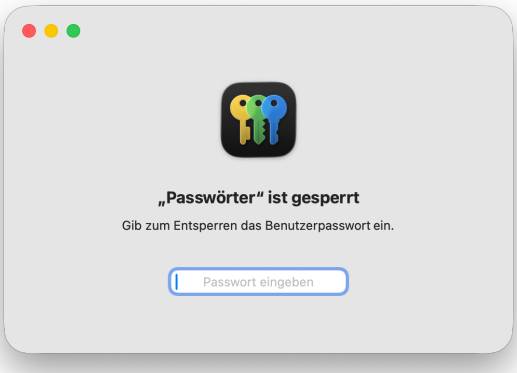
Apple erklärt, wie der Umstieg gelingen soll

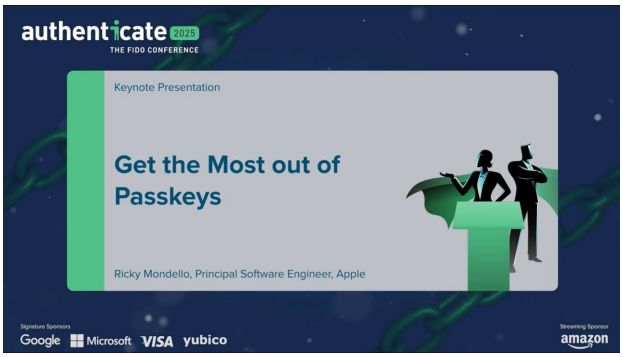
Passkeys statt Passwörter

Quelle: Nicolas auf ifun.de

Apple will die klassische Passwortanmeldung langfristig mit sogenannten Passkeys ersetzen. In einem aktuellen YouTube-Video erklärt Ricky Mondello, leitender Softwareingenieur bei Apple, wie dieser Wechsel gelingen soll.



Der Vortrag richtet sich an Entwickler, bietet aber auch für technisch interessierte Nutzer viele hilfreiche Einblicke. Wir empfehlen das Video allen, die bereits erste Berührungen mit Passkeys hatten, aber noch nicht ganz verstehen, warum diese die herkömmlichen Logins ersetzen sollen.

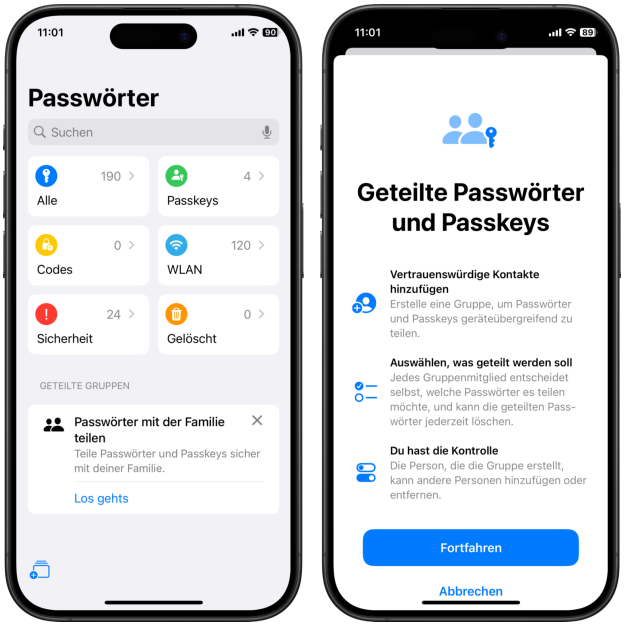


Auf das Bild klicken, um das Webvideo anzuschauen!

Im Mittelpunkt steht die Idee, Logins nicht nur sicherer, sondern auch deutlich einfacher zu gestalten. Passkeys speichern keine Passwörter auf Servern. Stattdessen erzeugen sie ein verschlüsseltes Schlüsselpaar auf dem Gerät des Nutzers. Die Anmeldung erfolgt über biometrische Verfahren wie Face ID oder Touch ID. So lassen sich Phishing-Angriffe und viele andere Sicherheitsrisiken vermeiden. Laut Mondello profitieren davon nicht nur Nutzer, sondern auch Anbieter von Webdiensten und Apps.

Neue Funktionen für Entwickler + Diensteanbieter

Der Vortrag stellt mehrere neue Schnittstellen vor, die Apple für App-Entwickler bereitstellt. Dazu gehört etwa die „Account Creation API", mit der sich neue Nutzerkonten schnell und ohne Passworteingabe anlegen lassen. Die Daten dafür, etwa Name, E-Mail-Adresse oder Telefonnummer, werden aus bestehenden Systeminformationen vorgeschlagen. Auch bestehende Nutzerkonten lassen sich über sogenannte automatische Passkey-Upgrades umstellen, wenn sich Nutzer mit einem Passwortmanager anmelden.



Ein weiteres Thema ist die Nutzerführung bei der Anmeldung. Viele Menschen wissen beim nächsten App-Start oft nicht mehr, wie sie sich ursprünglich registriert haben. Eine neue Systemfunktion zeigt ihnen automatisch passende gespeicherte Zugangsdaten an. Wenn keine vorhanden sind, bleibt die App-Oberfläche unverändert.

Schrittweise weg vom Passwort

Apple ruft Entwickler dazu auf, sich aktiv mit der Umstellung auseinanderzusetzen. Dienste, die Passkeys unterstützen, könnten ihren Nutzern schrittweise erlauben, das Passwort aus dem Konto zu entfernen. In Apples Systemen gibt es dafür eine Schnittstelle, die auch Passwortmanager darüber informiert, dass ein Konto künftig passwortfrei verwaltet wird.

