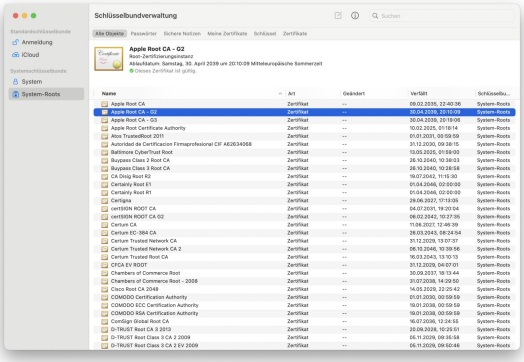
Eine Einführung in Schlüsselbunde und wie sie sich verändert haben

von Howard Oakley (eclecticligh.co) • Übersetzung KJM

Viele Anwendungen und Dienste sind auf Geheimnisse angewiesen. Ihr Browser benötigt zum Beispiel Zugriff auf die Kennwörter, die Sie für die Anmeldung bei Online-Diensten benötigen, und andere Apps müssen ihre eigenen geschützten Daten verwalten. Wenn Sie sich all diese Kennwörter merken und manuell eingeben müssten, bräuchten Sie eine sehr lange schriftliche Liste, und die Kennwörter, die Sie verwenden, müssten leicht zu merken und einzugeben sein. Schon zu Zeiten des klassischen Mac OS hat Apple beschlossen, die sichere Speicherung von Kennwörtern auf Systemebene zu unterstützen, um die Verwaltung und Verwendung von Kennwörtern, die nicht erraten werden können, zu vereinfachen, indem sie in einer sicheren Datenbank, dem Schlüsselbund, gespeichert werden.

Von dem Moment an, in dem Sie sich bei Ihrem Mac anmelden, bis zu dem Moment, in dem Sie sich wieder abmelden (und bei einigen Diensten auch dann, wenn gar kein Benutzer angemeldet ist), ist er auf Schlüsselbunde angewiesen, die in der Regel in den Schlüsselbund-Ordnern in den einzelnen Bibliotheksordnern gespeichert werden. Schlüsselbunde werden verwendet, um Geheimnisse zu speichern, darauf zuzugreifen und sie zu verwalten, einschließlich Passwörter für verschiedene Zwecke, Sicherheitszertifikate, private Schlüssel, Passkeys und sichere Notizen.

Bis OS X 10.9, als iCloud-Schlüsselbunde für Macs eingeführt wurden, basierten alle Schlüsselbunde auf Dateien, wobei der Master-Schlüsselbund derjenige ist, der bei der Anmeldung automatisch geöffnet wird, der Anmelde-Schlüsselbund. iOS-Geräte waren schon immer anders: Während Macs mehrere Schlüsselbunde haben, hat iOS nur einen, und dieser eine Schlüsselbund ist von Anfang an so konzipiert, dass er in iCloud gespeichert und durch die Secure Enclave geschützt wird. Apple bezeichnet diese beiden Typen als dateibasierte und datenschutzbasierte Schlüsselbunde.



Die Schlüsselbundverwaltung von macOS

Anmelde-Schlüsselbund

Der persönliche dateibasierte Schlüsselbund eines jeden Benutzers ist standardmäßig der Anmelde-Schlüsselbund, der sich in ~/Library/Keychains/login.keychain-db befindet. Dieser wird automatisch entsperrt, wenn sich der Benutzer anmeldet, da er das gleiche Passwort wie das Benutzerkonto hat. Hier sollte jeder Benutzer seine Zertifikate, sicheren Notizen usw. für den allgemeinen Gebrauch speichern.

Obwohl der Speicherplatz nicht gesperrt ist und gelesen und beschrieben werden kann, solange der Benutzer angemeldet ist, ist der Zugriff auf den Inhalt nicht garantiert. Wenn eine Anwendung das macOS-Sicherheitssystem aufruft, um ein gespeichertes Kennwort für ihre Verwendung abzurufen, bestimmt dieses System, ob der Anwendung der Zugriff auf diese Informationen vertraut wird und ob der Schlüsselbund gesperrt ist. Angenommen, das Kennwort ist dort gespeichert, die App ist vertrauenswürdig und der Schlüsselbund ist entsperrt, dann wird das Kennwort abgerufen und an die App zurückgegeben. Wenn die App nicht vertrauenswürdig ist oder der Schlüsselbund gesperrt ist, zeigt das Sicherheitssystem, nicht die App, ein Dialogfeld an, in dem das Kennwort für den Schlüsselbund zur Authentifizierung abgefragt wird, bevor es das Kennwort an die App weitergibt.

