Richtlinien - Apple

- Apple-Richtlinien
- Apps & Profile
- Kiosk und Home-Bildschirm
- Code
- Einschränkungen
- Netzwerk
- Softwareupdates
- macOS
- Standort und Geofences
- Konten
- Compliance-Regeln

Apple-Richtlinien

Apple-Richtlinien definieren Verwaltungseinstellungen, die Cerberus Enterprise über MDM auf Apple-Geräte anwendet. Diese Einstellungen werden im Dashboard im Apple-Richtlinieneditor konfiguriert.

Bevor Sie beginnen

Die Apple-Geräteverwaltung erfordert, dass Apple Management (APNs) konfiguriert ist. Bei Bedarf lesen Sie die Seite Apple Management setup (APNs).

Apple-Richtlinieneditor öffnen

Öffnen Sie im Dashboard **Richtlinien** und klicken Sie auf **Neue Apple-Richtlinie erstellen**. Um eine vorhandene Apple-Richtlinie zu bearbeiten, klicken Sie auf ihre Zeile in der Richtlinientabelle.

Layout des Editors

Der Apple-Richtlinieneditor ist als eine Reihe ausklappbarer Bereiche organisiert. Oben auf der Seite können Sie immer Folgendes bearbeiten:

- **Name** (erforderlich)
- **Id** (schreibgeschützt)
- **Beschreibung** (optional)

Richtlinienbereiche

Die folgenden Abschnitte entsprechen den aktuell im Apple-Richtlinieneditor verfügbaren Bereichen. Wenn Sie eine gespeicherte Richtlinie öffnen, sind die Abschnitte mit geänderten Einstellungen bereits geöffnet, die übrigen bleiben geschlossen:

- **App-Verwaltung**: Konfigurieren Sie appbezogene Einschränkungen, verwaltete Apps und die Einstellungen der Cerberus Enterprise App.

- **Kiosk und Home-Bildschirm**: Einzel-App-Modus, erlaubte und blockierte Apps, Layout des Home-Bildschirms, Webclips, Benachrichtigungseinstellungen und Sperrbildschirmmeldung.
- **Sicherheit**: Steuern Sie Funktionen wie automatische Entsperrung und biometrische Entsperrung.
- **Passcode-Einstellungen**: Konfigurieren Sie Passcode-Anforderungen und zugehörige Regeln.
- **Multimedia**: Kamera und zugehörige Funktionen erlauben/verhindern.
- **Mobilfunk**: Steuerung der Mobilfunk-Einstellungen (mobile Dateneinstellungen von Apps, eSIM, Tarifänderungen) und des Mobilfunk-APN.
- **Netzwerk**: Wi-Fi-Netzwerke (auch Enterprise 802.1X), VPNs, Zertifikate, globaler Proxy, verschlüsseltes DNS und Webinhaltsfilter sowie Konnektivitätseinschränkungen wie AirDrop und Bluetooth.
- **System und Benutzeroberfläche**: Systemfunktionen wie Handoff, Gerätename und Bildschirmschoner einschränken.
- **Softwareupdates**: Verlangen Sie eine OS-Version bis zu einer Frist und steuern Sie, wie Updates heruntergeladen und installiert werden.
- **macOS**: Firewall, Gatekeeper, Bildschirmschoner und Sperre, externe und Netzwerkspeicher, Bildschirmfreigabe, Datenschutzberechtigungen und Anmeldeobjekte der Macs.
- **Apple-Apps und -Dienste**: Apple-Apps und -Dienste wie iMessage, Game Center und Find My einschränken.
- **Siri und Apple Intelligence**: Siri, Diktat und die Apple Intelligence-Funktionen einschränken.
- **iCloud**: Erlauben oder verhindern Sie bestimmte iCloud-Dienste (Backup, Schlüsselbund-Synchronisierung, Private Relay usw.).
- **Standort und Geofences**: Bereiche, in denen iPhones und iPads mit der Cerberus Enterprise-App melden, wenn sie sie betreten oder verlassen, für Ereignisregeln.
- **Konten**: Schränken Sie die Kontenänderung ein und konfigurieren Sie Mail-, Exchange-, Google-, Kalender-, Kontakte- und Verzeichniskonten.
- **Compliance-Regeln**: Anforderungen (Passcode, minimale OS-Version, Überwachung, FileVault), die Geräte nicht compliant machen, mit optionaler Blockierung.

> Viele Optionen im Apple-Richtlinieneditor enthalten einen Tooltip, der Anforderungen und unterstützte OS-Versionen dokumentiert.

Speichern, löschen und zugeordnete Geräte

Verwenden Sie **Richtlinie speichern**, um Ihre Änderungen anzuwenden. Die Schaltfläche ist deaktiviert, wenn keine ausstehenden Änderungen vorhanden sind oder wenn die Lizenz

abgelaufen ist.

Wenn Sie eine vorhandene Richtlinie bearbeiten, zeigt die Seite außerdem die Aktion **Richtlinie löschen** an. Der Editor kann unten eine Liste **Zugeordnete Geräte** anzeigen, damit Sie sehen, wie viele Geräte derzeit die Richtlinie verwenden.

Nächste Seiten

- Apps & Profile: Konfigurieren Sie installierte Apps und Konfigurationsprofile.
- Kiosk und Home-Bildschirm: Einzel-App-Modus, erlaubte Apps, Layout des Home-Bildschirms und Webclips.
- Passcode: Konfigurieren Sie Passcode-Anforderungen und zugehörige Sicherheitsoptionen.
- Einschränkungen: Definieren Sie erlaubte Funktionen und Einschränkungen auf OS-Ebene.
- Netzwerk: Wi-Fi-Netzwerke, VPNs, Zertifikate und Konnektivitätseinschränkungen.
- Softwareupdates: erforderliche OS-Updates und Softwareupdate-Einstellungen.
- macOS: Firewall, Gatekeeper, Bildschirmsperre, Speicher, Datenschutzberechtigungen und Anmeldeobjekte der Macs.
- Standort und Geofences: Bereiche, die iPhones und iPads beim Betreten und Verlassen melden, und was sie zum Funktionieren benötigen.
- Konten: Mail-, Exchange-, Google-, Kalender-, Kontakte- und Verzeichniskonten.
- Compliance-Regeln: Anforderungen für die Geräte und Blockierung nicht compliant Geräte.

Apps & Profile

Dieser Abschnitt dokumentiert, wie verwaltete Anwendungen und Kontonutzlasten für Apple-Geräte konfiguriert werden.