Der Vortrag schließt mit einem Ausblick auf die zunehmende Interoperabilität zwischen Apps und Plattformen, etwa durch ein standardisiertes Austauschformat für Zugangsdaten.

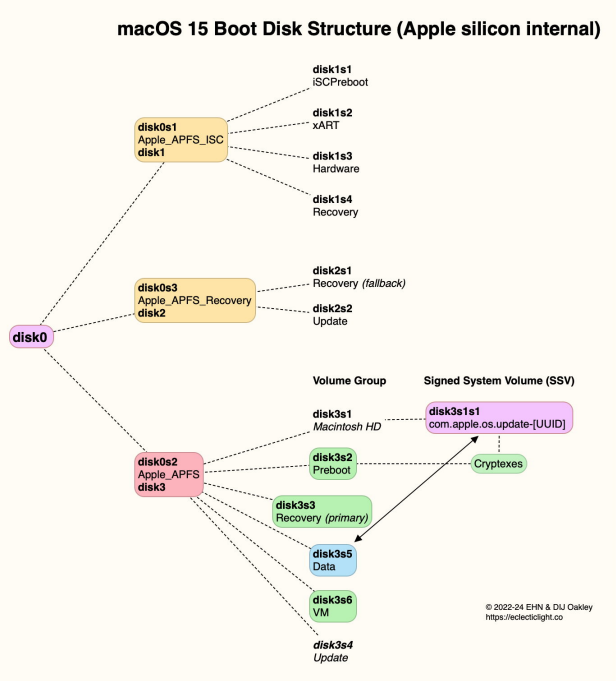
„Alle Inhalte und Einstellungen löschen“ tut genau das, was es sagt

von Howard Oakley, eclecticlight.co • Übersetzung: KJM

Das sichere Löschen von SSDs war lange Zeit ein Problem, das bei Macs mit T2- oder Apple-Silizium-Chips mit der Einführung von „Alle Inhalte und Einstellungen löschen“ („Erase All Content and Settings“, kurz: **EACAS**) vor vier Jahren in macOS Monterey gelöst wurde. In diesem Artikel wird erklärt, wie es funktioniert, was es tut und wann Sie es verwenden sollten.

Boot-Festplatte

Während Intel-Macs einfacher aufgebaut sind, ist die interne SSD eines Apple-Silizium-Macs in drei APFS-Container/Partitionen unterteilt.



Intel-Macs haben denselben Apple-APFS-Container mit der Boot-Volume-Gruppe, aber die beiden anderen Container werden durch eine einzige kleine EFI-Partition ersetzt.

macOS verwaltet und verwendet die ersten beiden Container, ISC und Recovery, wobei der Container mit der Boot Volume Group für uns von Interesse ist. Dieser umfasst das System- und das Datenvolume, wobei ersteres zu einem schreibgeschützten Snapshot gemacht wird, der als Signed System Volume (SSV) gemountet wird und macOS enthält. Alles, was Sie als Benutzer installieren, einschließlich Apps und Ihrem Home-Ordner, befindet sich im Datenvolume, das automatisch verschlüsselt wird, auch wenn Sie den FileVault nicht selbst aktiviert haben.

Datenvolume

Da das Datenvolume immer verschlüsselt ist, besteht die beste Möglichkeit, seinen gesamten Inhalt sicher zu löschen, darin, seinen Verschlüsselungsschlüssel zu zerstören. Vorausgesetzt, dies kann zuverlässig durchgeführt werden, sodass der Schlüssel niemals wiederhergestellt werden kann, kann niemand den Inhalt entschlüsseln. (Es besteht die Erwartung, dass es eines Tages möglich sein könnte, die Verschlüsselung mit Quantencomputern zu knacken, aber darüber sollten Sie sich derzeit keine Gedanken machen.)

Der zur Verschlüsselung des Datenvolumens verwendete Verschlüsselungsschlüssel ist selbst verschlüsselt und Teil des Mechanismus, den FileVault verwendet, wenn es aktiviert ist. Um sicherzustellen, dass diese Verschlüsselungsschlüssel die Secure Enclave nicht verlassen, werden sie erneut verschlüsselt, und der von EACAS zerstörte Schlüssel ist einer davon. macOS verwendet außerdem Anti-Replay-Techniken, um sicherzustellen, dass frühere Schlüssel nicht wiederverwendet werden können.

Zusätzliche Funktionen

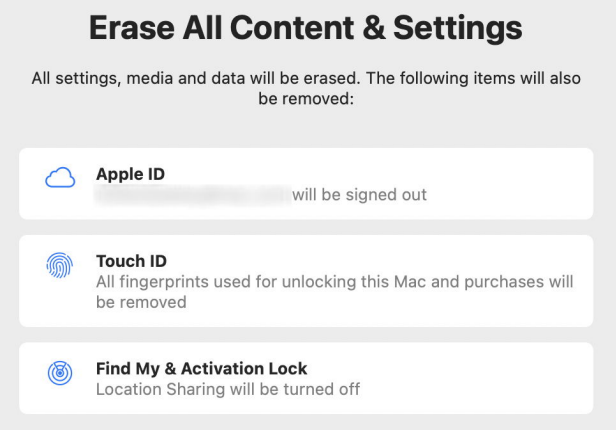
Neben der Zerstörung des Verschlüsselungsschlüssels für das Datenvolume führt EACAS weitere nützliche Aufgaben aus. Dazu gehören das Abmelden von Ihrem Apple-Konto, einschließlich iCloud und iCloud Drive, das Löschen aller für Touch ID verwendeten Fingerabdrücke und das Deaktivieren der Standortfreigabe, um „Find My“ und die Aktivierungssperre zu deaktivieren.

