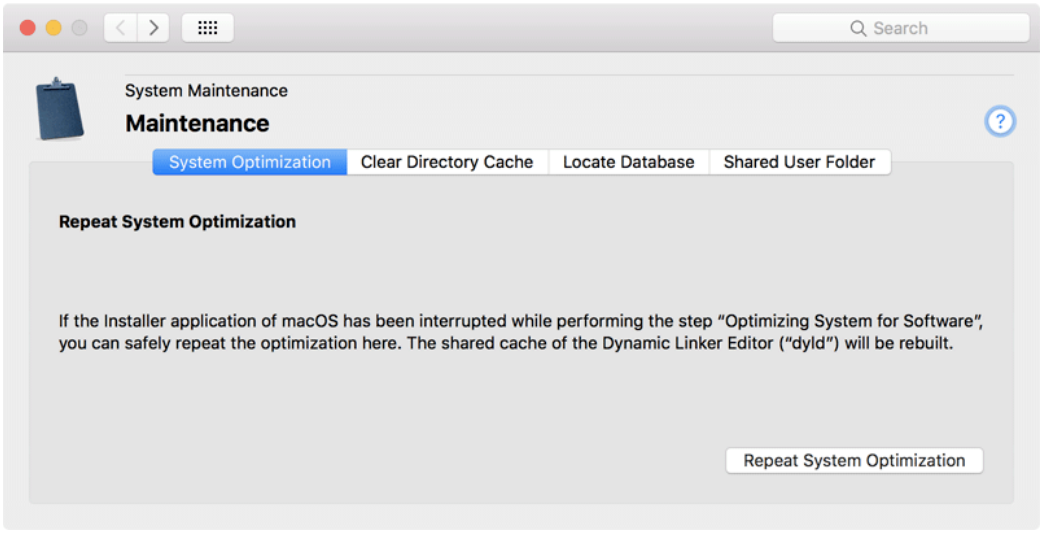


Figure 2.1: System Optimization

installer to simply tell all applications on the computer to re-prebind themselves during, or more precisely, just after the update has been installed. The macOS Installer indeed performs this step as last part of each system update. It is done when the message "Optimizing system for installed software" is shown.

> It is one of the macOS myths that the system no longer uses any kind of prebinding. This is *not* true, although many Internet pages claim it does. The truth is that modern system versions indeed use a new improved linking technique which eliminates the need of prebinding *for applications and third-party code libraries*. *System libraries are still prebound*, however, and they benefit from this optimization.

This means that if a system update installation was somehow interrupted, or if you manipulated one of the system libraries (for example by "downgrading" a specific library via a Time Machine backup) all prebinding information in the system should be updated. To manually initiate a system-wide prebinding process, perform the following steps:

1. Open the tab item **System Optimization** of the pane **Maintenance**.
2. Click the button **Repeat System Optimization**.

2.1.2 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.

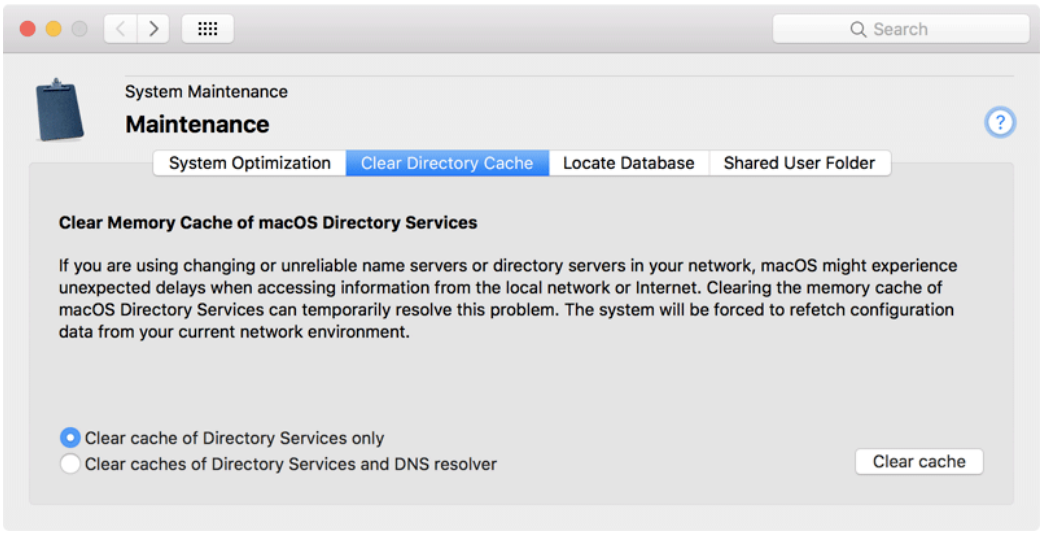


Figure 2.2: Clear directory cache

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:

1. Open the tab 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**.

2.1.3 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.

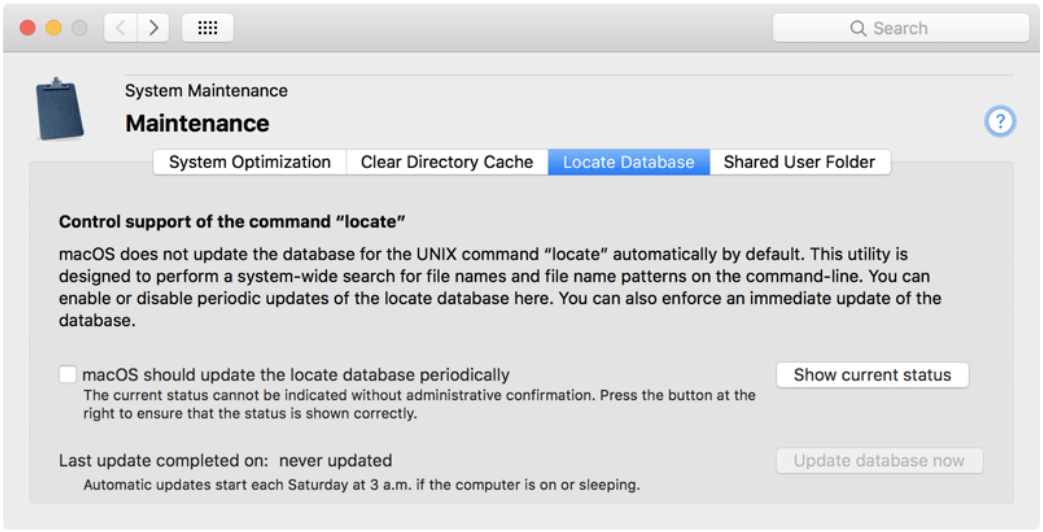


Figure 2.3: Locate database

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 tab 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**.

2.1.4 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, iTunes uses hidden contents in this folder to store licensing information for the use of copyright-protected media.

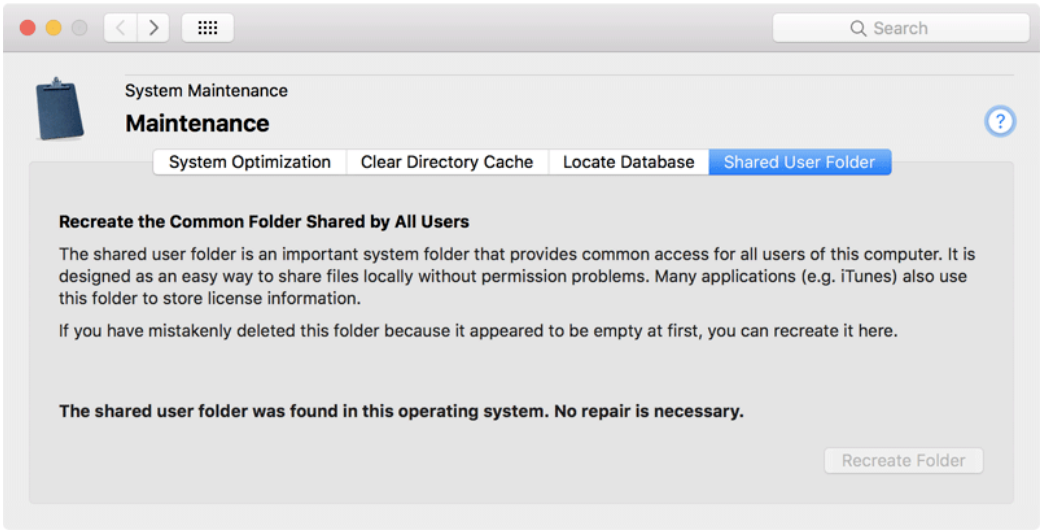


Figure 2.4: Shared User Folder

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 tab 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 cache deactivation for the following two categories:

- Personal standard caches of the current user
- System-wide caches used when computer-related information relevant to all users is stored.

Two other cache categories can only be cleaned because smart deactivation is prevented by *System Integrity Protection* (section 1.3 on page 7) of macOS:

- Personal high-speed caches of the current user (see the next paragraph),
- 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**. Select the cache sets which might be causing the problem. Then click the button **Deactivate selected caches**.

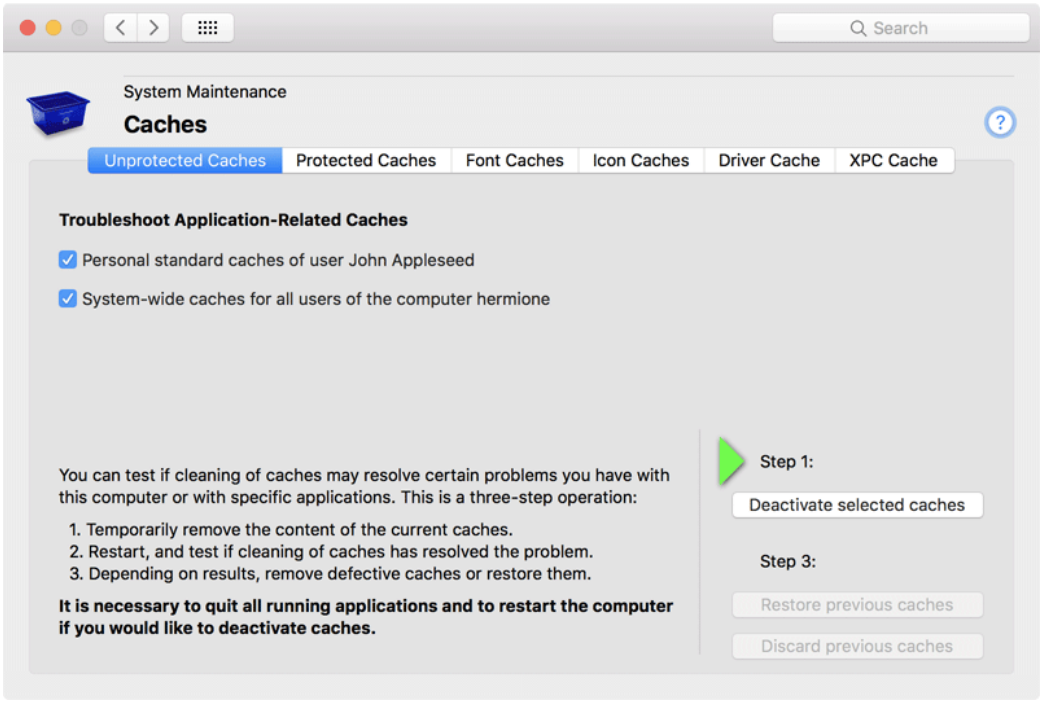


Figure 2.5: Unprotected caches

3. TinkerTool System will ask you to quit all running applications. You can also have TinkerTool System do this automatically for you. Depending on the cache sets you have selected, the program will then perform a logout or restart.

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 or restart, respectively, 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 window.

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

If you activated the option **Caches of the operating system** and were forced to discard these caches, macOS will not only run more slowly but will also record a large number of warning messages in the system log, indicating that the so called *XPC Helper Cache* is no longer active. Because this particular cache might not be rebuilt until the next operating system update, it is strongly recommended that you trigger a manual update of this cache. For more information, please see the paragraph **XPC Cache** at the end of this section.

Cache Cleaning (Protected Caches)

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

1. Open the 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.

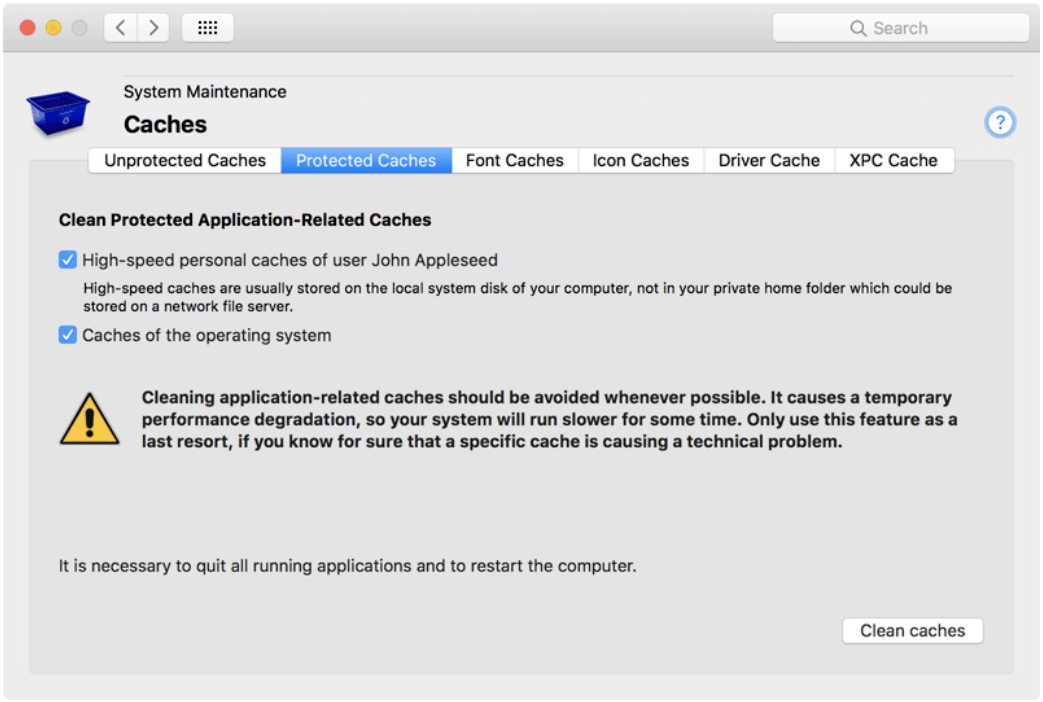


Figure 2.6: Cleaning of protected caches

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 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."

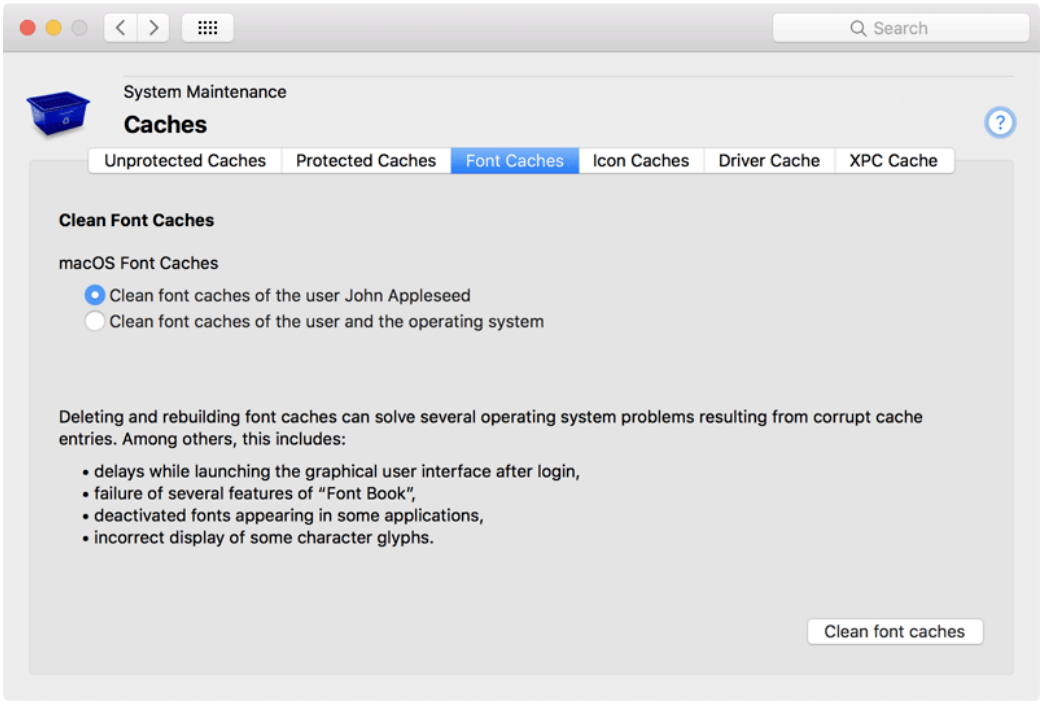


Figure 2.7: Font caches

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 automatically 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 tab 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 white rectangle with the symbolized letter A.

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 tab 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 Drivers and Kernel Extensions

Driver Cache

macOS can be loaded on a large number of different Macintosh systems. Because each computer model contains different devices, such as network cards, graphics chips, or disk interfaces, the part of the operating system that controls these devices is structured into small software modules, called *drivers*. Each type of hardware device corresponds

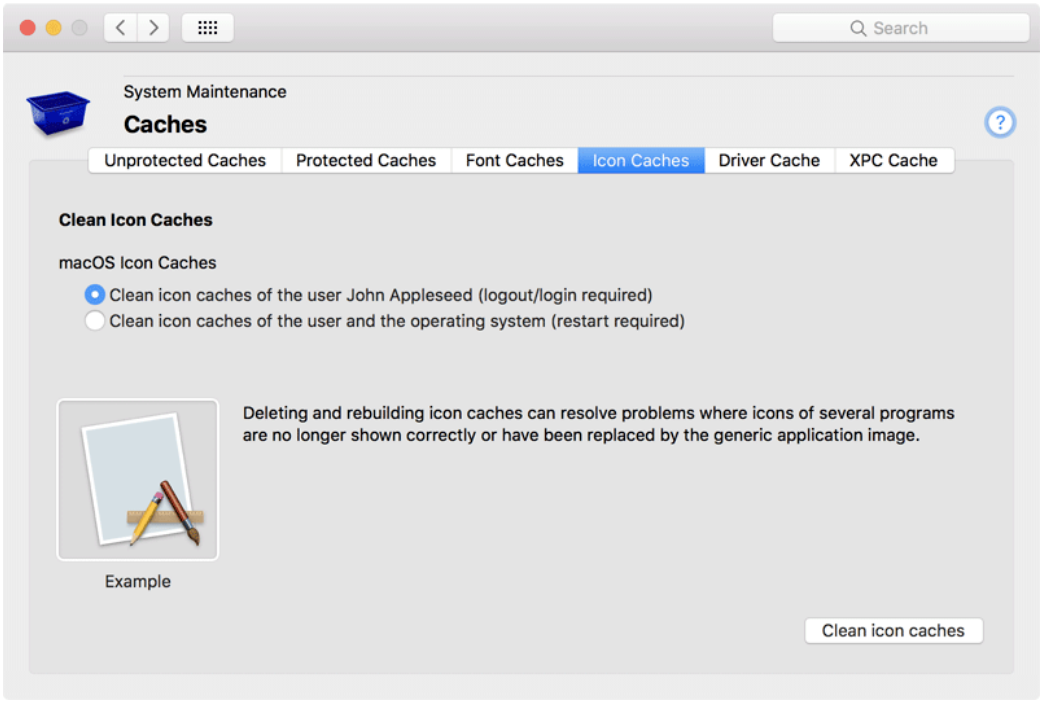


Figure 2.8: Icon caches

to a specific macOS driver that controls the device, or more precisely, all devices of its kind. macOS needs only to load the drivers which correspond to the actual devices in the computer upon which it is running. This way the OS does not need to load all the software components used to control all Macintosh systems ever built. Drivers are organized as *kernel extensions*, a more general term used for the small software modules that add specific functionality to the inner core of the operating system.

macOS keeps several internal caches used to optimize the startup phase of the operating system. Among other things, these caches hold the data about which kernel extensions are needed to operate your particular computer, and which are not. Thus, the system knows in advance which drivers it does and does not need to perform a complete search which drivers and devices are available, and how these two sets must be matched with each other. The use of caches significantly shortens the startup process.

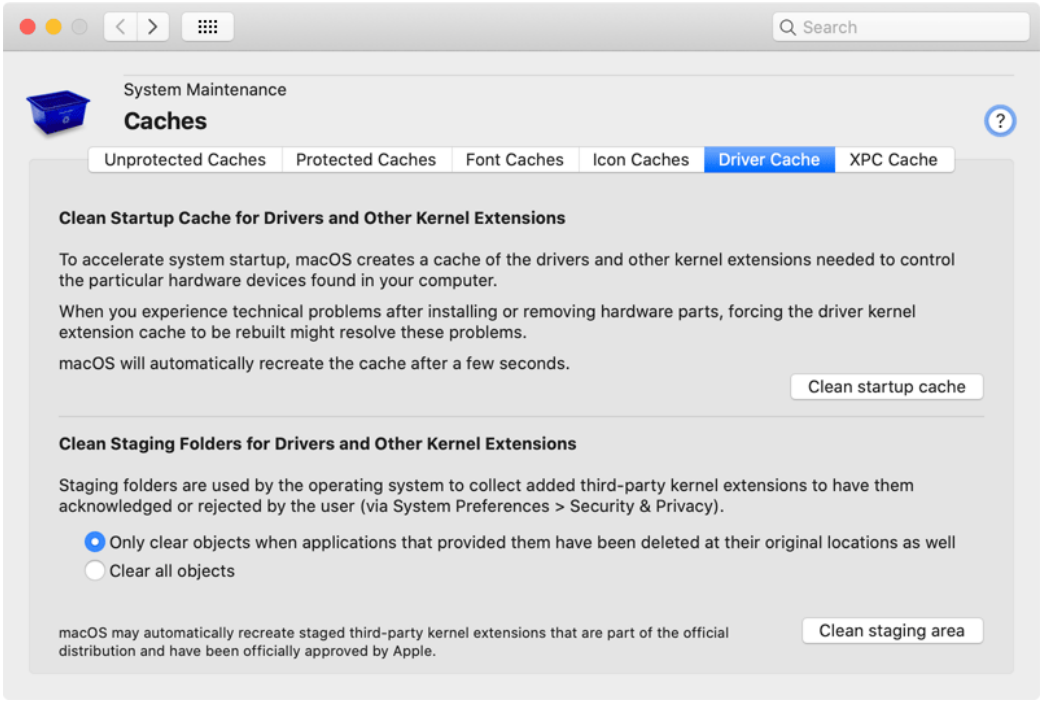


Figure 2.9: Driver cache and staging area

Under certain conditions, these caches can become corrupted or contain outdated information. This could happen for example if a third-party kernel extension does not work (or was not installed properly), or if you added or removed devices from your computer and due to some technical issue, macOS lost track as to which driver needed to be activated or deactivated.

TinkerTool System can assist you in cleaning these startup driver caches. macOS will automatically rebuild the caches after a few seconds. No restart is required. To clean these caches, perform the following steps:

1. Open the tab item **Caches** > **Driver Cache**.

2. Click the button **Clean startup cache**.

Staging Area

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 Preferences** > **Security & Privacy** > **General.**

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 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.

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 tab item **Caches** > **Driver Cache**.

2. Use the radio buttons at the bottom of the window 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.

2.2.7 XPC Cache

Modern versions of macOS and applications developed for the macOS platform make extensive use of an Apple technology known as *XPC (Cross Process Communication)*. Running processes can use XPC functions to communicate with each other via secure and reliable channels. Programs especially need XPC when they have been split into different parts internally, e.g. to distribute work onto multiple processor cores, or for privilege separation (see also the notes on the security policy of TinkerTool System (section 1.2 on page 3)).

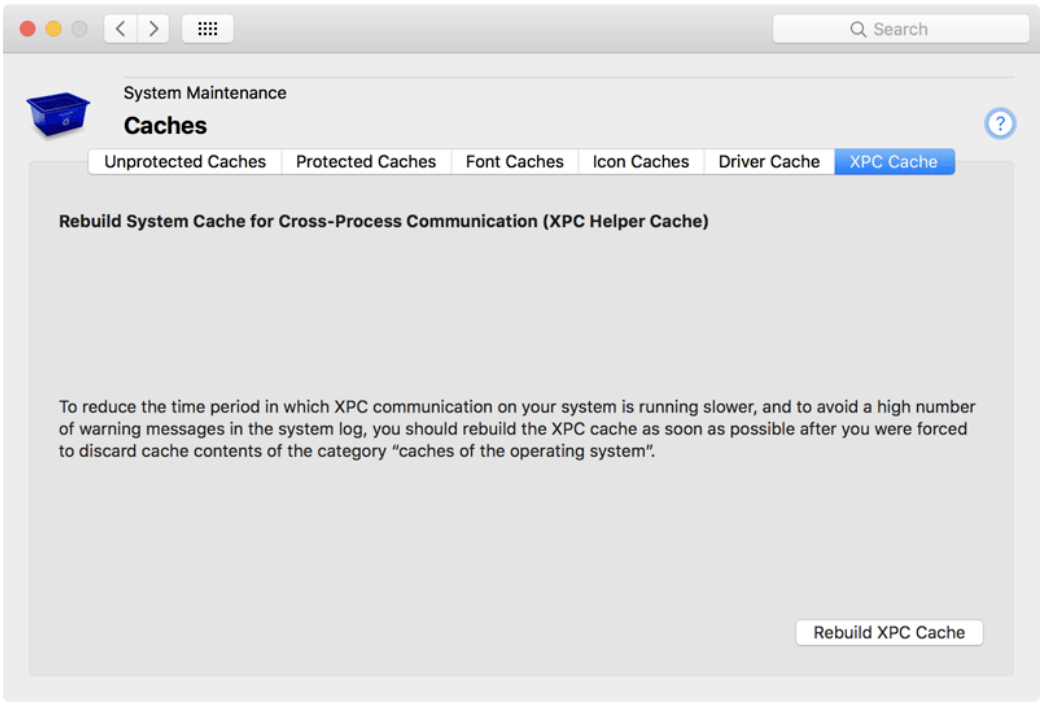


Figure 2.10: XPC Helper Cache

Many applications and parts of macOS come with hidden internal helper programs, known as *XPC services*. These services contain components which talk to each other via XPC. Because macOS requires significant time to determine which XPC services are offered by each application, and to locate all of the different services, it uses a dedicated cache, the *XPC Helper Cache*, to store this information.

After you have used TinkerTool System's feature to deactivate or even to discard the **Caches of the operating system**, the inter-process communication can slow down. In addition, macOS may record thousands of error messages in its internal system log indicating that the XPC helper cache has been lost. This also slows down the system and wastes storage space. To quickly recover from such a situation, you can use TinkerTool System to let macOS rebuild the XPC cache. Perform the following steps:

1. Open the tab item **Caches** > **XPC Cache**.

2. Click the button **Rebuild XPC Cache**.

2.3 The Pane 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 each hour. Outdated file sets are automatically removed, keeping hourly backups for the last day, daily backups for the last week, 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. Although the entire system 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 of the destination is shown at the left bottom of the Time Machine pane (**Active Time Machine disk**). If you replace Time Machine devices while TinkerTool System is running, you can click the button **Rescan** at the right side of the pane to ensure that the application learns about the possibly changed active device immediately. In most cases, TinkerTool System will detect this automatically after a short time. However, from within TinkerTool System you cannot change which destination device Time Machine currently considers the active one.

If your Time Machine destination is network based, click the button **Connect to network disk** to let macOS connect to your backup. You cannot use any of the Time Machine features until the connection is made. To disconnect later, click the button **Eject network disk**. You should only disconnect if no Time Machine operations are currently running.

TinkerTool System automatically tries to determine if a backup operation is currently in progress. In this case, the warning message **A backup or other Time Machine operation is currently running.** is shown at the bottom of the window. Although it is usually safe to use other Time Machine features during this phase, we don't recommend doing so, because the two simultaneously running operations could slow down each other, causing significant performance problems.

There can also be the warning message **Time Machine is not ready at the moment. Please wait**. In this particular case, Time Machine indeed cannot be accessed at all and TinkerTool System has to wait until the backup system becomes operational again. The two most typical causes are:

- Time Machine has been enabled only recently, but the very first backup has not been completed yet. In this case you have to wait until there is at least one backup session available.
- With some versions of macOS, Time Machine may experience an internal error state which causes it to send contradictory data when being asked about its current configuration. This defect usually resolves itself within a few minutes. We recommend waiting and clicking the button **Rescan** after some time to check whether macOS has recovered. You can expedite this by opening the Time Machine user interface, verifying that the timeline is completely filled and then quitting the Time Machine screen again.

It is also recommended to disconnect from a network-based Time Machine backup volume when you completed your work with Time Machine features in TinkerTool System. The application needs to perform some monitoring tasks in the background while the network connection is active. This could slightly slow down the program and your network, especially if you are using WiFi.

2.3.3 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.

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. For a network-based backup, you will need to connect to the file service hosting the backup first. Here, the backup set is stored in a *sparsebundle* disk image. It also bears the name of the previous computer.

Depending on how Time Machine was configured before inheriting the foreign backup set, you might need to re-enable Time Machine on the **Time Machine** pane of **System Preferences** 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

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:

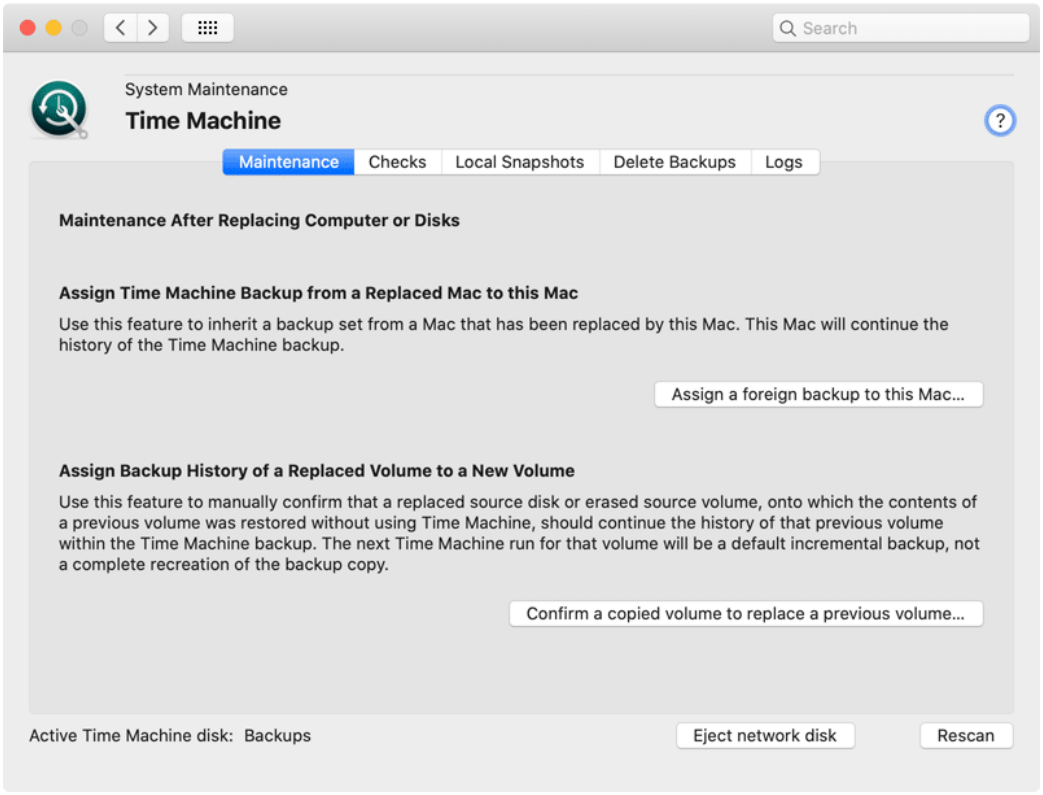


Figure 2.11: Maintenance after replacing Time Machine data sources

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.

2.3.4 Backup Verification and Statistics

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.

Computing Statistics on the Change Rates between All Snapshots

As mentioned in the introduction, Time Machine simulates that each snapshot contains a complete copy of all data that was part of the backup at the recorded point in time. So if your computer always stored approximately 500 GB of data on its disks and 50 snapshots have been recorded by Time Machine, the destination volume appears to virtually contain 500 GB $\times$ 50 = 25,000 GB of data. This large amount of data is not really stored on the disk, however. In reality, Time Machine optimizes storage space on its destination disks by recording only changes between consecutive backup runs. To estimate the storage space that is usually consumed by each snapshot, it can be helpful to evaluate the changes between backup runs and to compute the average rate of change. To do this, perform the following steps:

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

2. Click the button **Compute Statistics**.

> Note that all files on the entire Time Machine disk need to be analyzed for this computation. This will take a considerable amount of time.

TinkerTool System creates a text report after Time Machine has completed the computation. This report can be saved to a text file if necessary.

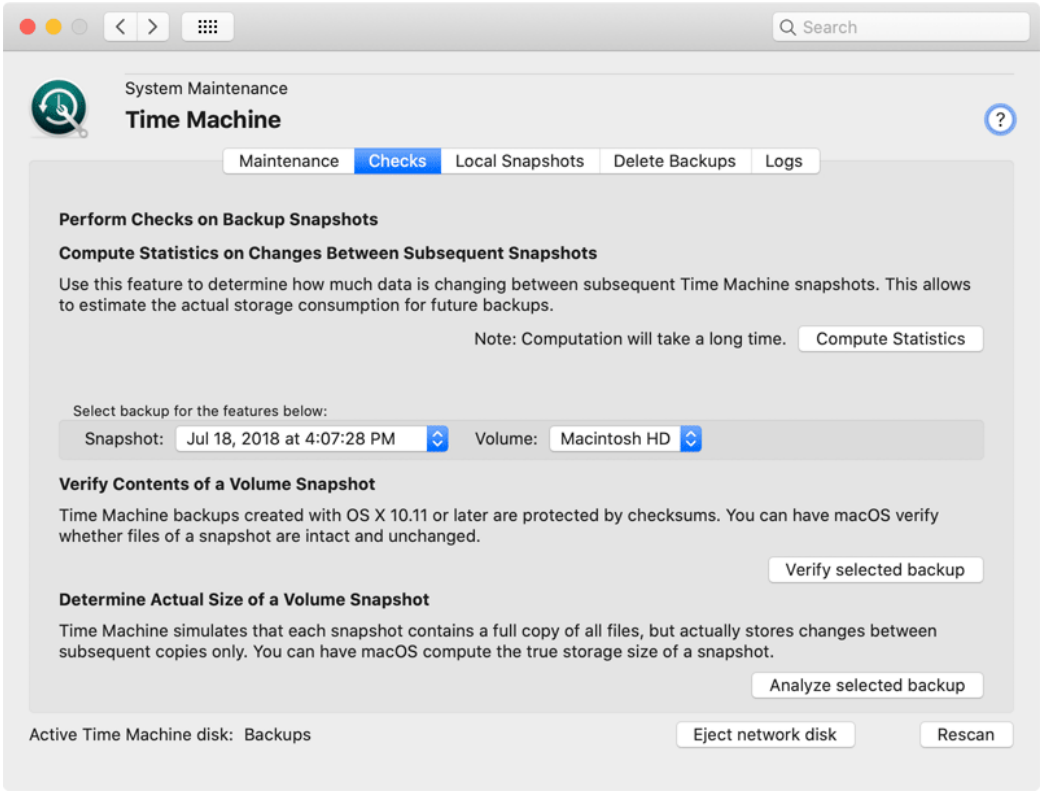


Figure 2.12: Features for backup verification and statistics

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**.

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

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**.
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.

For additional features related to verifying Time Machine operation and the size of snapshots, please also see the chapter The Pane Diagnostics (section 2.5 on page 59).

2.3.5 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 3.6 on page 167).

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.

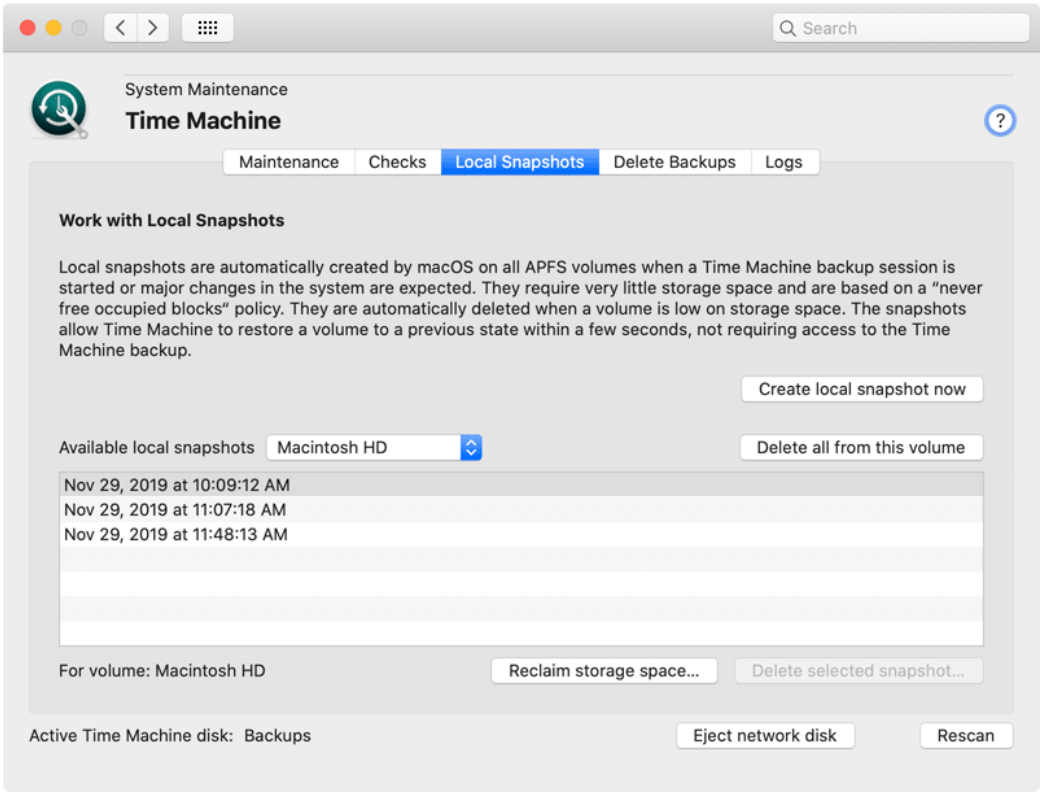


Figure 2.13: Working with local APFS snapshots

- 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**….

2.3.6 Deleting Time Machine Backup Data

Remove a backup snapshot from the currently active Time Machine disk

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** in the upper part of the window.

3. Click the button **Delete…** next to it.

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.

Remove any Time Machine data from local backup disks

Time Machine disks can be in use by multiple computers. You can store other data on a Time Machine disk as well, although this is definitely not recommended, because this additional data cannot become part of a Time Machine backup. (In case of disk failure, you would lose both the original data and the backup at the same time.) If you like to remove some or all Time Machine data from such disks, e.g. when you no longer need backups for a decommissioned computer, you again must not use the Finder to do so. This would risk that the entire file system of this disk and the Trash are damaged.

TinkerTool System can also help in this case, where the Time Machine data on disk does not necessarily belong to your currently active backup of the local computer. You can remove data from inactive backups or from backups of other Macs. In particular, you can delete

- all Time Machine data on disk (leaving other files and folders on that disk untouched),
- all Time Machine backups for a specific computer on a specific disk,
- a single backup snapshot for a specific computer on a specific disk.

> Only directly attached hard drives are supported. You cannot use this feature to purge Time Machine data on network file servers.
>
> If you have a "pure" Time Machine disk that only contains backups for a single computer and has no other data stored on it, the fastest solution to clean this disk will be to simply re-format it with Disk Utility, executing *Erase* on its main partition. However, if the disk was encrypted and should be re-used for new, encrypted Time Machine backups later, a delete operation via TinkerTool System could be faster overall, because the necessary re-encryption (that is not necessary for a manual delete process) could take a very long time.

1. Open the tab item **Delete Backups** on the pane **Time Machine**.

2. In the lower part of the window, make your choices for **Time Machine disk**, for **computer** and the Time Machine items to remove.

3. Click the button **Delete**....

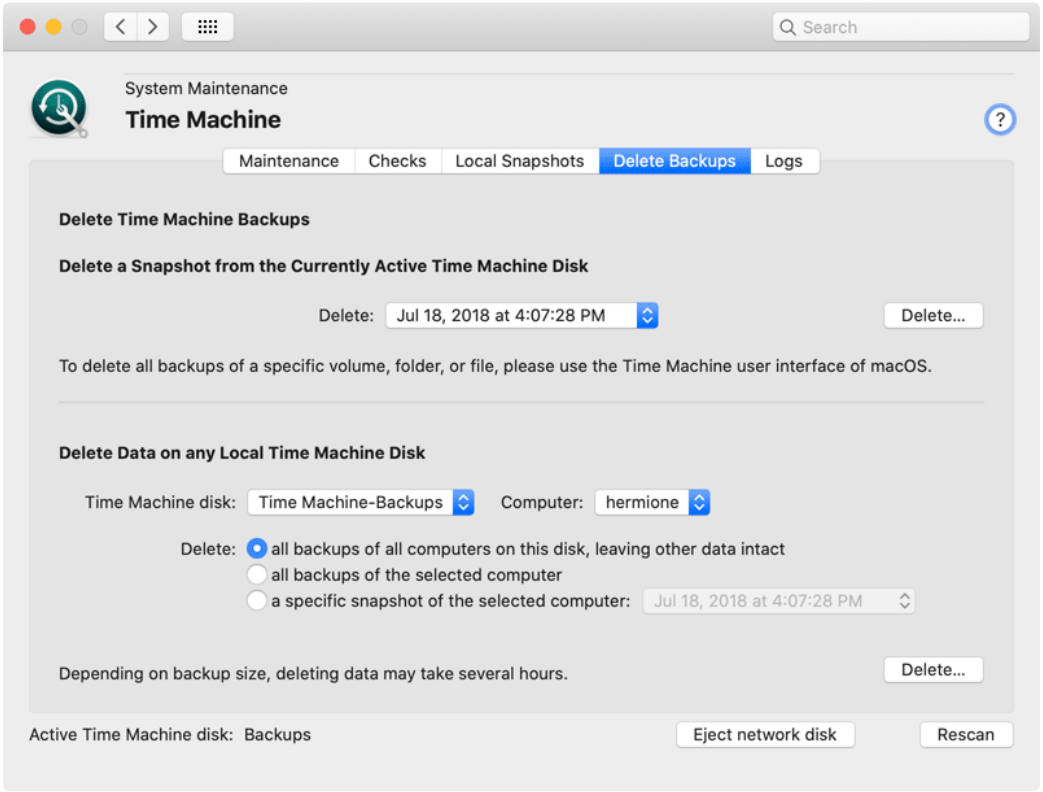


Figure 2.14: Deleting Time Machine backup data

2.3.7 Retrieving Time Machine Logs

macOS records a log file each time a Time Machine backup has run and a new snapshot was created. These logs are usually invisible, but TinkerTool System can retrieve them for each snapshot if required. 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.

> 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 **Logs** on the pane **Time Machine**.
2. Click the button **Select snapshot**... to select the time of the backup that is of interest.
3. Click the button **OK**.
4. Confirm to macOS that its helper program *authopen* should have permission to read the log.

TinkerTool System shows the contents of the log in the text area at **Backup Log**.

2.4 The Pane Issues

2.4.1 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 two 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 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*.