Der Benutzer kann nicht bestimmen, welche Apps aus Sicht des Sicherheitssystems vertrauenswürdig sind. Diese werden vom Sicherheitssystem, dem spezifischen Zugriff, den es einer App gewährt, und den einzelnen Elementen im Schlüsselbund des Benutzers bestimmt. In seiner restriktivsten Form kann das System allen anderen Anwendungen den Zugriff auf ein bestimmtes Geheimnis im Schlüsselbund verwehren, aber bestimmte Geheimnisse können auch von mehreren verschiedenen Anwendungen gemeinsam genutzt werden.

System-Schlüsselbunde

Für das System gibt es zwei wichtige Gruppen von Schlüsselbunden:

- in /System/Library/Keychains, in der SSV, befindet sich SystemRootCertificates und andere, die den Satz von Root-Sicherheitszertifikaten für diese Version von macOS bereitstellen;
- in /Library/Keychains befinden sich der System-Schlüsselbund und andere, die Zertifikate und Passwörter enthalten, die für alle Benutzer erforderlich sind, einschließlich derer, die Zugriff auf die Wi-Fi-Verbindungen des Macs erhalten.

Benutzerdefinierte Schlüsselbunde

Apps und Benutzer können auch ihre eigenen Schlüsselbunde erstellen. Zu den Schlüsselbunden, die ich auf meinen Macs habe, gehören gemeinsame Schlüsselbunde mit virtuellen Maschinen von Parallels, mehrere für Microsoft-Anwendungen und einige für Produkte von Adobe. Ich neige auch dazu, eine Kopie des Anmelde-Schlüsselbundes meines letzten Macs zu erstellen und sie unter einem anderen Namen nach ~/Library/Keychains zu kopieren, damit ich, falls ich bei der Migration auf einen neuen Mac wichtige Zertifikate oder Passwörter vergessen habe, diese dort finden kann.

Obwohl diese zusätzlichen Schlüsselbunde in den Suchpfad für den Schlüsselbund aufgenommen werden können, werden sie, wenn macOS nach einem Geheimnis in einem Schlüsselbund sucht, im Gegensatz zum Anmeldeschlüsselbund normalerweise gesperrt gehalten. Wenn ich oder eine Anwendung auf sie zugreifen möchte, werde ich nach dem Kennwort des Schlüsselbundes gefragt. Bei alten Anmeldeschlüsselbunden ist das natürlich nur mein altes Anmeldekennwort für diesen Mac.

Datenschutz-Schlüsselbund

Seit OS X 10.9 gibt es auf Macs auch nur noch einen einzigen Datenschutz-Schlüsselbund, auf den über eine andere API zugegriffen wird. Wenn Sie Ihren Schlüsselbund in iCloud freigeben, ist dies die lokale Kopie des freigegebenen Schlüsselbundes und wird als iCloud-Schlüsselbund bezeichnet; wenn Sie ihn nicht in iCloud freigeben, wird er stattdessen als Lokale Objekte bezeichnet. Die lokale Kopie davon wird normalerweise in ~/Library/Keychains/[UUID]/keychain-2.db gespeichert, wobei die UUID diejenige ist, die diesem Mac zugewiesen wurde.

Der Datenschutz-Schlüsselbund speichert alle Standardtypen von Geheimnissen, einschließlich Internet- und andere Passwörter, Zertifikate, Schlüssel und Passkeys, obwohl er normalerweise nicht für sichere Notizen verwendet wird. Vor macOS 11 wurden nur Internet-Passwörter mit iCloud synchronisiert, aber ab Big Sur werden alle Inhalte synchronisiert, einschließlich der Passwörter. Im Gegensatz zu dateibasierten Schlüsselbunden können die Geheimnisse im Datenschutz-Schlüsselbund durch die Secure Enclave geschützt werden und können daher durch biometrische Merkmale wie Touch ID (und unter iOS und iPadOS auch Face ID) geschützt werden. Daher sind sie für Passkeys erforderlich, die von herkömmlichen dateibasierten Schlüsselbunde nicht unterstützt zu werden scheinen.