Obwohl ich keine offiziellen Angaben dazu finden kann, welche Daten noch von EACAS gelöscht werden, gehe ich davon aus, dass auch alle in Apple Silicon Macs gespeicherten LocalPolicy-Datensätze zerstört werden. LocalPolicy autorisiert den Zugriff auf externe bootfähige Festplatten, sodass diejenigen, die eine externe Festplatte für den Start ihres Mac konfiguriert haben, diese wahrscheinlich erneut autorisieren müssen, bevor sie diesen Mac wieder starten können.

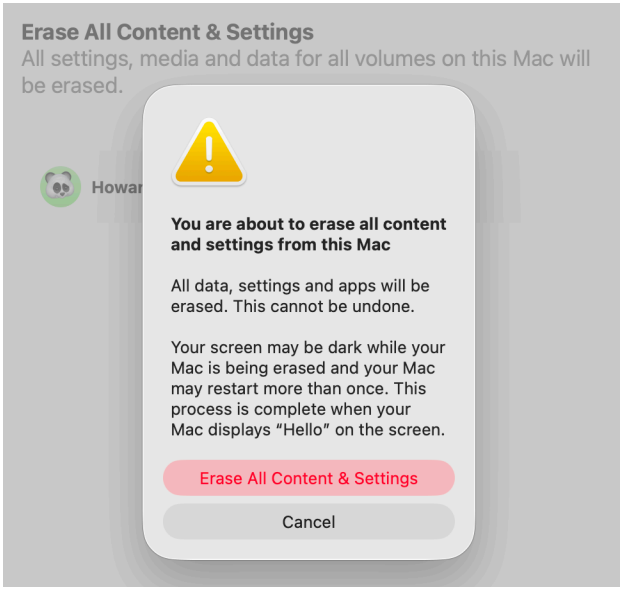
Was EACAS jedoch nicht tut, ist, Sie aus Cloud-Diensten von Drittanbietern oder anderen Diensten wie Adobe Creative Cloud abzumelden oder diesen Mac für Apple-Medien wie Musik zu deaktivieren. Auch auf das SSV (das versiegelte System-Volume) Ihres Macs hat EACAS keinen Einfluss: Dieses bleibt unverändert; der Mac läuft weiterhin mit derselben Version von macOS.

So verwenden Sie EACAS

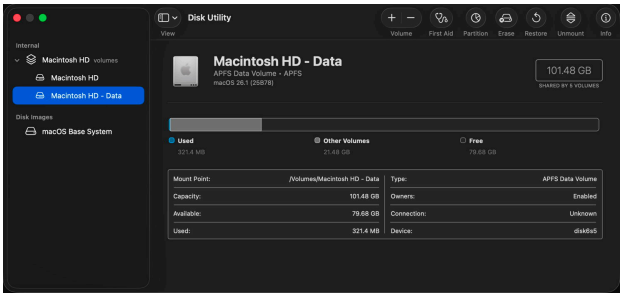
Starten Sie EACAS über „Systemeinstellungen“ > „Allgemein“ > „Übertragen oder zurücksetzen“ > „Alle Inhalte und Einstellungen löschen…“. In älteren Versionen von macOS, die noch System Preferences verwenden, öffnen Sie diese und wählen Sie den Befehl im App-Menü aus.



Wenn Sie fortfahren, sollten Sie eine letzte Warnung sehen, bevor der Inhalt des Datenvolumens in den großen Bit-Speicher im Himmel verschwindet.



Was von Ihrem Datenvolumen übrig bleibt, hier im Wiederherstellungsmodus angezeigt, sind nur noch etwa 300 MB.



Wann sollte EACAS verwendet werden?

Wenn Sie das Datenvolume Ihres Mac löschen möchten, um dessen Benutzer neu zu installieren, ist EACAS die einfachste und schnellste Methode dafür, ohne dass Sie den Wiederherstellungsmodus starten müssen. Die zusätzlichen Funktionen stellen sicher, dass bei der Installation des neuen Hauptbenutzers alles ordnungsgemäß funktioniert und keine „Geister-Macs“ aus der Vergangenheit zurückbleiben.

Dies ist die Methode der Wahl, wenn Sie Ihren Mac für die Entsorgung vorbereiten, insbesondere wenn Sie ihn an jemand anderen weitergeben, da sie sicherstellt, dass niemand die in Ihrem Home-Ordner oder an anderer Stelle auf dem Datenvolume gespeicherten Daten wiederherstellen kann. Um dies manuell durchzuführen, müssen Sie eine Reihe zusätzlicher Schritte ausführen, die in EACAS fast alle automatisch erfolgen.

Die einzige Situation, in der Sie wahrscheinlich eine andere Methode bevorzugen, ist, wenn Sie sowohl das Daten- als auch das Systemvolume löschen möchten, beispielsweise um zu einer älteren Version von macOS zurückzukehren. Sie können dies zwar mit dem Festplatten-Dienstprogramm im Wiederherstellungsmodus tun, dabei wird jedoch nicht die passende Firmware installiert. Wenn Sie wirklich zu den Werkseinstellungen zurückkehren möchten, ist es am besten, den Mac in den DFU-Modus zu versetzen und ihn dann aus der IPSW-Image-Datei für diese Version von macOS wiederherzustellen. Dazu benötigen Sie zwar einen zweiten Mac, aber es geht schnell und ist umfassend.