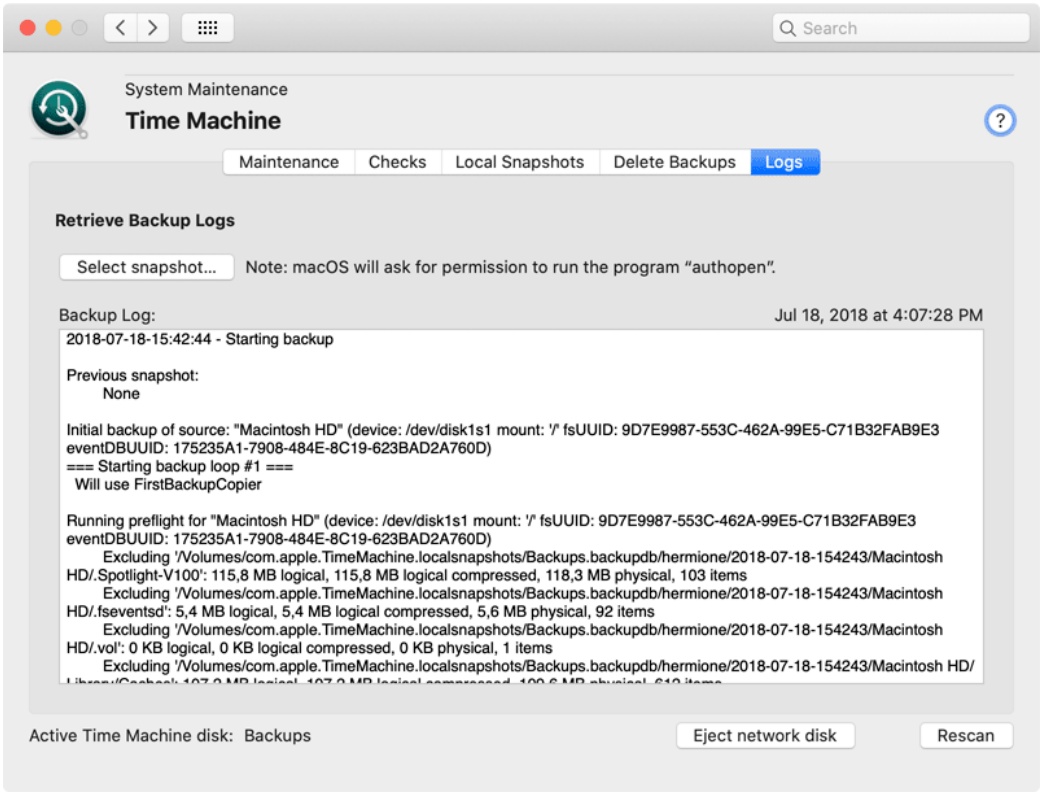


Figure 2.15: Access to Time Machine logs

App updates are presented in the **App Store** application, item **Updates**. On the other hand, macOS software updates are listed in **System Preferences**, pane **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.

Reset a Hanging Search for Updates

With several of the macOS updates published by Apple in 2022, the software update feature may not always work correctly if you are using an operating system prior to macOS 12 Monterey. When you try to search for the latest updates on the pane **Software Update** in **System Preferences**, the progress indicator may begin to rotate endlessly and no actual search is performed. A similar effect occurs when you try to execute the equivalent search command in Terminal. This can be a critical problem, because it blocks the possibility to download important security updates.

TinkerTool System can reset the software update component which will usually resolve this issue immediately. Perform the following steps if your version of macOS is affected by this problem:

1. Quit **System Preferences** or the **softwareupdate** command in Terminal if these programs should be running at the moment.

2. In TinkerTool System, open the tab item **Software Update** on the pane **Issues**.

3. Click the button **Reset Running Operation**.

If the reset has been successful, you can immediately start a new attempt to search for macOS updates.

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 tab 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 Preferences will automatically list them as soon as the synchronization process is completed.

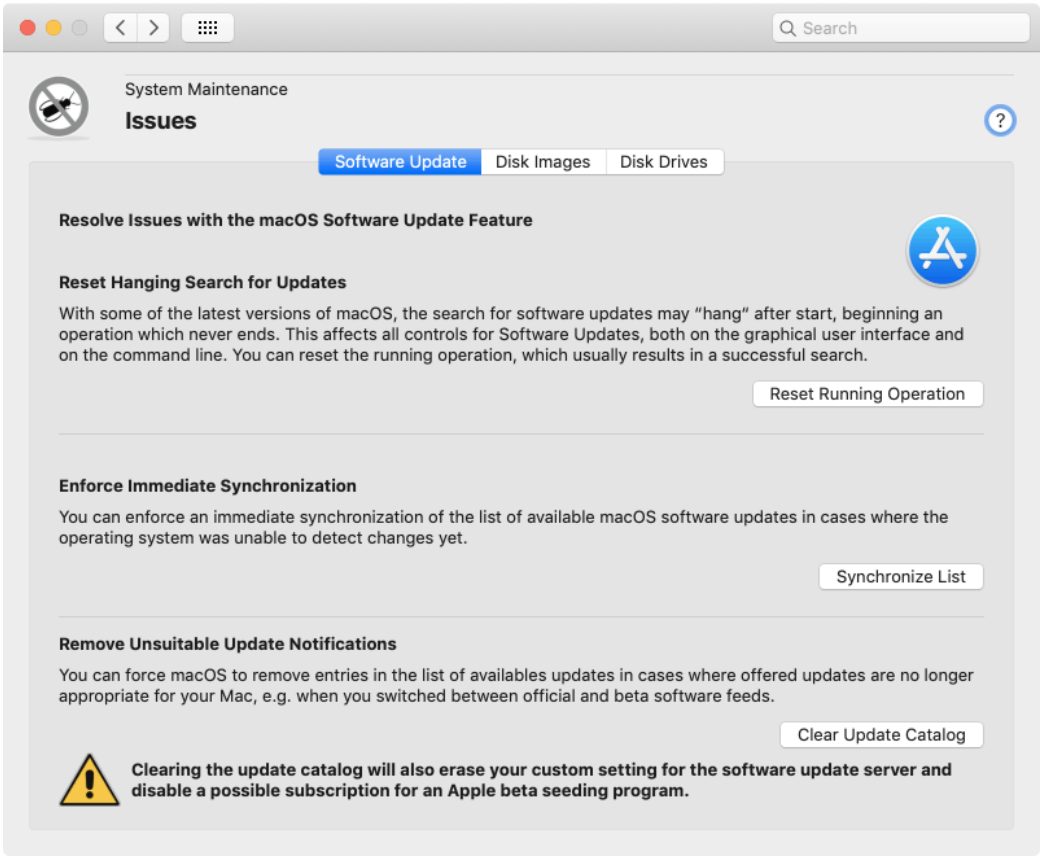


Figure 2.16: Resolving Issues with the Software Update Feature of macOS

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 Preferences 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:

1. Open the tab item **Software Update** on the pane **Issues**.

2. Click the button **Clear Update Catalog**.

2.4.2 Resizing Disk Images

If you have tried to use the feature of Disk Utility to resize disk images in the last years, you may have noticed that it has never been working correctly. After the resize operation, the resulting DMG file usually takes up an absurdly large amount of storage space.

You can use TinkerTool System to perform a correctly working resize operation on macOS disk images. The application supports all standard images, i.e. DMG files that contain a default partition layout with an HFS+ volume at the trailing position containing the payload data of the image file.

> We cannot guarantee that unusual variants of disk images, e.g. with multiple data volumes or APFS file systems are supported. Typical HFS+ extensions like journaling, case-sensitivity, or encryption should work, however.

When changing the size of a disk image, you need to enter the new size of the data partition. The possible limits, that depend on the payload in the image and the remaining space on the underlying disk, will be shown to you in advance. The partition table in the image, and the total size of the DMG file will be automatically adapted to the new size. The file will be modified in place without creating a temporary copy, so you won't need twice the storage space for the payload data.

To resize a disk image with standard layout, perform the following steps:

1. Open the tab item **Disk Images** on the pane **Issues**.

2. Click the button **Resize disk image**….

3. Select the image file you like to resize.

4. Enter the new size and click the **OK** button.

2.4.3 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.

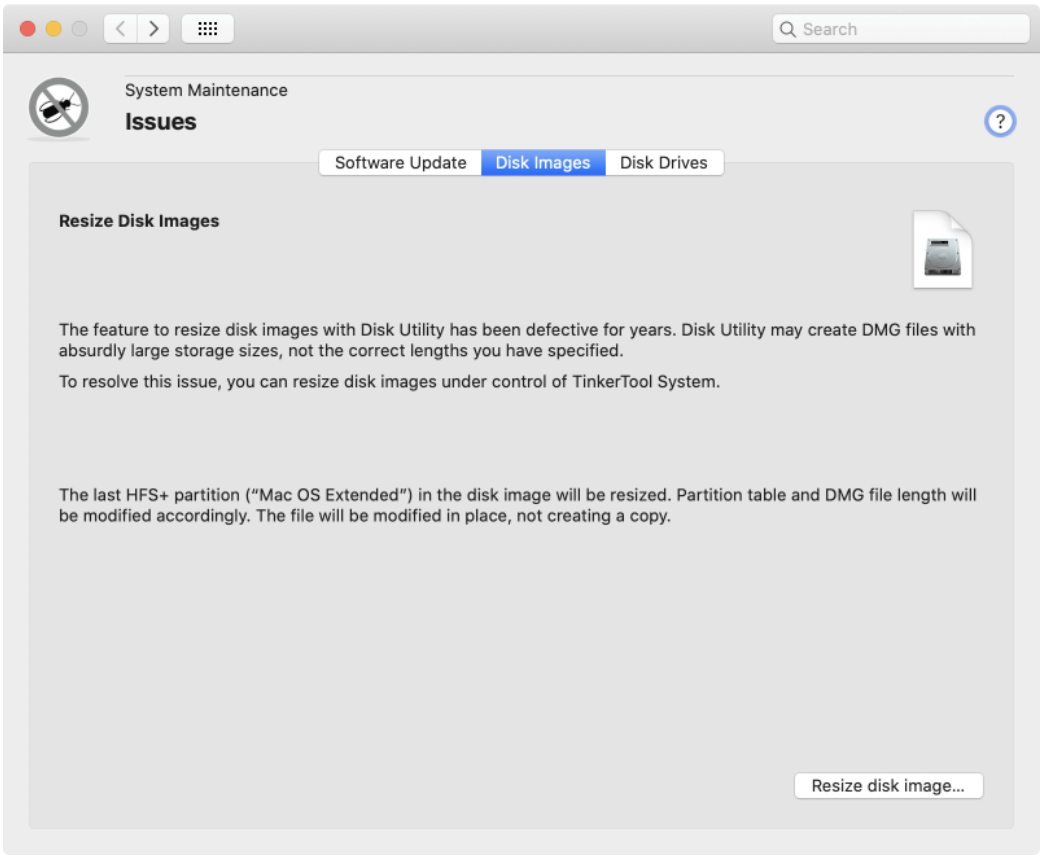


Figure 2.17: TinkerTool System can resize disk images correctly

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 tab 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.

You can only select a drive for erasure when all of its volumes are inactive. If a volume is still in use, eject it in the Finder or in Disk Utility.

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.

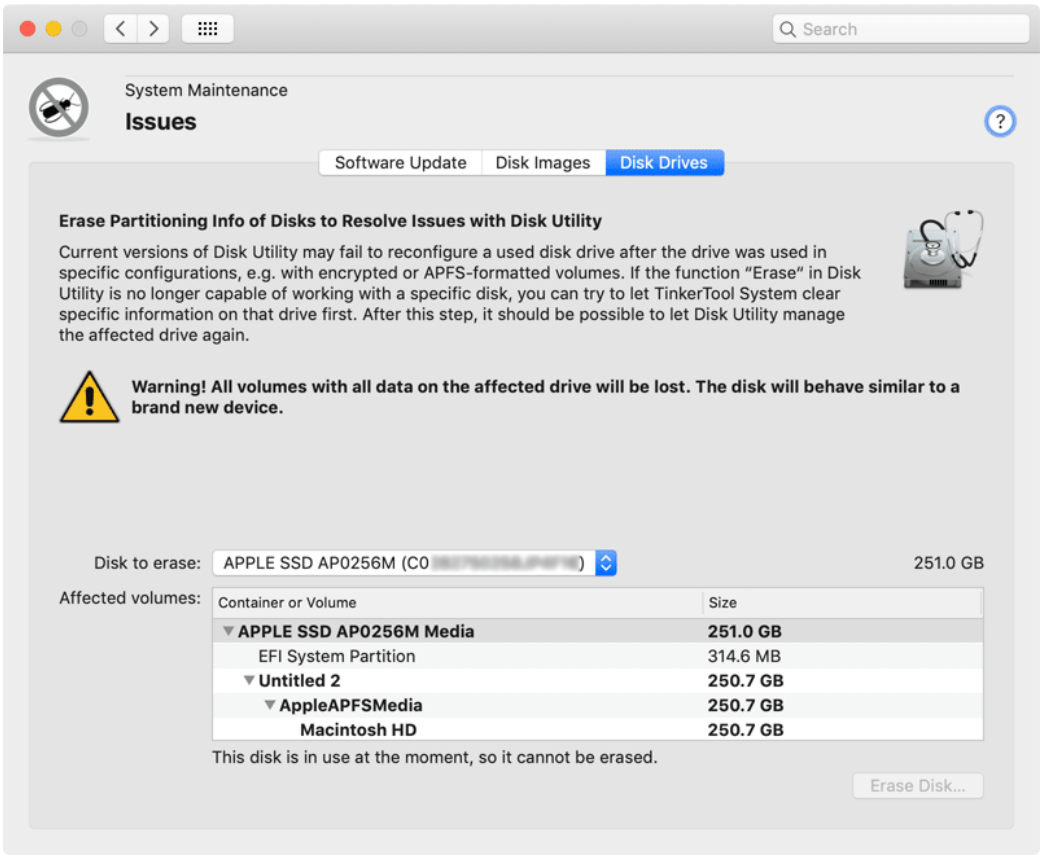


Figure 2.18: Clear disks which can no longer handled by Disk Utility

2.5 The Pane Diagnostics

2.5.1 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 tab 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.

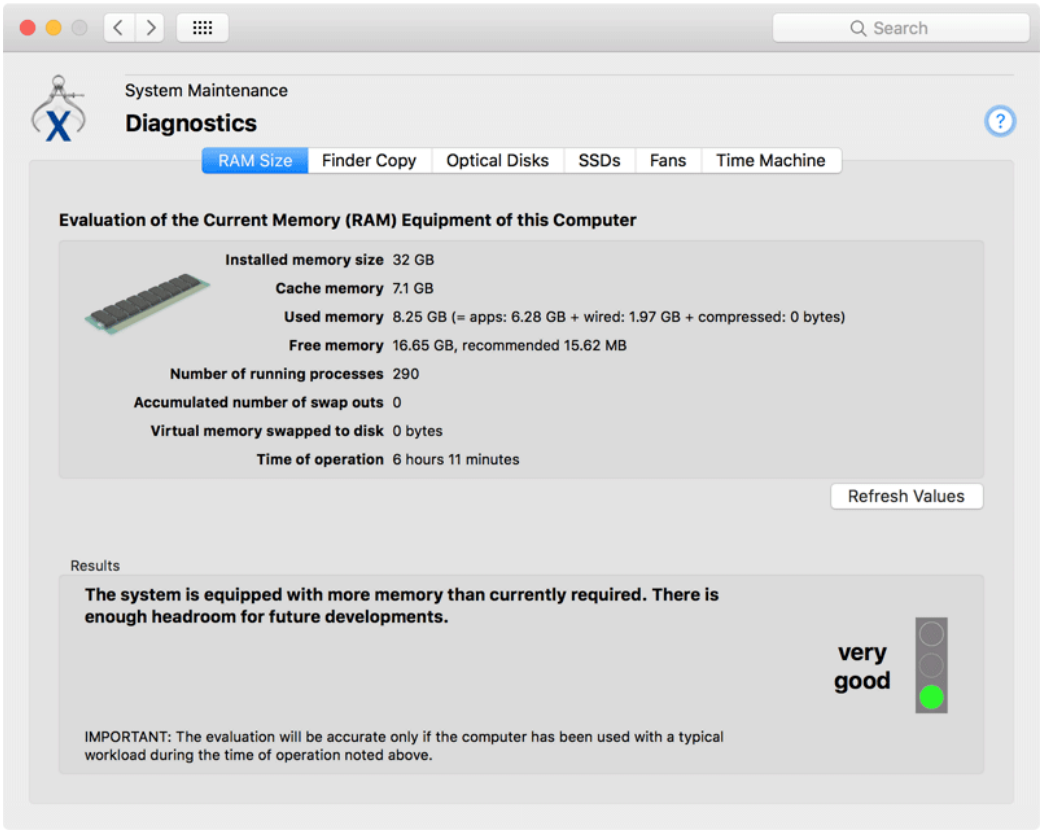


Figure 2.19: Evaluate RAM size

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).

- **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.

2.5.2 Test Finder Copy

The macOS Finder is known to be affected by specific bugs, depending on which version you are using. The issues affecting Finder file copy operations between disk volumes are especially problematic. You cannot assume that a copied file will always be identical to the original. Under certain circumstances, data loss can occur. This is especially true when you consider that the Finder also plays a role in the operation of Time Machine, the backup solution of macOS.

TinkerTool System can verify if the Finder is capable of performing the following operations correctly:

- Copying files with emulated Extended Attributes (so-called *AppleDouble* files)
- Copying symbolic links that have native Extended Attributes

These operations are known to be unreliable when specific versions of the Finder and specific file system types are used as the source and destination of the copy operation.

File system type means the format of a disk or disk partition, or the transfer protocol used when accessing a file server in the network, respectively. The Finder behaves differently when copying between two HFS hard drives, for example, or between an HFS disk and a memory stick formatted using the Windows FAT standard.

You can let TinkerTool System check two given disks against your version of the Finder. TinkerTool System can control the Finder remotely to test whether the operation runs as expected or not. To perform the check, you only have to specify two folders between which test files should be copied.

- Both folders must lie on different disks to ensure that a real physical copy operation takes place and not only a simple move operation on the data.

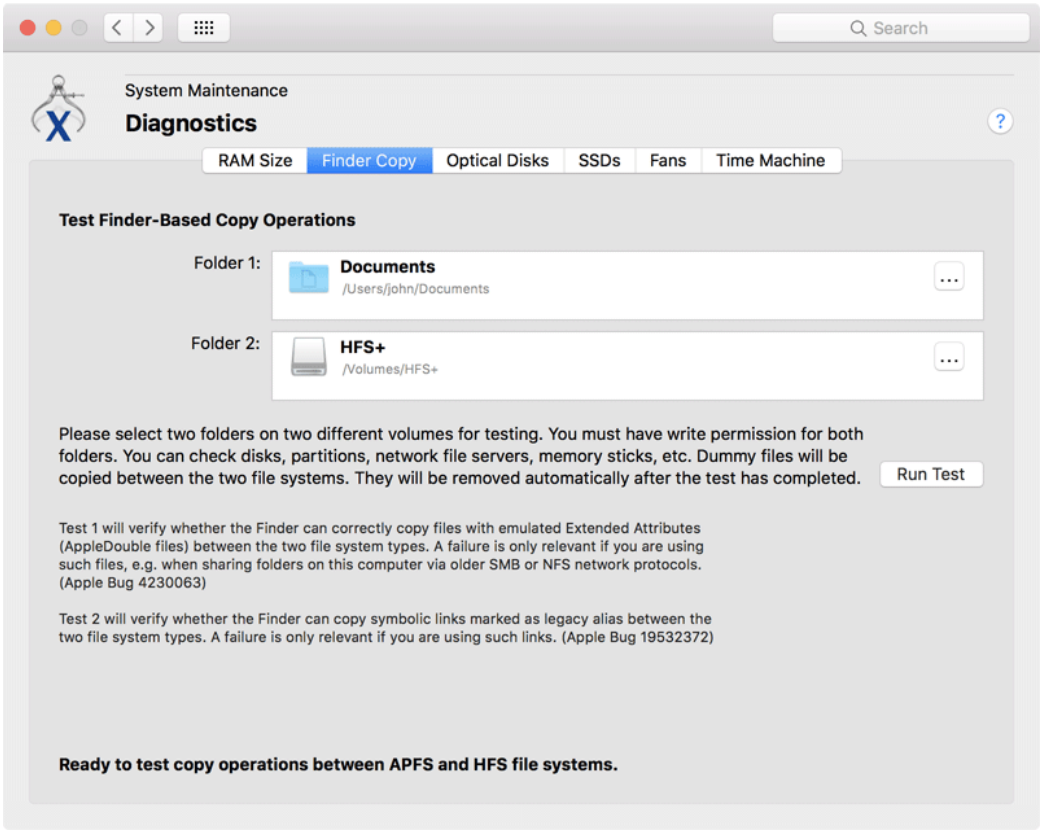


Figure 2.20: Check file copy operations

- You must have read and write permission for both folders to make sure the Finder running for your account has the right to perform the copy operation.

To run the tests, TinkerTool System needs less than 200 kB on both disks. All files written during the check will be erased automatically after the tests have been completed.

When working with file system types, only the file system *families*, not specific sub-types, affect the behavior of the Finder. Messages shown by TinkerTool System during this check refer to the family only. For example, the file systems "HFS" and "HFS+ journaled, case-sensitive, encrypted" are both represented by the family "HFS."

TinkerTool System needs approval for Finder automation before you can use this feature. For more information, please see the last section in chapter Basic Operations (section 1.3 on page 7).

Perform the following steps to test the Finder:

1. Open the tab item **Finder Copy** on the pane **Diagnostics**.
2. Drag a folder on the first disk to be checked from the Finder into the field **Folder 1**. 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. In the same fashion, specify a different folder lying on the second disk to be tested in the field **Folder 2**.
4. Now click the button **Run Test**. After a few seconds, the outcome of the test will appear in the lower section of the pane.

The button can only be clicked if the previously specified conditions are met for the two folders. The pane will show you in advance whether the test can be performed, or if a problem exists with the selection of folders.

TinkerTool System automatically tests the copy operations in both directions, i.e. copying from folder 1 to 2, and from 2 to 1. The order of the two folders does not matter. Because TinkerTool System is controlling the Finder remotely, you might hear the sound effects the Finder uses for copy operations during the test.

A successful test will be marked by a check mark with green background. A test that has failed is marked by a cross marked red.

A failure of test 1 indicates that the Finder is not capable of copying Extended Attributes for files and folders if they are not stored natively, i.e. not on a disk using the formats "HFS+," or "APFS", or on an AppleShare file server. *This failure may not be relevant to you*. Emulated Extended Attributes are mainly used when you operate the system as a file server, sharing files with older SMB or NFS network protocols. If you don't use your computer that way, it's likely that your installation of macOS has never created files with such attributes.

A failure of test 2 indicates that the Finder cannot copy symbolic links which have Extended Attributes attached. This failure may also not be relevant to you, but such situations are more likely than the ones of test 1. For example, you may see such objects as part of applications which have older software library frameworks embedded. These frameworks could store symbolic links which are additionally marked as legacy alias via an Extended Finder Attribute. In practice, you will notice such a problem in situations where the Finder unexpectedly cancels a running copy operation with the message that an object could not be found *(error –36)* although the object is there.

Please note that TinkerTool System is only testing whether the Finder is working as expected. The application cannot repair any defects it might have detected in the Finder.

> Unfortunately, if one of the tests fails when you select two HFS+ disks for the copy operation, you have to expect that will also not work correctly. Because the Finder is an indirect part of some copy operations performed by Time Machine, backing up or restoring data can also lead to corruption of copied files.

2.5.3 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:

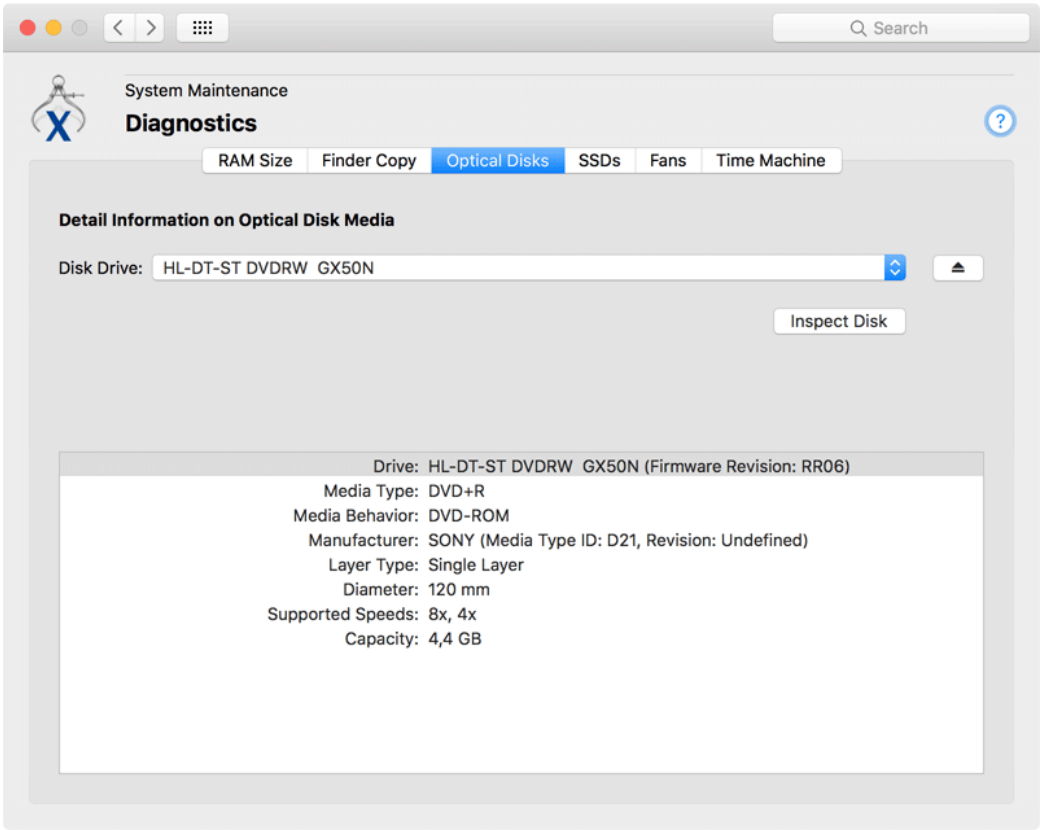


Figure 2.21: Inspect optical disks

1. Open the tab 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.

2.5.4 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, OS X 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 were 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 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 tab item **SSDs** on the pane **Diagnostics** to do that.

The table on this tab 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.

2.5.5 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 the latest Macs this is

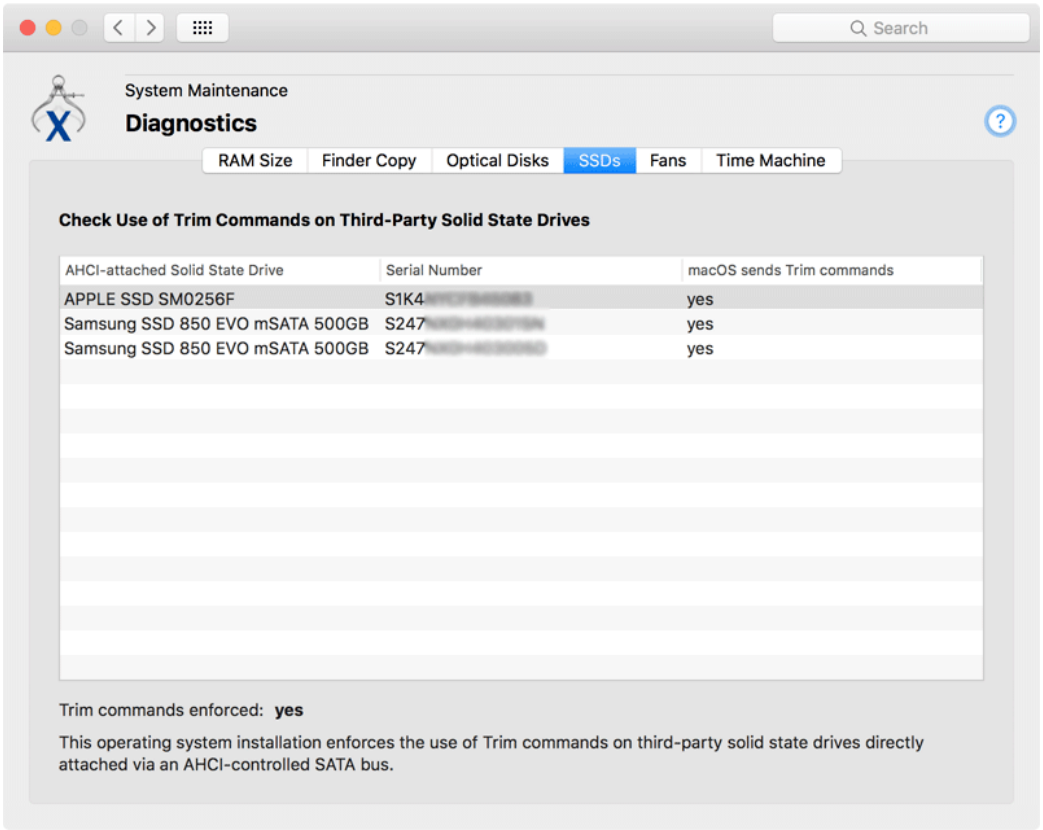


Figure 2.22: SSD

an *Apple T2* processor running Apple's BridgeOS operating system. Fans are mechanical components which are constantly in use when the computer is active, and as such 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.

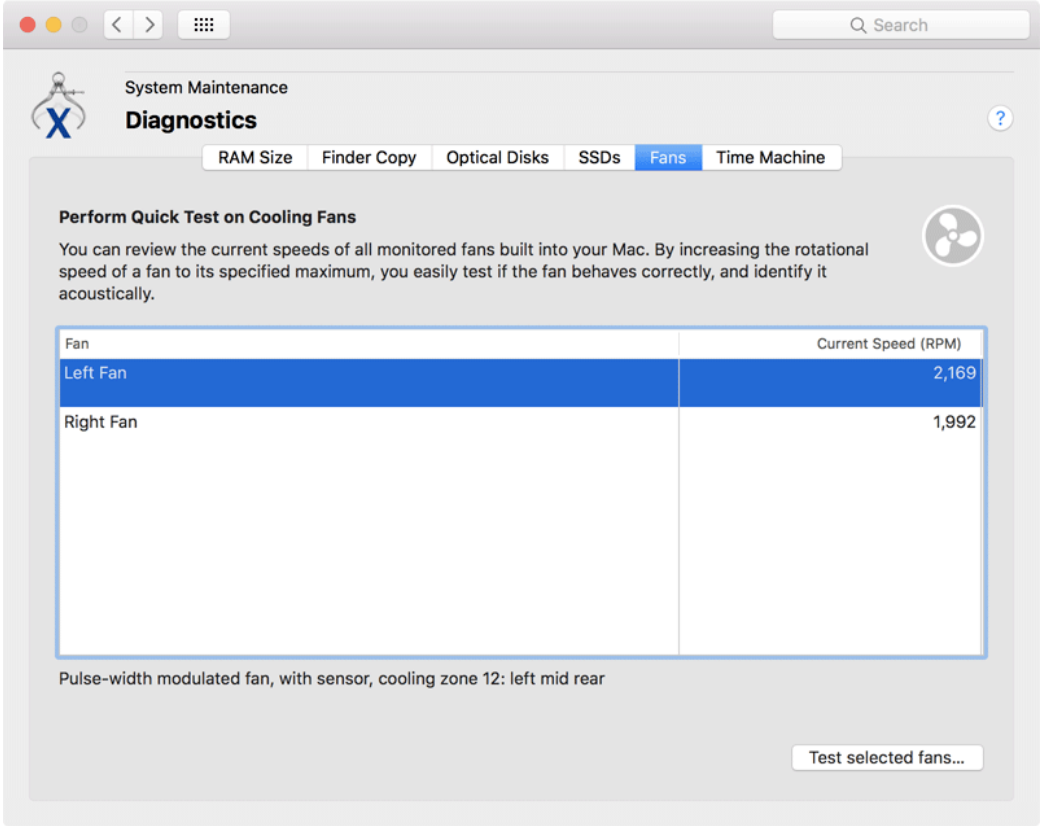


Figure 2.23: Check the cooling fans of your Mac

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

1. Open the tab 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 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.

> 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.

2.5.6 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 tab 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:

- 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).

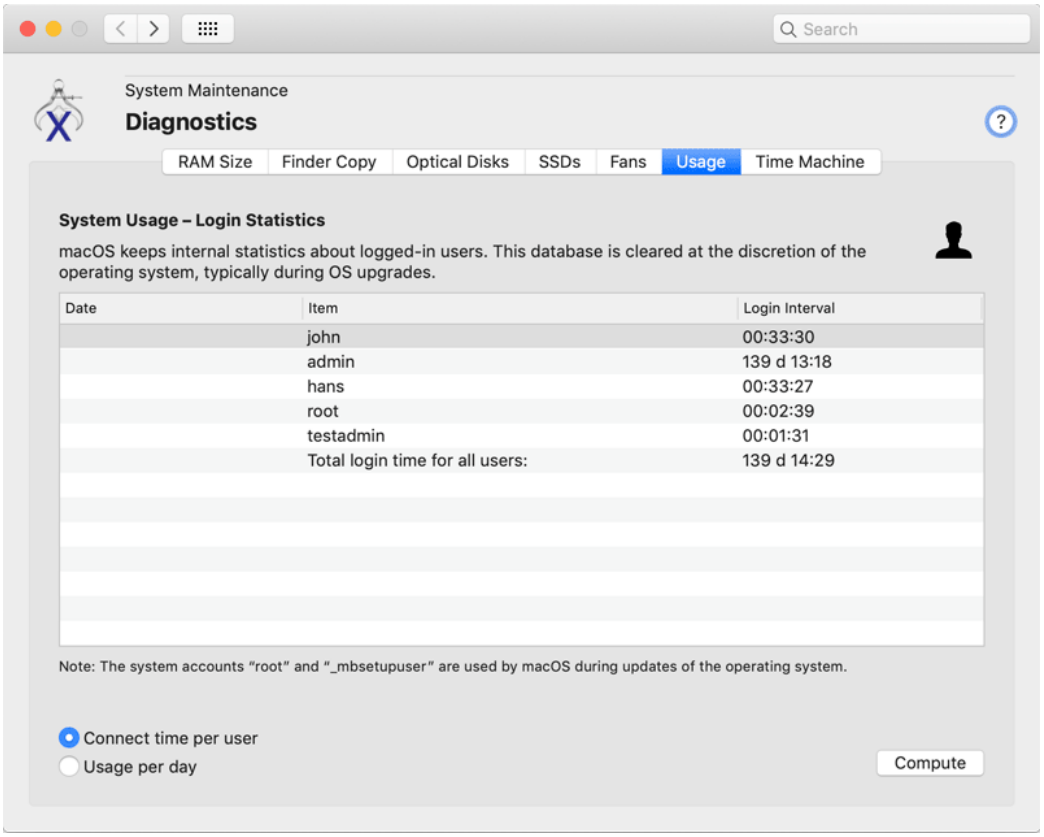


Figure 2.24: Retrieve the login time statistics kept by macOS

- 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 User pane of System Preferences 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.

2.5.7 Check Time Machine

Time Machine does not usually need any maintenance as long as you don't replace the source or destination disks. For more information, please also see the chapter on Time Machine (section 2.3 on page 39). 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

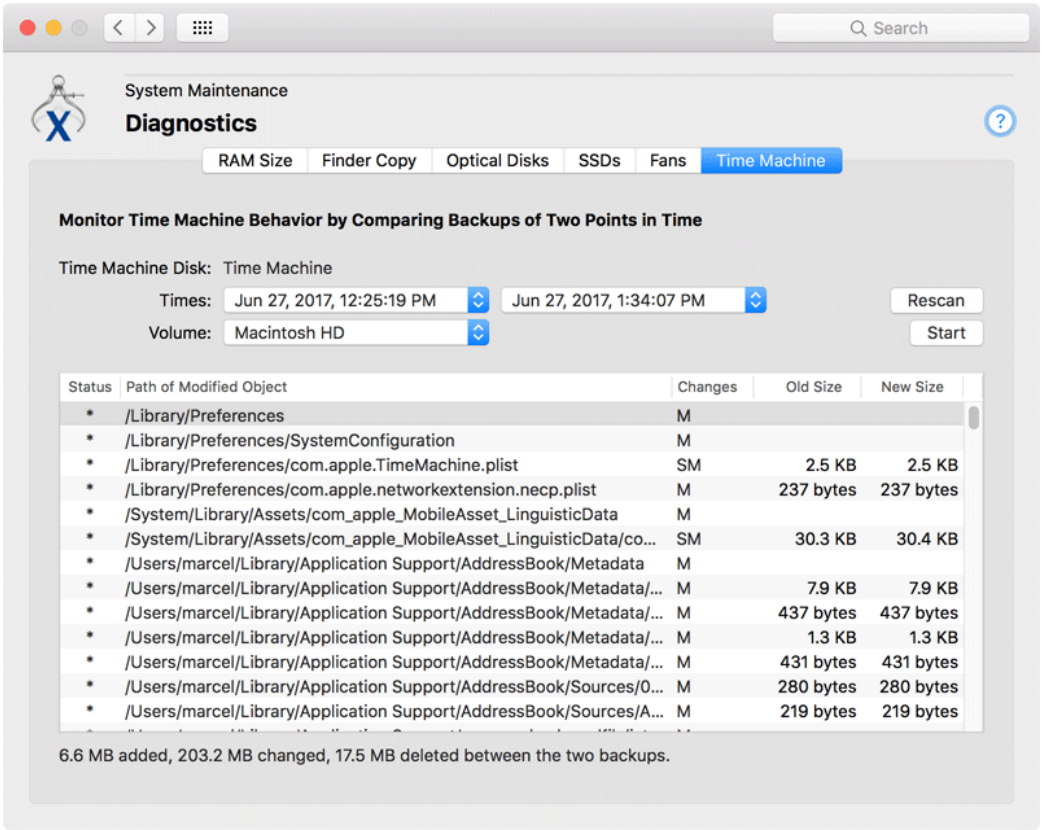


Figure 2.25: Check Time Machine

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:

1. Open the tab item **Time Machine** on the pane **Diagnostics**.
2. Ensure that the correct backup destination disk is shown at **Time Machine Disk**. This is the disk currently considered *active* by Time Machine. You cannot influence this automatic selection via TinkerTool System. In case Time Machine has been configured to use a network file server instead of a local disk drive (this includes the Apple Time Capsule), click the button **Connect to network disk**. TinkerTool System will then establish the connection to the server and scan the remote data. For a slow WLAN network, this scan may take several minutes.
3. At **Times**, select the two points in time for which the backup sets should be compared. The times must be different, but their order doesn't matter. To choose the "live" data on your computer for comparison, select the last item **—All backup items—**.
4. 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 won't be necessary if you had selected **—All backup items—**).
5. Click the button **Start**.

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.

TinkerTool System can rescan the Time Machine disks connected to your computer when you change the configuration or replace the destination disk. To do so, click the button **Rescan**.

In the event that Time Machine is using a network volume for its backups, the connection to the remote drive will still be held open after the compare operation has completed. In fact the connection will remain after you have quit TinkerTool System. This allows you to quickly start a new scan operation later. However, if you do not want this persistent connection (for example if you have a mobile computer and wish to leave the network), click the button **Eject network disk** after you completed your work with Time Machine diagnostics.

2.6 The Pane Emergency Tool

2.6.1 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 an “indestructible” disk image. 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.

2.6.2 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.

2.6.3 Instructions to Launch the Emergency Tool

In case you have printed this reference manual of TinkerTool System, the short instructions to launch the emergency tool are included here as well. Please note however, that the specific start command to launch the program can be different on each Mac, depending on where you copied TinkerTool System.

1. Turn on your Mac and immediately press and hold the keys ⌘ + R until the Apple logo appears.
2. If your Mac is protected by FileVault or by a security processor, you will see a password request after a while. Enter the requested password and continue. (This step is automatically skipped for unprotected Macs.)
3. The window **macOS Utilities** opens. Use it to start **Disk Utility** and ensure your operating system volume is mounted. If not, mount it, which can require to enter a passphrase for decryption. If you are using *macOS 10.15 Catalina or later*, there will be two different visible volumes for the operating system, by default called **Macintosh HD** and **Macintosh HD - Data**. For such a modern setup, make sure *both* volumes are mounted.
4. Quit **Disk Utility** and start **Terminal** via the menu **Utilities**.
5. Enter the following command, including the quotation marks and with correct capitalization, pressing ⏎ at the end.