Werkzeuge

Das gebündelte Tool für die Arbeit mit Schlüsselbunden ist die App **Schlüsselbundverwaltung** in /Programme/Dienstprogramme, und einige der Funktionen des Befehlstools `security`. Einige Dienstprogramme von Drittanbietern, darunter mein eigenes kostenloses Mints, liefern zusätzliche Informationen, die bei der Lösung von Schlüsselbundproblemen hilfreich sein können. Diese basieren jedoch größtenteils auf den APIs für die Arbeit mit dateibasierten Schlüsselbunden und haben nur begrenzte Fähigkeiten bei der Arbeit mit Datenschutz-Schlüsselbunden. Keychain Access kann beispielsweise nur Kennwortelemente in iCloud- und lokalen Schlüsselbunden anzeigen und mit ihnen arbeiten, aber keinen Zugriff auf Zertifikate, Schlüssel oder Passkeys bieten, die dort gespeichert sind, obwohl mir nicht bekannt ist, dass Apple dies in der Hilfe der App oder in Man Security dokumentiert. Derzeit scheint Apple kein Befehlswerkzeug anzubieten, das vollständig mit Data Protection-Schlüsselbunde arbeitet, und das scheint Absicht zu sein.

Die beste Möglichkeit, mit Passwörtern und Schlüsseln zu arbeiten, die in einem Datenschutz-Schlüsselbund gespeichert sind, ist der Abschnitt Passwörter in den Systemeinstellungen oder sein Äquivalent in den Safari-Einstellungen.

Zukunft

Derzeit unterstützt macOS noch Schlüsselbunde in ihrem ursprünglichen klassischen Mac OS-Format, und dateibasierte Schlüsselbunde sind nach wie vor weit verbreitet. Da sie niemals das gleiche Sicherheitsniveau wie Datenschutz-Schlüsselbunde bieten und nicht von Biometrie oder Secure Enclave profitieren können, ist Apple bestrebt, so weit wie möglich zu Datenschutz-Schlüsselbunden überzugehen. Es heißt sogar, dass „der dateibasierte Schlüsselbund auf dem Weg zur Abschaffung ist. Er ist nicht offiziell veraltet, aber einige der ihn umgebenden APIs sind es.“ Dieser Weg liegt jedoch noch weit vor uns, denn er erfordert, dass jede App, die auf Schlüsselbunde angewiesen ist, das neue API und die vollständige Zuverlässigkeit übernimmt.

Apple hat noch ein großes Problem zu lösen: Code wie LaunchDaemons und LaunchAgents, die nicht in einem Benutzerkontext, sondern über Launchd laufen, können derzeit nicht auf einen Datenschutz-Schlüsselbund zugreifen und müssen sich auf dateibasierte Schlüsselbunde verlassen. Traditionelle Schlüsselbunde werden noch nicht so bald verschwinden.

Einstellungen, Berechtigungen und Problemlösungen

von Howard Oakley (eclecticligh.co) • Übersetzung KJM

Seit der ersten Betaversion leidet Mac OS X unter undefinierten und weit verbreiteten Problemen, von denen man annimmt, dass sie auf eine Beschädigung der vom System verwendeten Einstellungsdateien zurückzuführen sind.

Reparieren von Berechtigungen Mark 1

Bis zur Einführung des Systemintegritätsschutzes (SIP) in 10.11 El Capitan resultierten diese Probleme im Allgemeinen daraus, dass Dateien innerhalb des Systems falsche Berechtigungen erhielten. Um dies zu beheben, verfügte das Festplattendienstprogramm über eine Funktion, mit der es die Berechtigungen aller wichtigen Teile des Systems auf der Grundlage der in den BoM-Dateien für Systemaktualisierungen und Installationen enthaltenen Informationen überprüfen und reparieren konnte. Das Reparieren von Berechtigungen auf diese Weise wurde zu einem der wichtigsten Allheilmittel in diesen älteren Versionen.

Obwohl SIP in erster Linie für einen besseren Sicherheitsschutz gedacht war, bestand einer der Vorteile darin, dass es weitgehend verhinderte, dass Systemdateien falsche Berechtigungen erhielten, und die Funktion zum Reparieren von Berechtigungen wurde aus dem Festplattendienstprogramm entfernt. Auf jeden Fall war es aufgrund von SIP nicht mehr möglich, die Berechtigungen von Dateien, die durch SIP geschützt waren, mit dem Festplatten-Dienstprogramm zu ändern.