App-Verwaltung

Das Panel **App-Verwaltung** enthält sowohl allgemeine appbezogene Einschränkungen als auch eine Liste verwalteter Apps.

Allgemeine App-Einschränkungen

- **App-Clips erlauben**
- **App-Installation erlauben**
- **Entfernen von Apps erlauben**
- **Automatische App-Downloads erlauben**
- **Ausblenden von Apps erlauben**
- **Sperren von Apps erlauben**
- **In-App-Käufe erlauben**
- **Änderung des Standardbrowsers erlauben**
- **Vertrauen für Unternehmens-Apps erlauben**

Verwaltete Apps

Verwenden Sie **Anwendung hinzufügen**, um der Richtlinie eine App hinzuzufügen. Jede verwaltete App wird als Karte angezeigt. Sie können die Karte aufklappen, um ihre Einstellungen zu bearbeiten, und die App über die Löschaktion entfernen.

- **App Store-ID**: die App Store-Kennung der verwalteten App.
- **Bundle-ID**: die Bundle-Kennung der App.
- **Installationsverhalten**: steuert, ob die App installiert bleiben muss oder vom Benutzer installiert/entfernt werden kann.
- **Zuweisung**: der Lizenztyp, den Cerberus für jedes Gerät wählt: eine Gerätelizenz auf Unternehmensgeräten, eine Benutzerlizenz des Managed Apple Account auf privaten iPhones und iPads (Benutzerregistrierung). Das Feld kann nicht geändert werden.
- **VPP-Lizenz**: VPP-Lizenztyp, der für die Installation über den App Store verwendet wird.

Die App-Auswahlliste zeigt die verfügbaren und die gesamten Lizenzen jeder App an. Kostenlose Apps zeigen **Unbegrenzt**: Apple stellt ihnen unbegrenzte Lizenzen bereit. Eine App kann einer Richtlinie nur einmal hinzugefügt werden: Eine App mit derselben App Store-ID oder Bundle-ID wie eine bereits in der Richtlinie enthaltene App wird abgelehnt, ebenso eine Richtlinie, die dieselbe App zweimal auflistet, wenn Sie sie speichern.

Die App-Auswahlliste zeigt die Apps Ihrer Apple Business-Mediathek. Um eine App hinzuzufügen, öffnen Sie in Apple Business **Apps & Services → Apps & Books → App Store**, suchen Sie nach der App und klicken Sie auf **View**. Klicken Sie bei einer kostenlosen App auf **Add**, wählen Sie **All current and future** (oder die Organisationseinheit Ihres Apps and Books-Tokens) in **Organizational Units**, klicken Sie auf **Add** und dann auf **Review** und bestätigen Sie. Klicken Sie bei einer kostenpflichtigen App auf ihren Preis, wählen Sie **Managed Licenses** als **License Type** (Einlösecodes können von Cerberus Enterprise nicht verwendet werden), wählen Sie die **Organizational Unit** Ihres Apps and Books-Tokens, geben Sie die Anzahl der **Licenses** ein (bis zu 1.000 pro Bestellung) und klicken Sie dann auf **Review** und kaufen Sie. Eine Zahlungsmethode muss zuvor unter **Settings → Payments & Billing → Apps & Services → Payment Methods** eingerichtet werden. Die Apps erscheinen dann in der App-Auswahlliste.

Apps auf privaten Geräten (Benutzerregistrierung)

Private iPhones und iPads, die mit Benutzerregistrierung registriert wurden, haben keine Seriennummer. Daher erhalten sie die App Store-Apps der Richtlinie mit einer **Benutzerlizenz** des auf dem Gerät angemeldeten Managed Apple Account. Cerberus registriert das Konto bei Apps and Books und weist die Lizenzen selbst zu, auch für kostenlose Apps. Die Managed Apple Accounts und das Apps and Books-Token müssen zur selben Apple Business-Organisation gehören. Eine kostenpflichtige App verwendet eine Lizenz pro Konto, die von allen privaten Geräten dieses Kontos gemeinsam genutzt wird.

- **Warten auf eine Benutzerlizenz**: Die App wird erst an das Gerät gesendet, nachdem Apple die Lizenz bestätigt hat, in der Regel innerhalb weniger Minuten. Das Panel **Anwendungen** des Geräts zeigt den Grund an.
- **Benutzerlizenz fehlgeschlagen**: Apple konnte die Lizenz nicht zuweisen, zum Beispiel weil für eine kostenpflichtige App keine Lizenz mehr verfügbar ist. Fügen Sie in Apple Business Lizenzen hinzu und verwenden Sie dann **Erneut anfordern**; Cerberus versucht es außerdem jeden Tag selbst erneut.
- **Installationsaufforderung**: iOS fragt den Benutzer vor der Installation jeder App. Wenn der Benutzer abbricht, zeigt die App **Warten auf die Zustimmung des Benutzers zur Installation**; **Erneut anfordern** zeigt die Aufforderung erneut an.
- **Freigabe**: Wenn Sie die App aus der Richtlinie entfernen oder das letzte private Gerät des Kontos abmelden, wird die App entfernt und ihre Lizenz freigegeben, es sei denn, ein anderes registriertes Gerät desselben Kontos benötigt sie noch.

Einzelheiten finden Sie unter **Kontobasierte Apple-Registrierung**.

Verwaltete Konfiguration

Eine verwaltete Konfiguration gibt einer App ihre Einstellungen (zum Beispiel eine Serveradresse oder einen Kontonamen), so wie der Hersteller der App sie dokumentiert. Öffnen Sie die App in der Richtlinie und klicken Sie auf **Verwaltete Konfiguration hinzufügen**. Sie wird an iPhones und iPads mit **iOS oder iPadOS 18.4 oder höher** und an Macs mit **macOS 27 oder höher** gesendet; an Apple Vision Pro wird sie noch nicht gesendet. Die App muss verwaltete Konfigurationen unterstützen: Eine App, die sie nicht liest, ignoriert sie. Das App-Panel zeigt die Anzahl der Schlüssel neben dem App-Namen an.