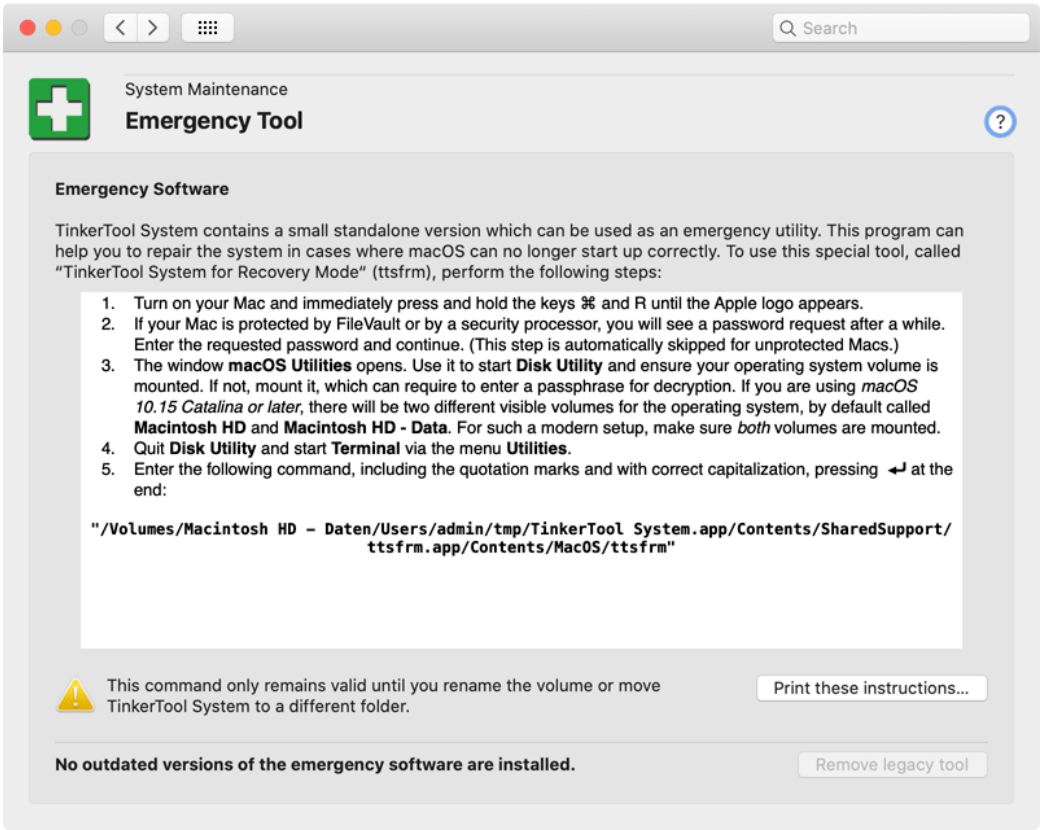


Figure 2.26: Emergency Tool

Structure of the Launch Command

As mentioned already, the command can be different depending on the location of the program and the names of your volumes, folder, and application. It could be, for example:

```
"/Volumes/Macintosh HD/Applications/TinkerToolSystem.app/Contents/SharedSupport/ttsfrm.app/Contents/Ma
```