Eine weitere Vorsichtsmaßnahme: Verwenden Sie EACAS niemals auf einer macOS-VM, da eine Wiederherstellung unwahrscheinlich ist. Es ist sinnvoller, einfach die gesamte VM zu löschen und damit fertig zu sein.

Zusammenfassung

- EACAS führt eine sichere Löschung des Datenvolumens sowie einige nützliche Extras durch.
- Es ist die Methode der Wahl, um Ihren Mac für die Entsorgung vorzubereiten.
- Es eignet sich auch für zum Löschen von Benutzerdaten, bevor Sie Ihren Mac unter Verwendung des vorhandenen macOS neu einrichten.
- Wenn Sie auch das Systemvolume löschen möchten, um macOS neu zu installieren, führen Sie eine Wiederherstellung aus einer IPSW-Datei im DFU-Modus durch.

Deinen Mac löschen und auf die Werkseinstellungen zurücksetzen

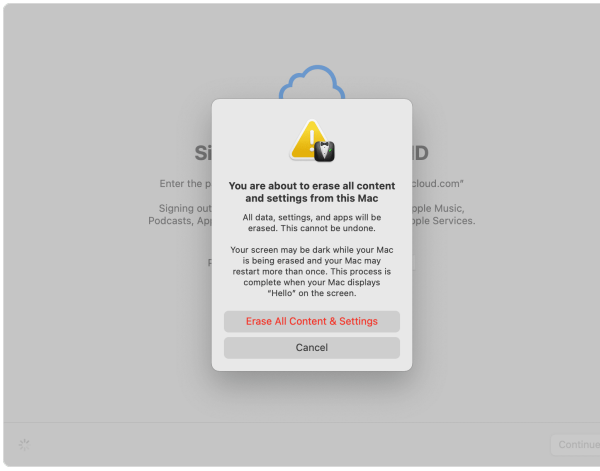
Apple-Support-Artikel vom 25.10.2025

Mit „Einstellungen und Inhalte löschen“ kannst du alle Einstellungen, Daten und Apps schnell und sicher löschen. Das aktuell installierte Betriebssystem bleibt dabei erhalten. — Inhaltsverzeichnis:

„Einstellungen und Inhalte löschen“ verwenden

Erfordert macOS Monterey 12 oder neuer auf einem Mac mit Apple-Chip oder Apple T2 Security Chip

1. Mit macOS Ventura 13 oder neuer:
   - Wähle im Apple-Menü (🍎) in der Bildschirmecke die Option „Systemeinstellungen“.
   - Klicke in der Seitenleiste auf „Allgemein“.
   - Scrolle rechts nach unten, und klicke auf „Übertragen oder zurücksetzen“.
   - Klicke auf „Einstellungen und Inhalte löschen“. Die Taste wird nicht angezeigt?
2. Mit macOS Monterey:
   - Wähle im Apple-Menü (🍎) in der Bildschirmecke die Option „Systemeinstellungen“.
   - Wähle in der Menüleiste im Menü „Systemeinstellungen“ die Option „Einstellungen und Inhalte löschen“. Die Option wird nicht angezeigt?
3. Ein Löschassistent wird geöffnet. Befolge die Anweisungen auf dem Bildschirm. Bevor der Löschvorgang beginnt, wird eine Zusammenfassung aller Einstellungen, Medien, Daten und anderen Objekten angezeigt, die gelöscht oder deaktiviert werden.
   - Wenn du aufgefordert wirst, dich mit deinen Anmeldedaten als Administrator anzumelden, gib das Passwort ein, mit dem du dich bei deinem Mac anmeldest. Hast du dein Anmeldepasswort vergessen?
   - Du wirst möglicherweise aufgefordert, dein Apple Account-Passwort einzugeben, damit sich dein Mac von Apple-Diensten abmelden kann. Passwort vergessen?
   - Du wirst möglicherweise gefragt, ob du ein Backup deines Mac erstellen möchtest, bevor du ihn zurücksetzt.
   - Nachdem du auf die Taste „Einstellungen und Inhalte löschen“ geklickt hast, um zu bestätigen, dass du fortfahren möchtest, wird der Mac neu gestartet und zeigt kurz einen schwarzen Bildschirm oder einen Fortschrittsbalken an.



4. Wenn dein Mac die Verbindung zu einem Bluetooth-Zubehör wie einer Tastatur oder Maus wiederherstellen muss, wirst du möglicherweise aufgefordert, das Zubehör einzuschalten. Wenn sich das Zubehör nicht innerhalb von 30 Sekunden verbindet, schalte es aus und wieder ein. Wenn du dich wieder mit einer Bluetooth-Tastatur verbindest, wirst du aufgefordert, eine Sprache auszuwählen.
5. Möglicherweise wirst du aufgefordert, ein WLAN-Netzwerk auszuwählen oder ein Netzwerkkabel anzuschließen. Um ein WLAN-Netzwerk auszuwählen, verwende das WLAN-Menü oben rechts auf dem Bildschirm.
6. Dein Mac wird dann aktiviert. Klicke auf „Neustart“.

7. Nachdem dein Mac neu gestartet ist, führt dich ein Systemassistent durch den Einrichtungsvorgang, als ob du deinen Mac zum ersten Mal einrichtest.

Wenn du deinen Mac verkaufen, verschenken oder in Zahlung geben und ihn dafür im Werkszustand lassen möchtest, verwende nicht den Systemassistenten oder deine zuvor verbundenen Bluetooth-Geräte, falls vorhanden. Halte einfach den Ein-/Ausschalter an deinem Mac gedrückt, bis er sich ausschaltet.

