macOS

Der Abschnitt **macOS** des Apple-Richtlinieneditors verwaltet die Sicherheits-, Datenschutz- und Anmeldeeinstellungen der Macs: FileVault, Firewall, Gatekeeper, Bildschirmschoner und Sperre, externe und Netzwerkspeicher, Bildschirmfreigabe, Datenschutzberechtigungen, Anmeldeobjekte sowie die System- und Kernel-Erweiterungen, die geladen werden dürfen. Er installiert außerdem Konfigurationsdateien von Systemdiensten und Hintergrundaufgaben. Die anderen Geräte der Richtlinie erhalten diese Einstellungen nicht. Aktivieren Sie eine Einstellung, um sie zu verwalten; solange sie deaktiviert ist, behalten die Benutzer ihre eigenen Auswahlmöglichkeiten.

> Die meisten Einstellungen werden auf dem Mac als Konfigurationsprofile installiert und sind in Systemeinstellungen > Allgemein > Geräteverwaltung sichtbar. FileVault, Datenschutzberechtigungen, Anmeldeobjekte und die Erweiterungseinstellungen erfordern eine vom Benutzer genehmigte MDM: Auf einem Mac, der mit der Registrierungs-URL oder dem QR-Code registriert wurde, genehmigt der Benutzer das Registrierungsprofil in den Systemeinstellungen. Die Geräteseite zeigt dies im Feld **Vom Benutzer genehmigte MDM** . Wenn der Benutzer es später genehmigt, erhält der Mac diese Einstellungen automatisch.

FileVault

FileVault verschlüsselt die Festplatte des Macs. Ist diese Einstellung aktiviert, werden Benutzer aufgefordert, FileVault mit ihrem Passwort zu aktivieren, und der Mac sendet seinen persönlichen Wiederherstellungsschlüssel an Cerberus Enterprise, verschlüsselt mit einem Schlüssel, der nur Ihrer Organisation gehört. Der Schlüssel wird im Feld **FileVault** der Geräteseite angezeigt und geändert (siehe Gerätebefehle). Die Einstellung erfordert macOS 13 oder neuer und eine vom Benutzer genehmigte MDM; ohne vom Benutzer genehmigte MDM wird der Mac nicht aufgefordert, FileVault zu aktivieren, aber wenn ein Benutzer es aktiviert, wird sein Schlüssel gespeichert.

- **Bei der Anmeldung erforderlich**: bei der nächsten Anmeldung, nach einer Anzahl von Überspringungen (der Benutzer wird bei jeder Anmeldung und beim Abmelden erneut gefragt) oder nur, wenn sich der Benutzer abmeldet.
- **Beim Abmelden nicht fragen**: Der Benutzer wird nur bei der Anmeldung gefragt. Die Option kann nicht mit „Nur beim Abmelden fragen“ kombiniert werden.
- **Dem Benutzer den Wiederherstellungsschlüssel anzeigen**: standardmäßig deaktiviert, sodass nur die Administratoren den Schlüssel von der Geräteseite aus kennen.
- **Deaktivieren von FileVault verhindern**: standardmäßig aktiviert.
- **Schlüssel im Bereitschaftsmodus aus dem Arbeitsspeicher entfernen**: Der Benutzer gibt das Passwort erneut ein, wenn der Mac aus dem Bereitschaftsmodus aufwacht.

- **Wo der Schlüssel aufbewahrt wird**: Text, der dem Benutzer im Anmeldefenster angezeigt wird, zum Beispiel wen man anrufen soll, um den Mac wiederherzustellen (Standard: „Cerberus Enterprise“).

> Ein Mac, der bereits verschlüsselt war, als er die Einstellung erhielt, behält seinen aktuellen Schlüssel, den Cerberus Enterprise nicht erhält: Der Schlüssel wird erst gespeichert, nachdem der Benutzer FileVault deaktiviert und erneut aktiviert hat (mit deaktivierter Option „Deaktivieren von FileVault verhindern“). Das Deaktivieren der Einstellung oder das Entfernen des Macs aus der Verwaltung deaktiviert FileVault nicht, und der gespeicherte Schlüssel funktioniert weiterhin. Die Einstellung kann nicht gespeichert werden, wenn der Server nicht für die Speicherung von Wiederherstellungsschlüsseln konfiguriert ist.