- **Schlüssel**: Jede Zeile enthält einen Schlüssel, einen Typ und einen Wert. Die Typen sind Text, Ganzzahl, Dezimalzahl, Boolescher Wert, Datum, Textliste und Ganzzahlliste. Schlüssel unterscheiden zwischen Groß- und Kleinschreibung und müssen eindeutig sein. **Schlüssel hinzufügen** fügt eine Zeile hinzu; **Konfiguration entfernen** entfernt alle Schlüssel.
- **Variablen**: Werte vom Typ Text und Textliste können $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$ und $UDID$ enthalten, die durch die Werte des jeweiligen Geräts und seines Benutzers ersetzt werden. Eine Variable ohne Wert (zum Beispiel $EMAIL$ auf einem Gerät ohne Benutzer) bleibt leer, und die Systemprotokolle geben dies an. Wenn sich die Daten eines Benutzers ändern, erhalten die Geräte die neuen Werte; bei Benutzern, die aus Google Directory synchronisiert werden, werden die Werte bei der nächsten Änderung der Richtlinie oder des Geräts aktualisiert.
- **Konfiguration importieren**: Öffnen oder fügen Sie die Datei ein, die der Hersteller der App für MDM veröffentlicht, und klicken Sie dann auf **Lesen**. Eine **AppConfig-Spezifikationsdatei** (specfile.xml) listet jeden von der App unterstützten Schlüssel mit Beschreibung, Typ, Standardwert und zulässigen Werten auf: Wählen Sie die zu importierenden Schlüssel aus (diejenigen mit Standardwert sind bereits ausgewählt) und füllen Sie die übrigen nach dem Import aus. Ein Warnhinweis erscheint, wenn die Spezifikationsdatei für eine andere App gilt. Eine **Property List** (eine vollständige Property List oder nur ihr <dict>) wird unverändert importiert. Wählen Sie anschließend, ob die aktuellen Schlüssel ersetzt oder ergänzt werden sollen. Verschachtelte Wörterbücher, Datenwerte und Listen mit gemischten oder unbekannten Typen werden nicht unterstützt und als übersprungen aufgeführt. Apple veröffentlicht die Konfigurationsschlüssel von Apps nicht; fragen Sie daher beim Hersteller nach der Datei, wenn sie nicht in dessen Dokumentation enthalten ist. **Als plist kopieren** kopiert die Konfiguration so, wie das Gerät sie erhält, bevor die Variablen ersetzt werden.
- **Grenzwerte**: bis zu 200 Schlüssel pro App; Schlüssel bis zu 255 Zeichen; Textwerte bis zu 4.096 Zeichen; Listen bis zu 200 Einträge mit jeweils bis zu 1.024 Zeichen; Datumsangaben zwischen 1970 und 9999; insgesamt 64 KB pro App.
- **Nicht für Passwörter**: Die Konfiguration wird nur an das Gerät gesendet, für das sie erstellt wurde, und die Protokolle zeigen nur Schlüsselnamen und -typen. Dashboard-Administratoren können die Werte jedoch lesen, und die Adresse, von der das Gerät sie

herunterlädt, ändert sich mit den Werten, sodass ein leicht zu erratender Wert (ein boolescher Wert oder eine kleine Zahl) daraus abgeleitet werden könnte. Legen Sie keine Passwörter oder andere Geheimnisse in einer verwalteten Konfiguration ab.
- **Status**: Wenn das Gerät meldet, dass die App seine Konfiguration nicht akzeptiert hat, zeigt das Panel Anwendungen des Geräts neben der App **Konfiguration nicht akzeptiert** an. Dadurch verliert das Gerät nicht seine Compliance. Eine Konfiguration, die das Gerät nicht herunterladen kann, führt jedoch dazu, dass es die Compliance verliert.

App-Optionen

Jede App der Richtlinie (App Store- und benutzerdefinierte Apps) hat diese Optionen. **Gerätestandard** überlässt die Wahl dem Gerät. Geräte, die eine Option nicht unterstützen, erhalten sie nicht; die App wird dennoch installiert.

- **Automatische Updates**: App Store-Einstellung, Immer oder Nie. iOS, iPadOS, macOS und visionOS 26 oder höher. Bei benutzerdefinierten Apps verhält sich die App Store-Einstellung wie Nie.
- **Downloads über Mobilfunk**: App Store-Einstellung, Immer oder Nie, für automatische Installationen und Updates. Nur überwachte iPhones und iPads mit iOS oder iPadOS 26 oder höher.
- **App-Daten sichern**: ob die App-Daten in die Gerätesicherungen einbezogen werden. Nicht auf dem Mac.
- **Benutzer kann die App ausblenden** und **Benutzer kann die App sperren**: iOS und iPadOS 18.1 oder höher, erzwungen auf überwachten Geräten. Wenn das Sperren nicht erlaubt ist, wird auch das Ausblenden verhindert. Die Einschränkungen **Ausblenden von Apps erlauben** und **Sperren von Apps erlauben** gelten für alle Apps.
- **Gerät nach Tap to Pay-Transaktionen sperren, die die PIN des Kunden erfordern** : nur iPhone.
- **Zugeordnete Domains**: die Domains, mit denen die App verknüpft ist (zum Beispiel für universelle Links oder die Passwort-Autofüllung), bis zu 50. Geben Sie einfache Hostnamen wie www.example.com ein, ohne applinks:, Platzhalter oder ?mode=. Nicht auf dem Mac.
- **Domains direkt überprüfen**: Das Gerät prüft die Site-Association-Datei der Domains direkt und nicht über die Server von Apple. Aktivieren Sie dies nur für interne Domains, die nicht über das Internet erreichbar sind.
- **Entfernung**: Apps, die als **Erforderlich** installiert wurden, können vom Benutzer nicht entfernt werden.

Mac App Store-Apps

Die App-Auswahlliste zeigt die Plattformen jeder App (iPhone/iPad, Mac, Apple TV, Vision); eine App, die nur für Mac existiert, zeigt ihr Mac-Symbol. Eine App, die nur für Mac existiert, gilt beim Hinzufügen für Macs. Eine App Store-App ohne Mac-Version wird nicht an Macs gesendet: Die

Richtlinie zeigt unter **Gilt für** „Diese App hat keine Mac-Version: Sie wird nicht an Macs gesendet“. Macs erhalten App Store-Apps anhand ihrer App Store-ID, sodass Apps mit einer anderen Bundle-ID auf dem Mac korrekt installiert werden.

Cerberus Enterprise App

Cerberus installiert seine **Cerberus Enterprise**-App auf jedem iPhone und iPad mit **iOS oder iPadOS 18.4 oder neuer**, mit oder ohne Richtlinie. Die App teilt den Gerätestandort und empfängt Benachrichtigungen und Live-Ortungsanforderungen. Sie wird als **Erforderlich** mit einer Gerätelizenz aus Apps and Books (einer Benutzerlizenz auf privaten Geräten) installiert, sodass der Benutzer sie nicht löschen kann.