Reparieren von Berechtigungen Mark 2

Als macOS 10.12 Sierra veröffentlicht wurde, trat ein anderes Problem auf, bei dem Berechtigungen offenbar nicht in Systemdateien im Allgemeinen, sondern im Home-Ordner des Benutzers und speziell in ~/Library/Preferences falsch gesetzt wurden. Um dieses Problem zu beheben, fügte Apple dem bereits komplexen Befehlswerkzeug `diskutil` ein neues Verb hinzu, `resetUserPermissions`, und beschrieb dessen Verwendung in einer Support-Notiz. Es ist vielleicht kein Zufall, dass dieses neue Problem etwa zur gleichen Zeit auftrat, als `cfprefsd` die Verwaltung dieser Einstellungsdateien übernahm.

Zu dieser Zeit wurden die folgenden Probleme von Apple auf falsche Berechtigungen in ~/Library/Preferences zurückgeführt:

- Änderungen an den Einstellungen, insbesondere an denen der Systemeinstellungen, bleiben nicht erhalten;
- Änderungen, die am Dock vorgenommen wurden, werden nicht übernommen;
- Sie werden aufgefordert, sich zu authentifizieren, wenn Sie versuchen, einige Ordner in Ihrem Home-Ordner zu verschieben oder zu ändern;
- beim Versuch zu speichern, wird Ihnen mitgeteilt, dass die Datei gesperrt ist oder dass Sie keine Berechtigung haben;
- Vorschau, TextEdit und App Store-Anwendungen (die in einer Sandbox laufen) können beim Öffnen abstürzen;
- es werden Warnungen angezeigt, dass auf der Startfestplatte kein Platz mehr für den Anwendungsspeicher verfügbar ist;
- Safari oder SafariDAVClient verbrauchen große Mengen an Ressourcen (Speicher);
- der Mac läuft sehr langsam;
- iTunes kann ein Gerät nicht synchronisieren;
- es gibt Probleme mit Fotos oder iPhoto-Mediatheken, einschließlich der Unfähigkeit, in die Mediathek zu importieren, oder das Vergessen der Mediathek bei jedem Öffnen der App.

Die meisten, wenn nicht alle dieser Probleme könnten auf Fehler in `cfprefsd` zurückzuführen sein.

Behebung von Einstellungsproblemen

Vor drei Jahren änderte Apple seine Empfehlungen dahingehend, das neue Tool `repairHomePermissions` im Wiederherstellungsmodus auszuführen und dann macOS neu zu installieren. Kurz darauf, im Juni 2020, als Big Sur noch in der Beta-Phase war, zog Apple diesen Support-Hinweis und jeden Hinweis auf die Reparatur von Berechtigungen zurück, obwohl das Tool im Wiederherstellungsmodus sogar auf Apple-Silizium-Macs noch verfügbar ist.

Unabhängig von Support-Hinweisen gibt es immer noch Gelegenheiten, bei denen Einstellungsdateien und ihre Berechtigungen Probleme verursachen können. Diese lassen sich in zwei Kategorien einteilen:

- Eine beschädigte oder fehlerhafte Einstellungsdatei kann zum Absturz einer Anwendung oder eines anderen Codes führen, normalerweise beim Start;
- Falsche Zugriffsrechte auf eine oder mehrere Einstellungsdateien können verhindern, dass sie funktionieren, und unbestimmte und weit verbreitete Probleme verursachen, wie früher.

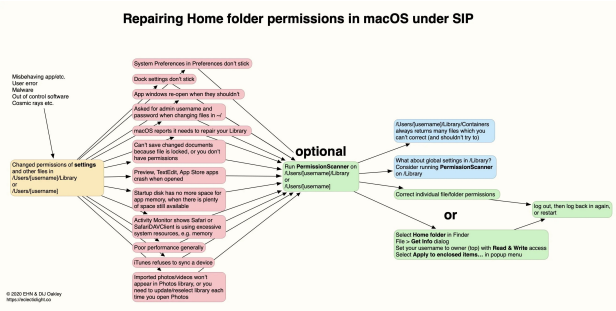
Obwohl diese Probleme jetzt viel seltener auftreten und die SSV sicherstellt, dass Systemdateien nicht mehr beschädigt werden können, wie es vor SIP der Fall war, ist es wichtig zu wissen, wie man mit ihnen umgeht.