Wenn „Einstellungen und Inhalte löschen“ nicht verwendet werden kann

„Einstellungen und Inhalte löschen“ ist nur in macOS Monterey oder neuer und nur auf einemMac mit Apple-Chip oder einem Mac mit dem Apple T2 Security Chip verfügbar. Wenn diese Funktion auf deinem Mac nicht verfügbar ist oder nicht funktioniert:

- Um deinen Mac zu löschen und ihn auf die Werkseinstellungen zurückzusetzen, folge den Schritten in Durchzuführende Schritte, bevor du einen Mac verkaufst, weitergibst, in Zahlung gibst oder recycelst, aber ignoriere die Anweisungen für „Einstellungen und Inhalte löschen“.
- Du möchtest deinen Mac nur löschen, ohne ihn auf die Werkseinstellungen zurückzusetzen? Hier erfährst du, wie du einen Mac mit Apple-Chip löschst oder einen Intel-basierten Mac löschst.
- Wenn beim Verwenden von „Einstellungen und Inhalte löschen“ eine Meldung angezeigt wird, die sagt, dass andere Volumes gelöscht werden müssen, bevor du alle Inhalte und Einstellungen löschen kannst, hast du möglicherweise Microsoft Windows mithilfe von Boot Camp installiert. Ist das der Fall, entferne Windows und seine Partition mit Boot Camp.

Unabhängig von Modell oder Zustand können wir dein Gerät in etwas Gutes für dich und für den Planeten verwandeln: Hier erfährst du, wie du deinen Mac mit Apple Trade In in Zahlung geben oder recyceln kannst.

Mein Dank gilt allen Lesern, die mir bereits geholfen haben, die MACtreff-Köln-Homepage und den Newsletter auch in diesem Jahr zu finanzieren.

Wer meine Arbeit ebenfalls unterstützen will, kann das gern durch eine Spende auf mein Paypal-Konto tun: paypal.me/KJM54

Erklärung: Einstellungsdateien

von Howard Oakley, eclecticlight.co • Übersetzung: KJM

Wenn Sie ein Befehlstool im Terminal ausführen, rufen Sie dessen Optionen in dem von Ihnen eingegebenen Befehl auf. Diese Optionen werden bei jeder Ausführung des Tools bereitgestellt und bleiben nicht erhalten. Apps unterscheiden sich davon, da sie über eine grafische Benutzeroberfläche verfügen, die dem Benutzer in der Regel Optionen anbietet, und sich auf Informationen stützen, die bis zur nächsten Ausführung der App erhalten bleiben. Dabei handelt es sich um Einstellungen, Konfigurationen oder Standardwerte, je nachdem, wie man sie betrachtet.

Im traditionellen Unix können dauerhafte Einstellungen als Konfigurationen implementiert werden, die in einer einfachen Textkonfigurationsdatei definiert sind. Im klassischen Mac OS wurden Fenstereinstellungen und vieles mehr als Ressourcen im Ressourcen-Zweig der App oder ihrer Dokumente gespeichert. Dies führte zu einer praktischen Funktion, die heute in macOS selten zu finden ist: Die Fenstereinstellungen eines Dokuments werden in seiner Datei gespeichert, sodass sie beim nächsten Öffnen des Dokuments wiederverwendet werden können.

Eine der Innovationen in NeXTSTEP war die für Menschen lesbare Eigenschaftsliste, die zum Speichern serialisierter Objekte wie Einstellungen verwendet wurde. Diese bestehen aus bestimmten Variablen, die von der App verwendet werden und in eine Darstellung umgewandelt werden, die in Text ausgedrückt werden kann. Wenn eine App beispielsweise dem Benutzer die Wahl lässt, ob er US-amerikanische oder metrische Maßeinheiten verwenden möchte, könnte dies als boolesche Variable (wahr oder falsch) im Speicher abgelegt und als Wort „wahr” oder „falsch” in einer Eigenschaftsliste serialisiert werden, die zur Speicherung der Einstellungen der App verwendet wird.

Inhalt

Um alle von einer App benötigten Einstellungen unterzubringen, ist in der Regel ein Wörterbuch dieser serialisierten Werte erforderlich, wobei jeder Wert einen Schlüssel zur Identifizierung erhält und einen expliziten oder impliziten Datentyp hat. Somit könnte diese Benutzeroption zu „key: `metricUnits` value: `true`“ werden, einer booleschen Angabe mit zwei möglichen Werten.

Mac OS X hat das alte NeXTSTEP-Format für Eigenschaftslisten durch zwei Formatierungsschemata ersetzt, XML und JSON, wobei XML der Standard für App-Einstellungen ist. Dies ist eine Datei, die Wörterbücher mit Schlüssel-Wert-Paaren enthält, die die serialisierten Daten darstellen:

```
<dict> <key>metricUnits</key> <true/>
<key>filePrefix</key> <string>MyFile</
string> </dict>
```

Anfangs wurden alle Eigenschaftslisten als Klartext gespeichert, was jedoch äußerst ineffizient war. Daher wurde zwischen Mac OS X 10.2 und 10.4 ein kompakteres Binärformat eingeführt, das bis heute als Standard in der UserDefaults-API implementiert ist.

cfprefsd

Entwickler können die Standardeinstellungen/Voreinstellungen ihrer Apps zwar auf Wunsch mit ihrem eigenen Code verwalten, aber macOS stellt den Standardeinstellungsserver **cfprefsd** zur Verfügung, und diese praktische API wird von den meisten Apps verwendet. Dabei öffnet cfprefsd zu Beginn der Initialisierung einer App automatisch die Voreinstellungen dieser App und lädt dann ihre Schlüssel-Wert-Paare, damit sie der App während der Einrichtung zur Verfügung stehen.

cfprefsd ist für den Entwickler transparent, dessen Code einfach bei Bedarf auf Schlüssel-Wert-Paare zugreift. cfprefsd kann sich dafür entscheiden, die gesamte Einstellungsdatei im Speicher zu behalten und sie nach eigenem Ermessen zu verwalten. Daher entsprechen die Inhalte der Eigenschaftsliste auf der Festplatte möglicherweise nicht denen, die für die App im Speicher gehalten werden, und alle Änderungen an der Eigenschaftslistendatei können überschrieben werden, wenn cfprefsd geänderte Werte aus dem Speicher speichert.