Firewall

- **Firewall aktivieren**: Wenn die Option deaktiviert ist, bleibt die Firewall deaktiviert und Benutzer können sie nicht aktivieren.
- **Alle eingehenden Verbindungen blockieren**: Nur die grundlegenden Netzwerkdienste (DHCP, Bonjour, IPSec) können Verbindungen empfangen.
- **Tarnmodus**: Der Mac antwortet nicht auf Ping-Anfragen und Verbindungen zu geschlossenen Ports.
- **Integrierte Software erlauben** und **Heruntergeladenen signierten Apps erlauben**, Verbindungen zu empfangen, ohne den Benutzer zu fragen (macOS 12.3 oder neuer).
- **Regeln für bestimmte Apps**: Erlauben oder blockieren Sie die eingehenden Verbindungen einer App anhand der Bundle-ID.

Gatekeeper

Gatekeeper prüft die Apps, bevor sie geöffnet werden. Wählen Sie aus, ob die Macs nur Apps aus dem App Store oder auch Apps identifizierter Entwickler öffnen. Bei deaktiviertem Gatekeeper kann jede App geöffnet werden, auch nicht signierte oder beschädigte. Unter macOS 15 oder neuer können Sie außerdem auswählen, ob Benutzer aufgefordert werden, blockierte Malware an Apple zu senden.

Bildschirmschoner und Sperre

Starten Sie den Bildschirmschoner nach einer gewissen Inaktivitätszeit, und fordern Sie das Passwort an, wenn der Bildschirmschoner startet oder das Display in den Ruhezustand wechselt,

sofort oder nach einer Verzögerung. Eine Einstellung, die auf **Nicht verwaltet** belassen wird, bleibt die Wahl des Benutzers.

Externer und Netzwerkspeicher

Erlauben, schreibgeschützt machen oder blockieren Sie den externen Speicher (USB-Laufwerke, SD-Karten, externe Festplatten) und den Netzwerkspeicher (Dateifreigaben) der Macs. Erfordert macOS 15 oder neuer.

Bildschirmfreigabe

Einschränkungen für Personen, die sich mit der Bildschirmfreigabe mit diesen Macs verbinden: Kopieren von Dateien vom oder auf den Mac, Hochleistungsverbindungen und die Anzahl virtueller Displays. Das Aktivieren der Bildschirmfreigabe bleibt die Wahl des Benutzers. Erfordert macOS 14 oder neuer.

Datenschutzberechtigungen

Gewähren oder verweigern Sie Apps den Zugriff, den Benutzer andernfalls in den Systemeinstellungen > Datenschutz & Sicherheit erlauben würden, zum Beispiel Vollständiger Festplattenzugriff für eine Backup-App, oder verweigern Sie einer App den Zugriff auf die Kamera. Wählen Sie für jede Berechtigung:

- **Berechtigung**: Vollständiger Festplattenzugriff, Bedienungshilfen, Automatisierung, die Ordner, Kontakte, Kalender, Fotos, Kamera, Mikrofon, Bildschirmaufnahme und die übrigen unter Datenschutz & Sicherheit.
- **Zugriff**: Erlauben oder verweigern. Kamera, Mikrofon, Bildschirmaufnahme und Eingabeüberwachung können durch ein Profil nicht erlaubt, sondern nur verweigert werden; bei Bildschirmaufnahme und Eingabeüberwachung können Sie Benutzern erlauben, sie auch ohne Administratorrechte zu erlauben.
- **App**: die Bundle-ID einer App oder der Pfad eines Programms (zum Beispiel eines Befehlszeilentools).
- **Codeanforderung**: identifiziert die App anhand ihrer Signatur. Rufen Sie sie im Terminal mit `codesign -dr - /Applications/Example.app` ab und kopieren Sie den Text hinter `designated =>`.
- **Automatisierung** erfordert außerdem die gesteuerte App (zum Beispiel den Finder) und ihre Codeanforderung.