Löschen einer beschädigten Einstellungsdatei

In den meisten Fällen kann eine Einstellungsdatei auf normale Weise gelöscht werden, entweder im Finder oder im Terminal, und sie kehrt nicht zurück, da sie derzeit nicht von `cfprefsd` verwaltet wird. Die Alternative ist die Verwendung von `defaults`: `defaults delete com.mycompany.appname` löscht alle Schlüssel-Wert-Paare innerhalb der Einstellungsdatei für com.mycompany.appname und hinterlässt nur die leere Eigenschaftsliste. Dies hat den Vorteil, dass es verwendet werden kann, wenn `cfprefsd` den Inhalt dieser Datei verwaltet, und sollte daher immer zuverlässig sein. Vorausgesetzt, die Anwendung verwaltet die Einstellungen korrekt mit UserDefaults, sollte sie in der Lage sein, die leere Eigenschaftsliste beim nächsten Start der Anwendung wieder aufzufüllen.

Berechtigungen für Einstellungsdateien prüfen und reparieren

Abgesehen von dem Wiederherstellungswerkzeug `repairHomePermissions` bietet macOS keine Unterstützung, um sicherzustellen, dass Einstellungsdateien und andere Dateien die richtigen Berechtigungen haben. Vor drei Jahren schlug ich eine Methode vor, bei der mein kostenloses Dienstprogramm PermissionScanner verwendet werden kann, um festzustellen, bei welchen Dateien die Berechtigungen korrigiert werden müssen. Es funktioniert immer noch in Ventura und kann, wenn man es sorgfältig einsetzt, diese Probleme lösen.



Die größte Vorsicht ist geboten, wenn Sie mit Dateien in ~/Library/Containers, ~/Library/Group Containers, ~/Library/Daemon Containers und ähnlichen verwalteten Ordnern arbeiten. Da es sich hierbei um Sandkästen handelt, werden sie von macOS anders verwaltet und eine Manipulation ihres Inhalts hat wahrscheinlich unbeabsichtigte Auswirkungen.

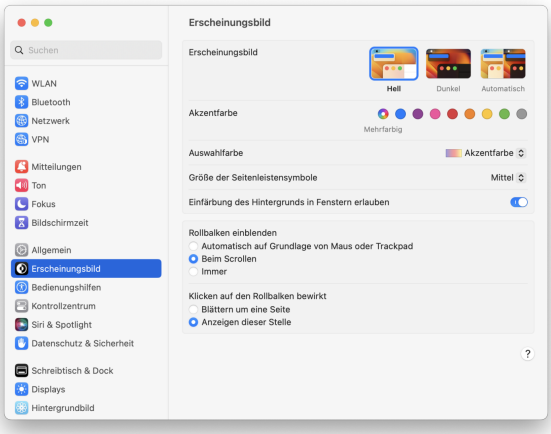
Zusammenfassung

- Das Reparieren von Berechtigungen auf Systemdateien wurde mit SIP in El Capitan eingestellt.
- Das Reparieren von Berechtigungen für Einstellungsdateien im Home-Ordner wird von Apple seit Big Sur nicht mehr empfohlen.
- Sicheres und robustes Löschen des Inhalts einer Einstellungsdatei kann mit dem Standard-Löschverfahren durchgeführt werden.
- Die Überprüfung und Reparatur von Einstellungsdateien und anderen Dateien kann durch PermissionScanner unterstützt werden.
- Manipulieren Sie nicht an Dateien in ~/Library/Containers, ~/Library/Group Containers und ähnlichen Ordnern.
- Das Reparieren von Berechtigungen ist nicht mehr das Allheilmittel, das es vor Big Sur war.

Systemeinstellungen außerhalb der macOS-Systemeinstellungen

von „Nicolas“ (ifun.de), Quelle: Howard Oakley

Nicht alle Systemeinstellungen des macOS-Betriebssystems lassen sich auch in dem gleichnamigen Dienstprogramm konfigurieren, das Apple erst kürzlich neu gestaltet und mit einer komplett neuen Oberfläche versehen hat. Viele der Basiskonfigurationen wurden im Laufe der Jahre auch an anderer Anwendungen ausgelagert oder in versteckte Bereiche des Macs verschoben.