Für eine einfache App sollte die Arbeit mit cfprefsd ebenfalls unkompliziert sein. Die Einstellungs-Eigenschaftsliste der App wird kurz nach dem Start der App von cfprefsd geöffnet, und der Code der App arbeitet über UserDefaults, um während der Ausführung der App Änderungen an Schlüssel-Wert-Paaren vorzunehmen. Wenn die App geschlossen wird, aktualisiert cfprefsd die Einstellungsdatei, und der Benutzer kann diese Eigenschaftsliste wieder nach Belieben ändern oder löschen. Es gibt jedoch zahlreiche Möglichkeiten, wie dies komplizierter werden oder missbraucht werden kann.

Probleme

Viele Apps sind heute in ihrer Struktur nicht mehr so einfach und verwenden Hilfs-Apps und anderen ausführbaren Code, der möglicherweise auch nach dem Beenden der Haupt-App noch mit Zugriff auf die Einstellungen der App ausgeführt wird. Wenn der Benutzer glaubt, dass es sicher ist, den Inhalt dieser Eigenschaftsliste zu ändern, wird diese möglicherweise noch von `cfprefsd` verwaltet. Der bevorzugte Ansatz ist daher die Verwendung des Befehlstools „`defaults`“, das mit `cfprefsd` zusammenarbeiten sollte, anstatt mit ihm zu konkurrieren.

In der Vergangenheit waren UserDefaults und cfprefsd nicht immer zuverlässig, und einige Entwickler umgingen ihre Probleme mit einer Kombination aus der offiziellen API und ihrer eigenen direkten Manipulation von Einstellungsdateien. Diese gefährlichen Praktiken sollten inzwischen ausgestorben sein.

Da beim Start einer App frühzeitig auf deren Einstellungen zugegriffen wird, können Fehler oder Inkompatibilitäten in diesen Schlüssel-Wert-Paaren fatale Auswirkungen haben, bevor die App vollständig geöffnet ist. Wenn beispielsweise eine neue Version einer App einen vorhandenen Einstellungsschlüssel mit einem anderen Datentyp wiederverwendet und eine alte Version ihrer Einstellungen liest, wird ein Fehler ausgegeben. Wenn dies nicht richtig gehandhabt wird, kann dies dazu führen, dass die neue Version der App beim Start abstürzt.

Glücklicherweise müssen alle Apps in der Lage sein, bei ihrer ersten Ausführung eine eigene Einstellungsdatei zu erstellen. Hier besteht jedoch die Möglichkeit weiterer Fehler, wenn die erstellte Datei nicht aktualisiert wird, um mit geänderten Schlüssel-Wert-Paaren in einer neueren Version der App zu funktionieren. Dies kann dazu führen, dass eine App beim Start abstürzt, selbst wenn keine Einstellungsdatei gespeichert ist — ein Problem, für das es keine Abhilfe gibt.

Schließlich haben viele Apps mehrere Einstellungsdateien. Wenn sie in einer Sandbox ausgeführt werden, befindet sich die normalerweise verwendete Kopie im Ordner „Data/Library/Preferences“ in ihrem Container unter „~/Library/Containers“. Sie können jedoch auch eine andere Eigenschaftsliste unter „~/Library/Preferences“ und manchmal auch eine Masterkopie unter „/Library/Preferences“ haben. Ich bin mir zwar sicher, dass cfprefsd weiß, auf welche Datei es zugreifen muss, aber Sie müssen dies möglicherweise überprüfen, indem Sie die Zeitstempel jeder Datei überprüfen.