- **Einmalige Einrichtung**: Fügen Sie die kostenlose App einmal zu Ihrer Mediathek hinzu. Öffnen Sie in Apple Business **Apps & Services** → **Apps & Books** → **App Store**, suchen Sie nach „Cerberus Enterprise“, klicken Sie auf **View** und dann auf **Add**, wählen Sie **All current and future** in **Organizational Units**, klicken Sie auf **Add** und dann auf **Review** und bestätigen Sie. Wenn die App **Manage** anzeigt, ist sie bereits in Ihrer Mediathek: Öffnen Sie sie und prüfen Sie, ob ihre Organisationseinheiten **All current and future units** sind. Bis dahin zeigt das Dashboard ein Banner an und die Geräte zeigen die App als nicht installiert. Siehe **Kontoeinstellungen**.
- **Nicht in Richtlinien**: Die App kann einer Richtlinie nicht hinzugefügt werden. Sie ist in der App-Auswahlliste deaktiviert und wird als benutzerdefinierte App abgelehnt (gleiche Bundle-ID). Bei einer Richtlinie, die sie bereits auflistet, wird der Eintrag beim Öffnen entfernt: Speichern Sie die Richtlinie, um dies zu bestätigen.
- **Nicht installiert auf**: Geräten mit iOS oder iPadOS älter als 18.4. Shared iPad wird für die Installation unterstützt, aber die App-Funktionen sind dort nicht verifiziert.
- **Private Geräte**: Auf iPhones und iPads, die mit der Benutzerregistrierung registriert sind, wird die App ebenfalls installiert, mit einer Installationsaufforderung und einer Benutzerlizenz des Managed Apple Account. Sie empfängt Nachrichten von Ihrer Organisation und greift nicht auf den Standort zu, es sei denn, die Richtlinie aktiviert **Standort und Geofences auf privaten Geräten** und der Benutzer lässt es zu.
- **Installiert beibehalten**: Wenn das Apps and Books-Token abläuft oder die App Ihre Mediathek verlässt, bleibt die App auf den Geräten und die Geräteseite meldet, dass Apps and Books Aufmerksamkeit erfordert. Sie wird nur entfernt, wenn die App 24 Stunden später noch immer in Ihrer Mediathek fehlt.

Benutzerdefinierte Apps

Benutzerdefinierte Apps sind Ihre eigenen iPhone- und iPad-Apps (.ipa-Dateien), die ohne den App Store verteilt werden. Exportieren Sie die App in Xcode für die **Enterprise**-Verteilung (Apple Developer Enterprise Program: Sie installiert sich auf jedem Gerät) oder die **Ad Hoc**-Verteilung (Sie installiert sich nur auf den Geräten, die in ihrem Bereitstellungsprofil registriert sind). App Store-Builds können nicht hochgeladen werden.

Klicken Sie auf **Benutzerdefinierte App hinzufügen**, um die benutzerdefinierten Apps Ihrer Organisation zu öffnen. **App hochladen** fügt eine .ipa-Datei hinzu (bis zu 2 GB). Wählen Sie eine App aus und klicken Sie auf **Zur Richtlinie hinzufügen**. Die Liste zeigt die Version, die Art der Signierung, die Anzahl der Geräte im Profil von Ad-hoc-Apps und das Ablaufdatum des Bereitstellungsprofils.

- **Neue Version**: Laden Sie eine App mit derselben Bundle-ID hoch. Sie ersetzt die vorherige Version, und die Geräte der Richtlinien, die sie verwenden, aktualisieren die App.
- **Voraussetzungen**: iPhone und iPad mit iOS 17.2 oder höher. Geräte, die die App nicht installieren können, erhalten sie nicht: eine reine iPad-App auf einem iPhone, ein älteres iOS als von der App benötigt, ein Gerät, das nicht im Profil einer Ad-hoc-App enthalten ist, oder ein abgelaufenes Bereitstellungsprofil.
- **Ablauf**: Wenn das Bereitstellungsprofil abläuft, öffnet sich die App nicht mehr. Laden Sie vor dem Ablaufdatum eine mit einem neuen Profil signierte Version hoch.
- **Reservierte Bundle-ID**: Eine benutzerdefinierte App mit der Bundle-ID der Cerberus Enterprise App (com.lsdroid.Cerberus.Enterprise) kann einer Richtlinie nicht hinzugefügt werden, da Cerberus diese App selbst installiert.
- **Löschen**: Entfernen Sie die App zuerst aus ihren Richtlinien; die Geräte entfernen sie dann.

Mac-Pakete

Die benutzerdefinierten Apps akzeptieren auch Mac-Installer-Pakete (.pkg-Dateien). Das Paket muss ein Distributionspaket sein, das mit **productbuild** erstellt wurde (ein Komponentenpaket, das nur mit pkgbuild erstellt wurde, wird abgelehnt), und mit einem **Developer ID Installer**-Zertifikat signiert sein. Es wird empfohlen, es zu notarisieren und das Ticket anzuheften (**notarytool** und **stapler**). Nicht signierte Pakete, nach der Signierung geänderte Pakete und mit anderen Zertifikaten signierte Pakete werden abgelehnt.

Laden Sie die .pkg-Datei mit **App hochladen** hoch und fügen Sie sie der Richtlinie hinzu: Sie erscheint unter **Mac-Pakete**. iPhones und iPads ignorieren sie.

Macs mit **macOS 26 oder neuer** (überwacht, was auch manuell registrierte Macs einschließt, aber nicht User Enrollment) erhalten das Paket als **Deklaration**: Der Mac lädt es herunter, installiert es, wiederholt den Vorgang bei Bedarf und aktualisiert es selbstständig und meldet seinen Status. Ältere Macs und als verwaltete Apps installierte Pakete erhalten es mit einem **MDM-Befehl**, in jeder macOS-Version. Ein Mac, der auf macOS 26 aktualisiert wird, wechselt selbstständig zur Deklaration; er installiert jedes Paket möglicherweise noch einmal. Dasselbe kann passieren, wenn ein Mac zu einer anderen Richtlinie wechselt, die dasselbe Paket enthält.

- **Neue Version**: Laden Sie ein Paket mit derselben Paketkennung hoch. Es ersetzt die vorherige Version, und die Macs der Richtlinien, die es verwenden, installieren die neue Version.