The actual call that must be typed 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.
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/
```

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.

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 and operating system where the application itself has been stored.

This results in the following consequences:

- TinkerTool System should always be placed on the volume where the operating system is located.
- If you work with multiple operating systems, each of the system volumes should have its own copy of TinkerTool System.

2.6.4 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 237).

2.6.5 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 shows 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.

2.7 The Pane Install Media

2.7.1 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 the *recovery partition*, which is usually installed for each operating system partition on your Mac and for each Time Machine destination disk. The 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 use Disk Utility, Terminal, or the "complete restore" feature of 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.

2.7.2 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 of the App Store application. 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. "Installer macOS High Sierra". You should find a web page that contains a link to a hidden entry in the App Store which offers the respective 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. Users of macOS Catalina or later can try to download installers without using the App Store (see below).
- any disk-like mass storage device supported by macOS which has a capacity of 8 GibiByte or higher. 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.

> 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.
>
> TinkerTool System 6 does not support installer applications for macOS 12 or later.

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. Select the device in the sidebar of Disk Utility.
3. Press the button **Erase** in the toolbar.

4. Specify **Format: Mac OS Extended (Journaled)** and **Scheme: GUID Partition Map**, enter a **Name** by your choice.
5. Press the button **Erase**.

After the device has been erased, macOS and TinkerTool System will accept it as destination medium.

2.7.3 Downloading Installer Apps without the App Store (macOS Catalina or later only)

> This feature is not available on macOS Mojave.

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, enter the full version number of the installer you are interested in, for example **10.14.6**, 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.

> 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.

You will see in the download sheet whether Apple is indeed offering an installer with the specified version number to you. 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. If you stop the download procedure, macOS may decide to continue the operation in the background. TinkerTool System has no influence on this.

2.7.4 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.

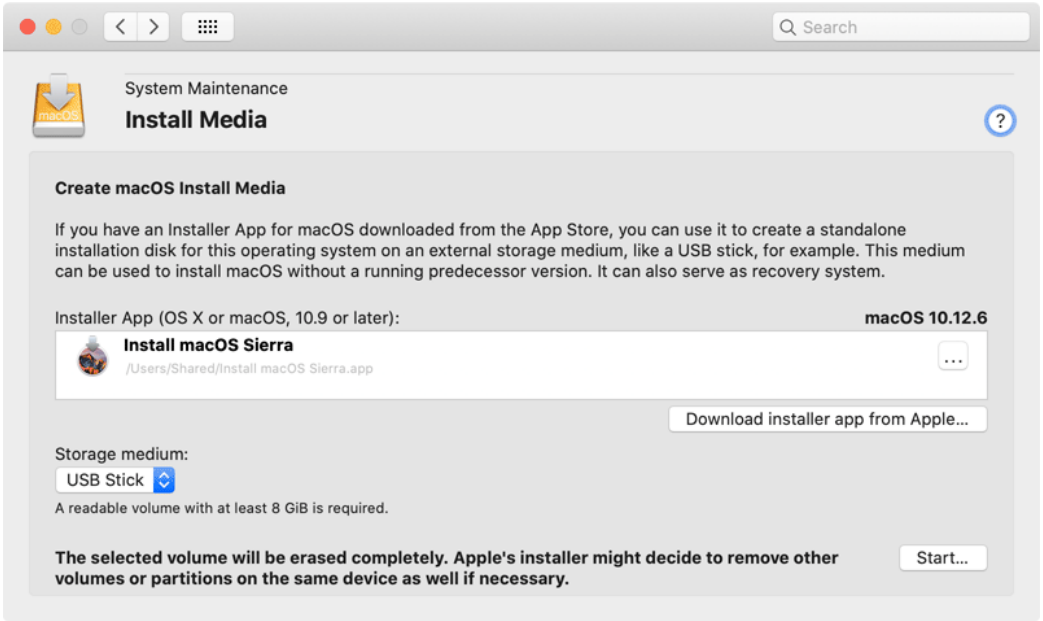


Figure 2.27: A standalone OS installation disk can be created with a few mouse clicks

If TinkerTool System doesn't list a device you like to use, please read the instructions in the previous section.

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.

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.

2.8 The Pane Info

2.8.1 System Information

The item **System Information** 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 and a picture 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.

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, available processor cores and active cores, the information whether each core is capable of executing multiple threads of instructions (Simultaneous Multi-Threading, if active, the hardware will simulate twice the number of processors), 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 code into one single number, 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 3 caches.

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 2.5 on page 59).

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. This 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.

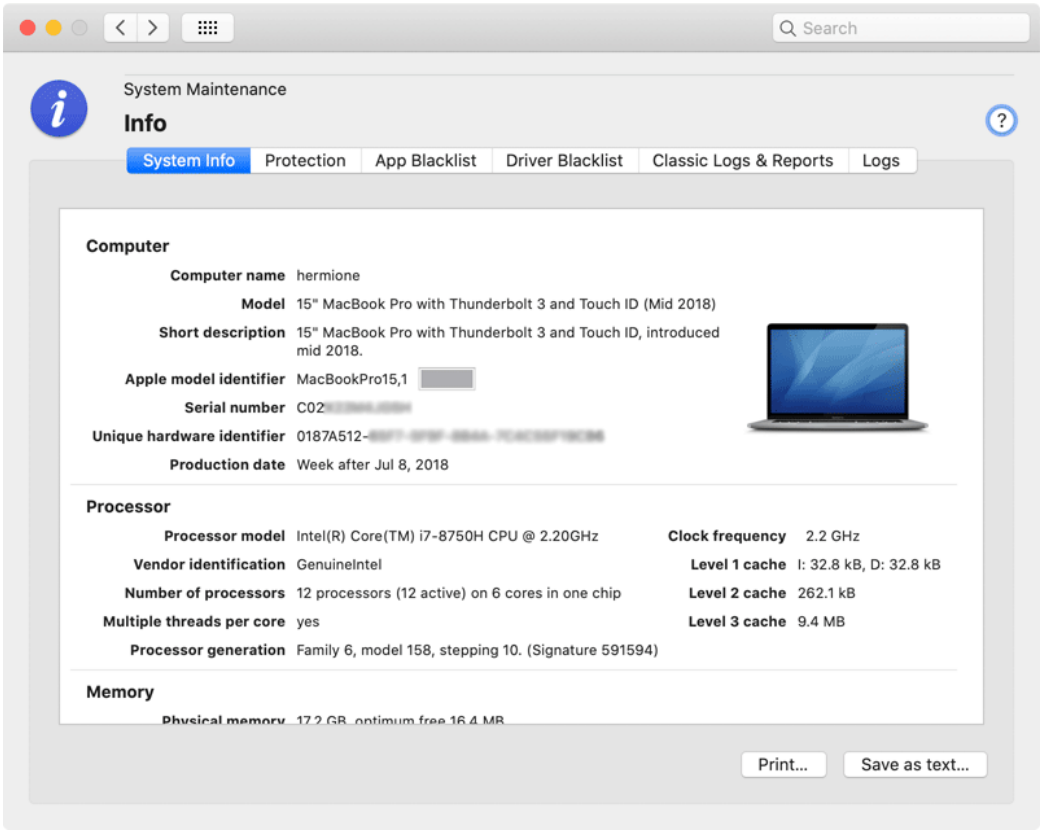


Figure 2.28: System information

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.

The last section **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 **Release Status** indicates whether you are using an officially released version of the operating system, or a preview version from one of Apple's software seeding programs.

> Note that the source of the operating system is more important to define its release status than the version number. When you receive a specific system version as a pre-release copy, exactly the same system may later become the official version. So identical operating systems can sometimes be marked as official and sometimes as pre-release, depending on where they came from.

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 7).) 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.

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**.

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.

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

2.8.2 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 system data files and security updates** is enabled on the pane **App Store** in **System Preferences**. 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 tab 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.

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.

- Data in the columns **Type** and **Name** 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.

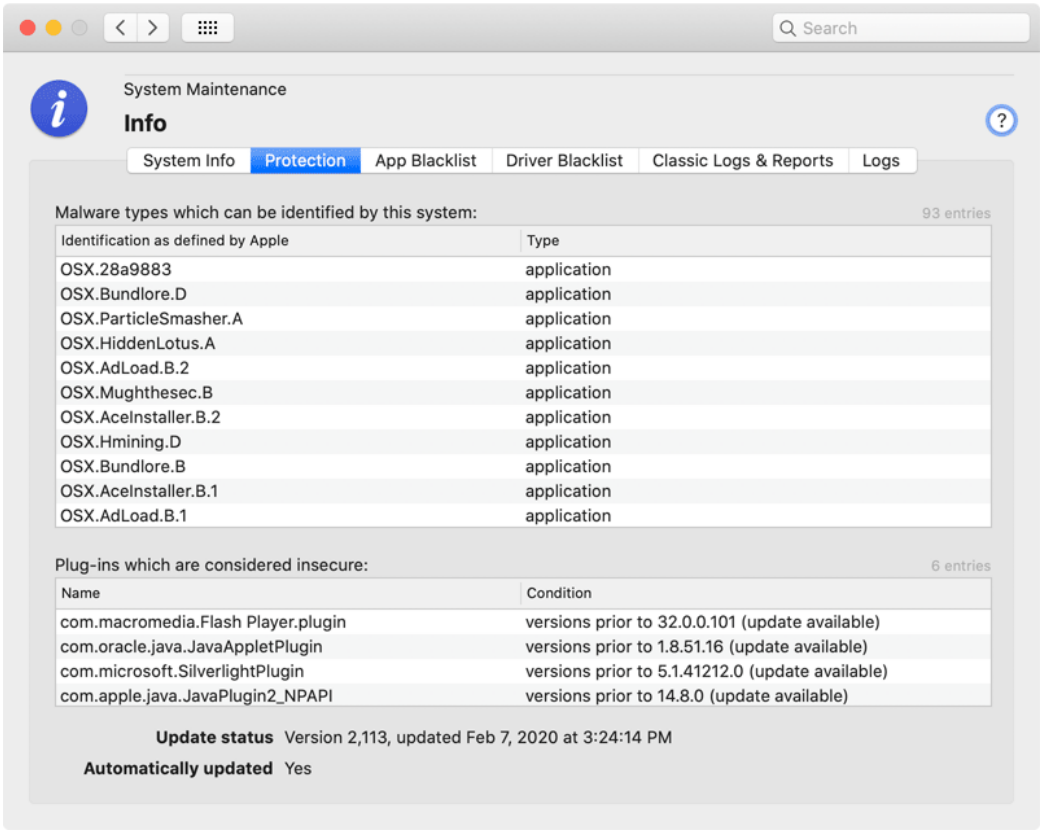


Figure 2.29: Malware protection

2.8.3 App Blacklist

After you open the tab **App Blacklist**, 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 system data files and security updates** is enabled on the pane **App Store** in **System Preferences**.

Three different types of blacklists 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* 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 blacklisted. 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. If the blacklist entry is not enforced, you can use the Finder to unblock the application. Please see the next paragraph for details.

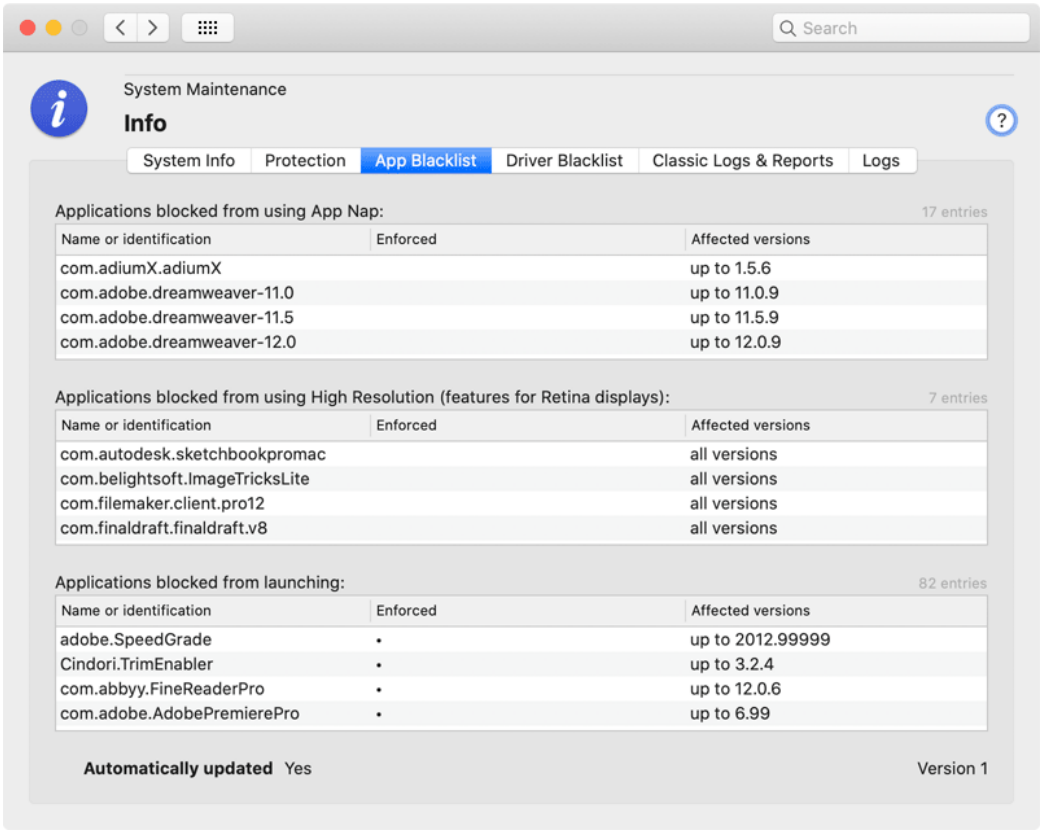


Figure 2.30: App Blacklist

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

You can override Apple's recommendation to block applications from using certain features if you have reason to do so. In that case, perform the following steps:

1. Select the affected application in the Finder.
2. Open the menu item **File** > **Get Info** or press ⌘+I.
3. Remove the check mark at **Prevent App Nap**, or **Open in Low Resolution**, respectively, if available.
4. Close the Info panel.

2.8.4 Driver Blacklist (macOS Mojave only)

> For technical reasons, this feature is not needed in macOS 10.15 or later. Catalina basically rejects *all* third-party drivers, but uses special certificates and internal whitelists to accept a few selected ones.

Similar to the application blacklist, macOS also maintains multiple **driver blacklists**, or more exact, lists which automatically deactivate certain kernel extensions when they are detected in your system installation. Because kernel extensions can cause the entire operating system to fail or prevent the computer from starting up, all blacklist entries are always enforced. TinkerTool System shows two lists in separate tables.

The upper list shows kernel extensions which are known to cause a crash of specific versions of macOS. The extensions in this list cannot be easily identified by comparing version numbers or are comprised of multiple components, so macOS uses additional internal checks to verify if these files have cause problems on your system in the past.

The column **Software component** shows a readable description of the affected driver or extension, while the column **Kernel Extension or other bundle to remove** shows the file name used by macOS to recognize and delete the component.

The extensions listed in the lower table can be identified by version numbers. The column **Identification** shows the known bundle names, the column **Affected versions** the ranges of versions that must not be loaded by the current operating system.

> Software publishers need explicit permission from Apple to develop kernel extensions. All extensions that don't have this permission are additionally blocked automatically, so they don't need to appear in this blacklist. The operating system only uses this blacklist to remove incompatible drivers in advance, for example when upgrading or migrating from a previous version of macOS, or when the security feature to ignore unauthorized kernel extensions has been switched off explicitly, for example on a developer computer. For more information, please also see the subsection on Security options in the chapter for the Startup pane (section 4.3 on page 198).

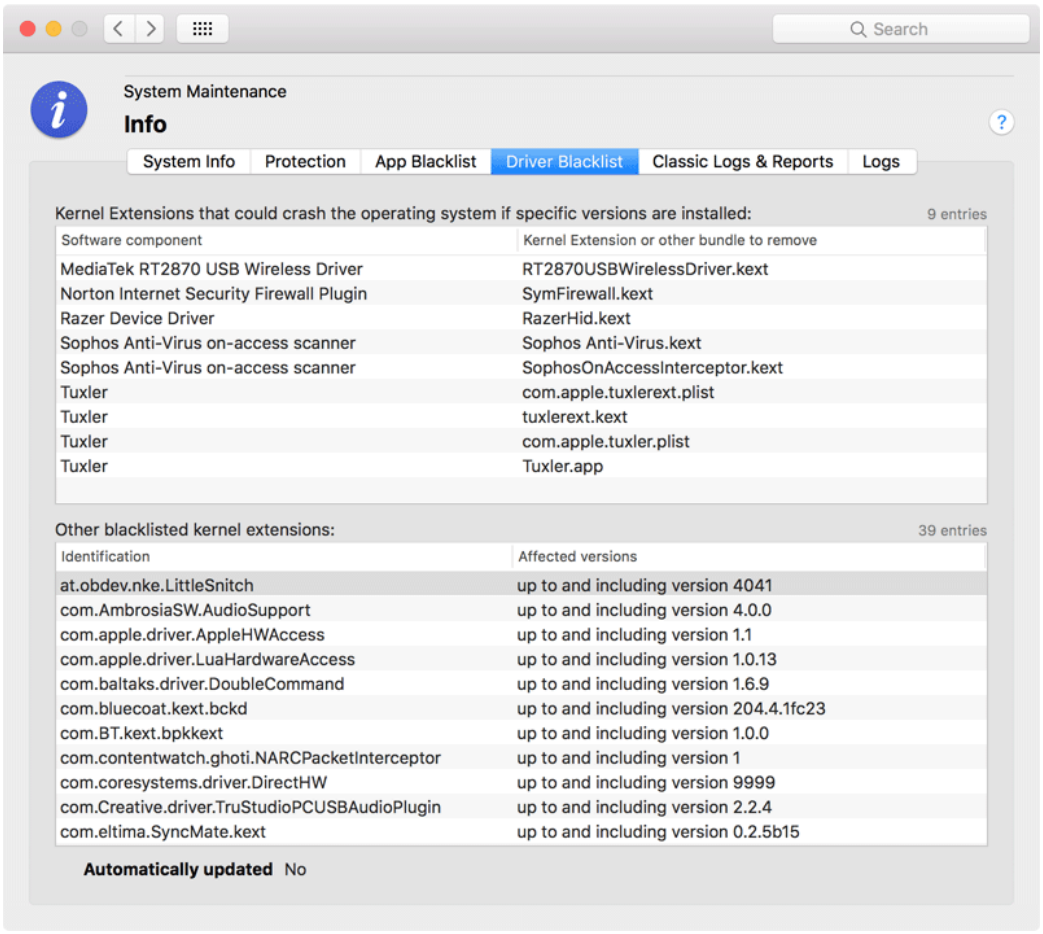


Figure 2.31: Driver Blacklist

2.8.5 Classic Logs and Reports

After selecting the tab item **Classic Logs & Reports**, you will have direct access to a high number of log recordings kept by macOS and the macOS Server app. 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.

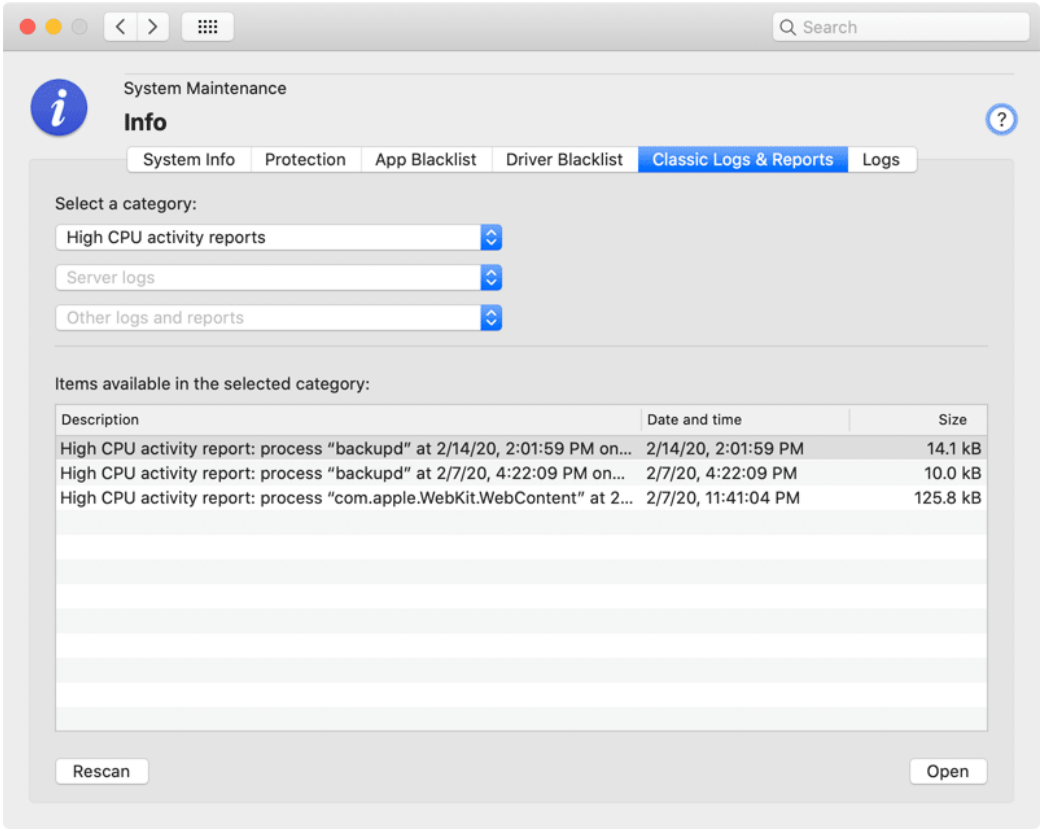


Figure 2.32: Logs and reports

The possibly available logs and reports are accessible via three 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 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*.
- **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 diagnostical 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 iTunes or 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.

The second pop-up button named **Server logs** permits access to the log files collected by the server features of macOS. Some of the logs are only kept when you install the macOS Server app in addition to macOS and enable the corresponding services, but some logs apply to network service features of macOS in general. TinkerTool System automatically adds menu items to the pop-up button depending on what services are active on your system. The names of the logs and reports should be self-explanatory and are not repeated here. TinkerTool System groups the individual items into the following service categories:

- **Open Directory**: logs of the Open Directory client and server components
- **Profile Manager**: logs of the Mobile Device Management (MDM) server

The third 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.

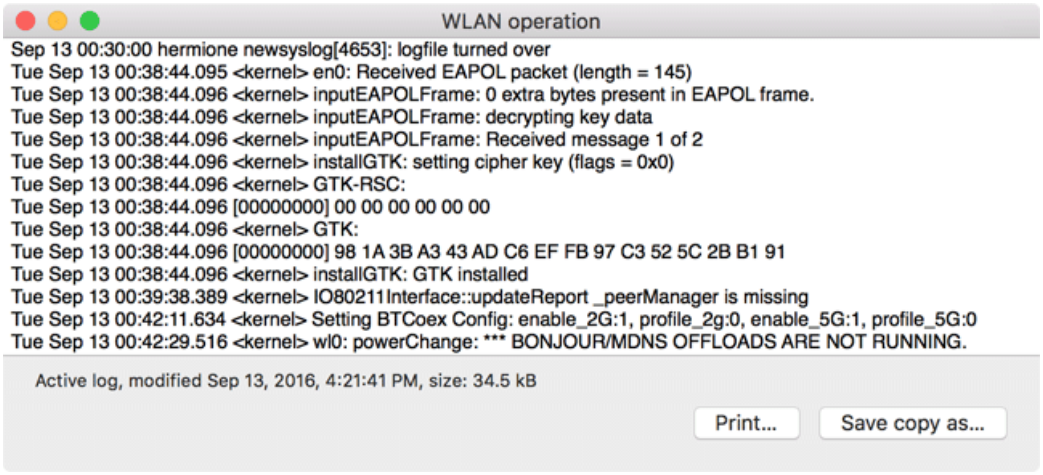


Figure 2.33: The contents of a log or report is shown in a separate window.

After you have selected a log category with one of the three 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.

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 tab item to update the pop-up buttons accordingly.

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

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).

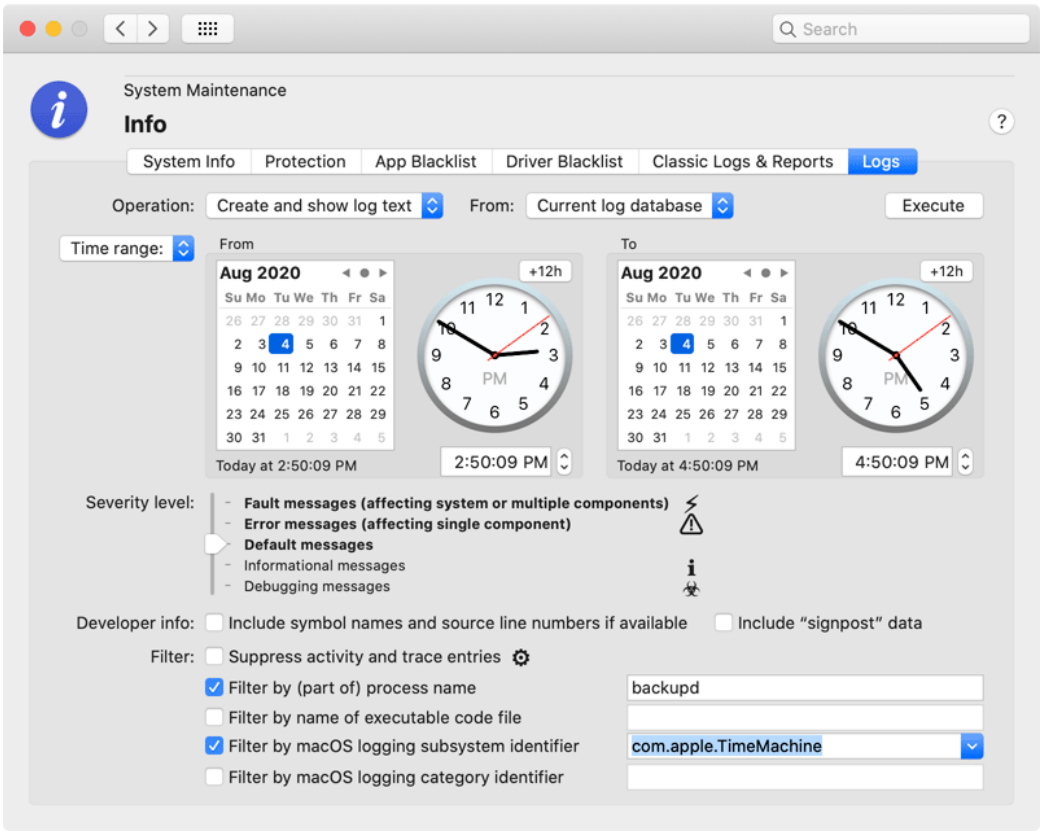


Figure 2.34: Working with modern logs

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

1. Open the tab 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 pop-up button at **Time range** to select either all log data available in the chosen source, or to specify a time interval. 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.

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** in the upper right corner.

By default, TinkerTool System will choose a time interval that includes the last two hours before the application was launched. 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 half a million lines.

Figure 2.35: Display of a macOS log

TinkerTool System uses the small icons shown next to the controls to also mark messages with the corresponding severity level or activity messages in the result text. The markers are shown at the beginning of the associated line.

> The marker <**private**> 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.

You can save the generated log text by clicking the button **Save**… in the display sheet. It will be stored in plain text format, so it can be opened by any text editor.

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 partition 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.

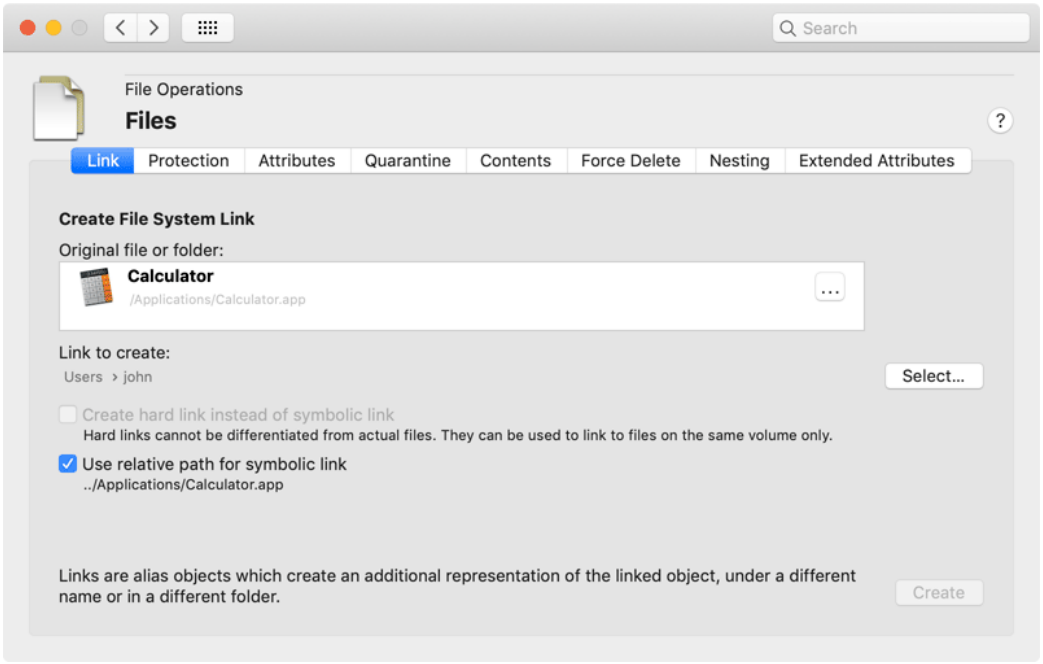


Figure 3.1: Link

> 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 tab 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.

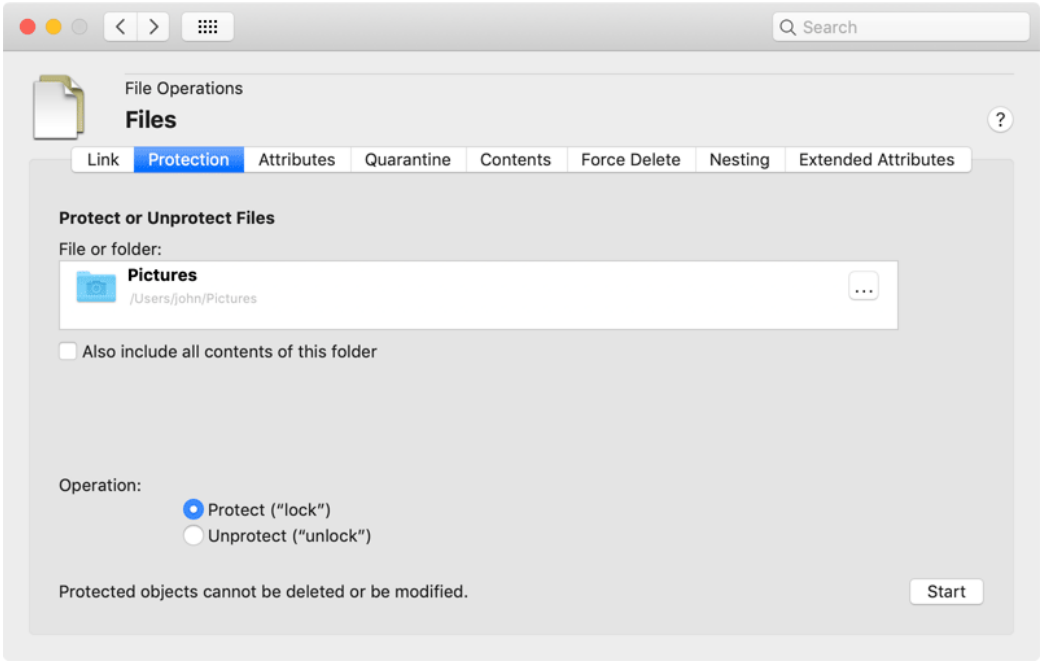


Figure 3.2: Protection

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 tab 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.
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.

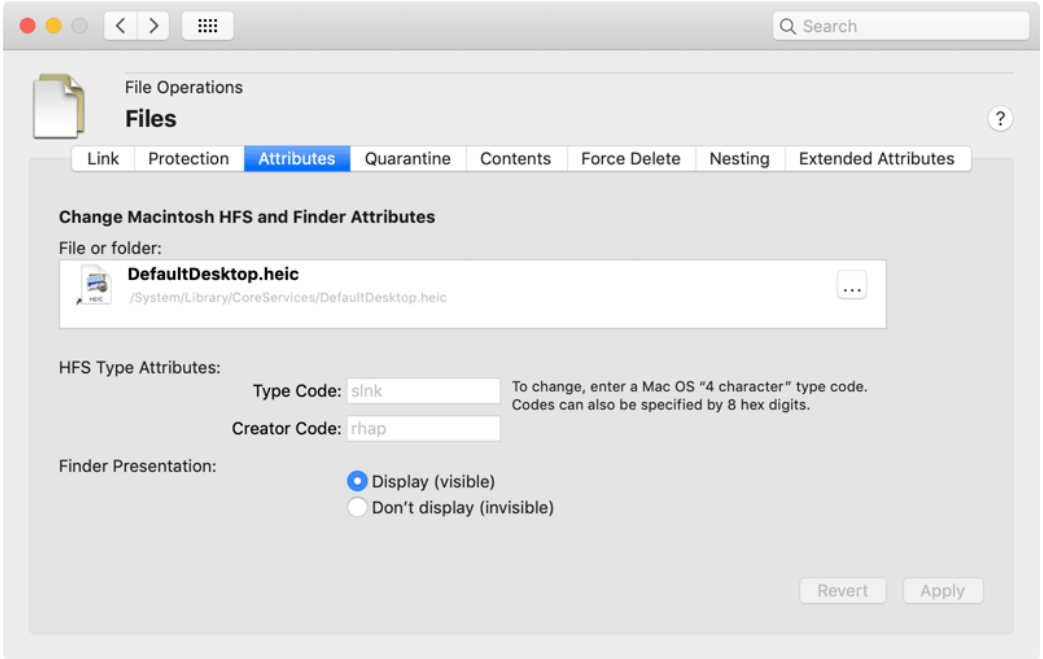


Figure 3.3: Attributes

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

1. Open the tab item **Attributes** 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. 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 could use its sister application **TinkerTool** to modify your Finder preferences to the effect that the Finder displays invisible objects, too.

3.1.4 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.

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 tab item **Quarantine** on the pane **Files**.

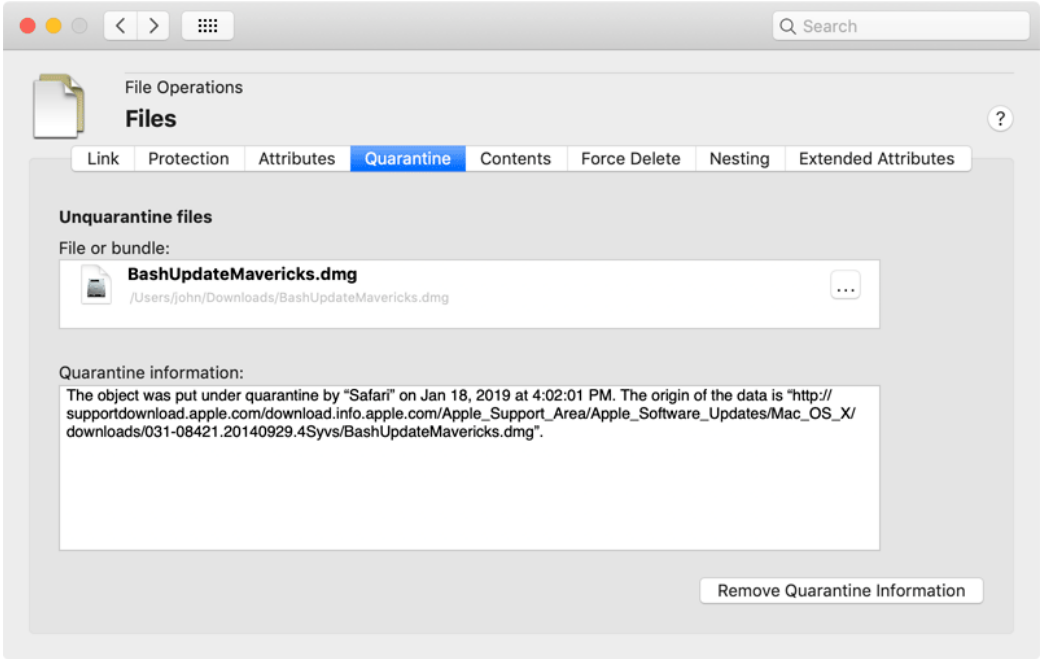


Figure 3.4: Quarantine

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**.

3.1.5 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 tab 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.

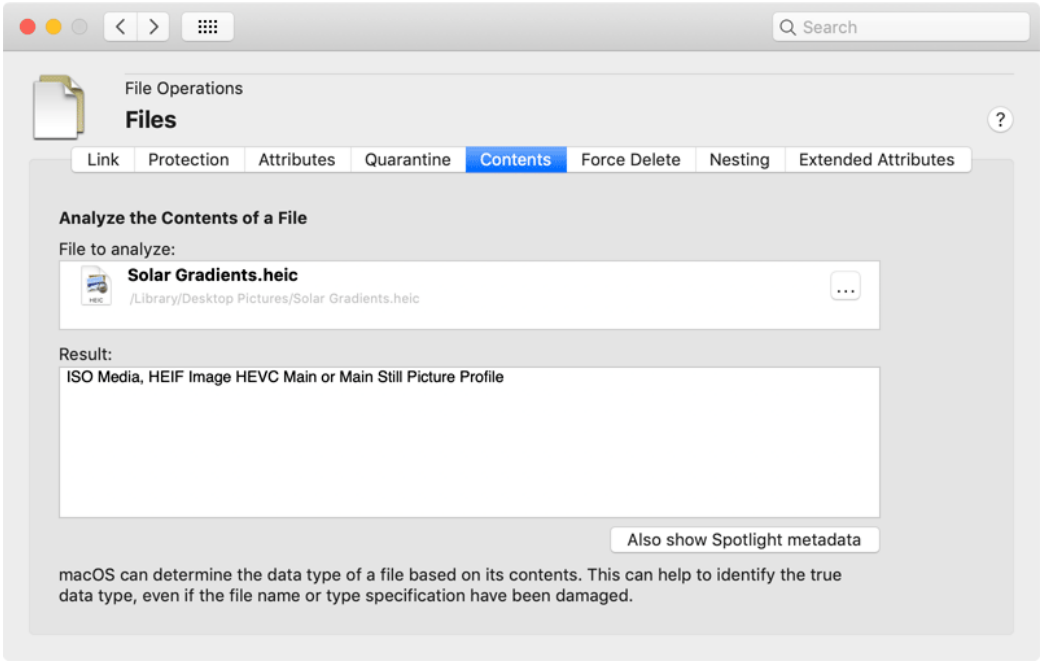


Figure 3.5: Contents

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.

3.1.6 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:

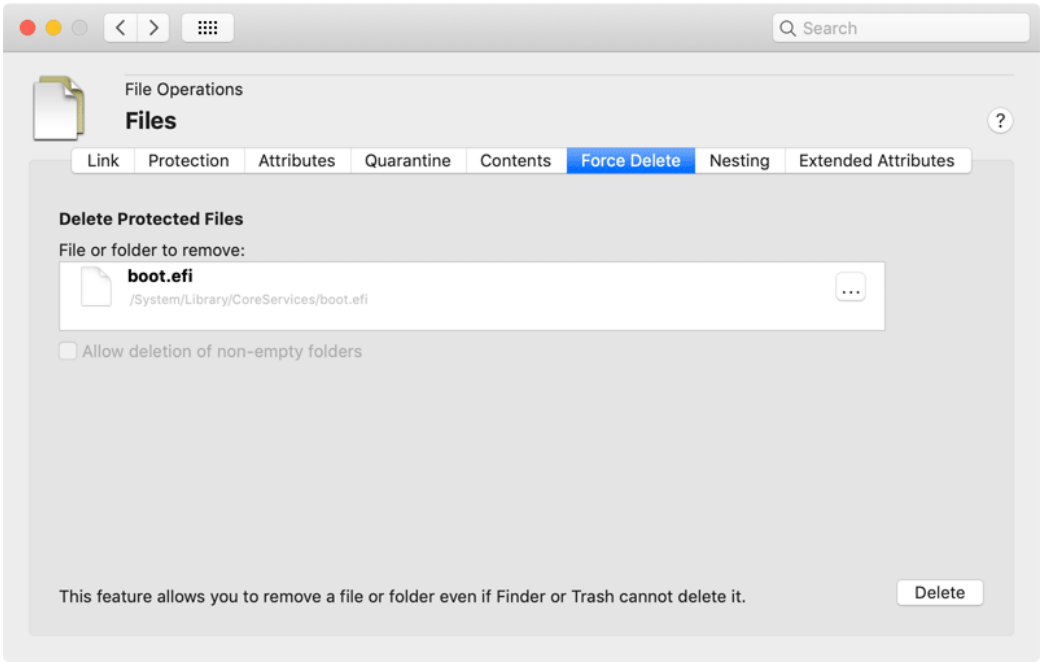


Figure 3.6: Force delete

1. Open the tab 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**.

3.1.7 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.

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.

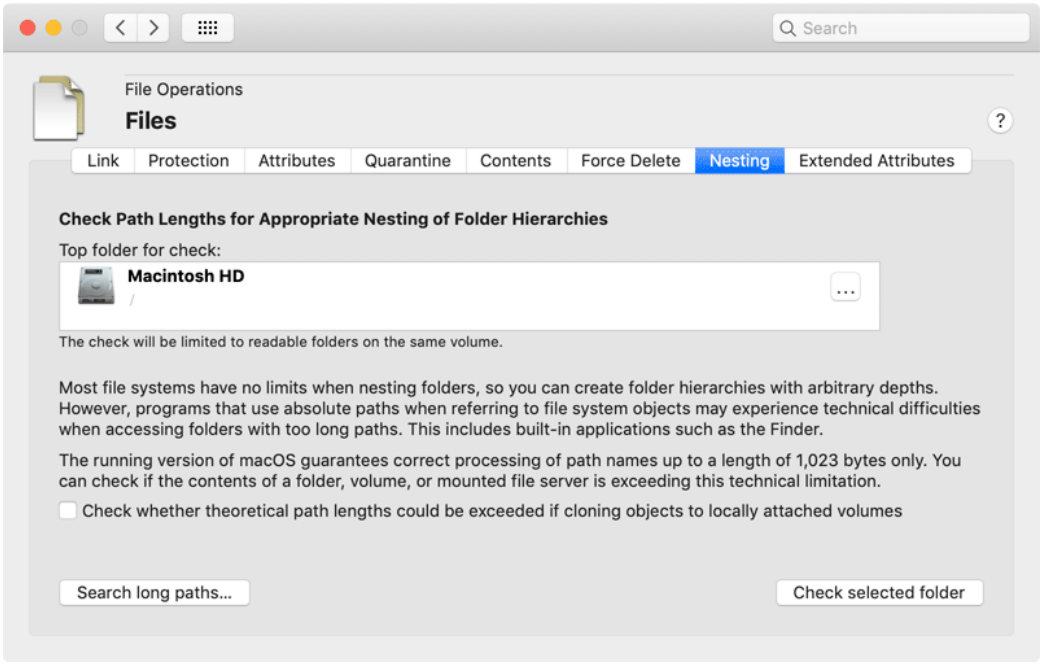


Figure 3.7: Find absolute paths that may be too long for many applications

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

1. Open the tab 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**.

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 tab 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 where the specified path length is exceeded. The results are displayed at the end of the search procedure, listing paths and their respective lengths.

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

3.1.8 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 color labels of the 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 tab 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:

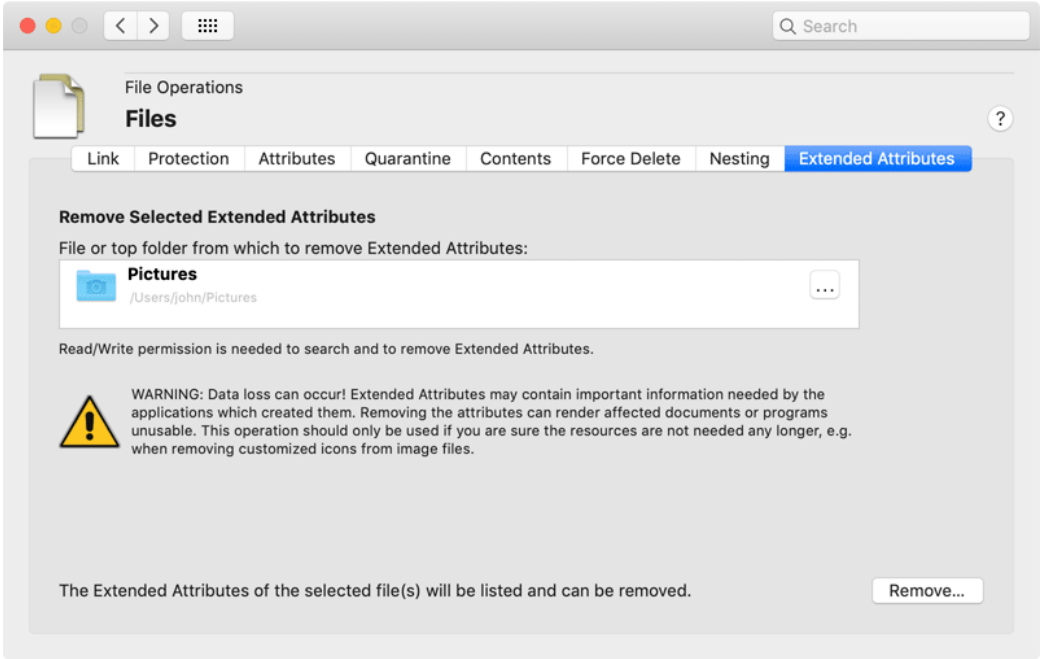


Figure 3.8: Remove Extended Attributes

- 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.

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 tab 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 preferences panel of the application (section 1.3 on page 7).

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 authoring a CD-ROM, 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 preferences the Finder was using the last time a user opened the folder containing that file. View preferences include the size of the Finder's display window, the view mode (icon, list, columns, Cover Flow), the position of the icons, the sorting preferences, background images, and much more. The Finder's view preferences 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 105). 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 preferences, 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 tab 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**.
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.

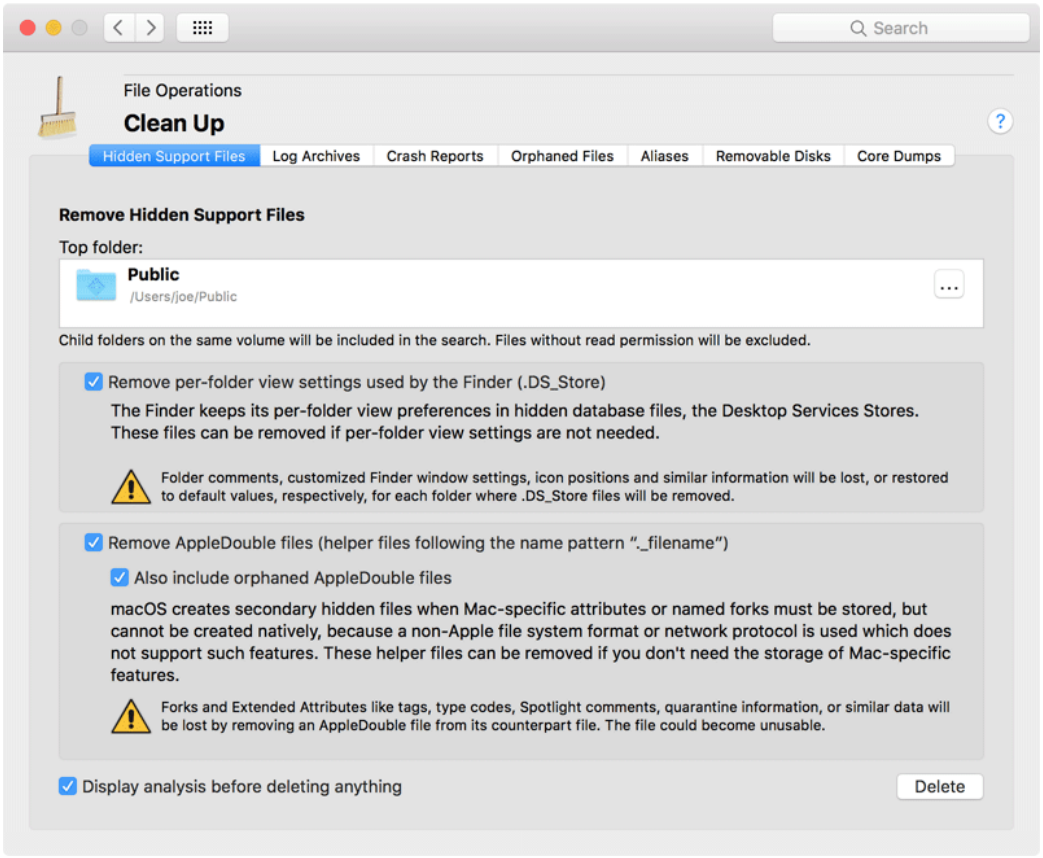


Figure 3.9: Hidden support files

3.2.3 Log Archives

As outlined in the chapter The Pane Info (section 2.8 on page 85), 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.

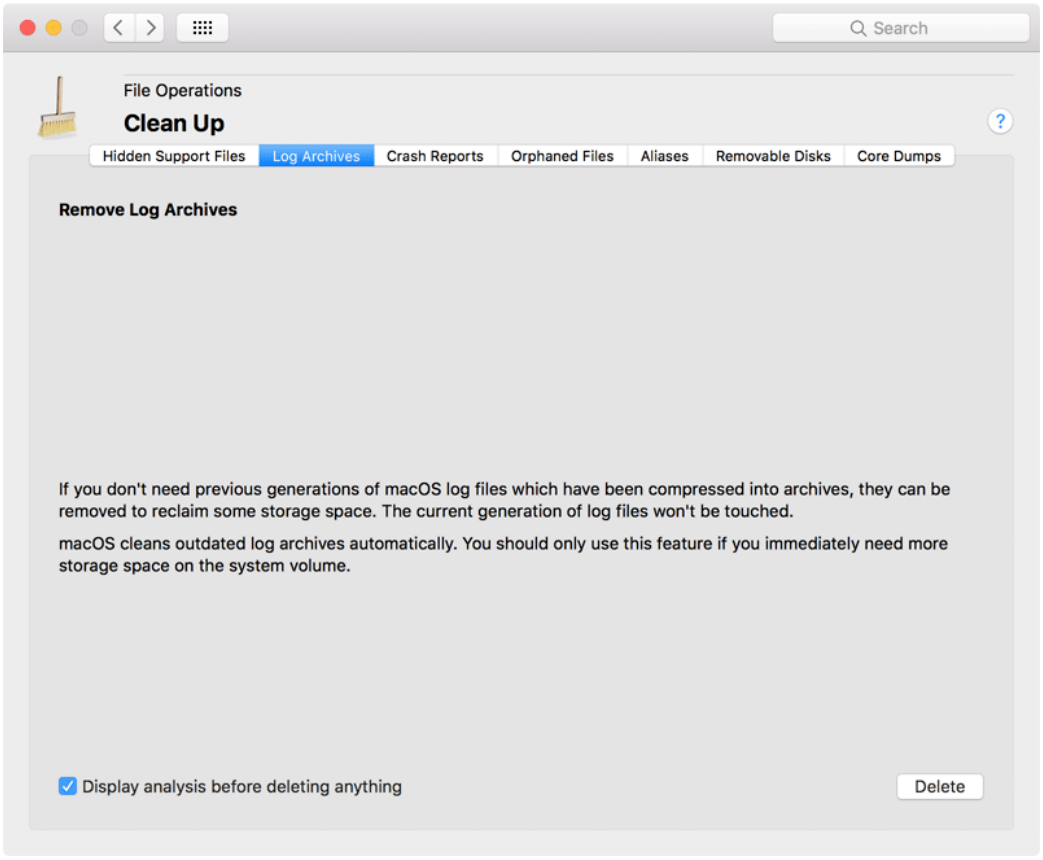


Figure 3.10: Log archives

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 tab 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.

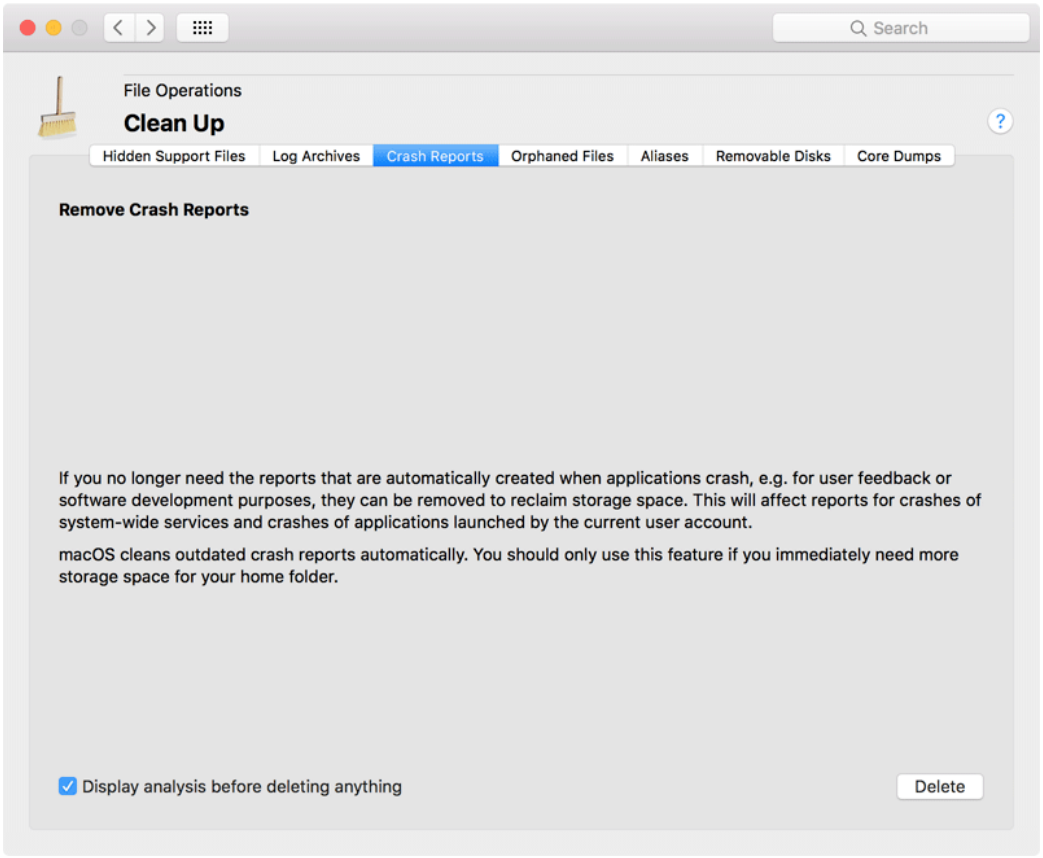


Figure 3.11: Crash reports

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.

> 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 tab 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 Preferences** 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 such a user was granted permission to create files *outside* his 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. 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 143) 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.

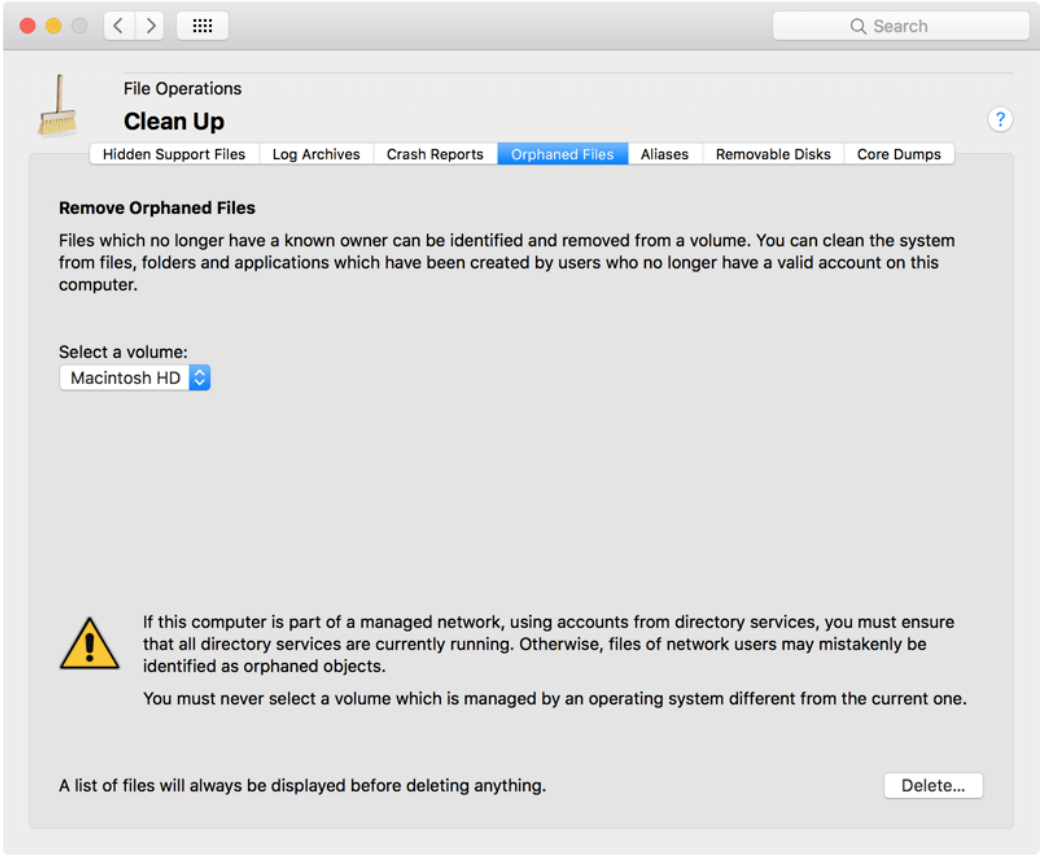


Figure 3.12: Orphaned files

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 and if necessary to delete them, perform the following steps:

1. Open the tab item **Orphaned Files** on the pane **Clean Up**.
2. Click the button **Delete**… 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. If multiple orphaned files have been found, TinkerTool System will ask you whether to save a list of file paths as text file. Make your choice and follow instructions.
5. The list of affected files and folders will always be displayed. By selecting or deselecting check marks in the column **Remove?** you can choose which objects to delete and which to keep.
6. Click the button **Delete** in the dialog sheet to remove the selected objects or click **Cancel** to perform no operation.

If you choose to create a report file in step (4), a text file with the name extension **.txt** will be created. This can be helpful if you don't actually like to delete orphaned files, but instead review the list to transfer all found objects to a new owner. The file contains the full paths of all objects, one per line, each path enclosed in quotation marks. This way, the file can be edited and easily converted to a Unix script that performs operations on the affected files.

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 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 105)). 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.

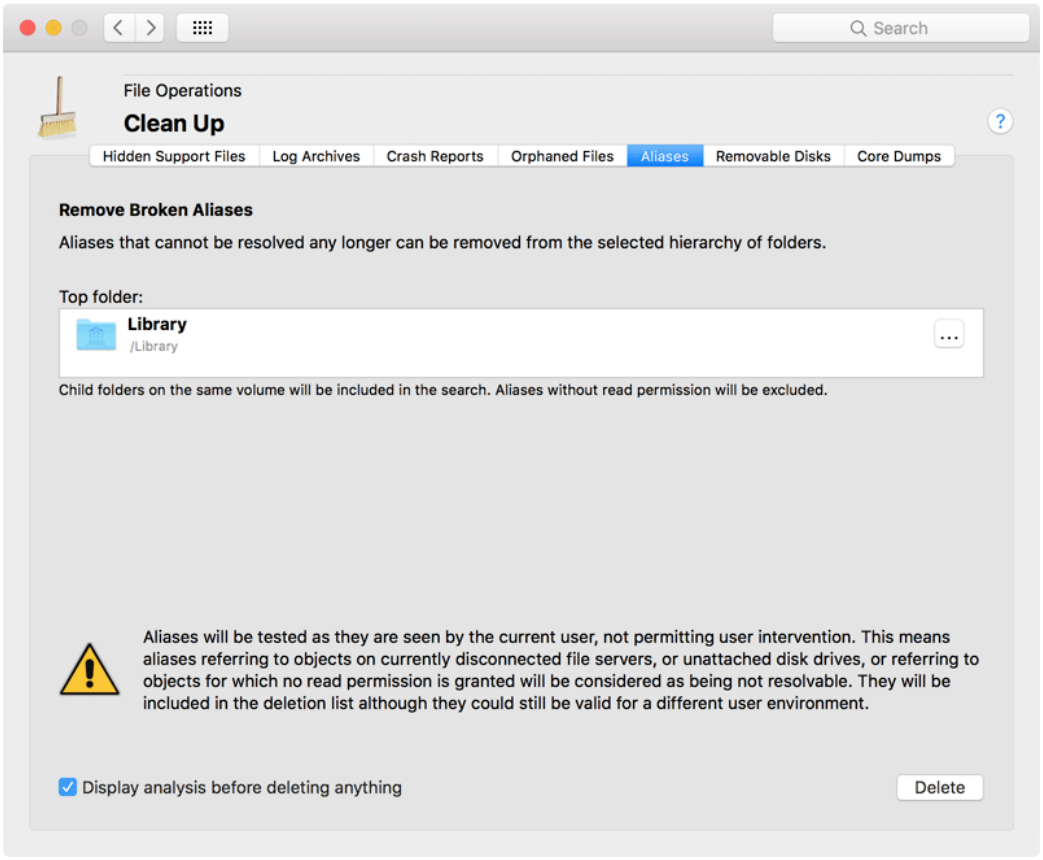


Figure 3.13: Aliases

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 memory stick, 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.

> 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 tab 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 memory stick.

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 tab 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**.

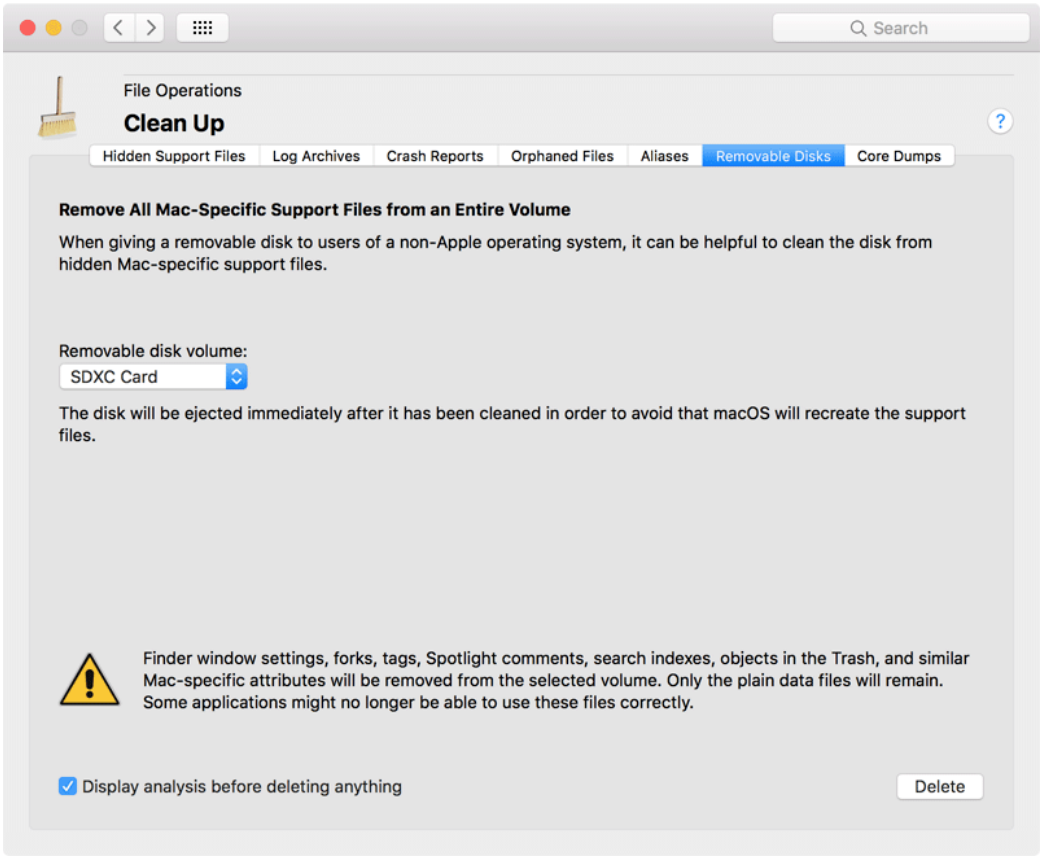


Figure 3.14: Removable disks

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.

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 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 tab 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.

For "Apps" bought from the Mac App Store, new, modified rules apply: Apps are installed automatically and they should be removed with the *Launchpad* application only.

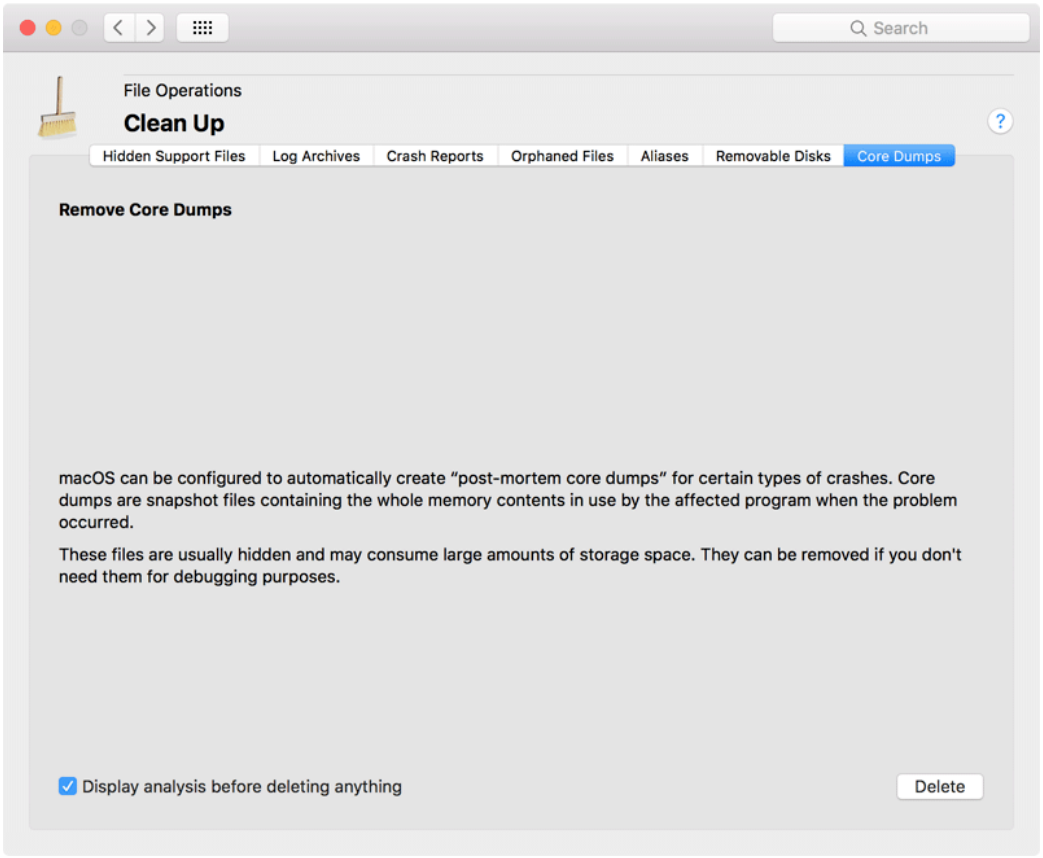


Figure 3.15: Core dumps

However, macOS automatically creates additional files when you work with a new application, for example files to store the personal preference 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 were the uninstallation assistant of TinkerTool System can help.

3.3.2 Let TinkerTool System search for software of a specific type (macOS Mojave only)

> This feature was initially designed for classic versions of Mac OS X which allowed users to install additional operating system plug-ins in specific folders. It no longer makes sense in modern versions of macOS and is not available in macOS Catalina or later.

It is possible to let TinkerTool System search for software components automatically, offering the potential candidates for the uninstallation assistant. The found components will be listed in a table with their names, icons, paths, version numbers, and the dates of last usage. TinkerTool System can search for the following categories of software:

- macOS applications, installed in any of the standard Application folders
- Widgets
- Screen savers
- Preference panes
- QuickTime plug-ins
- Internet plug-ins

To use the search, perform the following steps:

1. Select the tab item **Uninstallation Assistant** of the pane **Applications**.
2. Set or remove the check marks **(Available for)** where the search should be performed. You can select the private home folder of the current user account **(User)**, the folders offering software for all users of the current computer **(This Computer)**, or the item **macOS Network** to search in the shared **Applications** and **Library** folders of an macOS Server used as a central repository for that purpose.
3. Open the pop-up-button **Search components** and select one the software categories.
4. TinkerTool System will begin the search and list the found components in a table. You can select one of them and click the **OK** button even when the search is still running.

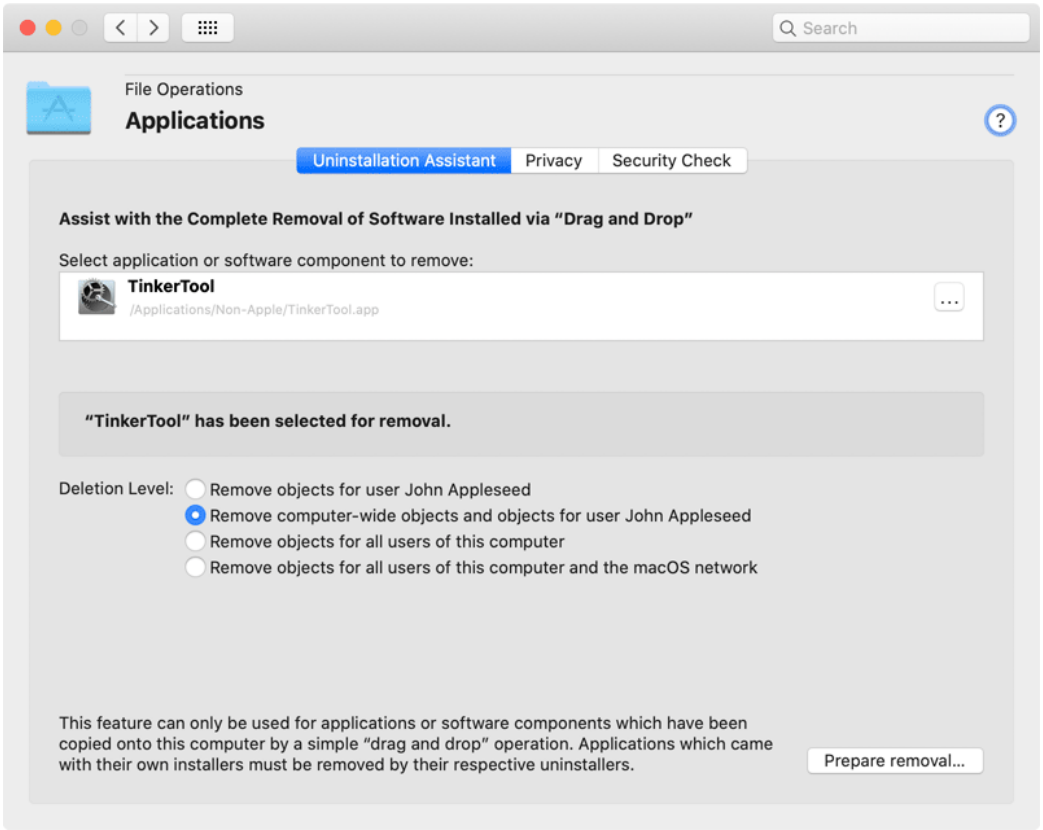


Figure 3.16: Uninstallation assistant (Catalina version)

3.3.3 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 Server 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 tab 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, which includes Apps from the Mac App Store, 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.

3.3.4 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 Preferences** > **Security & Privacy** > **Privacy**. 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.