Wer etwa die Anwendung festlegen möchte, die der Mac standardmäßig zum Senden und Empfangen von E-Mails einsetzen soll, der muss in die App-Einstellung der offiziellen Mail-Applikation abtauchen. Die Standard-App für den Aufbau von Anrufen, lässt sich nur innerhalb der FaceTime Applikation konfiguriert.

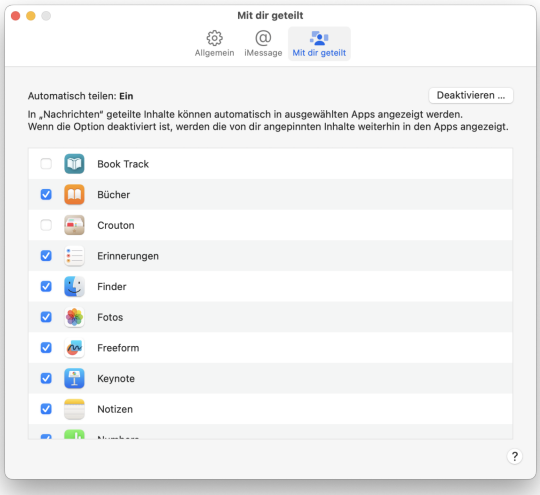
Orte, die der Software-Entwickler Howard Oakley in diesem Blog-Eintrag zusammengestellt hat und damit an die zahlreichen versteckten Systemeinstellungen erinnert, die sich außerhalb der Systemeinstellungen-Applikation befinden.

Einstellungen in anderen Apps versteckt

Zwar bieten sich mehrere Freeware-Anwendungen wie etwa das TinkerTool oder Onyx an, um die versteckten Systemeinstellungen mit einer einheitlichen Oberfläche zu konfigurieren, dies ändert jedoch nichts an der Tatsache, dass es aus Nutzersicht begrüßenswert wäre, alle vorhandenen Systemeinstellungen auch in der dafür zuständigen Werksanwendung vorzufinden.

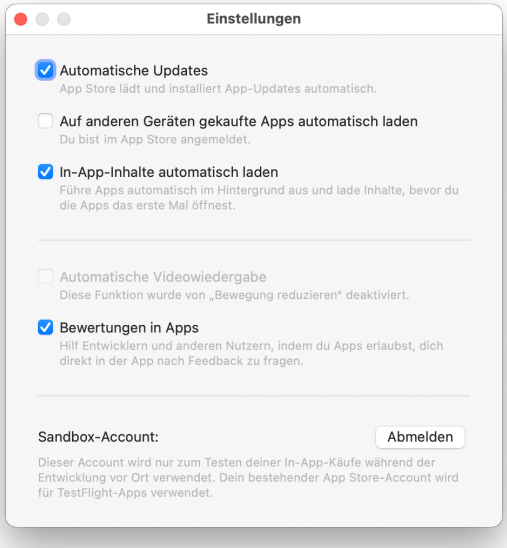
„Mit dir geteilt“

In den Einstellungen der Nachrichten-App lässt sich wählen, in welchen Apps die in Nachrichten geteilten Inhalte angezeigt werden sollen.



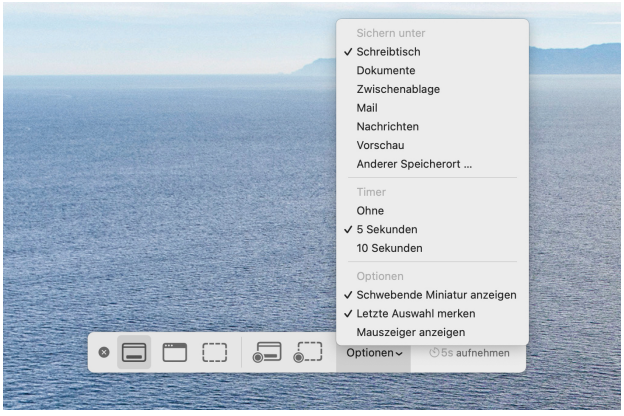
Automatische App Store Updates

Lassen sich im Bereich Allgemein > Softwareupdates der Systemeinstellungen, aber auch in den Einstellungen des App Stores konfigurieren.