- **Übersprungene Macs**: Macs mit einem älteren macOS als vom Paket erlaubt und Intel-Macs bei Paketen, die nur für Apple silicon erstellt wurden. Die Geräteseite zeigt das Paket als Übersprungen mit der Begründung an; die zuvor installierte Version bleibt auf dem Mac.
- **Installieren**: **Erforderlich** (Standard) installiert das Paket auf dem Mac; **Optional** stellt das Paket auf dem Mac bereit, ohne es zu installieren. macOS 26 zeigt optionale Pakete dem Benutzer nicht in den Systemeinstellungen oder im App Store an (getestet unter macOS 26.3), daher muss eine App oder ein Skript auf dem Mac sie installieren; wählen Sie Optional nur, wenn Sie eine solche haben. Dies gilt für Macs mit macOS 26 oder neuer; ältere Macs installieren das Paket immer. Die Auswahl ist für als verwaltete Apps installierte Pakete nicht verfügbar.
- **Paketdateien entfernen, wenn es die Richtlinie verlässt (macOS 27 oder neuer)**: Wenn das Paket aus der Richtlinie entfernt wird, löschen Macs mit macOS 27 oder neuer die von ihm installierten Dateien. Die Option ist standardmäßig deaktiviert. Auf älteren Macs bleiben die Dateien erhalten. Für als verwaltete Apps installierte Pakete nicht verfügbar.
- **Als verwaltete App installieren**: Aktivieren Sie dies für ein Paket der Richtlinie, um seine App als verwaltete App zu installieren (macOS 11 oder neuer, nicht mit User Enrollment). macOS meldet dann, wenn die Installation fehlschlägt, und MDM kann die App entfernen. Die App muss direkt im Ordner „Programme“ installiert, mit einem **Developer ID Application**-Zertifikat signiert und notarisiert sein; unter macOS 11 bis 13 darf das Paket nur diese App enthalten (keine anderen Dateien oder Skripte). Die benutzerdefinierten Apps zeigen, welche Pakete geeignet sind. Wenn die Option auf einem Mac nicht angewendet werden kann, wird das Paket dort wie üblich installiert und die Geräteseite nennt den Grund.
- **Entfernungsoptionen** einer verwalteten App: **Die App entfernen, wenn das Paket aus der Richtlinie entfernt wird** (standardmäßig aktiviert) und **Die App entfernen, wenn der Mac die Verwaltung verlässt**. Das Entfernen einer App löscht auch ihre Daten. Wenn der Benutzer dieselbe App bereits installiert hatte, wird diese Kopie verwaltet und ebenfalls entfernt.
- **Entfernung**: Der MDM-Befehl kann ein Paket nicht deinstallieren. Bei einem als verwaltete App installierten Paket wird durch Entfernen aus der Richtlinie die App entfernt (wenn die Option aktiviert ist); ihre anderen Dateien und der Paketbeleg bleiben erhalten. Pakete mit aktivierter Option **Paketdateien entfernen** werden von Macs mit macOS 27 oder neuer entfernt. Bei anderen Paketen: Das Entfernen aus der Richtlinie stoppt nur neue Installationen, die Dateien bleiben auf den Macs. Ein übersprungener Mac (zum Beispiel nach einer neuen Version, die ein neueres macOS erfordert) behält die App, solange das Paket in der Richtlinie ist; wird das Paket dann aus der Richtlinie entfernt, wird auch die App entfernt. Entfernen Sie verbleibende Dateien auf dem Mac (zum Beispiel mit dem eigenen Deinstallationsprogramm des Pakets), und führen Sie `sudo pkgutil --forget <identifier>` aus, um den Paketbeleg zu vergessen.
- **Status auf dem Gerät**: Das Bedienfeld „Anwendungen“ des Macs zeigt jedes Paket der Richtlinie als In der Warteschlange, Akzeptiert (der Mac hat den Befehl akzeptiert), Heruntergeladen, Installiert (nur für Pakete, die Apps enthalten, wenn die Apps auf dem Mac gefunden werden) oder Fehlgeschlagen (mit dem Fehler) an. macOS meldet die

Installation eines mit dem Befehl gesendeten Pakets nicht, daher ist Heruntergeladen der letzte Status für Pakete ohne Apps. Ein als verwaltete App installiertes Paket wird ebenfalls Fehlgeschlagen, wenn macOS meldet, dass die App nicht installiert werden konnte oder vom Mac entfernt wurde. **Erneut installieren** sendet das Paket erneut an den Mac.

- **Status mit der Deklaration**: Als Deklaration bereitgestellte Pakete zeigen den **Deklaration**-Chip und den Status, den der Mac meldet: In der Warteschlange, Verfügbar (ein optionales Paket, das der Benutzer nicht installiert hat), Warten auf den Benutzer, Wird heruntergeladen, Wird installiert, Installiert oder Fehlgeschlagen (mit der Begründung, zum Beispiel ein fehlgeschlagener Download oder eine fehlgeschlagene Installation oder eine vom Mac abgelehnte Deklaration). Der Chip **Dateien mit der Richtlinie entfernt** kennzeichnet Pakete, deren Dateien ein Mac mit macOS 27 entfernt, wenn sie die Richtlinie verlassen. **Erneut installieren** wird nur nach einem Fehler angezeigt und fordert den Mac auf, es erneut zu versuchen; es wird nicht angeboten, wenn der Mac die Deklaration abgelehnt hat.

Konten

Das Fenster **Konten** ermöglicht Ihnen die Konfiguration von Konten, die auf verwaltete Geräte angewendet werden. Es enthält außerdem einen Schalter für die Einschränkung der Kontomodifikation.

Einschränkung

- **Kontomodifikation erlauben**: Wenn deaktiviert, können Benutzer keine Konten wie Apple Accounts und Internetkonten ändern.

Konten hinzufügen

Verwenden Sie **Google-Konto hinzufügen** oder **Mail-Konto hinzufügen**, um Konto-Payloads zur Richtlinie hinzuzufügen. Jedes Konto erscheint als Karte mit seinen Konfigurationsfeldern.

Kontozugangsdaten von Benutzern

Sowohl Google- als auch Mail-Konto-Karten bieten einen Schalter **Kontozugangsdaten von Benutzern**. Wenn aktiviert, wendet das System die Kontozugangsdaten pro Benutzer an. Wenn deaktiviert, geben Sie die Kontoidentität in der Richtlinie ein.

Felder für Google-Konten

- **Sichtbarer Name**: der dem Benutzer für das Konto angezeigte Name.
- **Google-E-Mail-Adresse**: die E-Mail-Adresse des Benutzers.
- **Vollständiger Name**: der vollständige Name des Benutzers.

Felder für Mail-Konten

Mail-Konten umfassen Identitätsfelder sowie die Konfiguration des Posteingangs- und Postausgangsservers. Hostnamen sind erforderlich.

- **Sichtbarer Name**: der dem Benutzer für das Mail-Konto angezeigte Name.
- **E-Mail-Adresse**: die E-Mail-Adresse des Benutzers.
- **Vollständiger Name**: der vollständige Name des Benutzers.