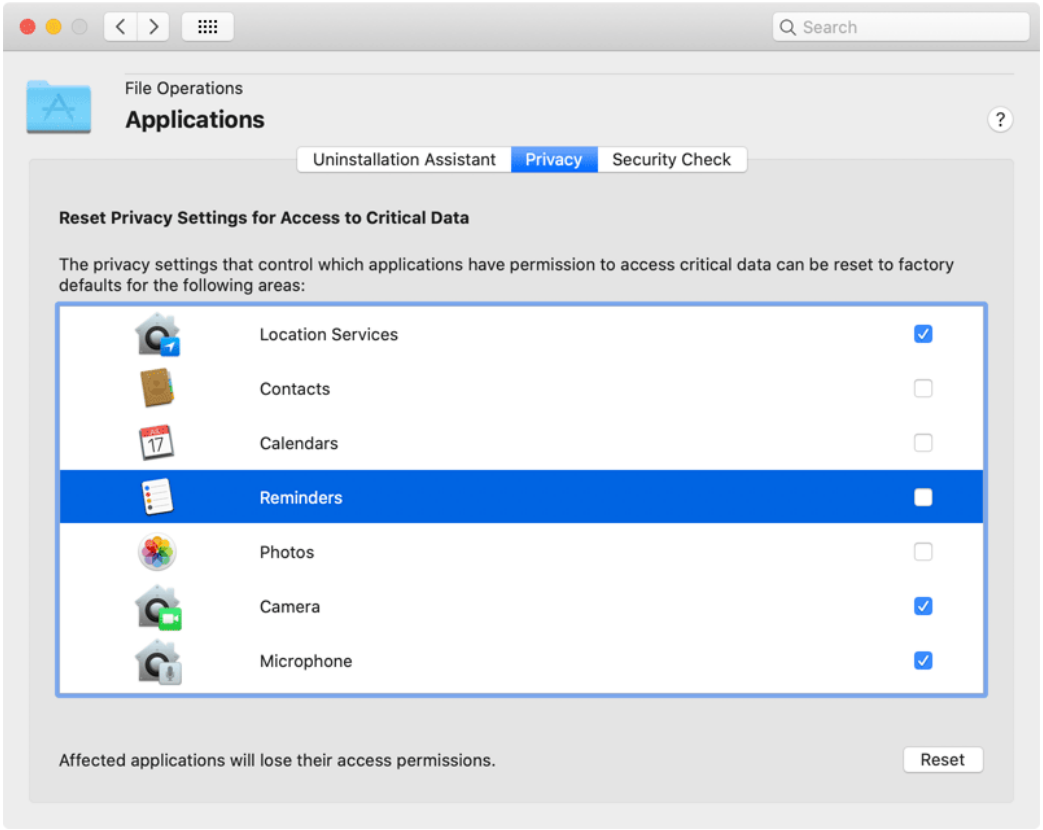


Figure 3.17: Reset application privacy settings

1. Open the tab item **Privacy** on the pane **Applications**.
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 *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 *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 tab 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:

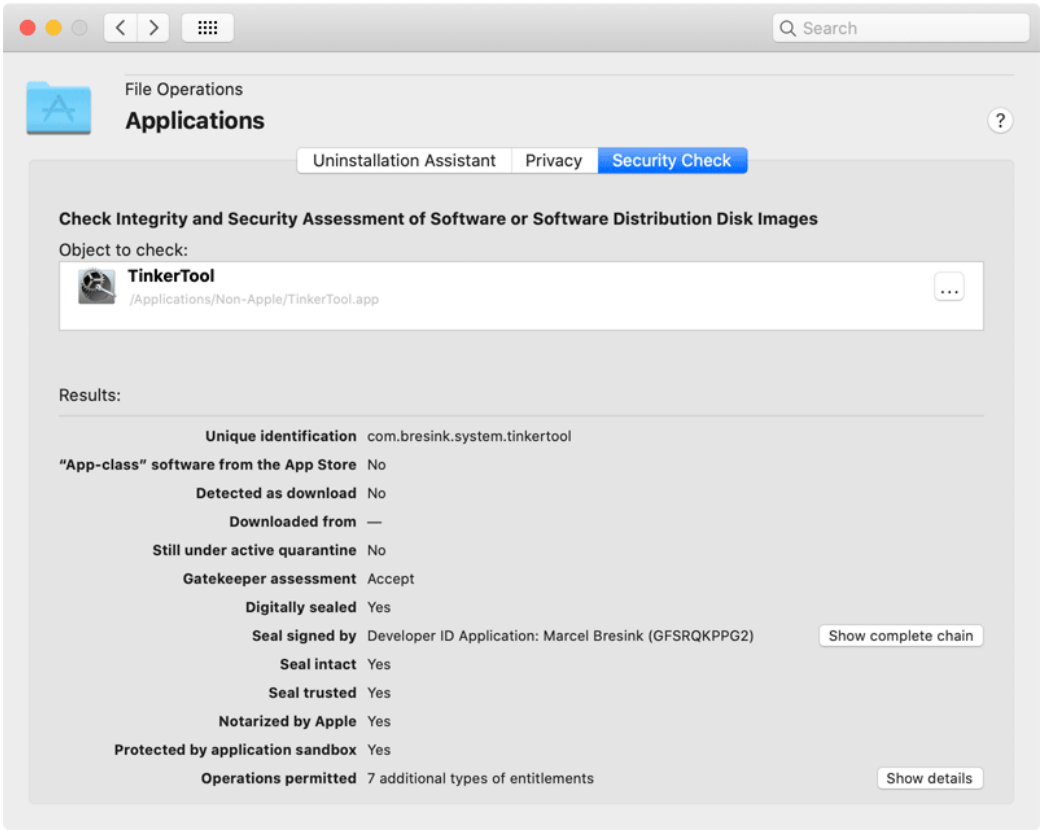


Figure 3.18: Security check

- **Unique identification:** the internal unique name used by macOS to identify this application. (Single executable files may not have such an identifier.)
- **"App-class" software from the 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.
- **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.
- **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 Preferences** > **Security & Privacy** > **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:** (available with macOS Catalina or later only) 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.

- **Protected by application sandbox:** A **Yes** value confirms that the selected application is protected by the macOS Application Sandbox when the program is launched.

- **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. An 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.

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 tab 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.

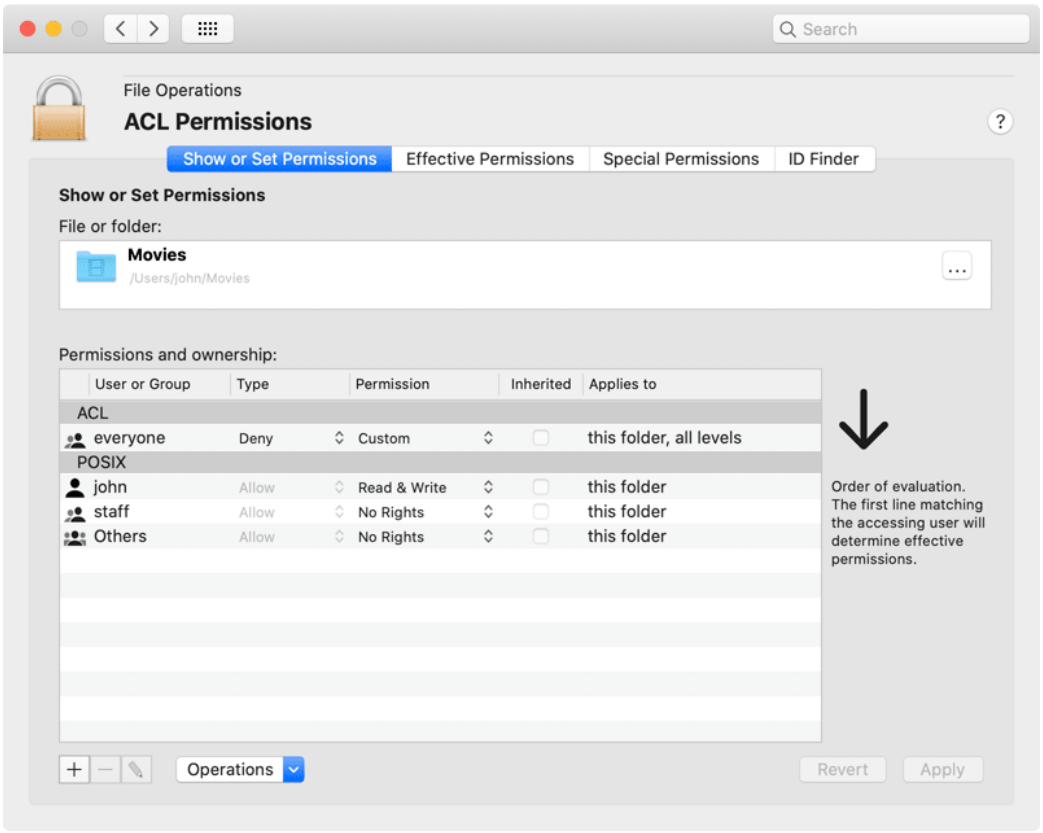


Figure 3.19: Show or set permissions

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.
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.

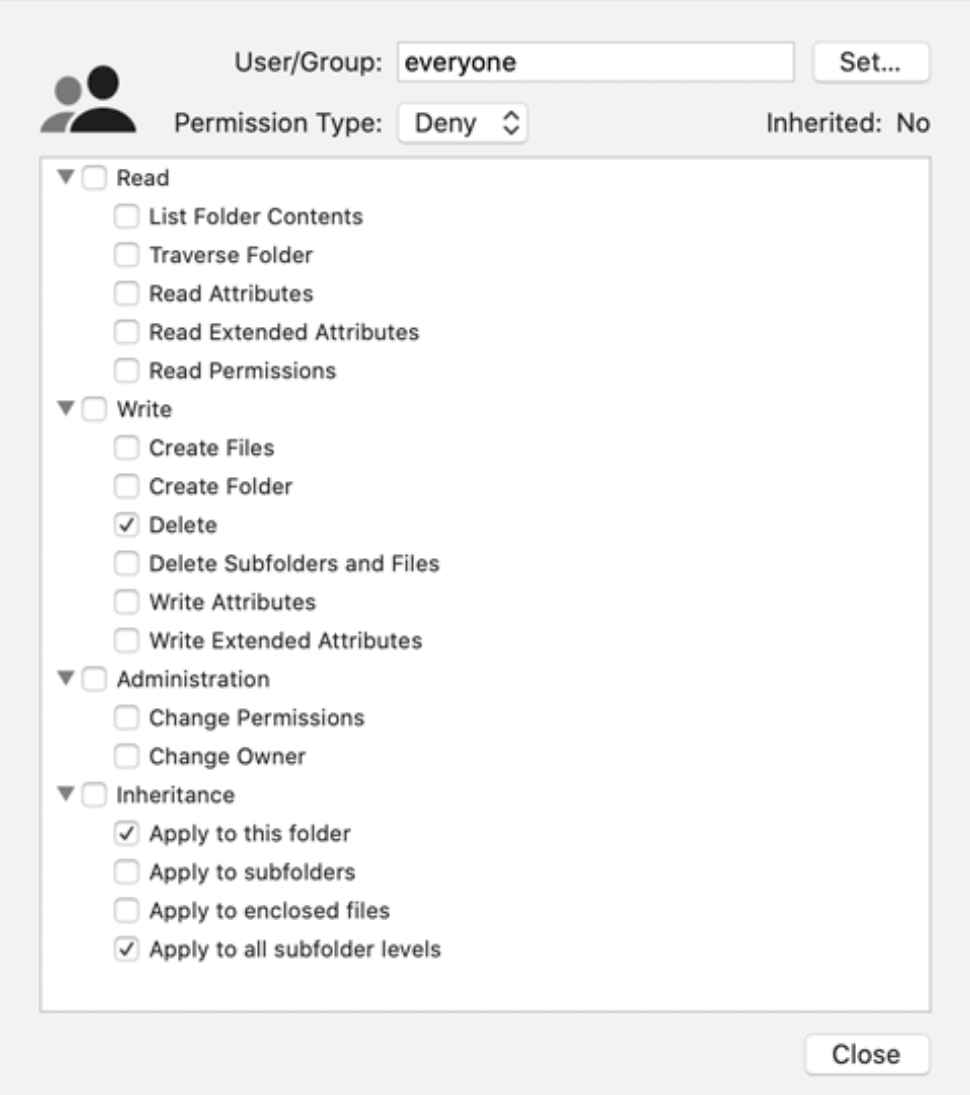


Figure 3.20: Set permission details

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 105).
>
> 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.

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 tab 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 tab item **Special 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. 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.

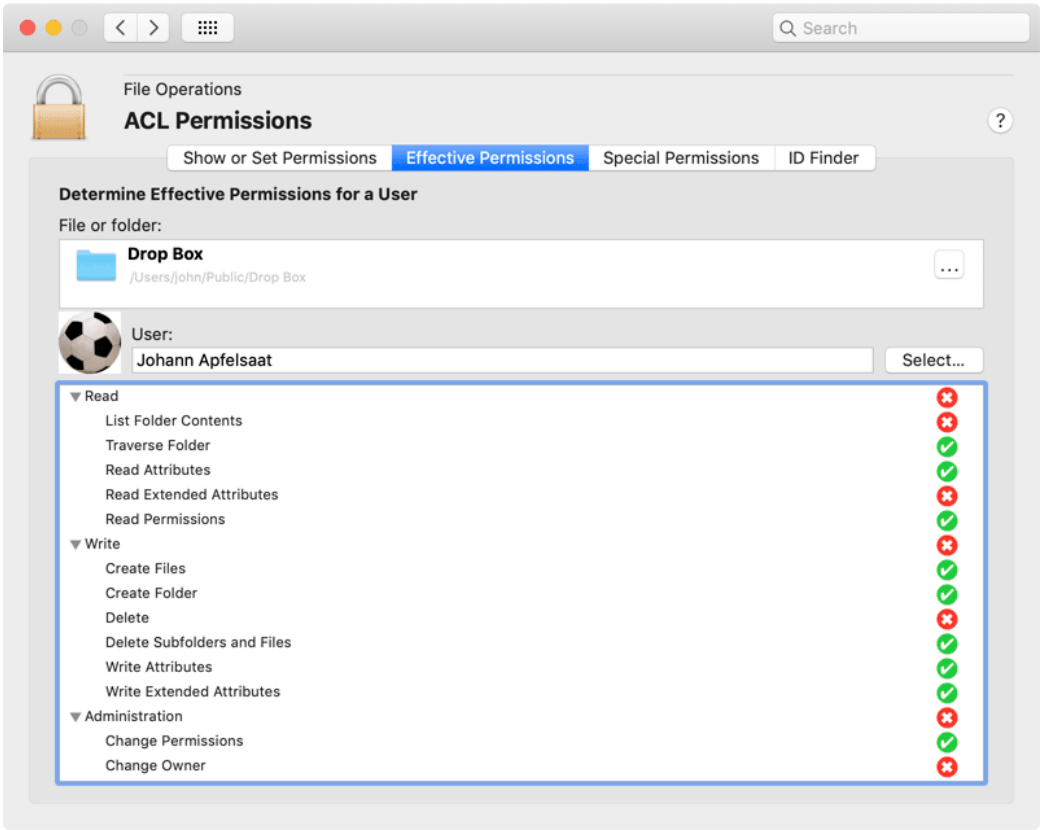


Figure 3.21: Effective permissions

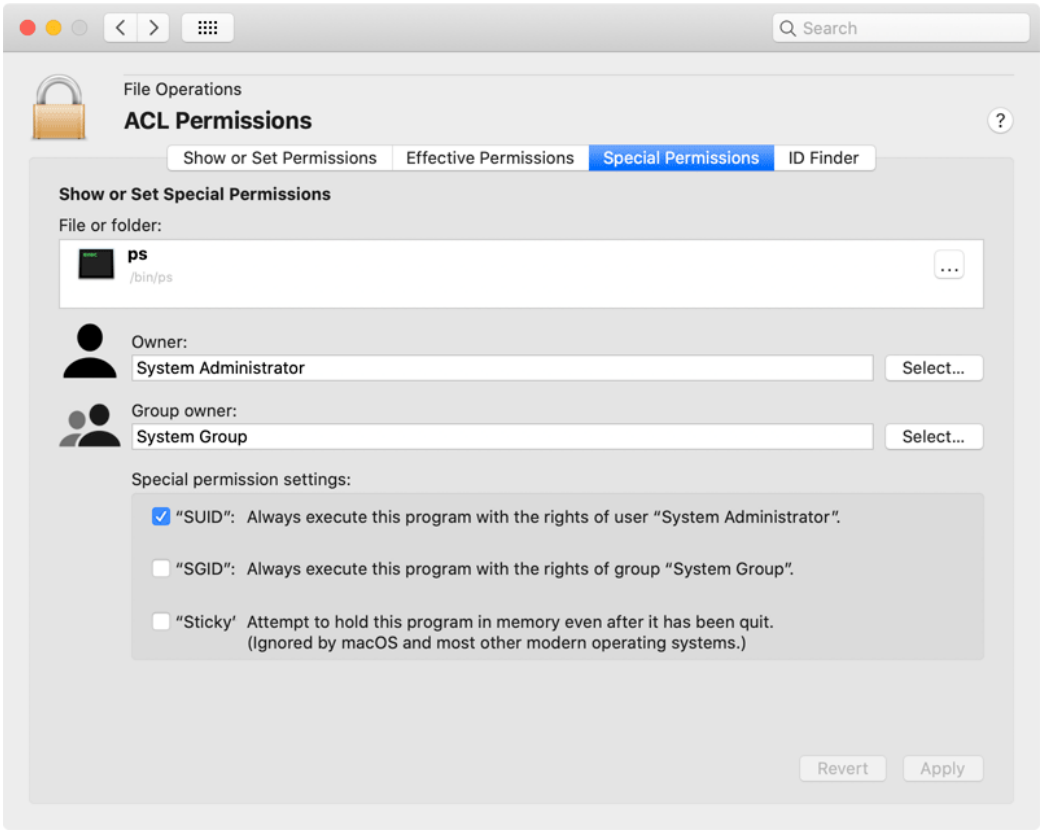


Figure 3.22: Special permissions

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 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*.

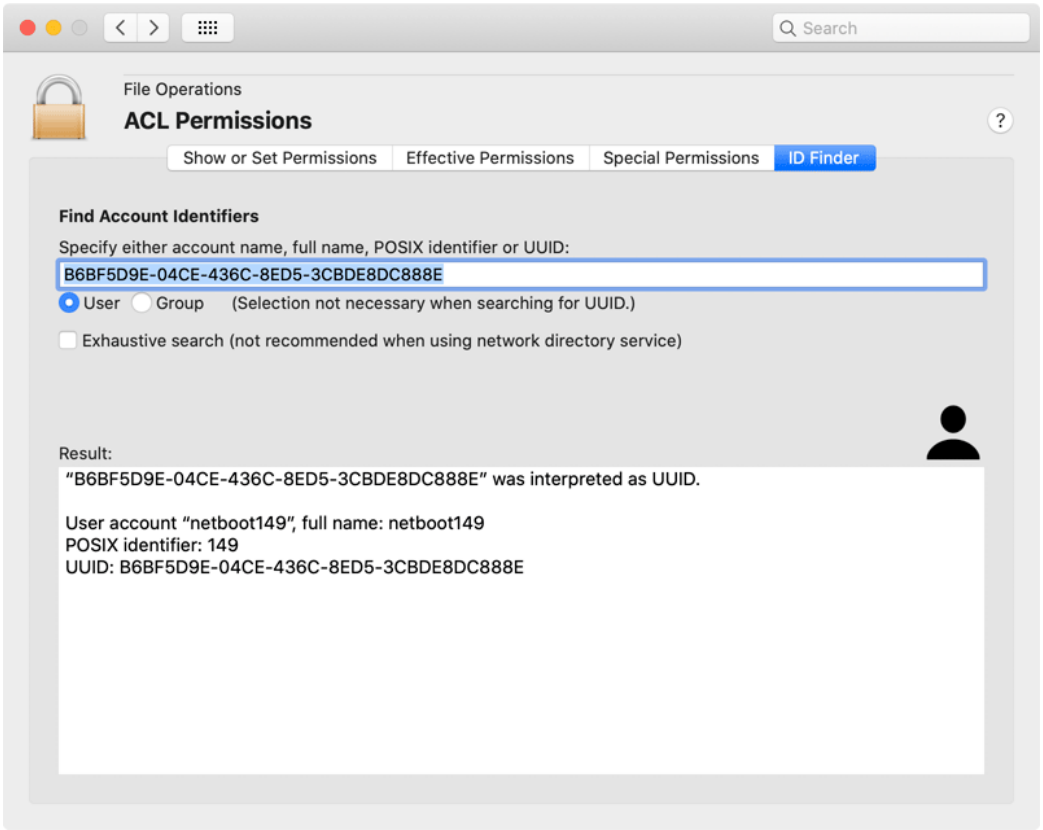


Figure 3.23: ID Finder

1. Open the tab 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.**

3.5 The Pane Operational Safety

3.5.1 Application Integrity

On the pane Applications (section 3.3 on page 131) 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.

1. Select the tab item **Application Integrity** of the pane **Operational Safety**.

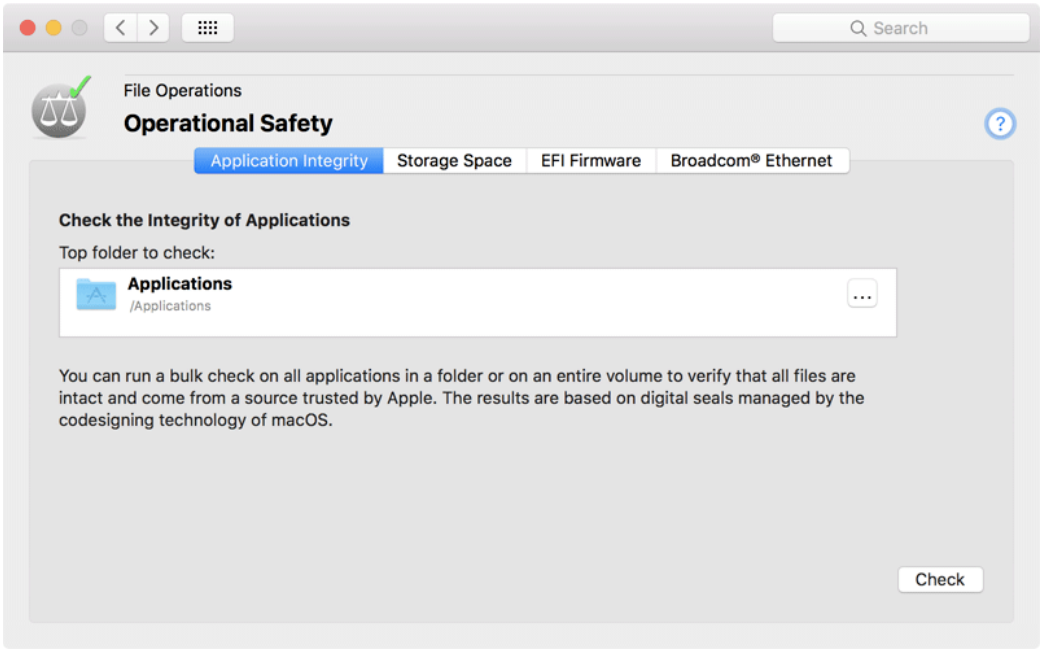


Figure 3.24: All applications of the system can be checked if necessary

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 131), 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.

3.5.2 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 7), 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. For further information, please see the chapter The pane Time Machine (section 2.3 on page 39).
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. (An 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.

TinkerTool System can show the different views on storage space supported by macOS for each volume:

1. Select the tab item **Storage Space** of the pane **Operational Safety**.
2. Choose the desired volume with the pop-up button **Volume**.

> On macOS Catalina or later, the system volume is internally split into a read-only system part, and a read/write data part. However, they 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 7), 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.

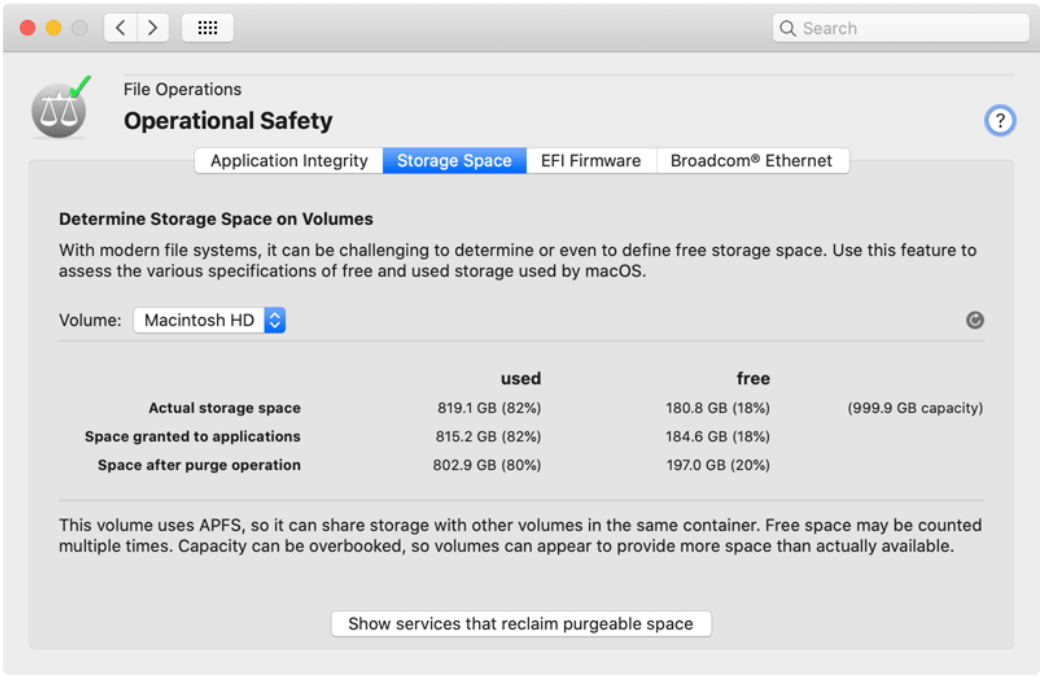


Figure 3.25: With modern operating systems, free storage space can have multiple definitions

- **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.

3.5.3 EFI Firmware

To start a computer and to load an operating system, an additional program, a kind of mini operating system, is needed that takes over this task. This program must be built into the computer and is therefore called *firmware*. This software is not so firmly anchored in the hardware however, otherwise it could not be updated and adapted to technical advancements itself. For this reason, it it stored in a special, electrically erasable memory, similar to flash memory. Apple updates the firmware in regular intervals without special notice, as subordinate task when updates of the "normal" operating system are installed as well.

The firmware is protected against manipulation by multiple measures. Nevertheless, with some criminal energy, it is possible to inject malicious programs even in the firmware, e.g. spy functions. This kind of attack on a computer is difficult to detect, because under normal circumstances the firmware is considered built-in and immutable.

For security reasons, Apple checks in regular intervals in their latest operating systems whether the firmware is still intact and unchanged. Block checksums of all firmware versions ever distributed for a respective Macintosh model are provided via Internet for this purpose, comparing it with checksums of the current firmware found. Such integrity checks are run in the background and only become noticeable if an anomaly has been found. An example warning is shown below.

TinkerTool System can initiate such a check manually, so it is possible to test and verify the integrity of the system firmware immediately. Perform the following steps:

1. Select the tab item **EFI Firmware** of the pane **Operational Safety**.
2. Click the button **Check**.

The test result will be shown in a user dialog and additionally in the window itself.

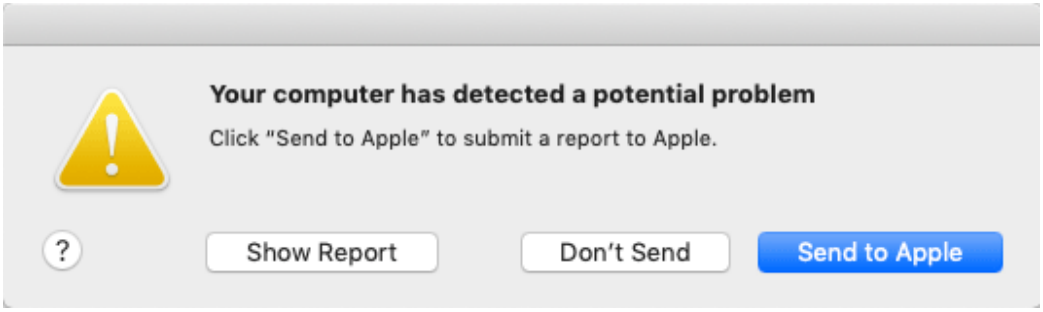


Figure 3.26: macOS runs regular integrity checks automatically. Possible problems are reported like this.

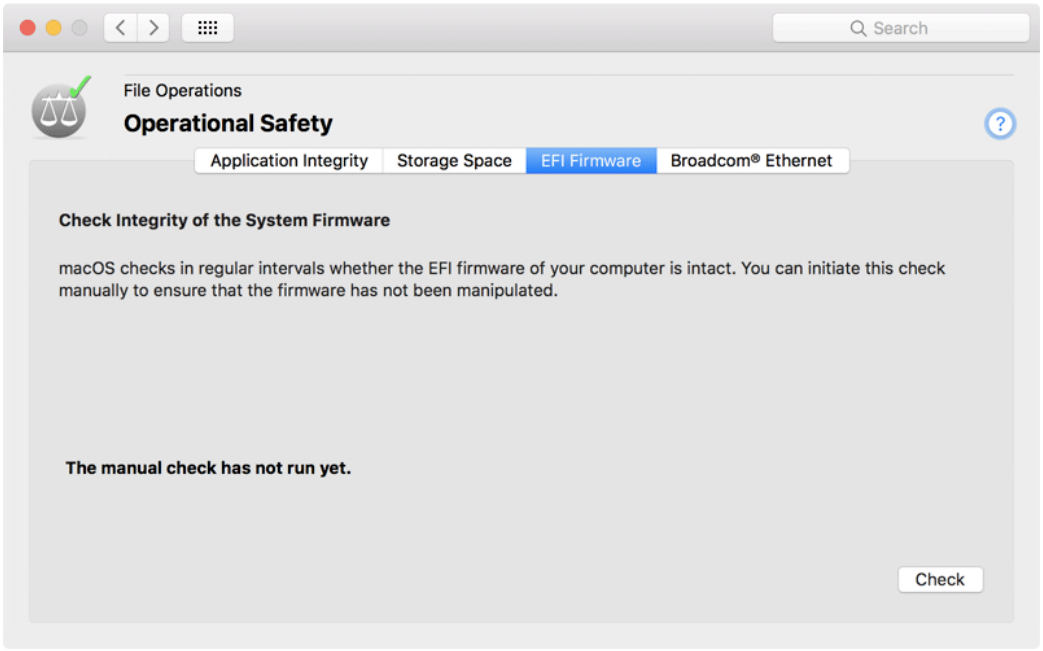


Figure 3.27: The integrity check for the firmware can be repeated immediately if necessary

Not all Macintosh model series support this type of firmware check. TinkerTool System will notify you in such a case. Especially the latest model series are affected where the computer is monitored and protected by an independent processor running its own operating system (Apple BridgeOS). On such a Mac, macOS cannot read the firmware any longer, and certainly cannot write it, so security is guaranteed by other means.

It can happen that Apple publishes a new version of macOS that installs a new firmware, but does *not* contain an up-to-date checksum for this firmware. *In this particular case, the integrity check will fail.* However, such a failure usually triggers an internal update of the checksum list via Internet, if the setting **System Preferences** > **Software Update** > **Advanced** > **Install system data files and security updates** is enabled, which is the default. So if you see an integrity warning shortly after a macOS update, repeat the integrity check after a few hours to verify whether this may have been a false alarm.

It can be normal to receive a false alarm if you are testing unreleased beta operating systems.

3.5.4 Broadcom® Ethernet

Ethernet ports made by the vendor Broadcom are characterized by the special feature that their firmware is also updatable in a relatively simple way. Monitoring this firmware is therefore security-critical as well.

TinkerTool System can check if one or more Ethernet ports made by Broadcom are built into your Mac, or attached externally. If yes, their firmware can also be tested for possible manipulations:

1. Select the tab item **Broadcom® Ethernet** of the pane **Operational Safety**.
2. Review the table whether affected Ethernet devices are present in your system. If yes, click the button **Check**.

The results of the check will be shown after a few seconds. If multiple ports are present, a number for each tested item in the report, the *PCI device ID*, is associated with each unit. You will find this number as back part in the column **PCI Device ID** in the table, allowing you to find the corresponding network interface.

macOS only checks Ethernet devices of the vendor Broadcom. Ethernet ports of other vendors are not tested, but usually have no vulnerable firmware either.

3.6 The Pane APFS

3.6.1 Overview on APFS Volumes

As explained in the previous chapter (section 3.5 on page 160), Apple's File System *APFS* uses modern techniques for storage organization that can be confusing upon first look.

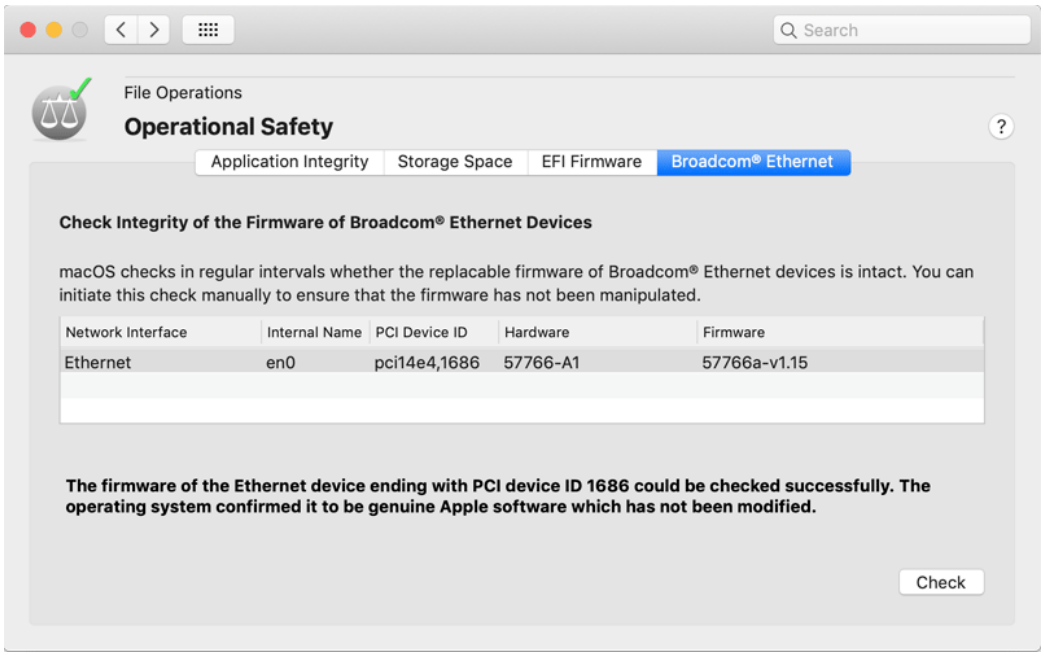


Figure 3.28: Integrity checks are also possible for Ethernet firmware provided by Broadcom

The tab 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 Type**, 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.

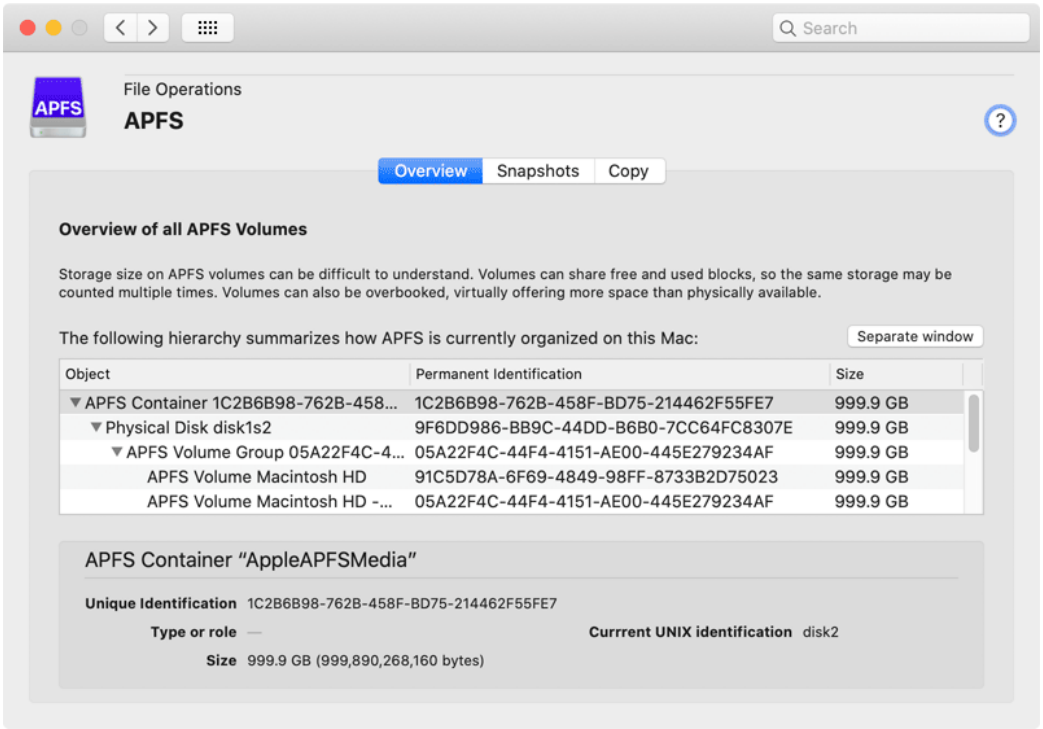
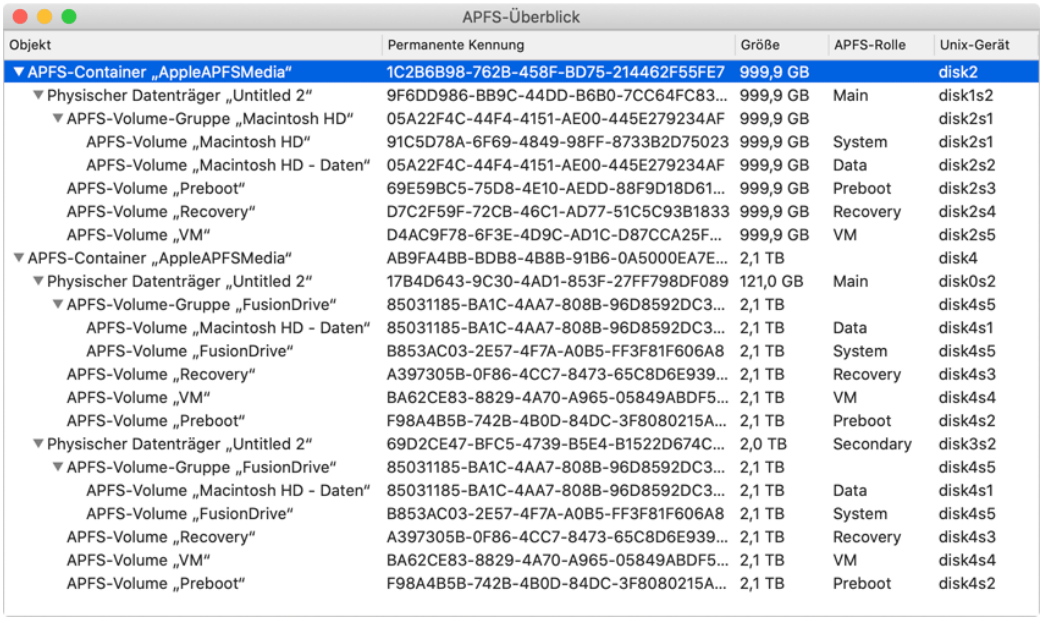


Figure 3.29: The relationship between the different APFS object can be visualized as hierarchy

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.

If you are working with multiple partitions or if multiple disks are connected to your Mac, the space in the table might not be sufficient to get a clear overview. To get a better view in this case, click the button **Separate window**. The APFS overview will then be

shown in a resizable window which can be extended to the whole screen if necessary. Keeping the overview window open can be especially helpful if you like to work with critical APFS operations, e.g. copying one disk to another one (see below).



Objekt	Permanente Kennung	Größe	APFS-Rolle	Unix-Gerät
▼APFS-Container „AppleAPFSMedia“	1C2B6B98-762B-458F-BD75-214462F55FE7	999,9 GB		disk2
▼Physischer Datenträger „Untitled 2“	9F6DD986-BB9C-44DD-B6B0-7CC64FC83...	999,9 GB	Main	disk1s2
▼APFS-Volume-Gruppe „Macintosh HD“	05A22F4C-44F4-4151-AE00-445E279234AF	999,9 GB		disk2s1
APFS-Volume „Macintosh HD“	91C5D78A-6F69-4849-98FF-8733B2D75023	999,9 GB	System	disk2s1
APFS-Volume „Macintosh HD - Daten“	05A22F4C-44F4-4151-AE00-445E279234AF	999,9 GB	Data	disk2s2
APFS-Volume „Preboot“	69E59BC5-75D8-4E10-AEDD-88F9D18D61...	999,9 GB	Preboot	disk2s3
APFS-Volume „Recovery“	D7C2F59F-72CB-46C1-AD77-51C5C93B1833	999,9 GB	Recovery	disk2s4
APFS-Volume „VM“	D4AC9F78-6F3E-4D9C-AD1C-D87CCA25F...	999,9 GB	VM	disk2s5
▼APFS-Container „AppleAPFSMedia“	AB9FA4BB-BDB8-4B8B-91B6-0A5000EA7E...	2,1 TB		disk4
▼Physischer Datenträger „Untitled 2“	17B4D643-9C30-4AD1-853F-27FF798DF089	121,0 GB	Main	disk0s2
▼APFS-Volume-Gruppe „FusionDrive“	85031185-BA1C-4AA7-808B-96D8592DC3...	2,1 TB		disk4s5
APFS-Volume „Macintosh HD - Daten“	85031185-BA1C-4AA7-808B-96D8592DC3...	2,1 TB	Data	disk4s1
APFS-Volume „FusionDrive“	B853AC03-2E57-4F7A-A0B5-FF3F81F606A8	2,1 TB	System	disk4s5
APFS-Volume „Recovery“	A397305B-0F86-4CC7-8473-65C8D6E939...	2,1 TB	Recovery	disk4s3
APFS-Volume „VM“	BA62CE83-8829-4A70-A965-05849ABDF5...	2,1 TB	VM	disk4s4
APFS-Volume „Preboot“	F98A4B5B-742B-4B0D-84DC-3F8080215A...	2,1 TB	Preboot	disk4s2
▼Physischer Datenträger „Untitled 2“	69D2CE47-BFC5-4739-B5E4-B1522D674C...	2,0 TB	Secondary	disk3s2
▼APFS-Volume-Gruppe „FusionDrive“	85031185-BA1C-4AA7-808B-96D8592DC3...	2,1 TB		disk4s5
APFS-Volume „Macintosh HD - Daten“	85031185-BA1C-4AA7-808B-96D8592DC3...	2,1 TB	Data	disk4s1
APFS-Volume „FusionDrive“	B853AC03-2E57-4F7A-A0B5-FF3F81F606A8	2,1 TB	System	disk4s5
APFS-Volume „Recovery“	A397305B-0F86-4CC7-8473-65C8D6E939...	2,1 TB	Recovery	disk4s3
APFS-Volume „VM“	BA62CE83-8829-4A70-A965-05849ABDF5...	2,1 TB	VM	disk4s4
APFS-Volume „Preboot“	F98A4B5B-742B-4B0D-84DC-3F8080215A...	2,1 TB	Preboot	disk4s2

Figure 3.30: The APFS table can be shown in a separate window to get a clearer overview.

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
- **User:** personal home folders of users
- **Recovery:** mini operating system for recovery
- **VM:** swap space as part of the virtual memory management
- **Preboot:** components to launch the operating system from encrypted volumes (e.g. the user interface of FileVault)
- **Installer:** temporary storage of data that is needed during the installation of the operating system

- **Data:** all mutable data of users and 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
- **Prelogin:** a volume that holds the mini operating system used by FileVault to control user logins before the actual (encrypted) operating system is started
- **Reserved:** reserved for future types of use.

3.6.2 Working with APFS Snapshots

The purpose of snapshots has been discussed in detail in the chapter for the pane Time Machine (section 2.3 on page 39) 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 tab item **Snapshots** on the pane **APFS** gives you the opportunity to work with *all* snapshots, not only the ones in use by Time Machine.

> In up-to-date versions of macOS 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. *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 tab item **Snapshots** on the pane **APFS**.
2. Choose the desired volume with the pop-up button **Select APFS volume:**.

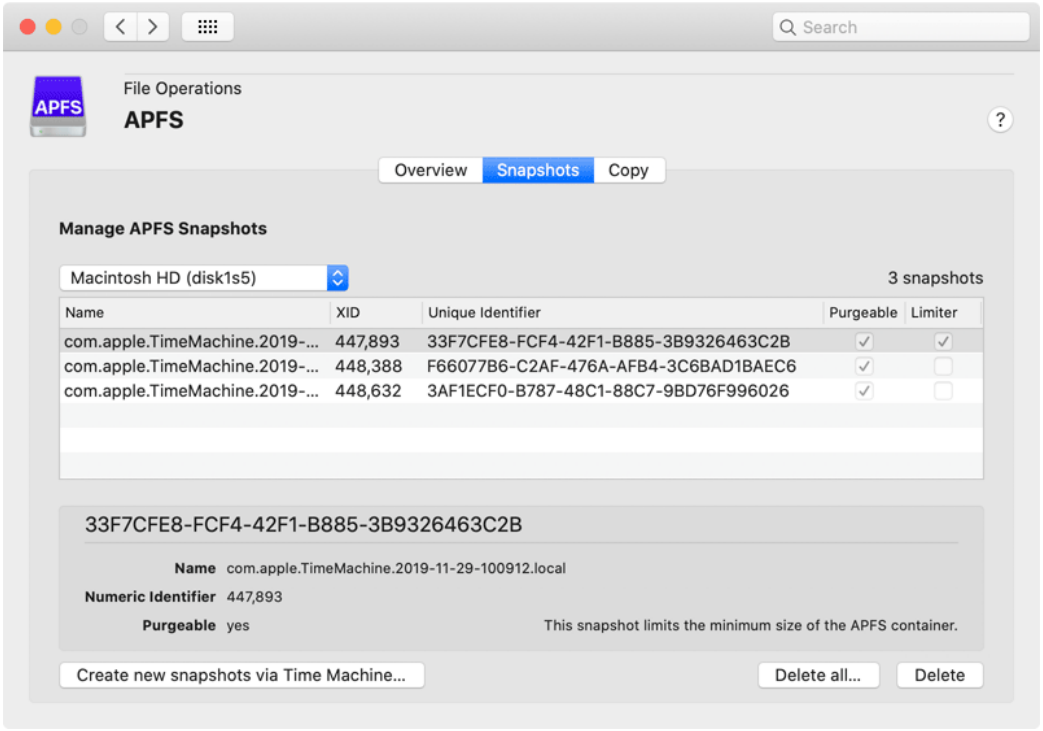


Figure 3.31: APFS snapshots can be listed and deleted

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 **purgeable** indicates whether this snapshot is designed to be automatically deleted by macOS in case of insufficient storage space. 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.

> Older versions of macOS don't provide a UUID for APFS snapshots. You can only use the XID on such systems.

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.

3.6.3 Copying APFS Data (macOS Catalina or later only)

> This feature is not available in macOS 10.14 Mojave.

As of macOS 10.15, Apple offers new 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.

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.

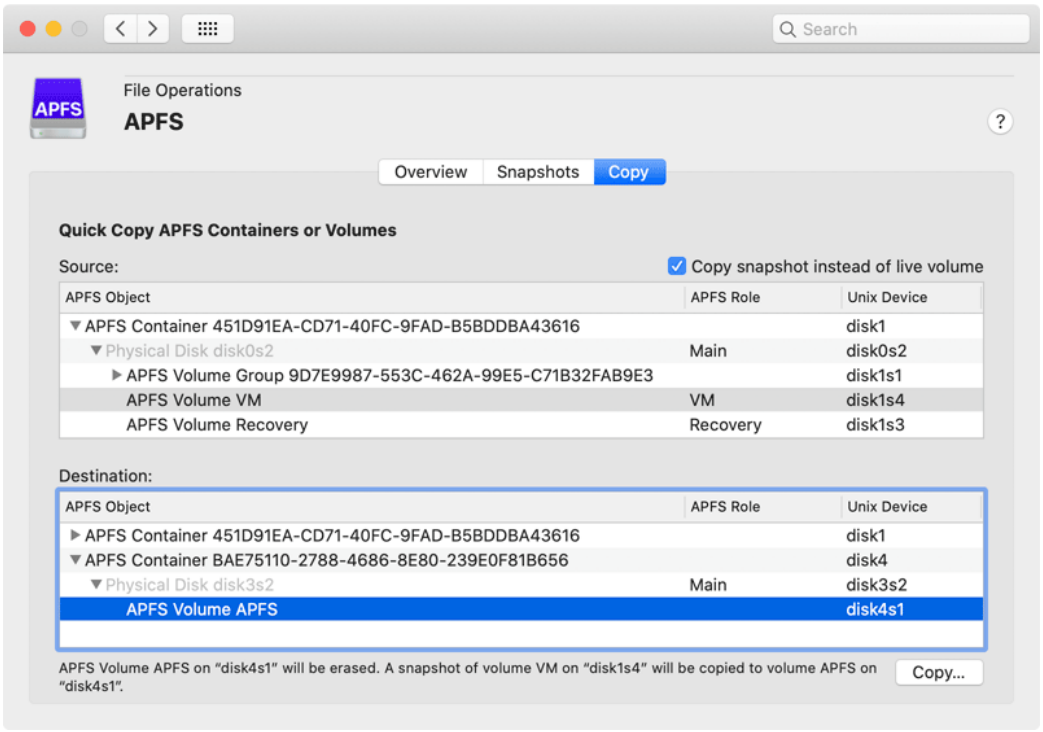


Figure 3.32: As of macOS Catalina, APFS objects can be copied quickly

Perform the following steps to copy an APFS object:

1. Open the tab item **Snapshots** 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 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 **Energy Saver** > **Put hard disks to sleep when possible** in the **System Preferences** 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 tab 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

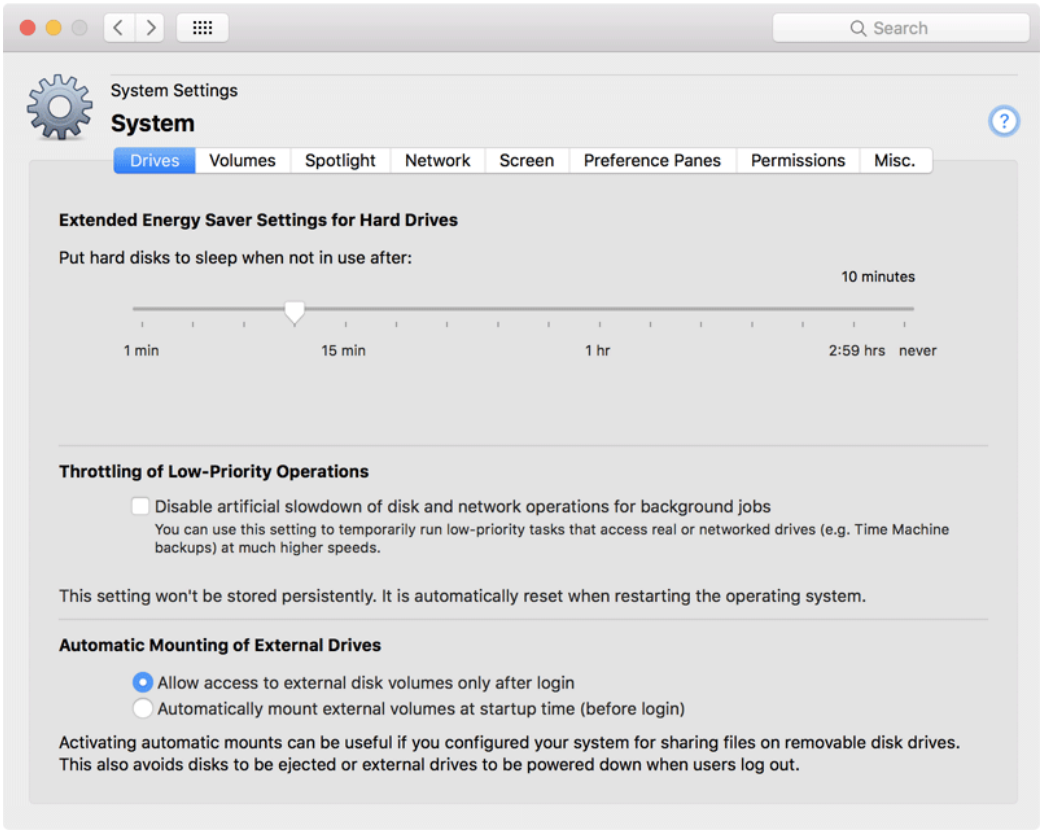


Figure 4.1: Drives

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 tab item **Drives** on the pane **System**.
2. Set a check mark at **Disable artificial slowdown of disk and network operations 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.

Disk Mounting without User Session (macOS Mojave only)

> This feature is not available in macOS Catalina or later. Disk volumes are mounted during startup by default.

macOS uses the policy to handle external hard drives like removable disk media. Similar to the management of a CD, which is inserted into a drive by the current interactive user, the user logged in at the front graphical user session is also considered the "owner" of all external disk drives. This has the consequence that the external drives will be ejected and become inaccessible after the user has logged out. Moreover, most drives will automatically power down in this situation.

This policy might not be useful in certain cases, for example when you operate the computer as a file server, and you are sharing files on external disks which should remain accessible, no matter if a user is logged in at the graphical console or not. To change this policy, perform the following steps:

1. Open the tab item **Drives** on the pane **System**.
2. Click on one of the two possible options at **Automatic Mounting of External Drives**.

This option affects all partitions on all hard drives which macOS considers to be "external" and owned by a user.

4.1.2 Volumes

macOS follows the strategy to automatically detect all disk drives and all their partitions 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 partition in reserve on a secondary disk drive. With the help of TinkerTool System, you can tell macOS not to activate specific partitions 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, the corresponding volumes will be mounted, because this is a manual activation of this disk.

A second, independent option allows you to choose whether the system should allow the execution of programs which are stored on specific partitions. 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.

In both cases, macOS must have a way of reliably referring to each drive and partition. 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 partition 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.

Perform the following steps when you like to exclude certain disk volumes from automatic mounting or execution of programs:

1. Open the tab item **Volumes** on the pane **System**.
2. Click the **[+]** button below the table which refers to the option you like to activate.
3. In the dialog sheet, select one or more disk volumes and click **OK**.
4. After all volumes have been set as intended, click the button **Apply** in the lower right corner of the window.

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.

After adding new volumes to the **Exclude volumes from automatic mounting** table, TinkerTool System will ask you whether you like to eject the affected volumes immediately when applying the changes.

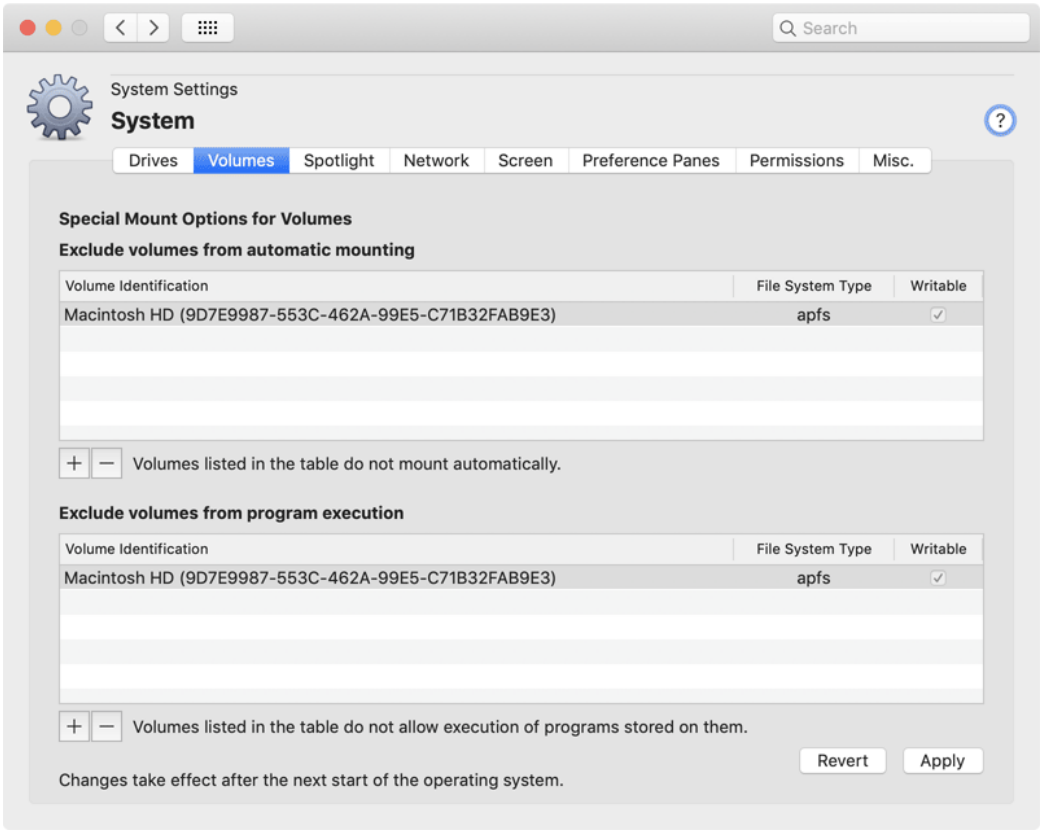


Figure 4.2: Volumes

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.

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, 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 one or multiple lines in the table, you can activate several operations that should be performed:

- You can **delete** the metadata store on the selected volume(s). This will reset the privacy preferences 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.

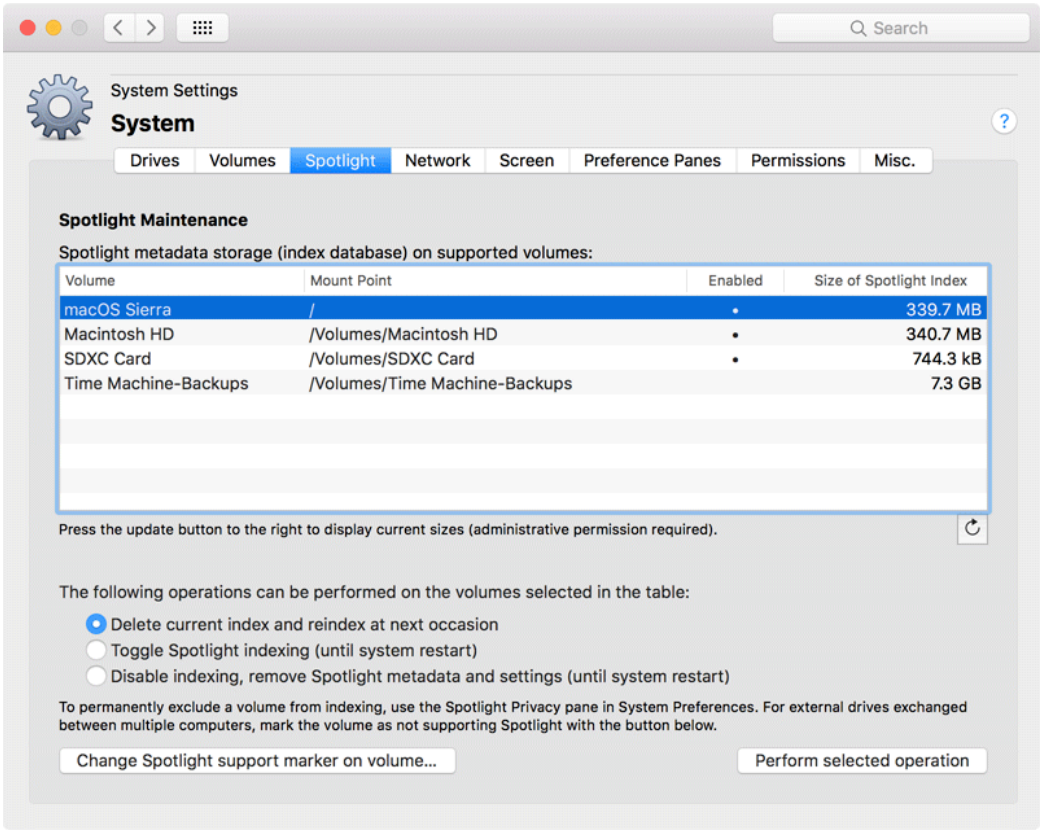


Figure 4.3: Spotlight

- 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(s) 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 **Spotlight** > **Privacy** in **System Preferences**, macOS will recommence its indexing services upon next startup.

Under specific circumstances, it might be helpful to disable Spotlight operations on a disk volume "forever," e.g. on a slow memory stick 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 tab item **Spotlight** on the pane **System**.
2. Click the button **Change Spotlight support marker on volume**... in the lower left corner of the window.
3. In the dialog panel, set or remove the check marks **Blocked from all Spotlight operations** for each of the volumes as desired.
4. Click the button **OK** in the panel.

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 tab item **Network** on the pane **System**.
2. Choose the desired option at **Suggested name in panel**.

Outdated authentication methods

Apple has deprecated the use of certain outdated authentication methods, which are considered unsafe according to today's standards when connecting to AFP servers. The operating system won't offer the affected authentication methods when contacting a server. This can however mean that you can no longer connect to old servers successfully. TinkerTool System allows you to unlock certain methods so that they can be used again. Perform the following steps:

1. Open the tab item **Network** on the pane **System**.
2. Set check marks for all desired options at **Allow outdated authentication methods**.

The following methods can be reactivated:

- Two-way random number exchange
- Diffie-Hellman Key Exchange, implemented with the CBC128 procedure (Carlisle Adams /Stafford Tavares encryption with 128 bits in Cipher Block Chaining mode)
- Password transfer in the clear
- Encryption method version 2 of "Microsoft® Services für Macintosh"

> Because all these methods are insecure and outdated and use of AFP technology is deprecated, you should only enable as few options as possible in order not to compromise the security of your network.

Support for Captive Networks (WiFi HotSpots)

> With macOS Catalina or later, this setting has become a visible part of the operating system. You'll find the function on the Network pane of System Preferences for each WiFi interface.

If your computer has access to an unprotected wireless network at the moment, which doesn't appear to be connected to the Internet however, macOS assumes that you are in vicinity of a WiFi Hotspot. Such hotspots are often implemented by a so-called *Captive Network:* Unless you haven't accepted the local Terms and Conditions for Internet use yet, which can sometimes require an additional login as well, all access attempts to HTTP services ("web pages") are captured and are redirected to a specific web page with the Terms of Service. In order to prevent that access to other Internet services, e.g. email, won't fail, macOS tries to detect such a situation, starting the assistent for Captive Networks as early as possible to make you aware of the hotspot by respective messages before applications begin to use further Internet services.

If you don't like this, e.g. if you often use an open WiFi network to access some local files without requiring the Internet, or if macOS experiences technical problems with the detection of a particular hotspot, you can disable Apple's guidance for such networks:

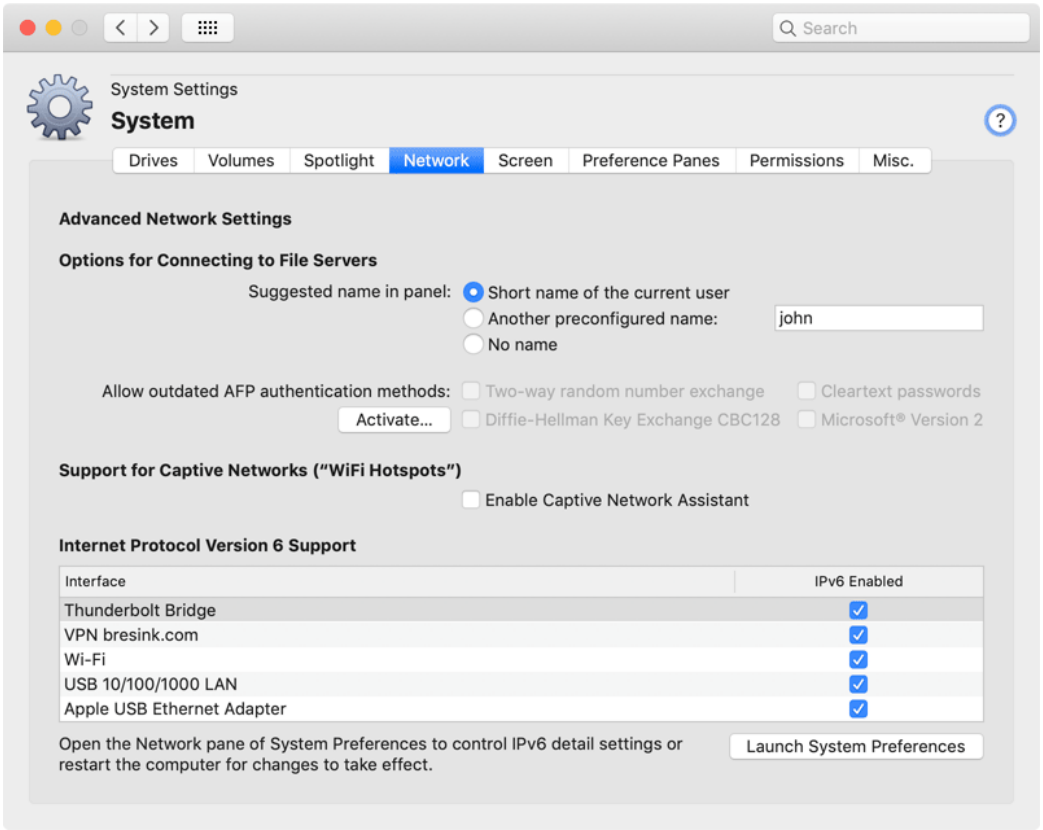


Figure 4.4: Network

1. Open the tab item **Network** on the pane **System**.
2. Remove the check mark at **Enable Captive Network Assistant**.

Internet Protocol Version 6 Support