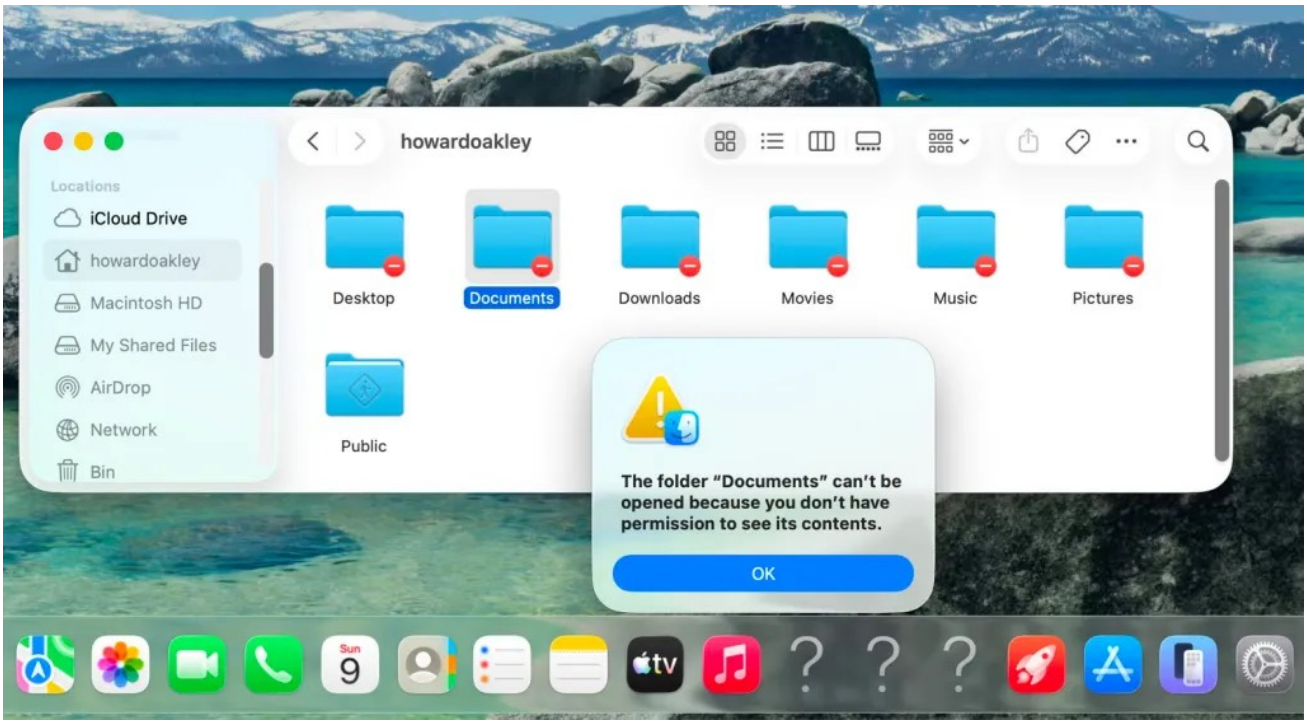
UserDefaults wurden mit SwiftUI erheblich verbessert, wodurch die persistente Speicherung von Einstellungen weiter integriert wurde. Obwohl sie immer noch zu Problemen führen können, sollten sie selten schwere Probleme verursachen, sofern Sie verstehen, wie sie funktionieren, und nicht versuchen, gegen das System anzukämpfen.

Weiterführende Literatur

UserDefaults (Apple)
Preferences and Settings Programming Guide (Apple) aus dem Jahr 2013
Thomas Tempelmanns Prefs Editor arbeitet mit cfprefsd

Schweres Geschütz für Tahoe-Probleme: Welche radikalen Lösungen funktionieren noch?

von Howard Oakley, eclecticlight.co • Übersetzung: KJM



Wenn Sie alle logischen Lösungen ausprobiert, einen Neustart durchgeführt, es im abgesicherten Modus versucht haben und das Problem immer noch nicht lösen können, müssen Sie möglicherweise schweres Geschütz auffahren. Dabei handelt es sich um radikale Lösungen, die das Risiko bergen, weiter zu gehen, als Sie möchten, aber sie sind alles, was Ihnen noch bleibt. Möglicherweise wurden sie Ihnen von jemandem empfohlen, der sich gut auskennt, oder aber, wie wir letzte Woche gesehen haben, von einer KI. In diesem Artikel wird der Stand dieser schweren Geschütze in Tahoe 26.1 beleuchtet und es wird erläutert, welche Sie noch ernsthaft in Betracht ziehen können.

NVRAM und SMC zurücksetzen ⛔

Das Zurücksetzen von NVRAM und SMC ist zwar schnell und einfach, aber dafür bekannt, dass es alle möglichen Probleme behebt. Bei Intel-Macs ist es immer noch sinnvoll, **aber bei Apple-Silicon CPUs können Sie darauf verzichten**, da das SMC bei jedem Start zurückgesetzt wird und der NVRAM vor dem Zugriff durch den Benutzer geschützt ist. Die einzige Möglichkeit, den NVRAM eines Apple-Silicon-Macs zurückzusetzen, besteht darin, ihn im DFU-Modus wiederherzustellen, was Sie zu diesem Zeitpunkt mit ziemlicher Sicherheit nicht tun möchten.

TCC zurücksetzen ⚠️

TCC ist das Subsystem, das für die Umsetzung des Datenschutzes zuständig ist und für sein rätselhaftes Fehlverhalten bekannt ist. Bevor Sie sich davon überzeugen, dass Maßnahmen in Bezug auf TCC zur Lösung eines Problems beitragen, sollten Sie wirklich nach einem Muster für Fehlverhalten suchen, das auf eine der Ressourcen hinweist, auf die TCC den Zugriff kontrolliert. Wenn möglich, verbinden Sie dies mit einer einzelnen App und verwenden Sie beispielsweise „`sudo tccutil reset All com.apple.clock`“, um ausschließlich die Datenschutzeinstellungen dieser einen App zurückzusetzen.

***TCC** steht für Transparency, Consent, and Control und ist ein Framework in macOS, das den Zugriff von Anwendungen auf sensible Nutzerdaten und Funktionen regelt. Es zeigt den Nutzern Pop-up-Meldungen an, um die Erlaubnis für den Zugriff auf Kamera, Mikrofon, Standortdienste, Fotos, Kontakte, Kalender und Dateien einzuholen und zu verwalten. TCC dient dazu, die Privatsphäre der Nutzer zu schützen, indem es sicherstellt, dass keine Anwendung ohne ausdrückliche Zustimmung auf sensible Daten zugreifen kann.*

TCC ist auch eine beliebte Empfehlung in Lösungen, denen eine solide logische Grundlage fehlt, bei denen nicht ver-

sucht wird, eine bestimmte App anzusprechen, sondern alle mit „`sudo tccutil reset All`“ gelöscht werden. Dies hat zur Folge, dass alle Bereiche (außer den Ortungsdiensten) in den Einstellungen für Datenschutz und Sicherheit geleert werden. Dadurch werden viele Apps sicherlich nicht mehr richtig funktionieren, und Sie werden sie in den folgenden Tagen oder Wochen wieder einzeln hinzufügen müssen. In einigen Fällen reicht selbst das nicht aus, und das Löschen der TCC-Datenbank scheint der einzige Weg zu sein. Dieses und andere Probleme werden hier diskutiert. — `tccutil` scheint sich in Tahoe nicht wesentlich verändert zu haben.