Posteingangsserver

- **Servertyp**: Mailprotokoll (zum Beispiel IMAP oder POP).
- **Authentifizierungsmethode**: Authentifizierungsmethode für den Server.
- **IMAP-Pfadpräfix**: wird nur angezeigt, wenn der Servertyp IMAP ist.
- **Hostname**: erforderlich.
- **Port**: Serverport (1–65535).

Postausgangsserver

- **Authentifizierungsmethode**
- **Hostname**: erforderlich.
- **Port**: Serverport (1–65535).

S/MIME-Optionen

Für Mail-Konten können Sie auch das S/MIME-Verschlüsselungs- und Signierungsverhalten konfigurieren.

Verschlüsselung

- **S/MIME-Verschlüsselung**
- **Identität durch Benutzer überschreibbar**
- **Schalter pro Nachricht aktiviert**
- **Durch Benutzer überschreibbar**

Signierung

- **S/MIME-Signierung**
- **Identität durch Benutzer überschreibbar**

- **Durch Benutzer überschreibbar**

> Konto- und Einschränkungsoptionen enthalten Tooltips im Dashboard, die Voraussetzungen und unterstützte Betriebssystemversionen dokumentieren.

Kiosk und Home-Bildschirm

Der Abschnitt **Kiosk und Home-Bildschirm** des Apple-Richtlinieneditors sperrt Geräte in eine App, wählt aus, welche Apps geöffnet werden dürfen, ordnet den Home-Bildschirm an und fügt Websitesymbole hinzu. Jede Einstellung wird auf den Geräten als Konfigurationsprofil installiert.

> Apple wendet die meisten dieser Einstellungen nur auf überwachte iPhones und iPads an (Geräte, die mit Automated Device Enrollment registriert oder mit Apple Configurator vorbereitet wurden). Andere Geräte erhalten sie nicht. Webclips funktionieren auch auf nicht überwachten iPhones und iPads. Macs erhalten keine dieser Einstellungen.

Apps auswählen

Apps werden anhand ihrer Bundle-ID identifiziert. Geben Sie den Namen einer App ein, um sie aus den integrierten Apple Apps und den Apps der Richtlinie auszuwählen, oder geben Sie eine beliebige Bundle-ID ein, zum Beispiel `com.example.app`.

Einzelapp-Modus

Das Gerät führt nur die ausgewählte App aus: Benutzer können nicht zum Home-Bildschirm zurückkehren oder andere Apps öffnen. Installieren Sie die App zuerst mit der Richtlinie. Das Gerät verlässt den Einzelapp-Modus, wenn Sie die Einstellung deaktivieren oder die App entfernen.

- **Optionen**: Deaktivieren Sie den Touchscreen, die Rotation, die Lautstärketasten, den Klingel-/Stumm-Schalter, die Seitentaste oder die automatische Sperre, und aktivieren Sie Bedienungshilfen wie VoiceOver oder Zoom.
- **Bedienungshilfen, die der Benutzer aktivieren kann**: Funktionen, die der Benutzer durch dreifaches Drücken der Seitentaste aktivieren kann.

Erlaubte und blockierte Apps

- **Blockierte Apps**: die Geräte blenden diese Apps aus und öffnen sie nicht. `com.apple.webapp` blockiert alle Webclips. Einstellungen und auf dem iPhone Telefon können nicht blockiert werden.

- **Nur einige Apps erlauben**: Die Geräte zeigen nur diese Apps an. Lassen Sie die Liste leer, um alle Apps zu erlauben. **Richtlinien-Apps** fügt die von der Richtlinie installierten Apps hinzu; `com.apple.webapp` erlaubt alle Webclips.
- **Apps, die den Einzelapp-Modus starten können**: Apps, die das Gerät während ihrer Nutzung in sich selbst sperren können, zum Beispiel während einer Prüfung.

> Mit **Nur einige Apps erlauben** verschwindet jede App, die nicht in der Liste steht, von den Geräten, einschließlich der Apps der Richtlinie. Einstellungen und auf dem iPhone Telefon bleiben immer erhalten.

Layout des Home-Bildschirms

Ordnen Sie das Dock und die Seiten des Home-Bildschirms an. Fügen Sie Apps, App-Ordner und die Webclips der Richtlinie hinzu, indem Sie mit **Hinzufügen zu** den Ort auswählen, und ziehen Sie die Symbole, um sie zwischen dem Dock und den Seiten zu verschieben. Klicken Sie auf einen Ordner, um seinen Namen und seine Apps zu ändern.

Benutzer können die Symbole nicht verschieben oder Apps vom Home-Bildschirm entfernen. Apps, die nicht im Layout enthalten sind, werden auf den Seiten nach den von Ihnen definierten angezeigt. Ein iPhone zeigt vier Symbole im Dock. Benutzer können Apps, die nicht Erforderlich sind, weiterhin im Speicherbildschirm der Einstellungen löschen. Um dies zu verhindern, deaktivieren Sie **Entfernen von Apps erlauben** in der App-Verwaltung.

Webclips

Ein Webclip ist ein Symbol auf dem Home-Bildschirm, das eine Website öffnet. Legen Sie die Bezeichnung und die URL und optional ein Bild fest (PNG oder JPEG, auf ein Quadrat zugeschnitten).

- **Benutzer können ihn entfernen**: Deaktivieren Sie die Option, damit das Symbol auf den Geräten bleibt.
- **Vollbild**: Die Website wird als Web-App ohne die Adressleiste von Safari geöffnet. **Bei anderen Websites im Vollbild bleiben** öffnet auch die Links zu anderen Websites in der Web-App.
- **Mit dieser App öffnen**: eine App, die die URL anstelle von Safari öffnet.

Mitteilungseinstellungen

Wählen Sie aus, wie die Geräte die Mitteilungen einiger Apps anzeigen: ob sie erlaubt sind, wo sie erscheinen (Sperrbildschirm, Mitteilungszentrale, CarPlay), Badges, Töne, kritische Warnungen, Bannerstil, Gruppierung und Vorschauen. Benutzer können diese Einstellungen nicht ändern.

Sperrbildschirmnachricht

Eine Nachricht, die unten auf dem Sperrbildschirm angezeigt wird, zum Beispiel wen man anrufen soll, wenn das Gerät gefunden wird, und eine Inventarnummer. Beide können die Variablen $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$ und $UDID$ enthalten: Eine Variable ohne Wert für das Gerät bleibt leer.