By default, the pane **Network** of the application **System Preferences** 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. In case your computer is configured to support multiple network configuration sets (called **Location** by macOS), ensure first that the desired location is currently active, selecting it with the pop-up button on the pane **Network** of **System Preferences**. If you never used that feature, your default location is **Automatic**.
2. Open the tab item **Network** on the pane **System** of TinkerTool System.
3. Locate the network service you like to modify in the table **Internet Protocol Version 6 Support**.
4. 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 Preferences will correctly reflect this, adding an **Off** menu item to the **Configure IPv6** option. You can either use System Preferences 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 Preferences.

> If you change your network location or the IPv6 mode in **System Preferences** while TinkerTool System is running, it is recommended to restart TinkerTool System to ensure that the application shows the updated status.

4.1.5 Screen (macOS Mojave only)

> Apple no longer supports this feature as of macOS 10.15 or later.

By default, macOS assumes that the display screen is rendering graphics with a physical resolution of 72 pixels per inch. This policy was taken over from the classic Mac OS. While this basic assumption was true when the Macintosh was introduced 30 years ago, today's display devices often have a much higher resolution. The pixels have become smaller, so your screen may actually use more than 140 pixels per inch. This is particularly the case when you are using a MacBook with a *Retina display* or an iMac with a *5k* screen. The operating system offers a feature named **HiDPI** (High Number of Dots per Inch) which

allows it to double the physical resolution on demand. This means the components creating the graphical output can select between the two resolutions 72 ppi (“low”) and 144 ppi (“high”). When your computer is connected to a Retina screen, HiDPI mode will be enabled automatically.

You can unlock HiDPI for your operating system independent of the monitor currently connected. For example, as a software developer you can use this feature to test applications in Retina mode although you don’t own a Retina screen.

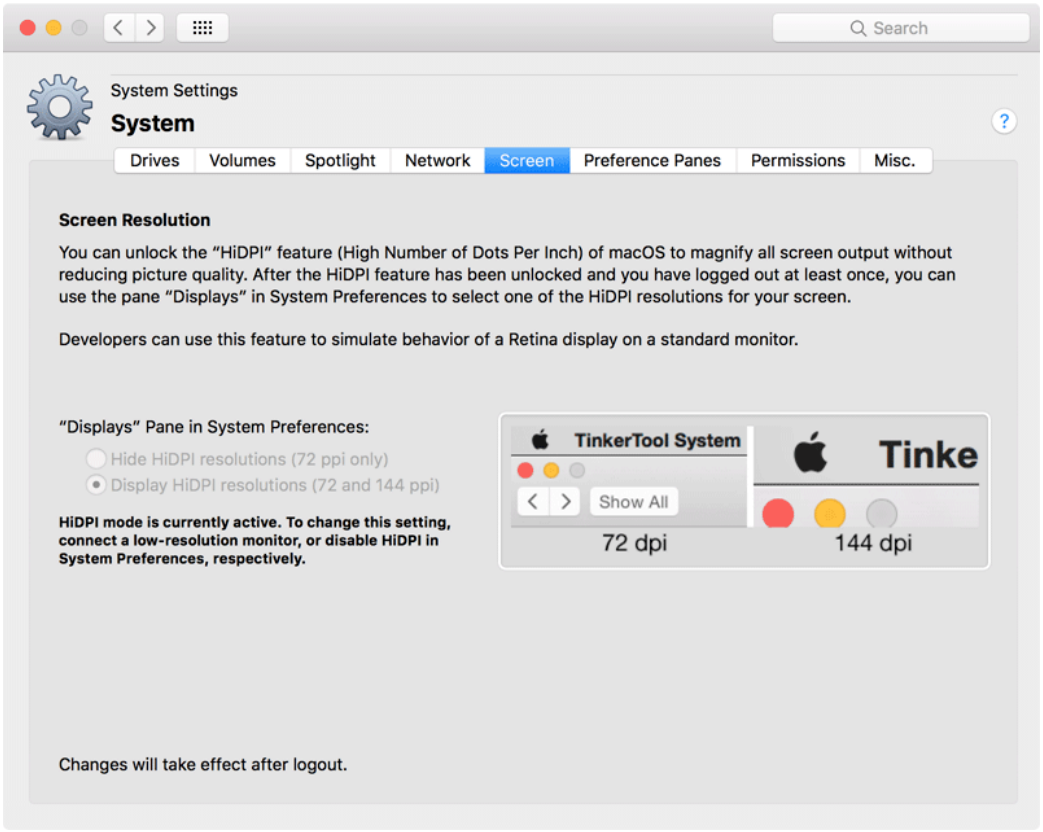


Figure 4.5: Screen

Enabling the HiDPI feature requires two steps: The first step is to unlock HiDPI mode via TinkerTool System. The second step is to select one of the HiDPI display resolutions on the pane **Displays** of **System Preferences.** Perform the following steps to work with HiDPI display modes:

1. Select the item **Screen** on the pane **System**.

2. Switch between the two possible modes **Hide HiDPI resolutions** and **Display HiDPI resolutions**.

3. Log out to let the change take effect.

When you log in again, you can launch **System Preferences**, go to **Displays**, set the **Resolution** to **Scaled** and choose one of the HiDPI settings shown in the table. Note that the table lists the *effective* pixels, not the physical pixels. Because Retina mode combines 4 physical pixels to one virtual pixel, the values are halved in each dimension. A display screen with 2400 x 1600 pixels would be shown as HiDPI resolution with 1200 x 800 pixels, for example.

macOS will switch to the new setting, enabling the actual HiDPI mode. The whole screen contents will immediately be magnified. However, currently running applications might not switch to the new resolution with full output quality at the same time. *You must log out and log in once again to ensure that you are actually getting the correct resolution and full picture quality in all applications.*

Warning: The display resolution is a very critical setting. If you set the resolution too high, the windows can become so large that they no longer fit on screen. This means you can no longer see or control all parts of some applications which can make your system unusable!

To use the system with 144 ppi, a screen with at least 2048 x 1536 pixels is strongly recommended, because macOS applications are designed by the rule that they can expect windows to have a minimum size of 1024 x 768 pixels at 72 ppi.

4.1.6 Preference Panes

The application System Preferences is designed to support a plug-in architecture: The different control areas, called *Preference Panes*, are automatically activated and deactivated depending on what type of computer you are using. For example, the pane **Trackpad** will only appear on computers having a trackpad, the item **Ink** will only be displayed if a graphic tablet or a similar device with pen support is attached to the computer.

System Preferences also supports an additional section that contains optional panes installed by the user. It will be displayed as fifth category, at the bottom of the window. TinkerTool System can help you to manage this section: It can activate additional preference panes which are part of macOS, but are reserved for advanced users and are normally hidden. It can also assist you in removing optional preferences panes you no longer need.

The following additional pane can be activated:

- A pane to control preference settings for the **macOS Archive Utility**. This utility is the helper program which is automatically activated when you open an archived or compressed file, for example a ZIP archive.

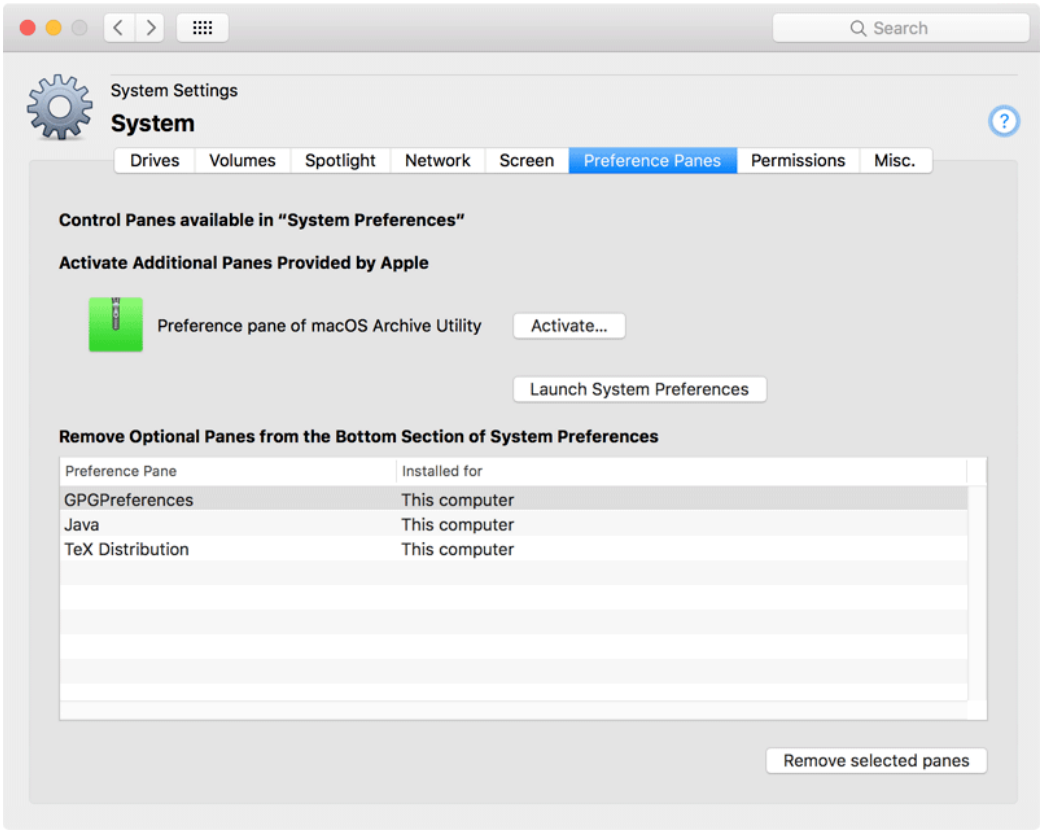


Figure 4.6: Preference panes

> Apple is providing additional panes as part of macOS. Their features may vary depending on OS version, and they may be changed without notice. The optical quality of the panes may not comply with the usual design standards.

To activate one of the hidden panes, perform the following steps:

1. Open the tab item **Preference Panes** on the pane **System**.
2. Click one of the buttons **Activate**... next to the listed preference panes.

You can start System Preferences directly from here to use the new panes immediately. Click the button **Launch System Preferences**.

Removing optional preference panes

The panes listed in the previous section and panes of other vendors which appear in the bottom line of System Preferences can be removed when you no longer need them. It is not necessary to know where the different vendors have installed the modules. Perform the following steps:

1. Open the tab item **Preference Panes** on the pane **System**.
2. Select one or more items in the table **Remove Optional Panes from the Bottom Section**.
3. Click the button **Remove selected panes**.

4.1.7 Permission Filter for New File System Objects

In the permission system of macOS, which is explained in detail in the chapter The Pane ACL Permissions (section 3.4 on page 143), 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 143) for details.

By default, macOS uses a permission filter which is preconfigured with the following policy:

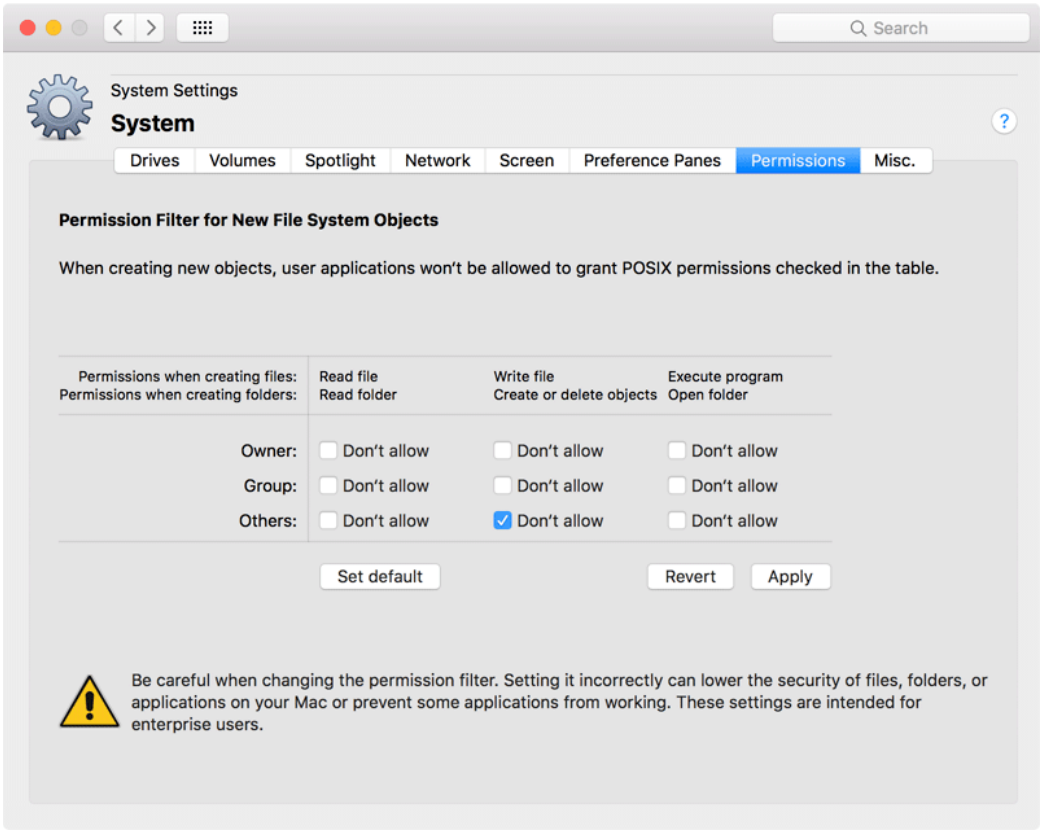


Figure 4.7: Permission Filter

- don't allow applications to grant initial write permission for the group owner of a new object
- 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 tab 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 at its left side. 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.

4.1.8 Miscellaneous

Private Software Update Server

macOS contains an automatic software update service which is designed to contact Apple in regular time intervals, checking whether updates for the operating system are available. This service is configured with the pane **Software Updates** of **System Preferences**.

It is possible to setup your own software distribution server which mirrors the software distributions and update information from Apple. This can be done by a feature which was available in old versions of the App *macOS Server*, or by using other third-party utilities which mimic the behavior of Apple's update servers. To redirect computers in your own network to contact your own update server instead of Apple's, a special system setting must be modified on each affected computer. This can be done automatically when you are using the **Profile Manager** of macOS Server but you can also configure this manually on each client. To change the setting via TinkerTool System, perform the following steps:

1. Open the tab item **Misc.** on the pane **System**.
2. Enter the IP address or the name of the custom update server into the field **Server**.
3. Enter the port number the update server is using into the field **Port Number**.
4. Press the return key ↵.

The change will take effect immediately, and the next time an automatic software update is started, the new server will be contacted. You can remove the customized setting by clicking the button **Remove Customization**.

Control the Security Policy for Remote Apple Events (macOS Catalina or later only)

macOS 10.15 (or later) follows stricter security guidelines as earlier operating system versions regarding the use of AppleScript and the associated Apple Events over a remote network connection. An Apple Event that targets an application on a remote system must authenticate as the same user on the remote system. If it doesn't do so, the sending application will receive a *procNotFound* error. If you like to relax this rule, using the less secure policy of older operating systems, perform the following steps on the computer that receives remote Apple Events:

1. Open the tab item **Misc.** on the pane **System**.
2. Remove the check mark at **Require matching user account on clients to access the current login session**.

The new setting does not take effect immediately. To enforce an update, either restart the computer, or toggle the **Remote Apple Events** setting in the **Sharing** pane of **System Preferences** twice.

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 tab item **Misc.** on the pane **System**.
2. Click on the item **Permit clients to take over frontmost screen session immediately**.

> You should check if this policy is compliant with local laws and the guidelines of your company, if applicable.

FileVault 2

If you enabled the modern version of FileVault (officially called *FileVault 2*) 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 recovery partition 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 partition 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 tab item **Misc.** on the pane **System**.
2. Click on the item **Use separate logins for disk decryption and first user session**.

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

Figure 4.8: Miscellaneous System Settings (Catalina version)

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 tab item **Misc.** 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.

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. The settings controlled by the pane are not available on other computer types.

4.2.1 Automatic Power-On

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.

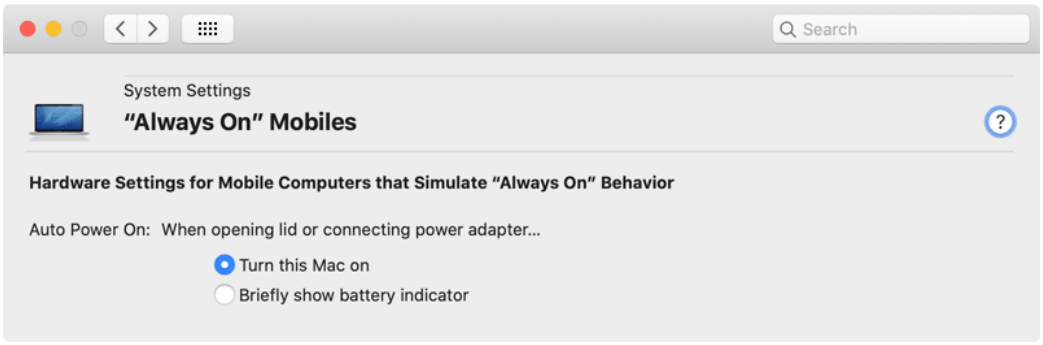


Figure 4.9: Settings for the automatic power-on feature

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 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.

4.3.1 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.

By setting a check mark at **Enable classic startup chime** you can force the Mac to play a check tone upon each start which confirms that the base components of the computers are working fine. Using a startup sound was common on Macintosh models built between 1988 and 2016. As of summer 2016, this feature was discontinued for all subsequently published Macs, because many users felt bothered by the loud sound which was undesired for many environments, e.g. working in libraries. However, the sound can be helpful for maintenance and diagnostic purposes, indicating when exactly the system self-test has been completed and the startup of the operating system will begin.

> We cannot guarantee that the startup chime is available on all newer Macintosh models. Apple can remove this feature any time without further notice by a firmware update in the background.

> The startup chime will be played with the volume setting that was active the last time the Mac was shut down.

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 Mac woken by network request or mobile device**.

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 applications 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 with macOS Server**. After restarting the computer, the kernel and some features of macOS Server will respect the new setting.

> Apple may change the exact meaning of this setting any time without further notice. With the latest versions of macOS, it can make sense to enable this setting when you like to use server features even if you don't have macOS Server installed. Nearly

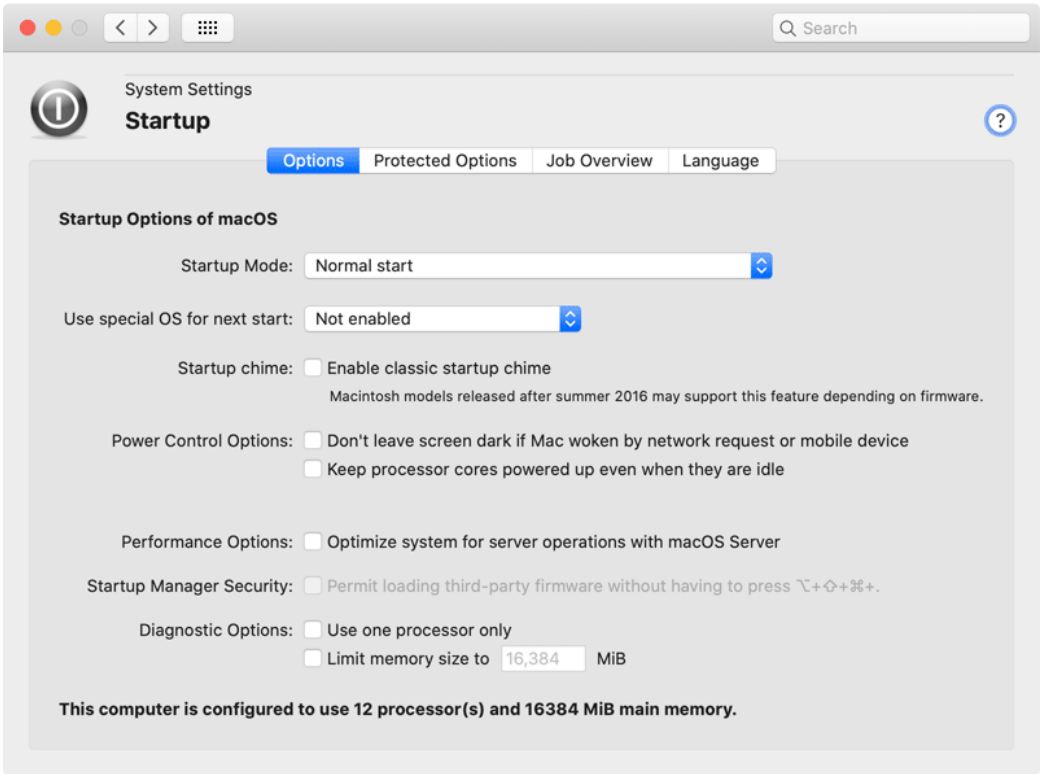


Figure 4.10: Startup options

> all server features have moved from the previous server App to the base operating system.

Startup Manager Security

You can attach additional hard drives to your Mac. If the physical interface used to attach such a drive is supported by the Mac's firmware, the drive can also be used to hold the operating system so that the Mac can start from that drive. In cases where you are using third-party disk interfaces to attach an additional drive, it might not always be possible to perform such a startup successfully, because the Mac's firmware might not support this. It may not "know" how to control the foreign interface at early startup time, when the actual operating system is not running yet.

Vendors of third-party disk interfaces can provide an "option ROM," an addendum to the firmware, to resolve this problem. However, the programs contained in that additional firmware run directly on the hardware. They cannot be monitored or restricted by the operating system, because macOS is not running at that moment yet. This could be a security risk, because an attacker could abuse this unrestricted mode of operation to steal confidential data (like the FileVault password) by connecting a deceptive hardware device. You must trust all option ROMs connected to your computer, hoping they only provide intended features.

To confirm that you trust the currently attached option ROMs of third-party vendors in order to start an operating system at the Mac's boot menu (also called *Startup Manager* or *Boot Picker*), users can press the key combination ⌥+⇧+⌘+.

> This feature is only available on Macintosh systems released by Apple before May 2015. The security policy of later systems no longer allows to disable this Startup Manager function.

If you are using such an older Mac, you can alternatively activate a hardware setting to automatically permit option ROMs, avoiding the key combination at each startup. To do this, enable the option **Permit loading third-party firmware without having to press** ⌥+⇧+⌘+.

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 tab item **Options** of the pane **Startup**.
2. Activate or deactivate the listed options as desired.

4.3.2 Protected Options

Kernel Settings

The advanced kernel settings of macOS can only be changed if *System Integrity Protection* (section 1.3 on page 7) has been disabled for your computer:

- **Use non-maskable interrupt (NMI) to let the kernel wait for remote debugger connection:** Very old Macintosh models had a special button at their front panels, known as *programmer's switch*. Pressing this button caused those Macs to generate an *NMI signal (Non-Maskable Interrupt)* which could activate certain diagnostic or debugger features sometimes needed by software developers. Up-to-date Macintosh systems no longer have such a switch. However, the computer can still be instructed to generate an NMI signal. If you enable the NMI feature, macOS will halt the machine and switch to kernel debugging mode when such a signal is received. You can then use Apple's developer tools on a second Mac, connecting via network to the halted Mac to inspect what exactly the system kernel was doing when the NMI signal arrived. An additional option allows you to specify how the NMI should be triggered:
  - **Use keyboard to generate NMI:** The interrupt should be sent when pressing both ⌘ keys and the Delete key (⌫). On older Macs that have no security chip, press both ⌘ keys and the power button.
  - **Use power button to generate NMI:** The NMI signal should be sent by using the power button only. This can be useful to switch to debug mode early in the startup phase, where the keyboard is not active yet.
- **Disable support for all 32-bit software ("x86 code"):** This item can be activated to block all legacy 32-bit software from execution. If you try to launch such a program, macOS will immediately stop it, causing an artificial application crash with a message similar to the one shown below.

> macOS Catalina cannot run 32-bit-software in general, so the aforementioned option does not make sense when using version 10.15 or later of the operating system.

- **Kernel should separate control register 3 and virtual memory tables from userspace:** Enabling this option causes the operating system to strictly separate the virtual

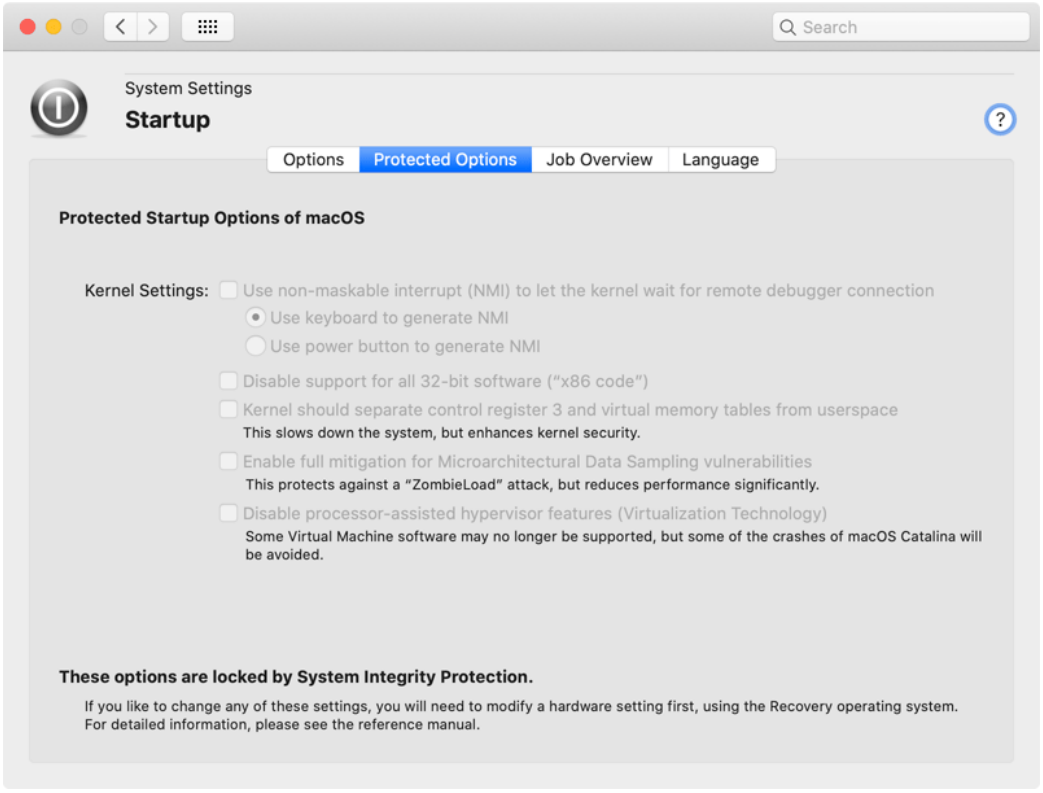


Figure 4.11: Advanced kernel settings are protected by SIP

memory used by its core *(kernel)* from the virtual memory used by user processes, and to have the processor hardware monitor this strict separation. Under normal conditions, the system only uses a single shared copy of the *"pmap"*, the hardware and software components that control virtual memory. The virtual memory is usually 128 TB in size, and simple separation is done by letting the kernel use the upper half of this memory area, while letting the currently running user process use the lower half of the 128 TB virtual memory. After enabling this option, the operating system will use two separate copies of the pmap for the kernel and user applications. The processor's control register 3 *(CR3)* is used to switch between these copies, depending on whether kernel or user code has to be executed. If a user application tries to access virtual memory of the kernel, which is a significant security risk, because access to the kernel means unlimited access to all hardware and software, the hardware will now notice this and the attempt will fail. In the other direction (e.g. when a bad driver accesses a running user program), the system will be stopped immediately with a Kernel Panic. This mode of operation increases overall system security and protects against specific attack patterns, e.g. the security hole published by the Italian teenager *Luca Todesco* in August 2015. However, it also means that the system now has to switch its entire virtual memory administration whenever the processor changes between executing kernel code and user code. This reduces system performance.

- **Enable full mitigation for Microarchitectural Data Sampling vulnerabilities:** In spring 2019, Intel disclosed a security issue affecting processors which support *hyper-threading,* a feature where hardware components within each processor core can be used in a way to efficiently simulate twice the number of cores (virtual processors) on the available physical cores. (To validate whether you are using an Intel processor with hyper-threading, open the tab System Information on the pane Info (section 2.8 on page 85) and check whether the section Processor lists a number of processors which is twice the number of cores.) The security issue makes it possible that an application currently running on a specific physical core could use a series of complex tricks to "see" data of another application running on the virtual processor of the very same core. This should never happen. Two running applications should always be strictly separated from each other. Trying to spy on data of other applications by using this technique is called a *ZombieLoad attack*. Intel has published a microcode update for some affected processors, and Apple has published an operating system update for the latest macOS versions that make it unlikely that exploiting this vulnerability will have success in practice. However, the likelihood for a successful attack is still not entirely zero yet. If you like to play it safe, making absolutely sure that ZombieLoad cannot work, you will have to disable the hyper-threading feature altogether. You can do so by activating this special macOS setting. Note that this will remove all performance gains of running twice the number of simultaneous threads on the physical cores. The total performance of the system could be decreased by up to 40%.
- **Disable processor-assisted hypervisor features (Virtualization Technology):** Macintosh computers with Intel processors are capable of supporting specific aspects of virtualization directly at the hardware level (running multiple operating systems

simultaneously in Virtual Machines). The kernel of macOS can fully utilize these features. By setting a check mark here, you can disable this support. Specific virtualization software products for macOS may depend on this feature, so it could happen that they no longer work. Disabling VT support can make sense in specific cases, however. Unfortunately, macOS Catalina is an unusually immature operating system with multiple defects in the kernel that can cause it to crash in certain situations. It has been observed that typical crashes that occur when transferring large amounts of data, can usually be avoided, after this kernel feature has been disabled.

Additional Technical Notes for Some of the Options

When macOS is blocking a 32-bit process as result of the option **Disable support for all 32-bit software**, it will trigger an exception that creates a crash log containing an error description of the following pattern:

```
Crashed Thread:     0  Dispatch queue: com.apple.main-thread
Exception Type:     EXC_CRASH (SIGKILL)
Exception Codes:    0x0000000000000000, 0x0000000000000000
Exception Note:     EXC_CORPSE_NOTIFY
Termination Reason: EXEC, [0xd] This binary requires 32-bit x86 support, which
                    has been disabled
```

Changing Protected Options

To use one of the listed protected options, perform the following steps:

1. Open the tab item **Protected Options** of the pane **Startup**.
2. Ensure that System Integrity Protection (section 1.3 on page 7) is currently not active. (The options are not greyed out.)
3. Activate or deactivate the listed options as desired.

4.3.3 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 tab item **Job Overview** of the pane **Startup**.

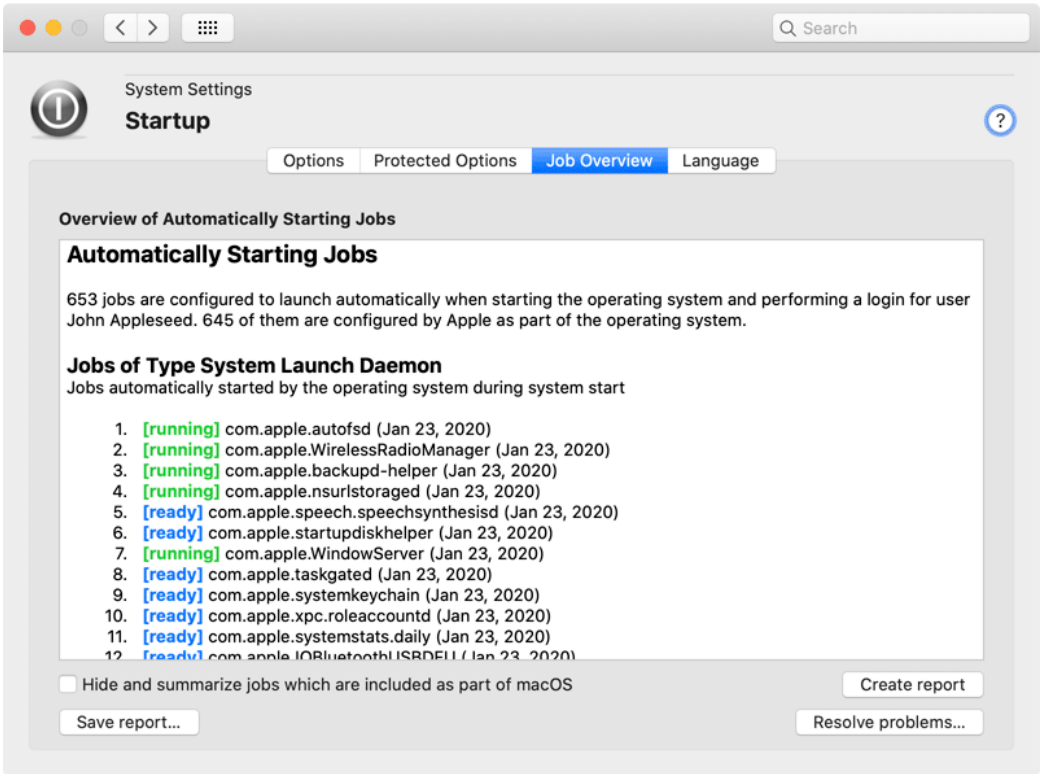


Figure 4.12: Overview of all automatically starting jobs

2. Click the button **Create report**.

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 **Users & Groups** pane of **System Preferences**, 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 in the lower right corner. 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 221).

4.3.4 Language

Users can individually set the languages they prefer when working with applications. This personal preference setting is controlled by the priority list displayed at **Language & Region** > **Preferred Languages** in System Preferences. However, this setting only affects applications started by each user, it does not apply to the startup phase of the operating system and its login screen, situations where no user has logged in yet. Under normal circumstances, this additional language preference can only be set when installing the operating system.

TinkerTool System allows you to modify this language preference without having to reinstall the system. Perform the following steps:

1. Open the tab item **Language** of the pane **Startup**.
2. Select the preferred language with the pop-up button **Startup Language**.

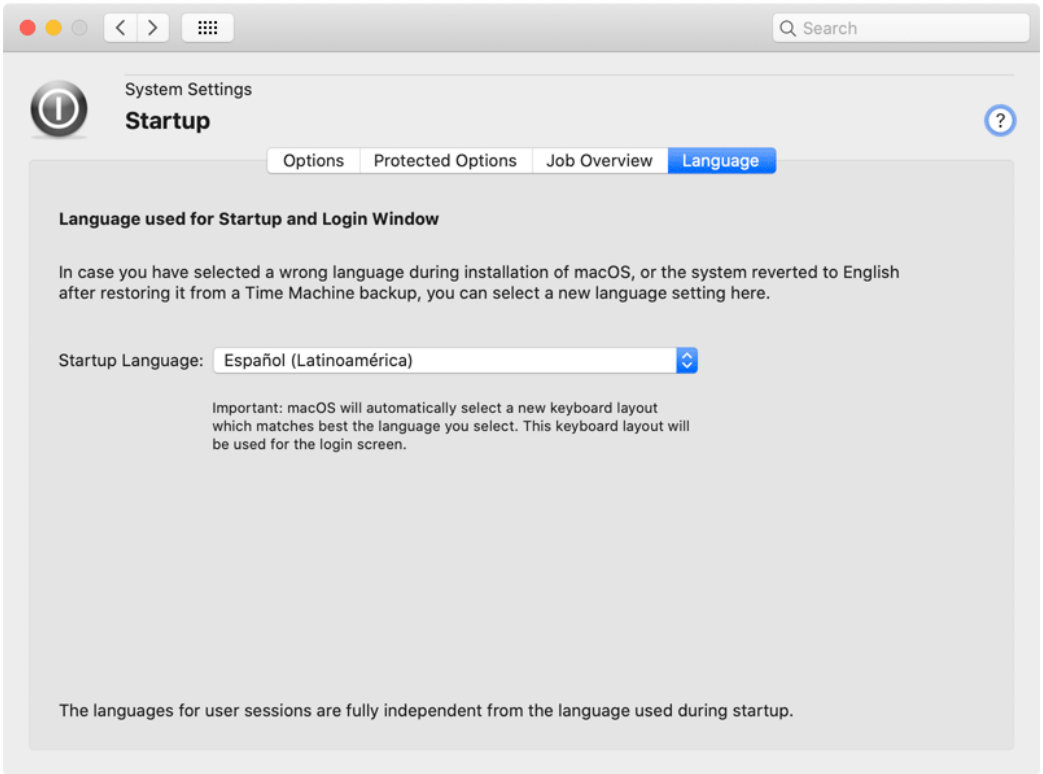


Figure 4.13: Startup language

> This will also change the keyboard layout used when running the login screen. If you don't own the keyboard type typically used for the selected startup language, it may become difficult to enter user name and password correctly.

Under certain circumstances, the startup language setting of macOS can have been damaged, e.g. when you have restored your system from a Time Machine backup. In this case, TinkerTool System will display an additional button with the option to repair the setting.

4.4 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** > **Login Options** > **Automatic login: Off** in System Preferences.

> 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 of the firmware (which partially depends on the recovery partition) 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 preferences 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.

4.4.1 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:

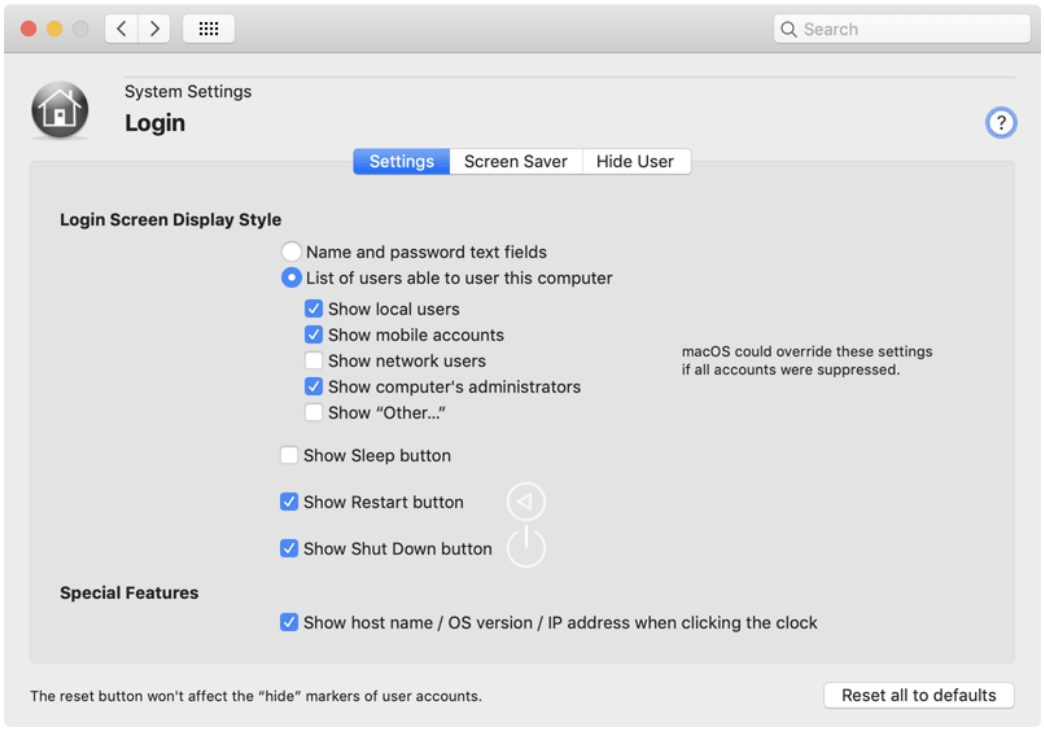


Figure 4.14: Login screen settings

- **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.
- **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 TinkerTool System Standalone Utility (section 2.6 on page 77) to reset the login screen to factory defaults. Remember that this tool must be installed in advance to be available.

Additional options allow the control which buttons should be displayed at the bottom of the window:

- **Show Sleep button:** the button used to manually switch to sleep mode,
- **Show Restart button:** the button used to restart the operating system,
- **Show Shut Down button:** the button used to switch the computer off.

By default, the login screen only displays the current time (and the battery status for mobile systems) in addition to the entry fields. For diagnostic purposes, especially in large networks, more information about the computer can be shown if necessary. The login screen can display the computer's TCP/IP host name, the OS version number, and the computer's primary IP address. The items will be shown in this order after you click onto the clock in the upper right corner of the login screen. To enable this feature, set a check mark at **Show host name/OS version/IP address when clicking the clock**.

4.4.2 Screen Saver (macOS Mojave only)

> Apple has removed this feature from macOS 10.15 or later.

If desired, you can choose the screen saver used for the login screen. Set a check mark at **Enable the custom screen saver set below** and select an activation time (**Start screen saver after**...). The interval can be set either by entering the numerical value in minutes, or by using a slider. The type of screen saver will be determined by the setting **Screen saver** which has three options:

- You can choose a basic screen saver which shows an animation of the computer's name. Apple has particularly designed this special screen saver for the login screen. Select the item **Computer name** to activate it.
- The same basic screen saver can show any short message that you specify instead of the computer name. Choose **Custom message** and enter the message into the field next to the item.
- You can activate any of the standard screen savers of macOS with the item **Use module at path**. The type of screen saver is then specified by the location where its plug-in program is stored.

In the latter case, click the button **Select**... to navigate to one of the screen saver plug-ins available in your installation of macOS. You can also select third-party screen savers under the condition that they can be opened by everyone. Note that the login screen does not allow to specify any additional options for these screen savers. They will always run with their default settings.

4.4.3 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.

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.

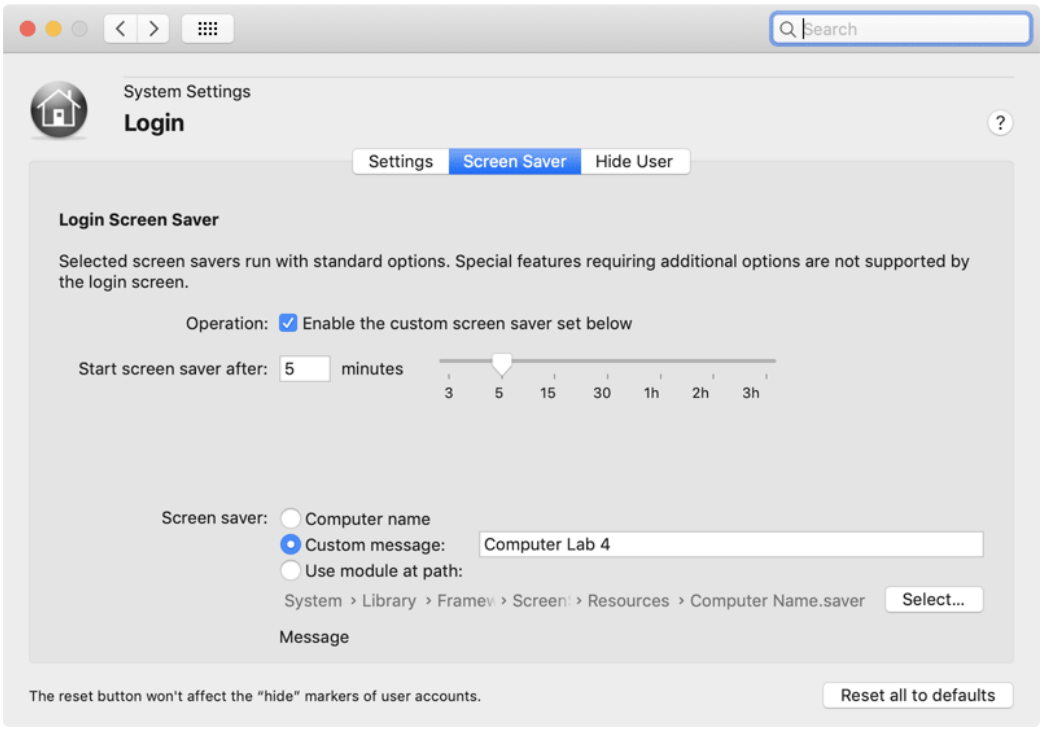


Figure 4.15: Screen saver

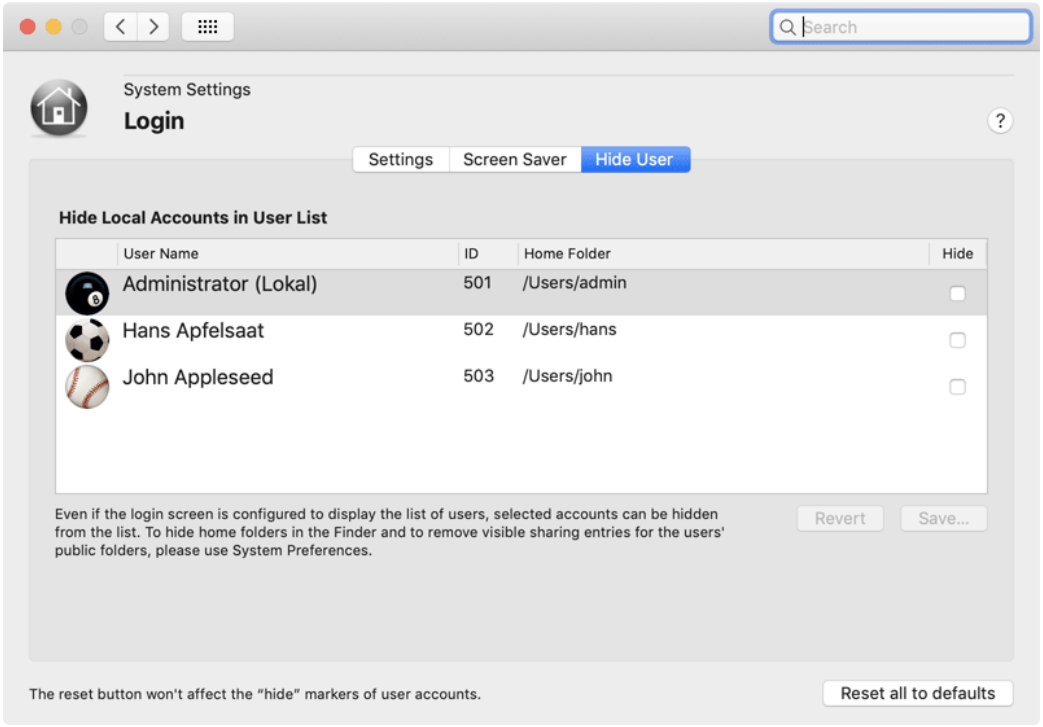


Figure 4.16: Hide accounts in the login list of users

> 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 Preferences** > **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 Preferences** > **Sharing** > **File Sharing** and remove all entries in the list **Shared Folders** which should no longer be active.

4.5 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 Preferences** > **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 you 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 preferences, nor the language packages within the application will be touched. This can be very helpful if you are working in a multi-lingual 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

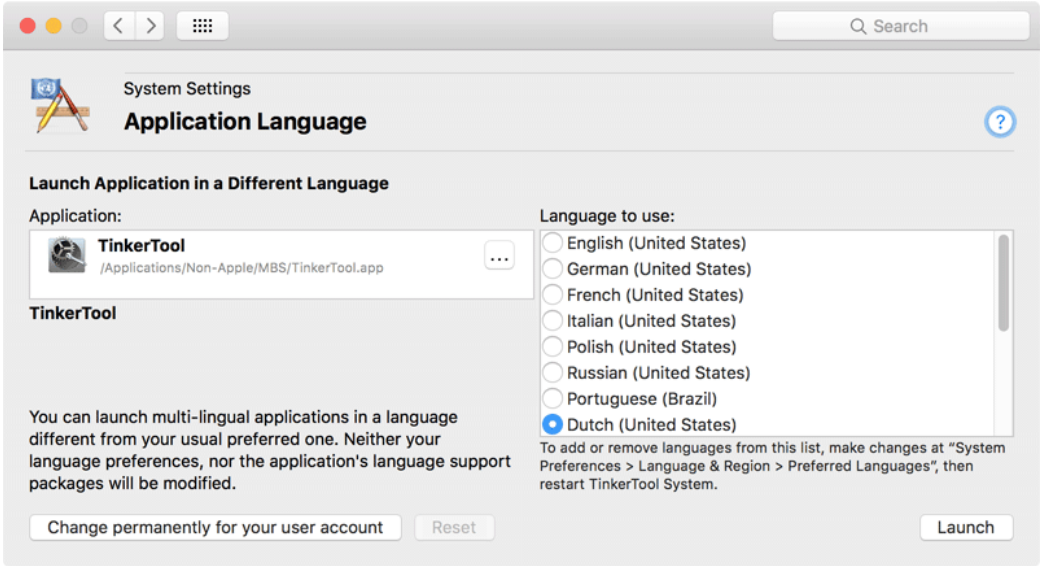


Figure 4.17: Application language

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 Preferences** 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.

4.5.1 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 Preferences** 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.

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 noted at the top headline of the TinkerTool System control window. Detail information about the selected user account can also be found on the tab 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 tab 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

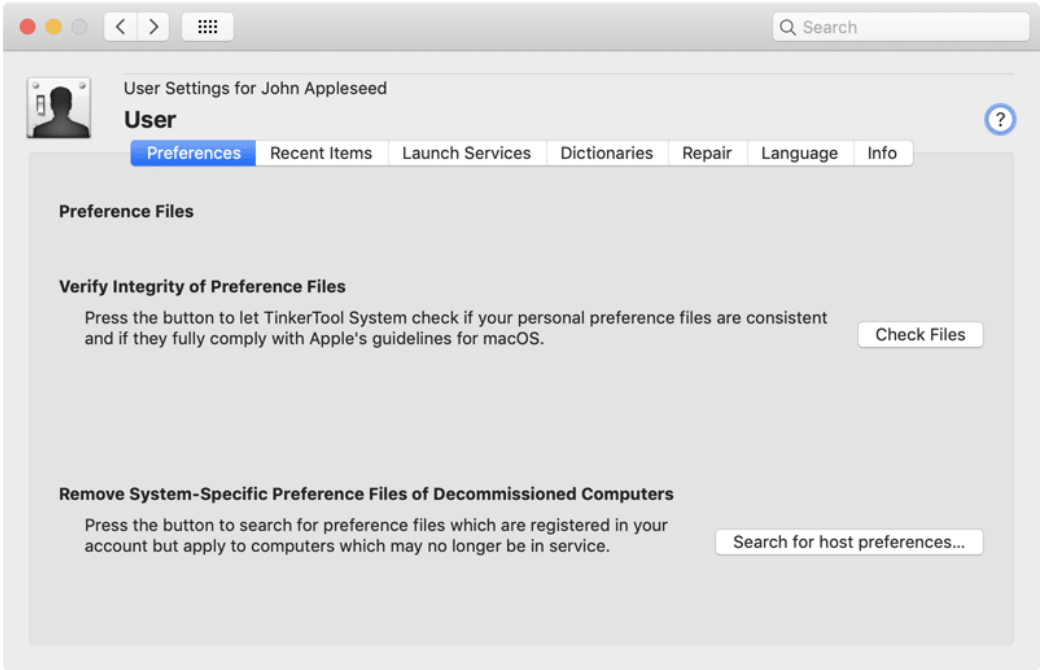


Figure 5.1: Preferences

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).

For old systems, the primary MAC address was printed on the serial number label of the computer, usually accompanied by a bar-code holding the same information. The address can also be retrieved by software, launching the program **System Information** from the folder **Utilities**. The address can be found after choosing the information category **Network**, then selecting the primary network interface **(en0)**, and looking at the information line **Ethernet** > **MAC address**.

On modern versions of macOS using UUID codes, TinkerTool System shows the identification at **Info** > **System Information** > **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 tab 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

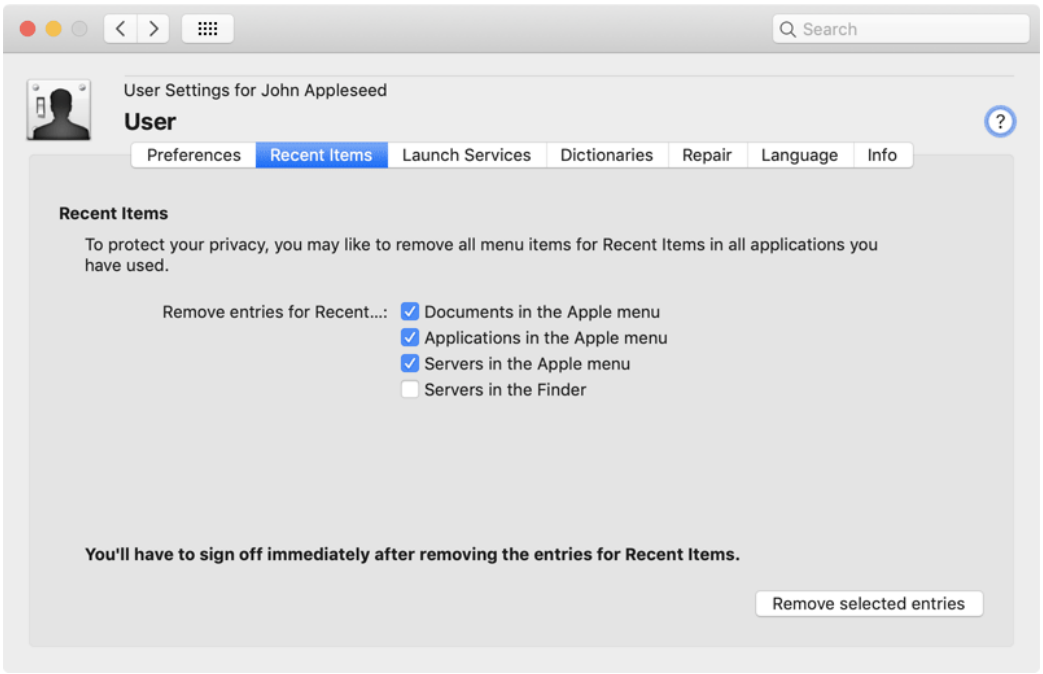


Figure 5.2: Recent items

To remove the entries for Recent Items, perform the following steps:

1. Open the tab item **Recent Items** on the pane **Privacy**.

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.

5.1.3 Launch Services

macOS keeps an internal database which lists all applications accessible by your computer. The data is used to display the correct icons for documents, and to keep track which application should be launched when you double-click a document. Under normal circumstances, macOS will constantly update the database in the background. In rare cases, the database might contain invalid information. Typical symptoms are:

- when you click the context menu item **Open with**... or use the **Open with** section in the Finder's **Get Info** panel, invalid or duplicate entries will be displayed,
- documents are shown with incorrect icons,
- the feature "Markup" (adding notes or similar changes to documents you received from others) is not working as expected,
- the Share button or Share menu shown by some applications is not working or not offering all services that can normally be used to share contents.

In this case you can force macOS to rebuild the database for the current user. Perform the following steps:

1. Open the tab item **Launch Services** on the pane **User**.

2. Click the button **Rebuild database**.

> This will also reset the security feature which prevents that documents are opened with unknown (potentially dangerous) applications. If you open a document associated with an application which has never been used before, macOS will ask for re-approval to launch the application.

If applications have been put to a folder outside an **Applications** folder (which is generally not recommended), macOS may forget that they exist, so they may disappear from the **Services** and the **Open with** menus. You'll have to use the Finder to open the folder containing the applications to make the system aware of these programs again.

After rebuilding the database, TinkerTool System asks whether it should restart the Finder. This way you can immediately verify if repair of the database had a positive effect on the Finder.

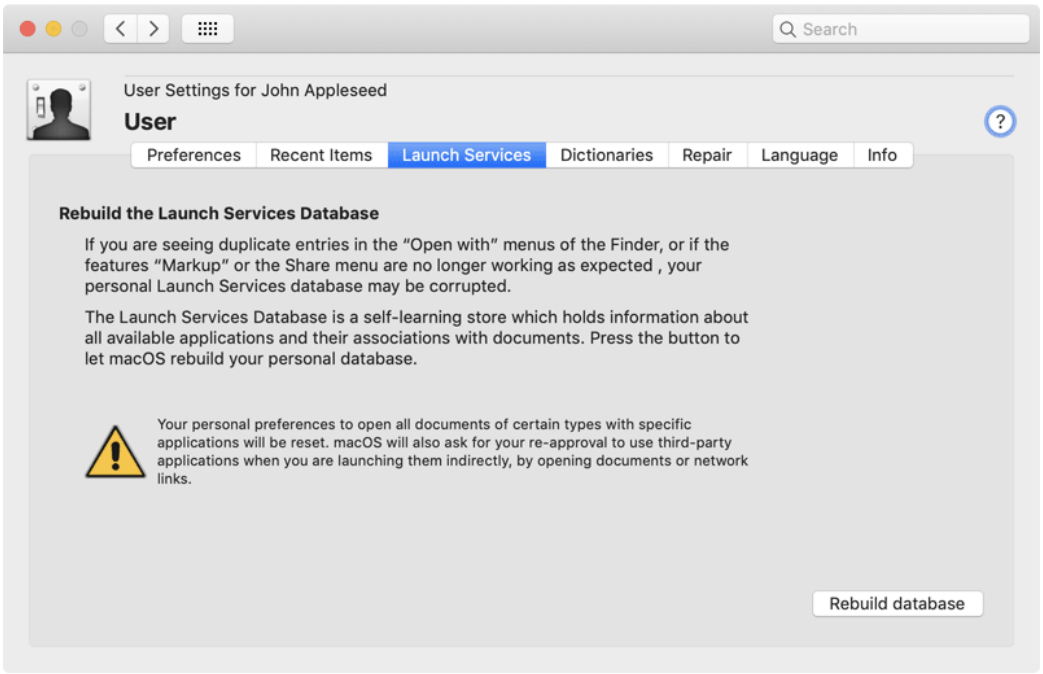


Figure 5.3: Launch Services

5.1.4 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.

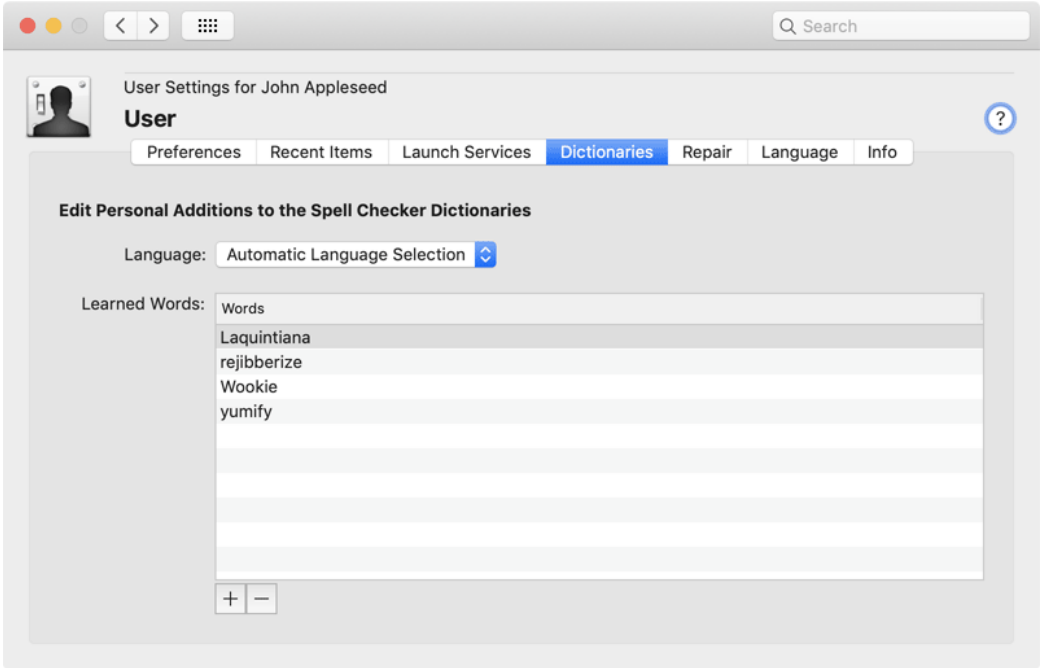


Figure 5.4: Spelling dictionaries

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 tab 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.

5.1.5 Repair

Repair "System Preferences"

Some versions of macOS have internal defects which can cause strange effects for the display of icons in the application **System Preferences**. If you open System Preferences and you are seeing one of the following problems in the overview of preferences panes, you should use the repair feature of TinkerTool System:

- panes are displayed with incorrect icons,
- some icons are displayed multiple times,
- some icons are damaged,
- some icons are displayed in the wrong category,
- some labels show nonsense text,
- some labels are displayed in a different language.

If you are affected by one or more of these problems, perform the following steps:

1. Open the tab item **Repair** on the pane **User**.
2. Click the button **Repair Now** in the section **Repair "System Preferences"**.

TinkerTool System will guide you through the repair 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.

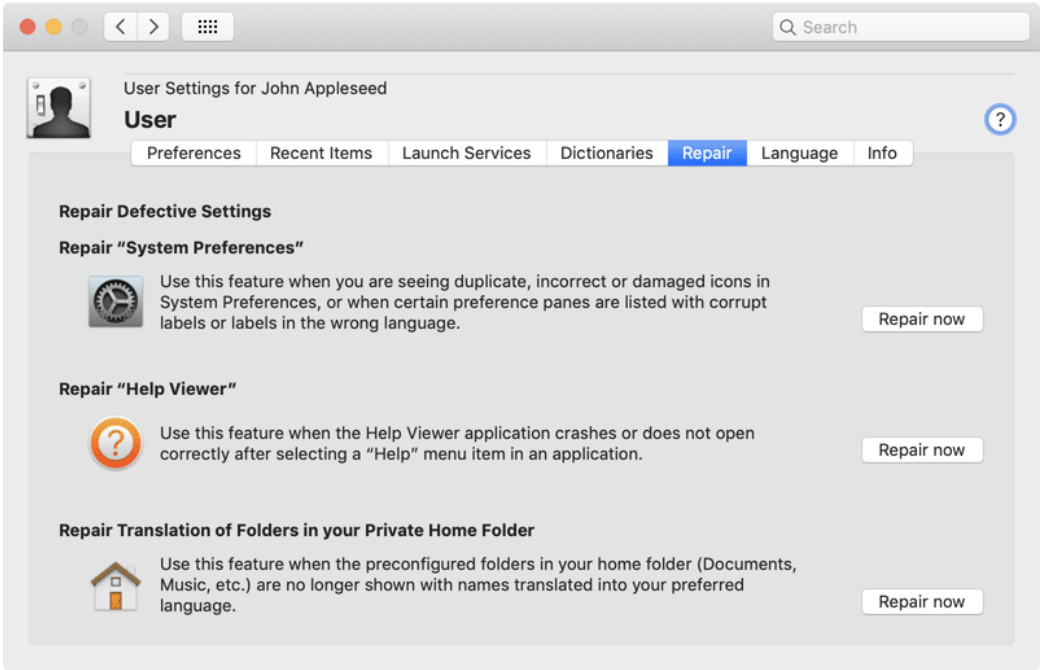


Figure 5.5: Repair features

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.
- 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 tab 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 tab 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.

5.1.6 Language

Some users can be affected by a problem where their language setting for the user interface unexpectedly changes. In this case, most or even all applications do not run in your preferred primary language, but in a different one. TinkerTool System can repair your personal language settings by a single mouse click. It will reset the language priority list to the defaults that have originally been set for your computer (typically when the computer was installed for the first time).

To reset your personal language preferences, do the following:

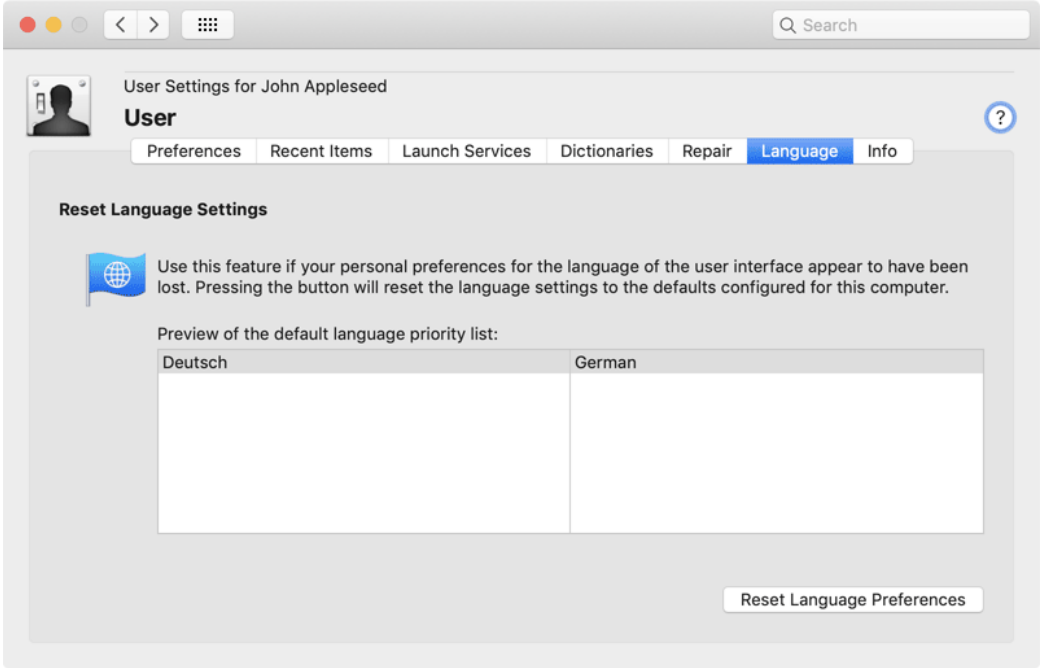


Figure 5.6: Language

1. Open the tab item **Language** on the pane **User**.
2. Verify that the priority list of languages shown in the preview table is the correct one.
3. Click the button **Reset Language Preferences.**

If you like to make changes to your language list, or if you like to add or remove languages, you can do so in the **System Preferences** application at **Language & Region** > **Preferred languages**. To ensure that all applications will restart with your new language settings, log out and log back in.

> The priority list of languages taking effect for you is the one visible in **System Preferences**. The list shown in the **Language** tab item of TinkerTool System is the one currently set as default for all users on this computer.

5.1.7 Info

The tab item **Info** can be used to display advanced information about the current user account, not visible in the System Preferences 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 in addition to the full user name already displayed at the top of the window:

- 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, or by switching to the Darwin console (section 4.4 on page 212).
- 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.

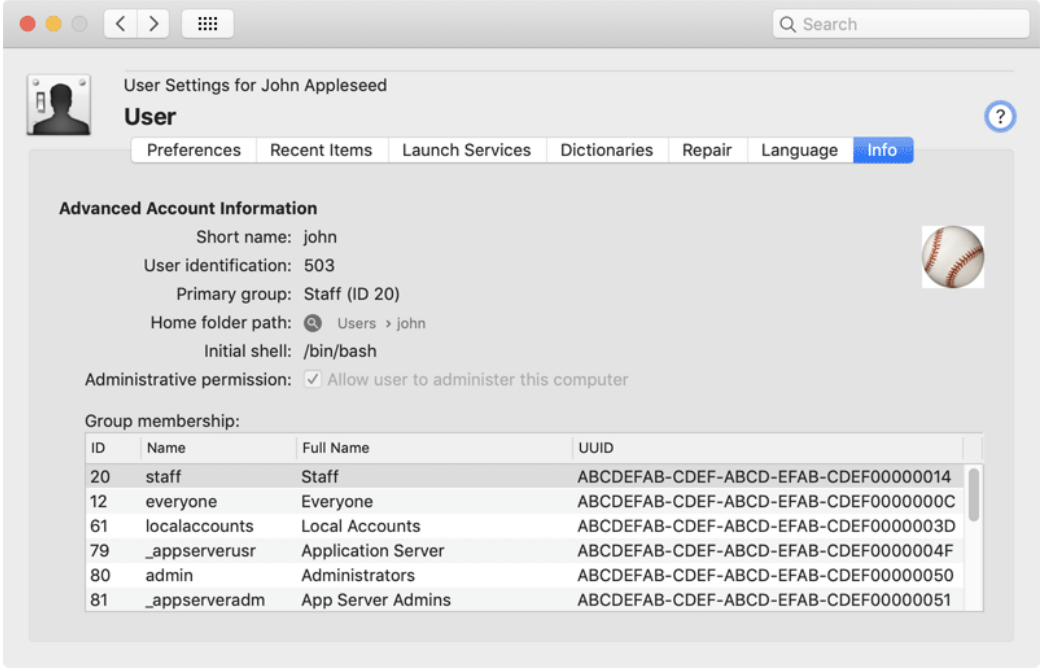


Figure 5.7: Info

> 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 21) 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 Preferences application or in the preferences windows of applications, like Safari. To change one of these advanced preference settings, perform the following steps:

1. Select one of the additional panes shown in the section **User Settings for**... in the control window 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.

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 2.6 on page 77).

> 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 2.6 on page 77).

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:

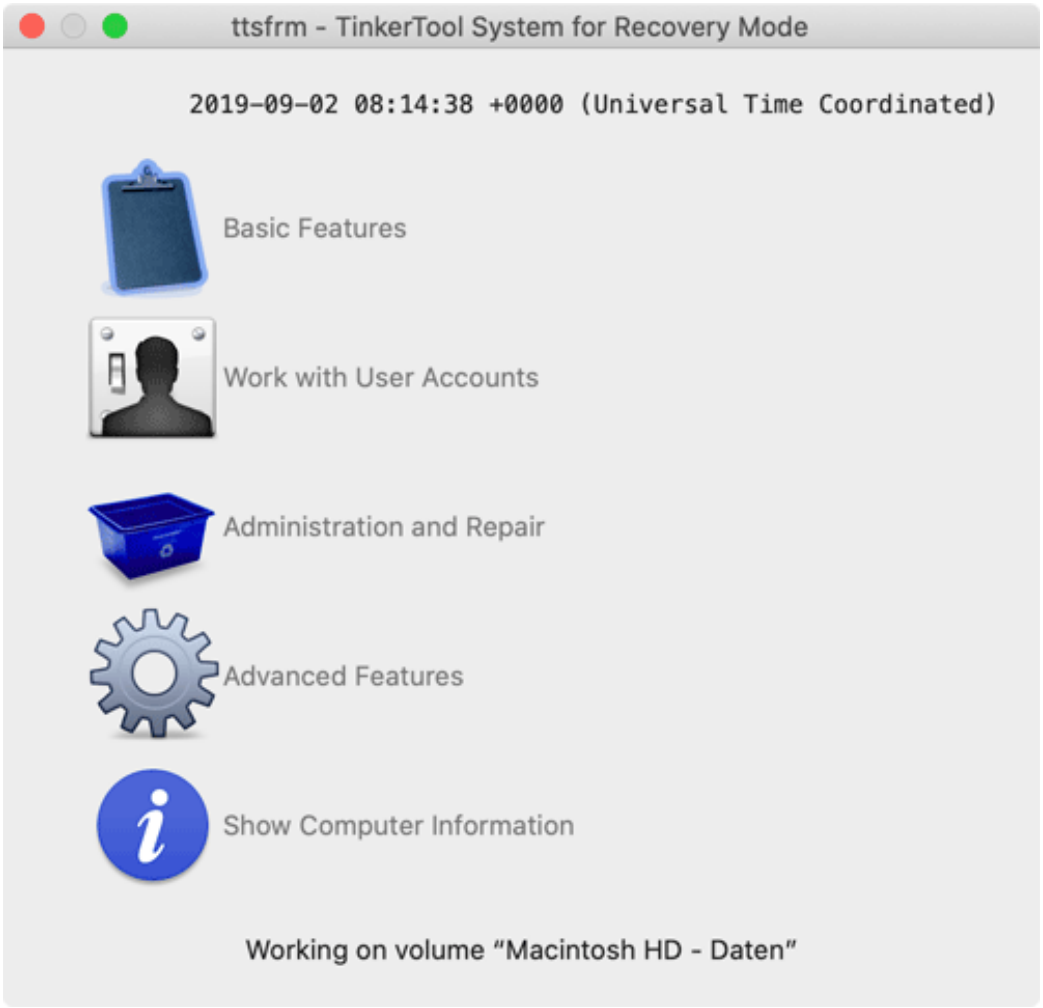


Figure 6.1: The main menu of TinkerTool System for Recovery Mode (ttsfrm

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 sheet **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.

6.2.2 System Integrity Protection (SIP)

When it becomes necessary to switch System Integrity Protection of your Mac on or off, as mentioned in the chapter Basic Operations (section 1.3 on page 7), you can also do this by mouse click in **TinkerTool System for Recovery Mode**. Simply click on the respective option at **System Integrity Protection (SIP)**. The setting has no meaning for the running recovery OS. It will take effect the next time the computer is restarted.

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.

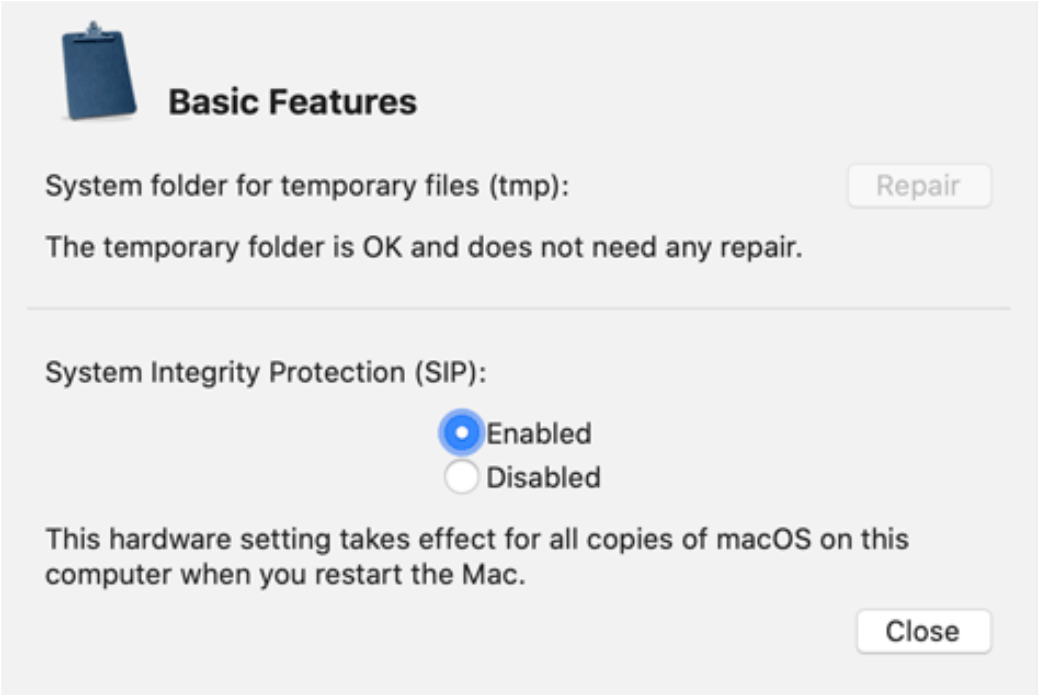


Figure 6.2: Basic Features

> 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 28), 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**.
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.

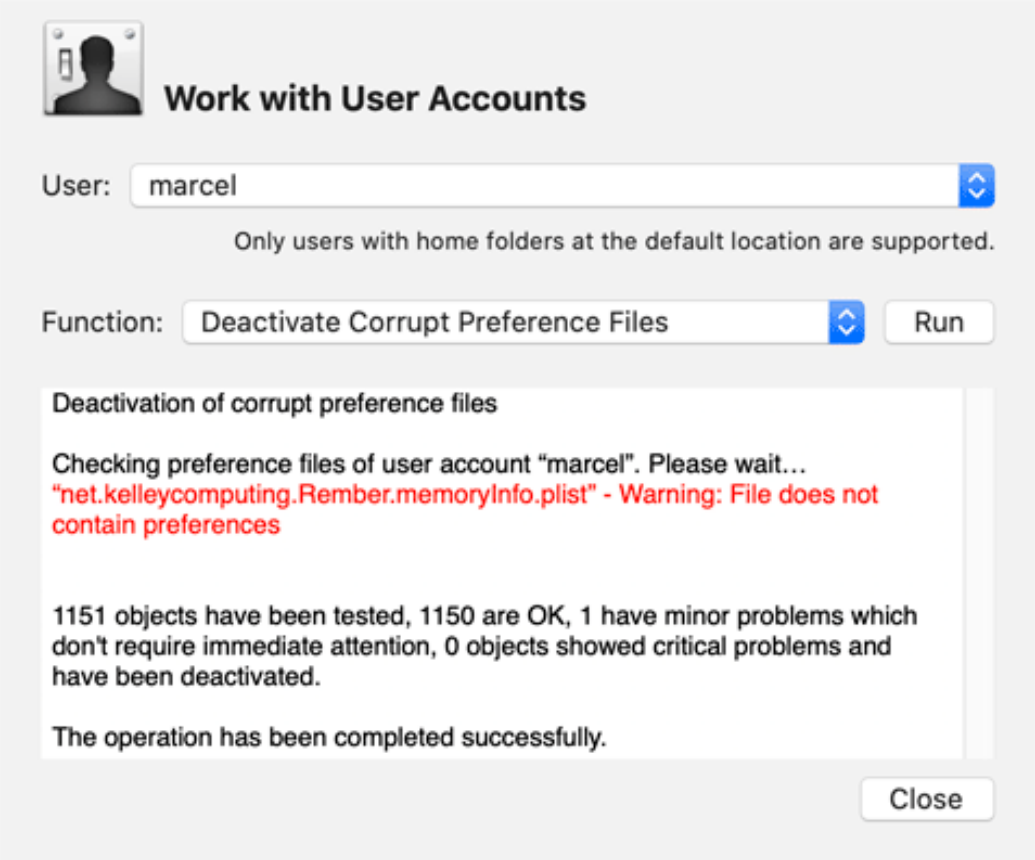


Figure 6.3: Working with user accounts

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**.
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 28).

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.

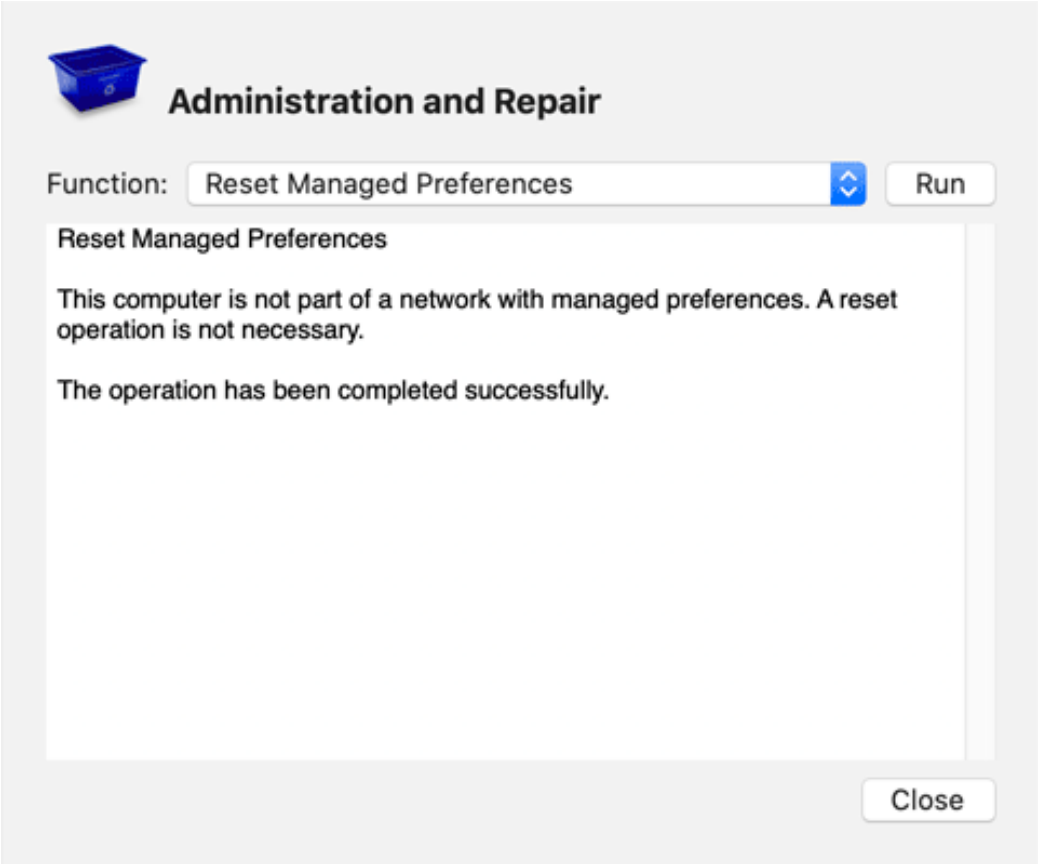


Figure 6.4: Administration and Repair

6.4.4 Resetting Managed Preferences

If your computer is part of a macOS network where management features or the Profile Manager of macOS Server 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 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

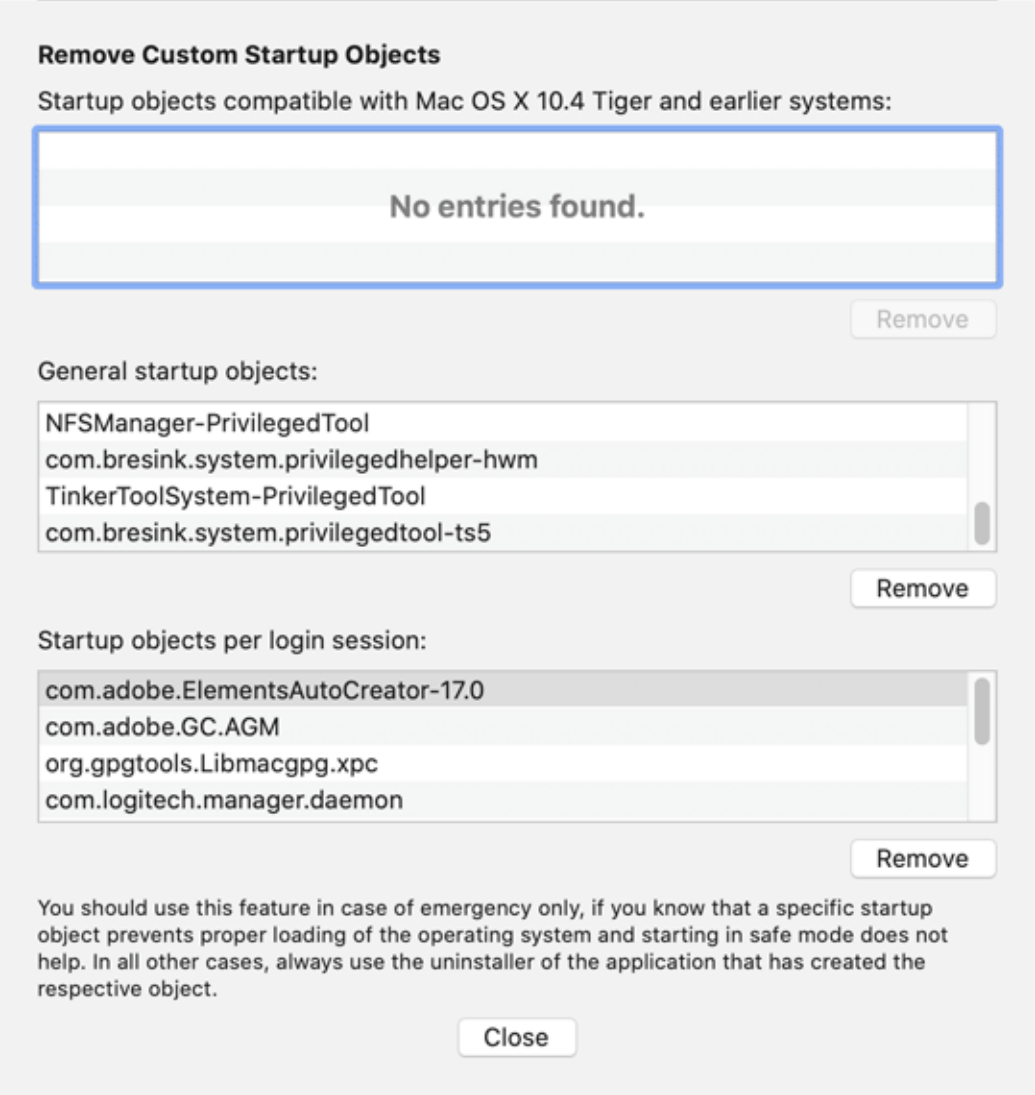


Figure 6.5: Remove Custom Startup Objects

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 Preferences** > **Users & Groups** > **Login Options** in macOS.

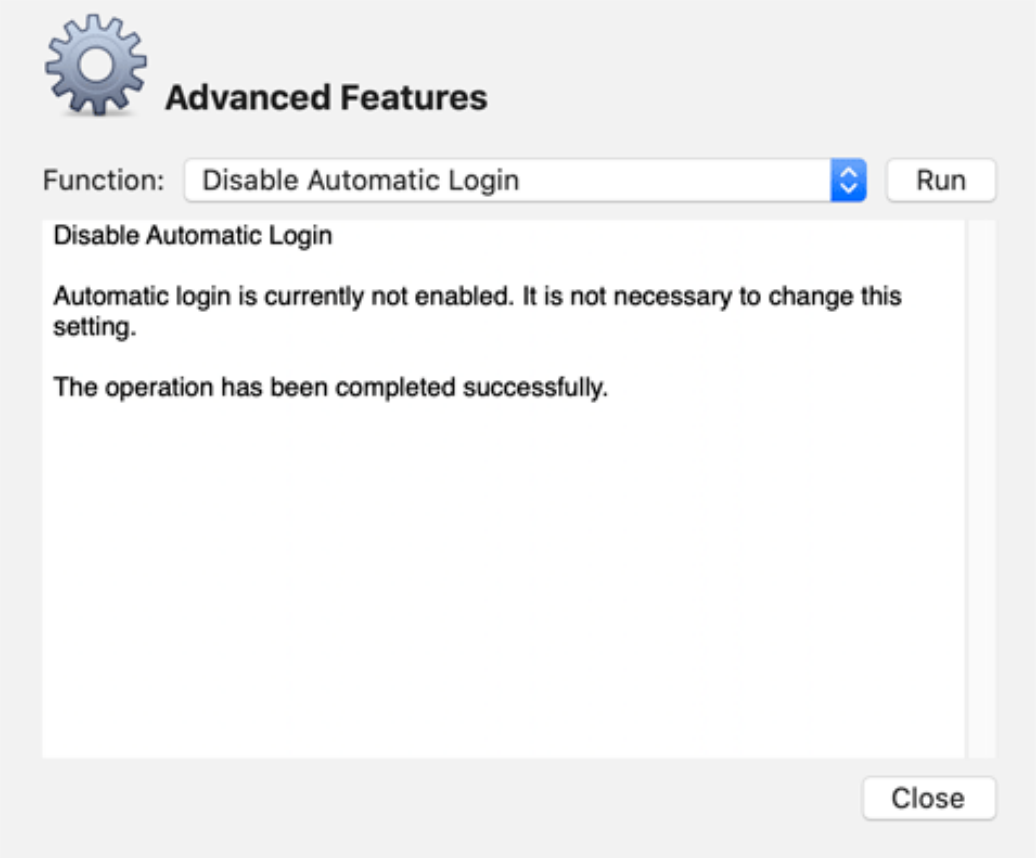


Figure 6.6: Advanced Features

6.5.2 Enforcing a Rerun of the Setup Assistant

It is possible to make configuration changes to the operating system that inadvertently disable all administrative user accounts. This is a very critical situation because you may lose access to the system and also can no longer authenticate in order to fix this. The easiest solution to resolve such a situation is to force the operating system to re-run its Setup Assistant, the application that is usually started after you have installed or upgraded the computer for the first time. The macOS Setup Assistant will allow you to recreate the primary administrative user account, without losing or changing any other data.

To force the system to re-run its Setup Assistant the next time the computer is started, perform the following steps:

1. In the main menu, click on **Advanced Features**.
2. Select the item **Re-run Setup Assistant upon next OS start** in the pop-up button **Function**.
3. Click on **Run**.
4. Wait until the utility confirms that the necessary steps have been completed.

After that, you can use **ttsfrm** > **Quit ttsfrm** and restart the computer via the Apple menu to let the system start with Setup Assistant.

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**.
2. Make sure the tab item **Hardware Overview** is selected.

This corresponds with a simplified version of the feature **Info** > **System Information** 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

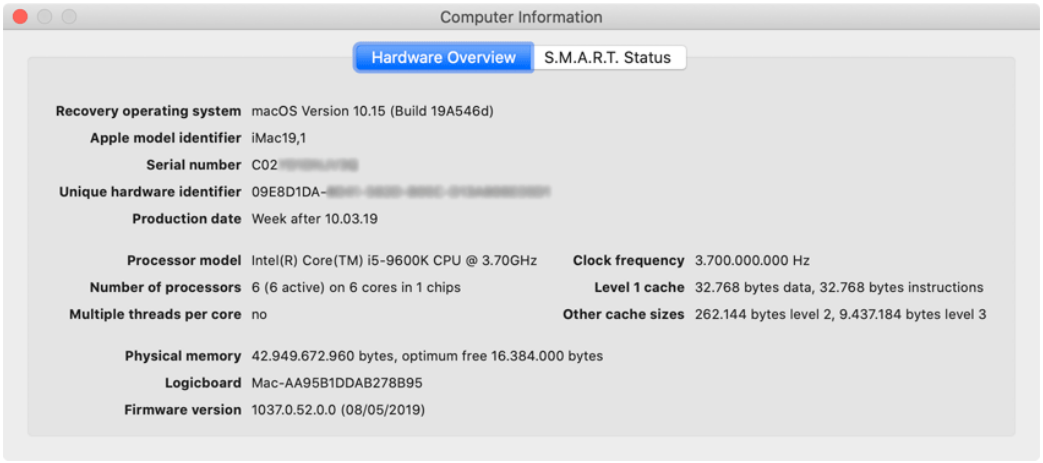


Figure 6.7: Hardware Overview

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.

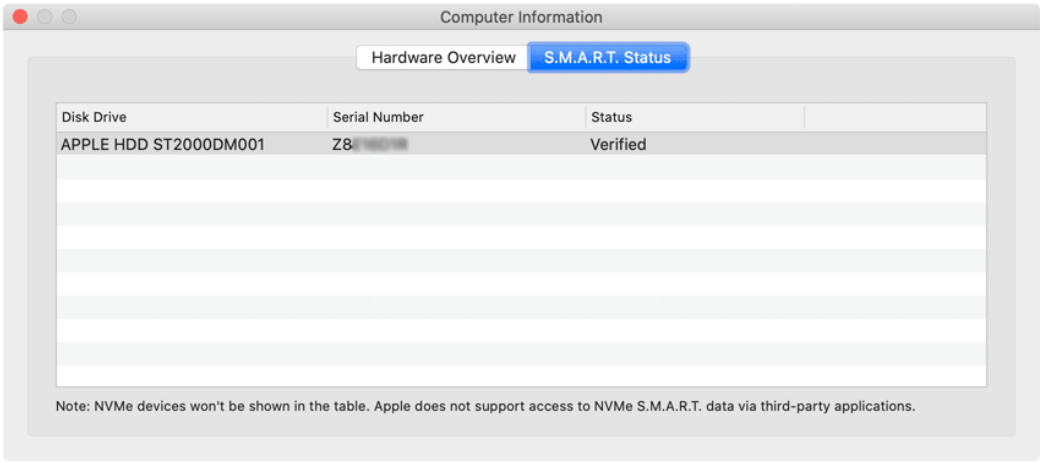


Figure 6.8: S.M.A.R.T. Status

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.

For SSD drives attached via modern NVMe technology, the retrieval of S.M.A.R.T. information would be technically possible, but Apple does not support this for applications of third-party vendors, e.g. TinkerTool System.

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 6 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
- Recovery from a deactivation of standard user caches
- Recovery from a deactivation of high-speed user caches
- Recovery from a deactivation of system-wide caches
- Recovery from a deactivation of operating system caches
- Evaluate RAM size in relation to typical workload
- Removal 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 blacklists for App Nap, HiDPI, application launch, and kernel extensions
- 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
- Changing the startup language
- 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 file* containing a *registration code* 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 Codes

Placing an order for registration codes of TinkerTool System 6 is possible via our distribution partner. The order can be placed via Internet, postal mail, telefax or phone. After our sales partner has acknowledged your payment, you will receive the requested number of registration codes as a single file. For an online order, you can download this file immediately after your order was processed, from the same web page where you placed the order, so no actual "delivery" will be necessary. You will receive an additional copy of the registration file together with your invoice by email. Payments are accepted in more than 40 different international currencies, with all common payment options supported.

To learn more about placing orders, please use the following Internet page of TinkerTool System 6:

`https://www.bresink.com/osx/300863620/order.html`

For first written information, you can alternatively select the menu item **Help** > **Purchase Registration Key**... in the application.

7.1.5 Registration via file or via text input

The registration info needed to fully unlock the application can have been delivered to you in two different forms, either as a file with a ticket icon, or as readable text with two entries named **Registration Name** and **Registration Key**. Delivery by file is the preferred method used for all recent orders, because the unlock procedure only requires a simple double-click. Registration by readable text is only used for very special licensing situations.

The necessary unlock procedure differs, depending on what type of registration you have received. The two following sections describe both unlock procedures in detail. Only one procedure will apply to you.

7.1.6 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 pair of *Registration Name* and *Registration Key* directly from Marcel Bresink Software-Systeme via email, please skip this section and look for more information at "Unlocking the Software with a registration mail" below.

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 by download, 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 memory stick 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 for the download. 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 **Software Product 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.

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 mail

> This section describes how to use a *registration message* containing a pair of *Registration Name* and *Registration Key* you have received via email directly from Marcel Bresink Software-Systeme. If you have received a *registration file* from the software reseller instead, please see the preceding section "Unlocking the Software with a registration file."

Please note that the registration code you have received by email 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 Mailed Registration Manually

Perform the following steps to unlock the application for unrestricted usage. These steps will always work, no matter how you received or stored the registration data, and they will allow you to unlock the application for all user accounts of a single computer if you like to do so:

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 6**....) The window **Software Product Registration and Activation** will appear.

2. Click the button **I only have Registration Name and Registration Key**. Fields for data input appear in the window.
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**.

If both parts of the code have been entered correctly, the window **Software Product 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 e-mail message which had been sent to you.

7.1.8 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 6. In this particular case, 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.

7.1.9 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.

7.1.10 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 received by email (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* (no visible Registration Name), you will need to activate your registration once again, using the instructions given previously in this chapter.

7.1.11 Creating a Combined Ticket for Upgrade Licenses

As outlined in the previous section, you will need to re-register the application when moving to a new computer. This usually requires that you provide your registration file, and in case of an upgrade, a second registration file (or name/key pair) for a previous product that proves that you are eligible to use an upgrade.

To avoid these tedious two steps, you can combine the two licenses in a single file. This file can then easily be loaded in one 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.

7.1.12 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.

Site and global licenses delivered before June 2016 were automatically connected to a kind of subscription service which gave administrators access to special copies of the application that had embedded volume licenses in them. These customized software versions could be copied freely within the organization and were "pre-registered," so the maintenance effort for administering registrations was kept at a minimum. This subscription plan was discontinued in June 2016.

As of that date, the distribution of custom software versions has been superseded by a new method, which works just as easy:

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

After updating Safari in macOS 10.14.6, the feature to repeat system optimization may fail: If you have updated macOS Mojave 10.14.6 with a specific version of Safari 14, the feature **Maintenance** > **System Optimization** will indicate error code 11 at the end of processing. The procedure cannot be completed successfully.

Workaround: This was a known defect in the operating system, caused by the Safari 14 installer for macOS Mojave, originally published by Apple on September 16, 2020. TinkerTool System detected correctly that this Safari installation damaged a particular part of the operating system. Apple has withdrawn the defective software on September 30. A corrected version was released under the name "Supplemental Update" together with a corrected version of Security Update 2020–005 on October 1. When you install these update packages, macOS 10.14.6 will be repaired. The optimization feature can then also be used with TinkerTool System again.

When using a network-based Time Machine setup, connecting to the backup may take a long time and may not be successful with specific versions of macOS: Specific versions of macOS have a defect that has influence on performing Time Machine maintenance features in cases where the backup sets are stored on a file server, not on a local disk. Connecting to the file server may take an unusually long time during which TinkerTool System cannot respond to user interactions. macOS will temporarily indicate a "not responding" status during that time. After the connection has been made, Time Machine may still not respond correctly. TinkerTool System shows the warning **Time Machine is not ready at the moment. Please wait.** when this happens.

Workaround: As a workaround, select an arbitrary folder in the Finder and open the Time Machine user interface. Wait until macOS begins to indicate available backup sets in the Time Machine timeline (which can also take a significant time), then quit the Time Machine screen. After that, press the button **Rescan** in the TinkerTool System pane showing the Time Machine data. Time Machine should now respond correctly.

When cloning an APFS object containing macOS, the system may add or omit volumes during the copy operation: If you use the feature to quick-copy an APFS object and this object contains a volume that contains an installation of a macOS operating system, the running operating system may automatically optimize the cloning operation, adding or omitting volumes at its own discretion, even if this contradicts the copy command sent by TinkerTool System 6. (1) macOS may automatically omit the volume with the role VM that is associated with the system installation that is copied. (2) macOS may automatically add volumes with the roles Preboot and Recovery that are associated with the system installation that is copied.

Workaround: This is a known issue of macOS Catalina. The operating system will auto-complete and optimize the data set being copied if it detects a macOS installation in

a volume that is part of the APFS object to be cloned. As workaround for item (1), just boot the cloned system. An additional volume with the role VM will automatically be created at the correct location. As workaround for item (2), use Disk Utility to delete the Preboot and Recovery volumes manually, if desired.

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 7), 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 Preferences, go to **Security & Privacy** > **Privacy** > **Full Disk Access**, authorize as administrator, and remove all entries for TinkerTool System and TinkerToolSystemPrivilegedTool if available.

4. Re-add the entry for TinkerTool System. In macOS Mojave, additionally add TinkerToolSystemPrivilegedTool (not for macOS Catalina or later).

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 report shown when repeating system optimization may contain many warnings: When macOS is instructed to repeat its system optimization phase, rebuilding the shared cache of the Dynamic Linker Editor, the messages shown by the operating system will contain many lines beginning with “update_dyld_shared_cache: warning”.

Workaround: This is the correct and normal behavior of macOS and of TinkerTool System. A warning line just indicates the technical reason why a particular optimization could not be performed for some specific software components. It is an expected part of its operation and no cause for concern. Only lines containing words such as “error” would indicate a technical issue.

Privileged operations fail after a downgrade of the application: The security features of TinkerTool System won't work as expected if you use a copy of the application and later use a copy with a lower version number. In this case, operations that require to be authorized by an administrator may no longer work. You will receive an error message instead, indicating that a "trust failure" has occurred.

Workaround: We strongly advise against any kind of downgrade of the software. However, if using an older version cannot be avoided for some reason, you'll have to make sure that the version of the privileged tool currently running in macOS is matching the version that came with the version of TinkerTool System you like to use. Perform the following steps:

1. In the running copy, select the menu item **Reset** > **Remove Security Component**....
2. Follow the instructions the program is giving. The program will quit itself as last step of this operation.
3. Launch the version of TinkerTool System you like to use.

Specifying a time interval when querying the macOS log database may not work: If you use the feature **Info** > **Logs** and specify a time interval at **Time range**, filtering by date and time may not work correctly with some macOS installations. Instead, the operating system returns entries for the entire recorded time range available. TinkerTool System detects this problem and will give you an error message in this case.

Workaround: This is a known defect of macOS. Only specific system installations are affected. We have informed Apple about this problem and hope they will fix it in future versions of the operating system. In case TinkerTool System detects this issue on your Mac, please see the recommendations given in the error panel for possible workarounds.

7.3 Version History

7.3.1 Version 6.995 (Build 220607)

Added new feature to resolve a known issue with the software update feature of macOS. It is now possible to reset Apple's software updater in cases where the user interface of System Preferences shows an endless wait status when the user tries to search for the latest security updates.

7.3.2 Version 6.99 (Build 220511)

- The user interface for registration was revised.
- The application can now offer automatic re-registration after it has been migrated to a new computer.
- Fixed a problem where exporting the list of orphaned files may not have worked as expected.

- Minor modernizations and adjustments.

7.3.3 Version 6.99 (Build 211227)

- This version fixes a problem where the startup job overview might not have reflected the true status of system launch agents under all conditions.

- Minor modernizations and price adjustment.

7.3.4 Version 6.99 (Build 210721)

This versions fixes a problem where the stop button may not have worked when trying to cancel a privileged operation that had already been running for a considerable time.

7.3.5 Version 6.98 (Build 210427)

- Added support for Security Update 2021–003 for macOS Mojave and Security Update 2021–002 for macOS Catalina.

- Added new feature for users of upgrade licenses: An administrator who activated the application via a upgrade registration file can now create a "single-step ticket" that combines the information about the upgrade license and the license for a pre-requisite product into one file. This file can be used to re-register the application in a single step without having to prove upgrade eligibility again, e.g. when migrating to a new computer.