Anmeldeobjekte und Hintergrundobjekte

Die Anmeldeobjekte und Hintergrundobjekte, die den Regeln entsprechen, werden verwaltet: Sie werden ohne Nachfrage ausgeführt, und Benutzer können sie nicht in den Systemeinstellungen > Allgemein > Anmeldeobjekte deaktivieren. Eine Regel entspricht der Entwicklerteam-ID einer App, ihrer Bundle-ID oder der Bezeichnung eines Launch-Daemons oder -Agents (auch anhand ihres ersten Teils). Erfordert macOS 13 oder neuer.

Systemerweiterungen

Systemerweiterungen sind die moderne Möglichkeit für Apps, macOS zu erweitern: Netzwerkfilter und VPNs, Endpoint-Security-Agenten und -Treiber. Ist diese Einstellung aktiviert, werden die Systemerweiterungen der aufgeführten Entwicklerteams ohne Nachfrage beim Benutzer geladen. Erfordert macOS 10.15 oder neuer und eine vom Benutzer genehmigte MDM.

- **Team-ID**: die 10-stellige Team-ID des Entwicklers (zum Beispiel in den Details „Signiert von“ der App oder mit `codesign -dv`). Jedes Team kann nur einmal vorkommen.
- **Erlauben**: jede Erweiterung des Teams oder nur die Erweiterungen mit den aufgeführten Bundle-IDs.
- **Typen**: beschränkt das Team auf Treiber-, Netzwerk- oder Endpoint-Security-Erweiterungen. Ist keiner ausgewählt, sind alle Typen erlaubt.
- **Entfernung** (nur für aufgeführte Erweiterungen): Die App kann ihre Erweiterung ohne Administrator entfernen (macOS 12 und neuer), die Erweiterung kann bei aktivem Systemintegritätsschutz nicht deaktiviert oder entfernt werden, oder sie kann nicht in den Systemeinstellungen und im Finder entfernt werden (macOS 15 und neuer). Macs mit einem älteren macOS erlauben die Erweiterung weiterhin, jedoch ohne die Entfernungsoption.
- **Benutzer können andere Systemerweiterungen genehmigen**: standardmäßig aktiviert. Wenn deaktiviert, können nur die von einem Profil erlaubten Erweiterungen geladen werden; wenn ein Profil auf dem Mac die Option deaktiviert, ist sie deaktiviert.

> Unter macOS 11.3 und neuer deaktiviert das Entfernen dieser Einstellung die Systemerweiterungen, die sie erlaubt hat, zum Beispiel einen Sicherheitsagenten oder einen Netzwerkfilter. Dies geschieht, wenn die Einstellung deaktiviert wird, wenn die Richtlinie gelöscht wird und wenn der Mac zu einer Richtlinie ohne sie wechselt. Der Editor fordert vor dem Deaktivieren der Einstellung eine Bestätigung an.

Kernel-Erweiterungen (Legacy)

Kernel-Erweiterungen sind die ältere, veraltete Möglichkeit, macOS zu erweitern: Bevorzugen Sie Systemerweiterungen, wenn der Anbieter sie anbietet. Die Kernel-Erweiterungen der aufgeführten Teams (jede Erweiterung eines Teams oder nur die aufgeführten Bundle-IDs) werden nach einem Neustart ohne Nachfrage beim Benutzer geladen. Erfordert macOS 10.13.2 oder neuer und eine vom Benutzer genehmigte MDM.

- **Benutzer können andere Kernel-Erweiterungen genehmigen**: standardmäßig deaktiviert, sodass nur die aufgeführten Teams Kernel-Erweiterungen laden können.
- **Standardbenutzer können sie ebenfalls genehmigen**: Bei aktivierten Benutzergenehmigungen können Benutzer ohne Administratorrechte sie ebenfalls genehmigen (macOS 11 und neuer).