Die Datenbank von LaunchServices löschen ⛔

LaunchServices verwaltet viele Funktionen, darunter das Öffnen von Apps, das Ausfüllen ihrer Befehle im Menü „Zuletzt geöffnet“ und einen Großteil der Integration von Apps mit ihren Dokumenten. Zu diesem Zweck unterhält es eine umfangreiche Datenbank mit Apps und anderen ausführbaren Komponenten.

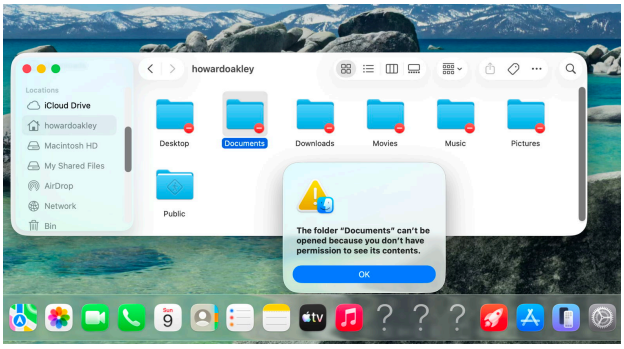
Der Zugriff auf die Datenbank von LaunchServices und die Kontrolle darüber erfolgt über den Befehl lsregister, der tief in /System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/LaunchServices.framework/Versions/A/Support verborgen ist, obwohl es ein öffentliches lsappinfo-Tool gibt, das verschiedene Funktionen bietet und selten verwendet wird. Anfang dieses Jahres habe ich über dessen Verwendung in Sequoia berichtet, aber die beliebteste Option zum Beenden der LaunchServices-Datenbank wurde aus Tahoe entfernt, „weil sie gefährlich und nicht mehr nützlich war“ — eine faire Einschätzung.

Zugriffsberechtigungen reparieren ⛔

Ich habe kürzlich die verschiedenen Formen der Reparatur von Berechtigungen erneut untersucht. Wenn Ihnen jemand oder etwas empfiehlt, `sudo /usr/libexec/repair_packages --verify --standard-pkgs` auszuführen, sollten Sie nicht auf weitere Empfehlungen hören, da diese Form mit El Capitan ausgelaufen ist und mit einer modernen Version von macOS nicht einmal mehr möglich ist.

Der modernere Ersatz, der mit dem Befehl repairHomePermissions im Wiederherstellungsmodus gestartet wird, mag einst einen Zweck gehabt haben, ist aber mittlerweile äußerst störend, da er den Benutzer aus den meisten Inhalten seines Home-Ordners aussperrt, indem er ihn als Eigentümer entfernt.

Es würde Stunden dauern, Ihren Mac nach Durchführung dieser „Reparatur“ wieder in einen nutzbaren Zustand zu versetzen. Wenn Ihnen jemand empfiehlt, dies zu versuchen, fragen Sie ihn, wann er es zuletzt erfolgreich angewendet hat.



Saubere Installation

Tahoe bietet praktische Methoden für eine saubere Installation von macOS, wie hier beschrieben. Eine der einfachsten ist das Löschen aller Inhalte und Einstellungen mit der Option „**EACAS**“ unter „Übertragen oder zurücksetzen“ in den allgemeinen Einstellungen. Dadurch werden alle Ihre Daten unzugänglich gemacht, indem der Verschlüsselungsschlüssel sicher gelöscht wird. Anschließend können Sie Ihre Daten von Ihrer letzten Sicherung migrieren, wenn Sie Ihre installierte Version von macOS auffrischen.

Wenn Sie auch zu einer neuen Firmware und macOS zurückkehren möchten, ist der einfachste Weg die Wiederherstellung im DFU-Modus, wie hier erläutert. Dabei haben Sie auch die Möglichkeit, jedes kompatible IPSW zu verwenden, sodass Sie auf Wunsch ein vollständiges Downgrade auf eine frühere Version von macOS durchführen können. Beachten Sie, dass Apple Silicon Macs keine Version von macOS ausführen können, die vor der Auslieferung dieses Modells veröffentlicht wurde. Im Zweifelsfall können Sie in der Datenbank von Mactracker nachsehen, welche Originalversion mit diesem Modell ausgeliefert wurde.

Zusammenfassung für Apple Silicon Macs:

Das Zurücksetzen von SMC und NVRAM ist nicht möglich (für Intel weiterhin verfügbar). ⛔

Das Zurücksetzen von TCC ist weiterhin verfügbar. ⚠️

Das Löschen der LaunchServices-Datenbank ist nicht mehr verfügbar (aber noch in Sequoia). ⛔

Das Reparieren von Berechtigungen ist sehr störend und sollte vermieden werden. ⛔

Eine Neuinstallation kann auf das Datenvolume beschränkt werden oder auch Firmware und macOS umfassen. ✅ Wie auch immer Sie sich entscheiden, ich wünsche Ihnen viel Erfolg!