Code

Der Abschnitt **Codeeinstellungen** steuert die Anforderungen an den Gerätecode und die damit verbundenen Sicherheitsregeln (zum Beispiel Mindestlänge und Komplexität). Auf einem Mac (macOS 13 oder neuer, nicht mit User Enrollment) gelten die Regeln für das Anmeldepasswort der Benutzer.

Optionen

Im Apple-Richtlinieneditor werden Codeoptionen mit einer Mischung aus Schaltern und Zahlenfeldern konfiguriert. Viele Felder enthalten Tooltips, die unterstützte Betriebssystemversionen und Überwachungsanforderungen angeben.

Code-Schalter

- **Bei nächster Authentifizierung ändern**: erzwingt das Zurücksetzen des Codes bei der nächsten Authentifizierung des Benutzers.
- **Alphanumerischen Code verlangen**: verlangt mindestens ein alphabetisches Zeichen und eine Zahl.
- **Komplexen Code verlangen**: verlangt einen „komplexen“ Code (keine wiederholten oder fortlaufenden Muster und mindestens ein nicht alphanumerisches Zeichen).
- **Code verlangen**: verlangt einen Code ohne zusätzliche Anforderungen an Länge/Qualität. Hinweis: Das Festlegen anderer Code-Schlüssel setzt implizit einen Code voraus.

Zahlenfelder

- **Zurücksetzen fehlgeschlagener Versuche (Minuten)**: Minuten, bevor der Zähler für fehlgeschlagene Versuche zurückgesetzt wird (erfordert Maximale fehlgeschlagene Versuche).
- **Maximale fehlgeschlagene Versuche**: erlaubte fehlgeschlagene Versuche, bevor ein iPhone oder iPad gelöscht oder ein Mac gesperrt wird (Bereich: 2–11).
- **Maximale Kulanzfrist (Minuten)**: wie lange das Gerät entsperrt bleiben kann, ohne den Code zu verlangen (0 = keine).
- **Maximale Inaktivität (Minuten)**: Leerlaufzeit, bevor das Gerät sperrt (Bereich: 0–15).
- **Maximales Alter des Codes (Tage)**: maximales Alter des Codes vor einer erzwungenen Änderung (Bereich: 0–730).
- **Minimale komplexe Zeichen**: Mindestanzahl „komplexer“ Zeichen (Bereich: 0–4).

- **Minimale Länge**: Mindestlänge des Codes (Bereich: 0–16).
- **Wiederverwendungslimit für Codes**: Länge des Code-Verlaufs, um die Wiederverwendung alter Codes zu verhindern (Bereich: 1–50).

Einschränkungen

Die Abschnitte „Einschränkungen“ steuern, welche Betriebssystemfunktionen auf verwalteten Apple-Geräten erlaubt sind. Im Apple-Richtlinieneditor werden diese Optionen als gruppierte Bedienfelder mit mehreren Schaltern dargestellt.

Die Schalter der Bereiche **App-Verwaltung** und **Netzwerk** werden auf den Seiten Apps & Profile und Netzwerk der Apple-Richtlinien beschrieben.

> Viele Einschränkungen werden nur in bestimmten Betriebssystemversionen unterstützt und erfordern möglicherweise überwachte Geräte. Verwenden Sie die Tooltips im Dashboard für verbindliche Anforderungen.

> Auf Geräten mit User Enrollment (persönliche Geräte, die durch Anmelden mit einem Arbeitskonto registriert wurden) werden die Einschränkungen, die Apple dort nicht zulässt, nicht gesendet. Wenn keine der Einschränkungen der Richtlinie gilt, erhalten diese Geräte kein Einschränkungsprofil. Der Richtlinieneditor zeigt an, wie viele Einschränkungen nicht für Geräte mit User Enrollment gelten.

Sicherheit

- **Automatisches Entsperren erlauben**
- **Fingerabdruck zum Entsperren erlauben**
- **Fingerabdruckänderung erlauben**
- **Löschen von Inhalt und Einstellungen erlauben**
- **Aktivieren von Einschränkungen erlauben**
- **Profilinstallation durch Benutzer erlauben**
- **Host-Kopplung erlauben**
- **Übermittlung von Diagnosedaten erlauben**
- **Änderung der Übermittlung von Diagnosedaten erlauben**
- **Personalisierte Werbung von Apple erlauben**
- **Änderung der Remote-Verwaltung erlauben**

Multimedia

- **Kamera erlauben**
- **Änderungen an der Dateifreigabe erlauben**
- **Zugriff von Dateien auf USB-Laufwerke erlauben**
- **Anrufaufzeichnung erlauben**
- **AirPrint erlauben**
- **Speichern von AirPrint-Anmeldedaten erlauben**
- **iBeacon-Erkennung für AirPrint erlauben**

Mobilfunk

- **Änderung der App-Mobilfunkdaten erlauben**
- **Änderung des Mobilfunkplans erlauben**
- **eSIM-Änderung erlauben**
- **Ausgehende eSIM-Übertragungen erlauben**
- **eSIM beim Löschen des Geräts behalten**
- **Hintergrundabruf beim Roaming erlauben**

Mobilfunk-APN

Mobilfunk-APN legt den Zugangspunktnamen (APN) fest, den Ihnen Ihr Mobilfunkanbieter gegeben hat, zum Beispiel für ein privates oder geschäftliches Mobilfunknetz. Legen Sie den **Zugangspunktnamen** sowie, falls der Anbieter sie verlangt, die Authentifizierung (PAP oder CHAP), den Benutzernamen (Variablen wie $EMAIL$ sind erlaubt), das Passwort, die IP-Versionen (auch beim Roaming), einen Proxy-Server mit seinem Port und XLAT464 fest. Aktivieren Sie **APN anhängen** nur, wenn der Anbieter Ihnen einen separaten APN für die Verbindung zum Netzwerk gibt.

- Nur iPhone und iPad mit Mobilfunk erhalten sie, auch ohne Überwachung. Geräte, die mit User Enrollment registriert wurden (persönliche Geräte), erhalten sie nicht.
- Sie gilt nur für die für mobile Daten verwendete SIM. Ein Gerät, auf dem bereits auf andere Weise ein APN-Profil installiert ist, installiert sie nicht.
- Das Passwort ist wie die anderen Netzwerkpasswörter geschützt: Das Profil wird nur an das Gerät gesendet, für das es erstellt wurde, und das Passwort wird nicht in den Protokollen geschrieben.

> Ein falscher APN lässt die Geräte ohne mobile Daten zurück: Testen Sie die Einstellungen zuerst auf einem Testgerät mit einer SIM des Anbieters.