> Auf Macs mit Apple silicon reicht ein Profil allein nicht aus: Jemand muss den Mac in recoveryOS starten, im Startup-Sicherheitsdienstprogramm „Reduzierte Sicherheit“ auswählen und die Benutzerverwaltung von Kernel-Erweiterungen identifizierter Entwickler erlauben. Der Mac benötigt möglicherweise außerdem ein in Cerberus Enterprise hinterlegtes Bootstrap Token, um sie zu genehmigen (siehe das Feld „Bootstrap Token“ auf der Geräteseite).

Mac-Dateien

Die Dienstkonfigurationsdateien und die Hintergrundaufgaben verwenden Dateien, die Sie in die **Mac-Dateien** Ihrer Organisation hochladen: ZIP-Archive und Eigenschaftslisten (.plist) bis zu 20 MB. Laden Sie sie hoch, prüfen Sie, wo sie verwendet werden, oder löschen Sie sie über die Schaltfläche **Mac-Dateien** des macOS-Abschnitts oder über **Datei auswählen** in einer Einstellung. Eine von einer Richtlinie verwendete Datei kann nicht gelöscht werden. Um eine Datei zu ändern, laden Sie die neue Version hoch und wählen Sie sie in der Richtlinie aus: Die Macs laden sie erneut herunter.

Dienstkonfigurationsdateien

Installiert die Konfigurationsdateien eines Systemdienstes aus einem ZIP-Archiv. Die integrierten Dienste sind der SSH-Server (sshd), sudo, PAM, Drucken (CUPS), der Apache-Webserver, bash, zsh, Smartcard-Anmeldung und Autorisierung. Sie können auch einen eigenen Dienst mit einer Reverse-DNS-Kennung wie `com.example.service` verwenden: Er findet die Dateien über die Bibliothek der verwalteten Konfigurationsdateien von macOS. Jeder Dienst kann eine Einstellung haben. Erfordert macOS 14 oder neuer.

> Ein integrierter Dienst verwendet nur die Dateien des Archivs und ignoriert seine eigenen Dateien, zum Beispiel /etc/ssh für sshd: Legen Sie die gesamte Konfiguration im Archiv in Ordnern ab, die vom Stammverzeichnis der Festplatte ausgehen (zum Beispiel `etc/ssh/sshd_config`). Die Dateien sind auf dem Mac schreibgeschützt und werden mit der Einstellung entfernt. Testen Sie das Archiv zuerst auf einem Mac: Eine falsche sudo- oder PAM-Konfiguration kann Benutzer daran hindern, sich anzumelden oder Administratorrechte zu verwenden.

Hintergrundaufgaben

Programme und Skripte, die im Hintergrund ausgeführt und von launchd gestartet werden. Benutzer können sie nicht deaktivieren, und sie werden mit der Einstellung entfernt. Erfordert macOS 15 oder neuer. Wählen Sie für jede Aufgabe:

- **Aufgabenkennung**: eine Reverse-DNS-Kennung wie `com.example.task`, die für jede Aufgabe unterschiedlich ist.
- **Programme und Skripte** (optional): ein ZIP-Archiv, das der Mac in `/var/db/ManagedConfigurationFiles/BackgroundTaskServices/Services/` gefolgt von der Aufgabenkennung entpackt. Behalten Sie die Ausführungsberechtigung der Dateien bei und legen Sie keine Eigenschaftslisten darin ab.
- **launchd-Eigenschaftslisten**: die Jobs, die die Programme starten, geladen als Daemon (für das gesamte System als root) oder als Agent (in jeder Benutzersitzung). Verweisen Sie auf die Programme mit ihrem Pfad im obigen Ordner.

Eine Aufgabe benötigt die Programme oder mindestens eine Eigenschaftsliste. Wenn sich die Dateien ändern, starten die Macs die Aufgabe neu.

Revision #7
Created 2026-11-10 15:14:10 UTC by Admin
Updated 2026-11-12 09:53:53 UTC by Admin