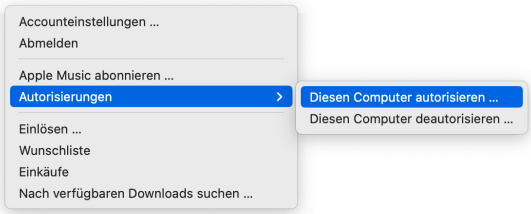
Bildschirmfoto-Optionen

In der Bildschirmfoto-App konfigurierbar. Aufrufen mit Command + Shift + 5, dann „Optionen“ wählen.



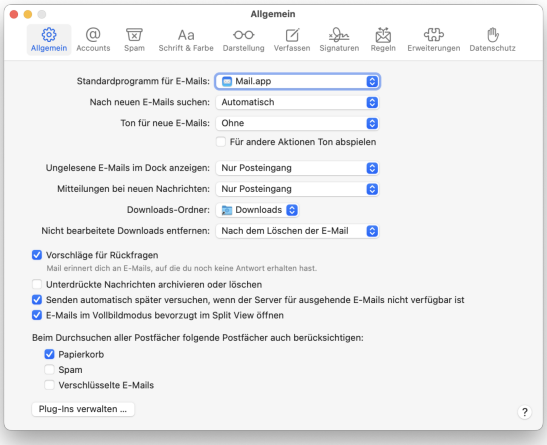
iTunes Autorisation

5 Macs können für iTunes-Käufe freigeschaltet werden. Musik-App > Account > Autorisierungen.



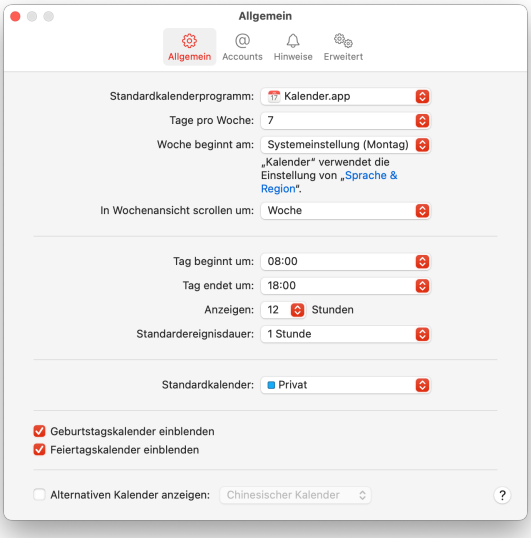
Standard E-Mail-App

In den Einstellungen der Mail-App konfigurierbar.



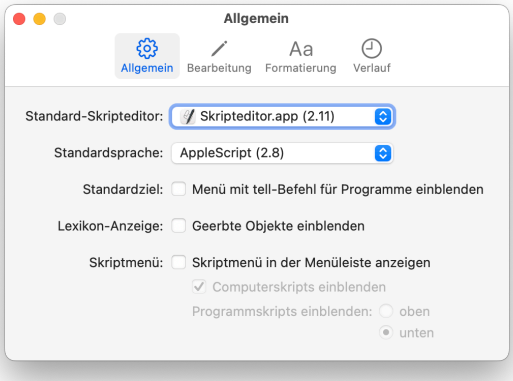
Standard Kalender-App

In den Einstellungen der Kalender-App konfigurierbar.



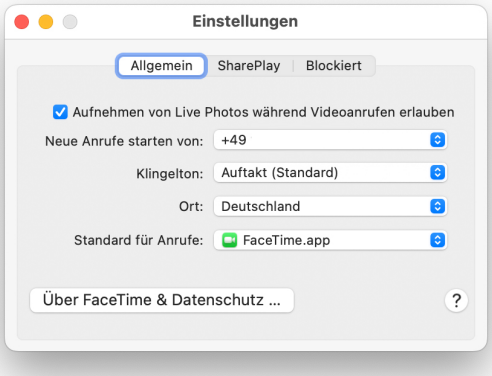
Standard Skripteditor

In den Einstellungen des Skripteditors konfigurierbar.



Standard-App für Anrufe

In den FaceTime-Einstellungen konfigurierbar.



Standard-Webbrowser

In den Safari-Einstellungen konfigurierbar.