- The application uses more detailed error messages if removing a bad startup job fails for some reason.

- Fixed a problem where candidates of software components pre-selected for deletion by the Uninstallation Assistant have been shown with type information in the wrong language.

- User guidance for evaluation mode uses better wording in the English user interface.

7.3.6 Version 6.97 (Build 210209)

Added new internal feature to allow normal users to check, remove and re-apply Access Control Lists for file system objects they own. This makes it possible that non-administrative users regain permission to deactivate, reactivate, or delete their personal caches if the cache folders use Apple's recommended default permission settings.

7.3.7 Version 6.96 (Build 210115)

- Communication with slow components of macOS in the background could sometimes be misinterpreted as alleged “hang” of the application. To avoid this, many user interface elements to control features of Time Machine, Spotlight, and CUPS have been changed over to asynchronous behavior. TinkerTool System will no longer wait for immediate response of macOS, but temporarily disable the affected controls until the corresponding operations have completed.
- This version fixes a problem with the creation of install media where installer apps of macOS 11 could be shown as invalid after such an app had been launched and quit in the same user login session.

7.3.8 Version 6.95 (Build 201214)

- Added support for the 4th generation of the System Management Controller used in the latest Mac models.
- The quick help feature was revised completely with updated links to new web pages of Apple that contain additional information on certain support and maintenance topics.
- Communication with external programs was optimized, especially regarding possible error situations, which could otherwise result in memory leaks, file handle exhaustion, or unexpected program termination.

7.3.9 Version 6.94 (Build 201111)

This version is aware of TinkerTool System 7 and the release of macOS 11.0 Big Sur.

7.3.10 Version 6.93 (Build 201007)

- The security feature that protects critical files has been modernized to respect recent changes in macOS.
- Added a new workaround and documentation for macOS defects that can cause Time Machine maintenance features to fail if the backup is network-based.
- Added a feature to detect broken versions of the installer application of macOS Sierra which are not capable of creating installation media. Apple has officially withdrawn any assertions that the Sierra 10.12.6 installation app is capable of performing this operation and TinkerTool System has been updated accordingly.
- Fixes a problem where the APFS pane is not shown or not updated correctly when attaching a disk containing a volume with future APFS features that is considered invalid by the running operating system.
- Fixes a problem where items in the table of privacy settings for applications may not have been translated to the user’s preferred language if running macOS Mojave.

7.3.11 Version 6.92 (Build 200910)

- Added SIP-protected startup option to control how a non-maskable interrupt (NMI) can be triggered. The settings and their description regarding start of the macOS remote kernel debugger have been clarified.

- The startup option to control how kernel panic messages should be shown was removed, because the underlying feature is no longer implemented in modern versions of macOS.

- Fixes a problem where network-based backups of Time Machine could not be selected for re-association with a volume if macOS Catalina was used.

- Fixes a packaging issue which could cause the quick help page for the ACL ID-Finder feature not to be shown.

- Includes the "build 200813 hotfix" which corrected minor issues with the user interface of version 6.91 for product activation. This affects remembering the position of the registration window, double-clicking a registration file, and the processing of manually entered prerequisite data for upgrade licenses.

7.3.12 Version 6.91 (Build 200804)

- Added preliminary support for creating installation media for and with macOS 11.

- Added support for detecting features of future APFS implementations.

- In specific situations, communication with Time Machine now runs in the background, so the user interface is more responsive even when using slow Time Machine devices.

- The accessibility has been further optimized by more than 800 changes in the user interface, especially for users of VoiceOver.

- The instructions for the emergency tool have been revised, taking into account the latest versions of the macOS Recovery operating system.

- Parts of the user interface for product activation and registration management have been redesigned.

7.3.13 Version 6.9 (Build 200702)

This version adds preliminary support for future operating systems.

7.3.14 Version 6.89 (Build 200527)

- This version adds support for macOS 10.14.6 Build 18G5033 (Security Update 2020–003): Because Apple intentionally sabotaged the operating system feature to ignore the macOS Catalina update in macOS Mojave, the corresponding settings have been removed.
- Added notification to suggest removal of the system setting to ignore the macOS Catalina update after an upgrade to macOS Catalina has been performed.
- Added a workaround for layout issues in some status displays for physical hard disks when working with specific third-party drives that provide excessively long serial numbers with more than 80 digits.
- Added a workaround for an issue with the authentication user interface of macOS where the system only showed an undocumented "ACMContextVerifyPolicyEx" error message.

7.3.15 Version 6.88 (Build 200427)

This version resolves a compatibility issue between the startup setting "Use special OS for next start: Recovery system" and specific firmware or Recovery OS versions: On some systems, the one-time setting remained permanently effective until clearing the parameter RAM. If you don't use this option of the startup setting, you won't need this update.

7.3.16 Version 6.87 (Build 200422)

- Added new feature to clear the staging area macOS uses to collect kernel extensions that wait for approval or denial by the user. This function is available at the tab item to clear the kernel extension cache.
- Added new feature to control the protected kernel option which disables processor-assisted support for Virtual Machines. This can help to avoid crashes of macOS Catalina when copying large amounts of data.
- The launch limit for unrestricted product evaluation without license has been increased by one, because macOS may relaunch the application to update its privacy settings. Six (6) launches per computer are permitted now.
- The application now accepts that the user provides a custom icon.
- Log files for kernel panics are now shown in a more readable fashion if macOS has stored them with embedded reports in JSON formats.
- Fixed a problem where Time Machine storage statistics reports could be shown with swapped lines and without a summary.
- Fixed a problem where the storage gain summary could sometimes show wrong numbers after Time Machine snapshots have been deleted.

- Fixed a problem where the display of the system's stored setting for handling trim commands on third-party AHCI SSDs could be wrong with some OS versions while the live policies for each affected drive were shown correctly.

7.3.17 Version 6.86 (Build 200323)

- Added support for macOS Catalina 10.15.4 and later. Note that previous versions of TinkerTool System are not compatible with this operating system version.

- Added a separate, fully resizable APFS overview window. This is helpful when performing complex APFS operations affecting multiple partitions or disks.

- Added percentage values to the Storage Space overview feature.

- Added new workarounds for continuing defects in macOS that can cause the system to lose preference and Resume settings when the user logs out too fast. The dialogs that indicate that the user must be logged out to continue a pending maintenance operation have been redesigned.

7.3.18 Version 6.85 (Build 200218)

- Added new feature to enable the classic startup chime on selected Macintosh model series released after summer 2016.

- Added new startup option to select special maintenance systems for the next restart. The Recovery OS, Internet Recovery, Apple Diagnostics, and Apple Diagnostics via Internet are available.

- Added new option to add available "signpost" information for software developers when retrieving log data from the operating system.

- The Startup pane was redesigned to consume less space on small screens.

- The Info pane was redesigned to consume less space on small screens.

- Internal diagnostic features have been optimized.

- Communication with the privileged component supports new features to ensure that data is processed in the correct order even under critical situations with high system load or strongly parallelized operations.

- Corrected a problem where some lines of log reports could be partially damaged or would appear in the wrong order.

7.3.19 Version 6.84 (Build 200117)

- The user interface to present the hierarchy of APFS objects was enhanced.
- The privacy protection warning that is shown when the user has not yet given consent for Full Disk Access by the application is now highlighted more prominently.
- Error messages and error handling have been optimized to better differentiate between the reasons of access failures caused by System Integrity Protection, privacy approval, user permissions, or other issues.
- This version adds a workaround for an ambiguity that could cause an incorrect display of production dates for Macintosh model series that have up-to-date operating system support for more than 10 years.
- This version fixes a problem where macOS may have refused to clone an APFS volume group if it was part of a container with multiple volume groups.
- Corrected a problem where resetting privacy settings did not work for all categories when using specific versions of macOS Catalina.
- The application now adds specific user guidance when resetting a privacy category that has influence onto the application itself.

7.3.20 Version 6.83 (Build 191211)

- Added new feature to get an overview on all details about the current APFS configuration, presenting the relationships between containers, physical disks, volume groups, and volumes.
- Added new feature to show the complete list of APFS snapshots on a volume.
- Added new feature to remove some or all APFS snapshots from a volume.
- Added new feature to copy APFS containers, volume groups, volumes, or snapshots by fast replication. (Only available for macOS 10.15 Catalina or later.)
- Added new feature to safely delete Time Machine snapshots from an active backup.
- Added new features to safely delete Time Machine snapshots, backup sets, or all Time Machine data from local disk drives.
- Added new user interface to show outstanding privacy approvals. If necessary, a missing approval will now be directly visible in the toolbar of the control window. This avoids that the application has to attempt a possibly failing operation before it can indicate a policy conflict to the user.
- Added new feature to create an optional text report when finding orphaned objects on a volume.

- The features to prevent volumes from automatic mounting or program execution will now additionally support invisible but mounted data volumes of non-running Catalina installations. This is helpful for users that have multiple copies of macOS Catalina installed. (Only necessary for macOS 10.15 or later.)
- The Info pane now supports retrieval of details about the Apple T2 processor in addition to the original iBridge system. The user interface has been modified accordingly.
- Printing the instructions for launching the emergency tool in recovery mode will now automatically resize the output to the printer's paper size to make sure the instructions are fully readable and not clipped.
- User guidance for changing file permission settings has been redesigned for cases where the operating system cannot fully support permissions.
- The application now adds warnings about possible APFS bugs affecting the handling of automatic ACL permission inheritance.

7.3.21 Version 6.82 (Build 191114)

- The check for slow system startup due to cleared NVRAM settings was modified in order not to cause false alarms on specific Mac Pro models.
- The check for correct communication with the security component was modified in order not to cause false alarms when the application was launched under extreme overload conditions.
- Added a fix for an issue with macOS 10.15.1 that could cause the warning for a missing user-based approval for full disk access not to be shown under specific conditions.
- Added a fix for an issue that could cause volumes with HFS+ format not to be offered for specific features of the System pane.
- Clarified the meaning of the "dark wake" startup option in the user interface and in the reference manual.

7.3.22 Version 6.81 (Build 191030)

- Added support for macOS 10.15.1.
- Added new feature to save the report on startup jobs into an RTF text file.
- Added new feature to download selected macOS installer apps provided by Apple without using the App Store (macOS Catalina only).
- Added new feature to suppress update notifications regarding macOS Catalina and the associated Dock reminder marker (macOS Mojave only).
- Added new feature to change the user account security policy for Remote Apple Events (macOS Catalina only).

- The feature to clear and refresh the driver (kernel extension) cache was reinstated for macOS Catalina.
- The feature to create macOS install media uses updated knowledge and revised safety policies regarding size requirements for target volumes.
- This version detects additional situations in the operating environment that can cause communication with system services to fail. The user will be automatically warned about such issues.
- The feature to search for software components of specific types as preparation for the Uninstall Assistant is no longer available when running macOS Catalina, because it no longer makes sense in modern system versions.

7.3.23 Version 6.8 (Build 191009)

- This version adds full support for macOS 10.15 Catalina.
- Added new feature to display the notarization state of applications or disk images (macOS Catalina only).
- The reference manuals have been updated with information that could not be published while the news embargo for macOS Catalina was active.
- Evaluation mode (“Try Before Buy” testing) is now unlocked for macOS Catalina.
- Fixed an issue where the list of startup jobs shown for the category User Service Login Item could be inaccurate, showing entries already deactivated.
- Fixed an issue where the data portion of the Catalina system volume was not offered for specific maintenance operations.

7.3.24 Version 6.7 (Build 190916)

- Added new feature to resize disk images (DMG files), hereby avoiding the flaws of Disk Utility.
- Added further support for future versions of macOS.
- The standalone version of TinkerTool System (tts in Single User mode) has been rewritten completely. The new “TinkerTool System for Recovery Mode” (ttsfrm) supersedes the previous emergency utility. This leads to the following advantages:
  - Compatibility with present and future versions of macOS is improved, because Single User mode is no longer officially supported by Apple.
  - For Macs with T2 security chip, it will no longer be necessary to change the security settings.
  - Issues with keyboard debouncing on certain Mac models are avoided.

  - Apple's Single User mode terminal is avoided, so readability on systems with Retina screens is fully restored.
  - The emergency tool can now use the full character set and a graphical user interface.
  - Separate, proactive installation steps for the emergency tool are no longer necessary.

- A graphical interface to disable or enable System Integrity Protection has been added to the emergency tool. The following features no longer make sense in macOS Recovery Mode and have been removed: file system check for the system volume, deleting Input Managers, rebuilding XPC caches, self-removal.

- The feature to create macOS installation media now accepts destination volumes which have slightly less than 8 GB of storage. This takes into account that Apple's installer is based on working with volumes (not disks) whose formatted capacity can be significantly lower than that of the physical storage device.

7.3.25 Version 6.6 (Build 190812)

- Many internal changes to support future operating system versions.

- Added new "ID Finder" feature for user and group accounts. After entering either account name, full name, POSIX identifier or UUID, the application will find the three remaining other items.

- Added new log type to retrieve the macOS log for disk write events.

- Added new log type to retrieve the macOS log for differential privacy submissions.

- Added new log type to retrieve the macOS log for iCloud services.

- Added new log type to retrieve the macOS log for baseband processor incidents.

- Added new log type to retrieve the macOS log for telephony monitoring.

- Added new log type to retrieve the macOS log for trust checks.

- Added new log type to retrieve the macOS log for iPhone software updates.

- Added new log type to retrieve the macOS log for iPad software updates.

- Added new log type to retrieve the macOS log proactive events.

- The user interface for license registration was redesigned.

7.3.26 Version 6.51 (Build 190625)

- This update is necessary to maintain compatibility with new versions of TinkerTool (7.4 or later).
- Added further support for future versions of macOS.
- Better guidance for the feature to remove unsuitable update notifications for users who have a customized update server set.
- Fixed a problem where the application could hang while beginning to display live output from external utility tools that have been started without privileged permissions.

7.3.27 Version 6.5 (Build 190611)

- Major architectural changes have been implemented that make it possible to make many long running operations interruptible.
- Added operating system setting for full protection against the "ZombieLoad" attack (Micro-Architectural Data Sampling Vulnerabilities). This setting can only be changed while System Integrity Protection is off.
- Added operating system setting to disable support of the assistant for Captive Networks (automatic configuration of access to "hotspots").
- Added new feature to automatically repair a specific damage of the Trash caused by third-party applications. This feature has no permanent user interface, but will be activated on demand during startup of the application if necessary.
- The system setting to optimize the operational parameters for use as server computer can now be activated even if macOS Server is not installed.
- Fixed a rare issue where the autostart settings of third-party services could not be determined correctly if the affected executable had unusual permission settings.
- Corrected a problem where new system services that have recently been added to macOS Mojave have not been shown as Apple-provided autostart component.
- Added preliminary support for future versions of macOS.

7.3.28 Version 6.4 (Build 190508)

- Added new feature to display "reveal in Finder" buttons for objects in the preflight list shown before deleting files as part of a clean-up operation.
- Added new feature to check a file system hierarchy against a user-specified limit for the length of absolute or relative paths.

- Added new warning feature for the ACL pane that makes the user aware if a selected file system may not support ACL permissions or uses virtual permission settings only. A new info panel offers guidance for inexperienced users.
- When propagating permissions onto a large folder hierarchy, the temporary memory consumption has been greatly reduced for specific use cases.
- Corrected an issue where specific locale settings of the user account could prevent a request to automatically free storage space of APFS Time Machine snapshots by a specified size to take any noticeable effect.

7.3.29 Version 6.3 (Build 190327)

- Added new feature to remove all local Time Machine APFS snapshots from a selected volume immediately.
- Added new setting to control whether FileVault should remove the decryption key for the system disk from memory when the system is entering standby mode.
- Added new feature to immediately eject all volumes when saving a modified automount configuration that have been set not to be automatically mounted by macOS.
- Added new feature to let the application copy itself to the system Applications folder if desired when the program is launched from the virtual distribution disk.
- The internal diagnostics features have been completely rewritten to be still operative in cases where operating system logging is not usable.
- The application has been made robust against dubious “cleaner” software that damages the launch configuration of the operating system.
- Better error messages for cases where users fail to register the application due to accidentally installing a wrong license file through dragging.

7.3.30 Version 6.2 (Build 190212)

- Added new diagnostics feature to retrieve the login time statistics from the operating system. Total login time per user or usage time per day can be reviewed.
- Added a workaround for a defect in macOS Mojave which can hang the operating system for 7 minutes if an application asks the operating system for the complete list of group accounts in a configuration with a network directory service. All user and group panels show only cached accounts now. The complete list of accounts can be retrieved on demand by clicking an extra button in the panels.
- User guidance for the selection of destination volumes was enhanced when creating macOS install media.
- Fixed a rare issue where the application showed the message “Interrupted system call” instead of the true error message when trying to delete specific files shielded by System Integrity Protection.

7.3.31 Version 6.1 (Build 190121)

- Added new option to the propagation of permission settings that can precisely simulate inheritance of Access Control Lists instead of copying them unconditionally. This emulates the behavior of old versions of macOS Server. The option to enforce activation of the inheritance flag was removed.

- Added new option to the propagation of permission settings that can be used to ignore all locked files during the operation. This emulates the behavior of old versions of macOS Server.

- Added new feature to the storage space overview feature that lists all system services that are currently registered to reclaim purgeable space.

- Added new feature to create a text report for the results of a bulk integrity check of applications. The report can be printed or be exported as RTF file.

- Added new feature to the check of absolute path lengths for deeply nested folders that not only tests existing objects, but additionally checks potential paths that would be created when copying the tested files to currently attached volumes.

- Added new preference setting to force the application to use Apple's "Identity Picker Window" instead of TinkerTool System's own user and group account management panels. This is less comfortable and does not offer OS accounts, but can be used as a workaround for a bug in the macOS Mojave directory services client which could lock the system for several minutes if one or more external directory services are configured when the UI for account selection was opened.

- Both the main application and the Standalone Utility now display the new "executable policy override" feature of System Integrity Protection if active in a custom configuration.

- Keyboard control of the Standalone Utility was optimized once again.

- The swap space volume (VM) is no longer offered as possible target for specific operations to avoid confusion.

- A layout issue of the path control that presents the top search folder in the results sheet for overlong paths has been resolved. This avoids that the panel can become wider than the screen.

- Broken symbolic links will no longer stop a propagation operation on the ACL pane, if the feature to propagate an Access Control List is active.

- Support code for legacy operating systems was removed from the Issues pane.

7.3.32 Version 6.02 (Build 181122)

- Added new feature to the Info pane to indicate whether your Mac uses Apple iBridge technology, which includes Apple T2 processors. A detail sheet shows additional information about its configuration.
- Added small changes to the non-English user interface for cases where Apple has modified the translation of specific terms as of macOS 10.14.1.
- The pane for the Emergency Tool has been redesigned and will now show a notice if your Mac uses an extremely small font in Single User Mode.
- Links to Apple documentation in connection with the Quick Help feature have been updated, or removed respectively, if Apple is no longer publishing specific information.
- Added a workaround for a keyboard control problem of Single User Mode that could affect the Standalone Utility. Depending on keyboard type and OS version, a single key press could sometimes be misinterpreted as multiple key events.
- Clarified the misleading label of the option to disable the dark wake feature of macOS.
- Fixed a compatibility problem with the automatic restart feature when the application was renamed.
- Internal technical update for changes in network infrastructure affecting the evaluation feature.
- The application will show more targeted error messages if licensing fails due to a misconfigured network firewall.
- The distribution package now uses the latest Gatekeeper security features.

7.3.33 Version 6.01 (Build 181002)

This is a maintenance update which corrects minor issues.

- Adds support for future versions of macOS Mojave.
- Adds a workaround for a declaration issue in the latest versions of the macOS Mojave installation App which could cause the installer not to be accepted as valid for the creation of install media.
- Several changes and optimizations in user guidance when working with startup jobs, login screen settings, and license registration.
- Fixes an issue where a private Software Update Server could not be used when macOS enforced HTTPS with TLS and extended validation.

- Fixes an issue where the application could not detect that it was already approved for full disk access on systems that had been upgraded from OS X 10.10 Yosemite.
- Fixes an issue where the user interface might not have been enabled for specific Time Machine features when the backup was stored on a network server.

7.3.34 Version 6.0 (Build 180918)

- Added full support for macOS 10.14 Mojave.
- Added new log type for slow application response to the feature to review classic system logs.
- Added new log type for slow shutdowns to the feature to review classic system logs.
- Added other new log types to the respective category in the log overview menu.
- Hundreds of other small changes and adjustments for macOS Mojave.
- The following features have been removed because they are no longer part of macOS Mojave, no longer make sense, or have been superseded by new macOS features: removing language support packages, validating login items, enforced Trash removal, repairing Safari font issues, repairing App Store licenses, enabling support for external accounts on the login screen, disabling support for text mode console login, temporary removal of swap files.
- The following features have moved to new locations: removal of Recent Items (User pane), reset of privacy settings (Applications pane).

TinkerTool System 6 begins a new product line. The section above lists changes in comparison to TinkerTool System 5, version 5.96. For more information about the version history of TinkerTool System 5, 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 5

The development of TinkerTool System 6 as a new application (and not as simple update of TinkerTool System 5) was necessary because Apple has significantly changed several aspects of macOS. This also had consequences on the user interface. Although the new application tries to make the switch between TinkerTool System 5 and TinkerTool System 6 as smoothly as possible, the locations of some features on the panes and their names had to change. If you have upgraded and you are searching for missing functions, please use the table below to find their new positions within the program.

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

Table A.1: Comparison of feature locations

Old Location	New Location
Issues > App Store Registration	*removed because either not compatible or no longer necessary with macOS 10.14*
Issues > Safari Fonts	*removed because no longer necessary with Safari 12*
Files > Trash	*removed because no longer necessary with the Mojave Finder*
Languages pane	*removed because more and more incompatible with nested application bundles and some third-party applications*
System > Network > Options for Connecting to AFP Servers	System > Network > Options for Connecting to File Servers
Login > Display Style	Login > Settings
Login > Special Features > Menu bar information	Login > Settings > Special Features
Login > Special Features > Don't allow to switch to text mode	*removed by Apple, no longer part of macOS*
Login > Special Features > Enable external accounts	*no longer supported*
User > Login Items > Verify Login Items	*removed because validation is now part of System Preferences*
Privacy > Recent Items	User > Recent Items
Privacy > App Privacy	Applications > Privacy
tts Standalone Utility > Advanced Features > Clean Virtual Memory Files	*removed because swap space is now always on a separate volume*

rebuild their caches, which can take days, depending on case. During this period, the 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 find out if my system might be affected by a cache-related problem?

TinkerTool System can assist you in identifying problems related to application-related cache files. The disadvantages of cache-cleaning can be avoided if possible. Perform the following steps:

1. Find a way to reliably reproduce the problem the system is experiencing.
2. Open the pane **Caches**.
3. Select the tab item **Application-Related Caches**.

4. Set check marks for all cache categories which could cause the problem.
5. Click the button **Deactivate selected caches**.
6. Let TinkerTool System restart the login session or computer.
7. Log in as the same user as before.
8. Try to reproduce the problem identified in step (1).
9. If the problem has been resolved, click the button **Discard previous caches**. If the problem can still be reproduced, click the button **Restore previous caches** and follow instructions.

Further information: The Pane Caches (section 2.2 on page 28).

A.4 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 tab 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 28).

A.5 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 tab 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 143).

A.6 What should I do when macOS can no longer open its Help Viewer?

The Help Viewer used to display the online documentation of applications suffers from several technical defects, so it might stop working correctly from time to time. To repair it, perform the following steps:

1. Open the pane **User**.
2. Select the tab item **Repair**.
3. Press the button **Repair now** in the section **Repair "Help Viewer"**.

Further information: The Pane User (section 5 on page 221).

A.7 Unlocking the Application

If you like to use TinkerTool System 6 without restrictions you'll have to purchase a registration that confirms that you have licensed the software.

1. Select the menu item **TinkerTool System** > **Unlock TinkerTool System**.... The window **Software Product Registration and Activation** appears.
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. Confirm your approval to let the application connect to the Internet.
5. 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 253)

Index