System und Benutzeroberfläche

- **Handoff erlauben**
- **Autokorrektur erlauben**
- **Automatisches Dimmen erlauben**
- **Automatischen Bildschirmschoner erlauben**
- **QuickPath-Tastatur erlauben**
- **Nachschlagen von Definitionen erlauben**
- **Änderung des Gerätenamens erlauben**
- **Ruhezustand des Geräts erlauben**
- **iPhone-Spiegelung erlauben**
- **iPhone-Widgets auf dem Mac erlauben**
- **Tastaturkürzel erlauben**

Apple-Apps und -Dienste

- **iMessage erlauben**
- **Game Center erlauben**
- **Hinzufügen von Game Center-Freunden erlauben**
- **Find My-Gerät erlauben**
- **Find My-Freunde erlauben**
- **Änderung von Find My-Freunde erlauben**
- **Book Store erlauben**
- **Erotik im Book Store erlauben**
- **Sicherung von Unternehmensbüchern erlauben**
- **Synchronisierung von Metadaten von Unternehmensbüchern erlauben**
- **iTunes Store erlauben**
- **Explizite Inhalte erlauben**

Siri und Apple Intelligence

- **Siri erlauben**
- **Benutzergenerierte Siri-Inhalte erlauben**
- **Siri bei gesperrtem Gerät erlauben**
- **Diktat erlauben**
- **Integrationen externer Intelligenz erlauben**
- **Anmeldung bei externer Intelligenz erlauben**
- **Genmoji erlauben**
- **Image Playground erlauben**
- **Image Wand erlauben**

iCloud

- **iCloud-Adressbuch erlauben**
- **iCloud-Backup erlauben**
- **iCloud-Lesezeichen erlauben**
- **iCloud-Kalender erlauben**
- **iCloud-Schreibtisch und -Dokumente erlauben**
- **iCloud-Dokumentsynchronisierung erlauben**
- **iCloud Freeform erlauben**
- **iCloud-Schlüsselbund-Synchronisierung erlauben**
- **iCloud Mail erlauben**
- **iCloud Notizen erlauben**
- **iCloud-Fotomediathek erlauben**
- **iCloud Private Relay erlauben**
- **iCloud Erinnerungen erlauben**

Konten (Einschränkung)

Das Konten-Panel enthält sowohl eine Einschränkung als auch (optional) eine Kontokonfiguration. Mit dem Schalter für die Einschränkung legen Sie fest, ob der Benutzer Systemkonten ändern darf.

- **Kontenänderung erlauben**

Netzwerk

Der Abschnitt **Netzwerk** des Apple-Richtlinieneditors konfiguriert Wi-Fi-Netzwerke und VPNs auf den Geräten, installiert Zertifikate und schränkt Konnektivitätsfunktionen wie AirDrop und Bluetooth ein. Jedes Wi-Fi-Netzwerk, VPN und Zertifikat wird als eigenes Konfigurationsprofil installiert, das Sie auf dem Gerät unter **Einstellungen > Allgemein > VPN & Geräteverwaltung** (Mac: **Systemeinstellungen > Allgemein > Geräteverwaltung** oder **Datenschutz & Sicherheit > Profile** unter macOS 13 und 14) und im Bereich **Profile, Zertifikate und Sicherheit** der Geräteseite sehen können.

> Zertifikate stammen von der Seite **Zertifikate**: Importieren Sie sie zuerst dort. Die Richtlinie verweist nur auf sie, daher wird ein Zertifikat nie in die Richtlinie kopiert.

Einschränkungen

- **AirDrop erlauben**
- **Eingehende AirPlay-Anfragen erlauben**
- **Bluetooth-Änderung erlauben**
- **Änderung der Bluetooth-Freigabe erlauben**
- **Zugriff von Dateien auf Netzwerklaufwerke erlauben**
- **Änderung der Internetfreigabe erlauben**
- **Inhalts-Caching erlauben**
- **iTunes-Dateifreigabe erlauben**

Wi-Fi-Netzwerke

Klicken Sie auf **Wi-Fi-Netzwerk hinzufügen** und füllen Sie aus:

- **Netzwerkname (SSID)**: der Name des Netzwerks, bis zu 32 Zeichen.
- **Sicherheit**: keine (offenes Netzwerk), WEP, WPA oder WPA2, WPA2 oder WPA3, nur WPA3 oder beliebig.
- **Passwort**: das Passwort eines persönlichen Netzwerks.
- **Automatisch beitreten** und **Verborgenes Netzwerk** (für Netzwerke, die ihren Namen nicht senden).
- **Proxy**: keiner, manuell (Server und Port) oder automatisch (eine PAC-Datei-URL oder leer, um die Einstellungen mit WPAD im Netzwerk zu finden).

- **Profilname** (optional) und **Gilt für**, um das Netzwerk auf bestimmte Gerätetypen zu beschränken.

Unternehmensnetzwerke (802.1X)

Aktivieren Sie **Unternehmen (802.1X)**, wenn Benutzer sich mit ihren eigenen Zugangsdaten oder einem Zertifikat anstelle eines gemeinsam genutzten Passworts authentifizieren.

- **Authentifizierung**: PEAP, TTLS (mit ihrer inneren Authentifizierung, zum Beispiel MSCHAPv2) oder TLS (nur Zertifikat).
- **Zugangsdaten des Gerätebenutzers**: Jedes Gerät verwendet die EAP-Identität, die anonyme Identität und das Passwort seines Benutzers, die auf der Seite „Benutzer“ festgelegt sind. Geräte ohne Benutzer erhalten das Netzwerk nicht.
- **Identität**, **Anonyme Identität** und **Passwort**: für jedes Gerät gleich. Die Identität kann die Variablen $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$ und $UDID$ enthalten. Lassen Sie das Passwort leer, damit der Benutzer es auf dem Gerät eingeben kann.
- **Identitätszertifikat**: das Client-Zertifikat, das das Gerät vorlegt (für TLS erforderlich). Siehe die Zertifikatoptionen unten.
- **Vertrauenswürdige Zertifikate**: die CA-Zertifikate, die das Zertifikat Ihres RADIUS-Servers ausgestellt haben. Sie werden mit dem Netzwerk installiert.
- **Vertrauenswürdige Servernamen**: die Namen der RADIUS-Serverzertifikate, die die Geräte akzeptieren, zum Beispiel radius.example.com oder *.example.com.

VPN

Klicken Sie auf **VPN hinzufügen**, um ein IKEv2- oder Cisco-IPSec-VPN zu konfigurieren, das in iOS, iPadOS und macOS integriert ist (keine VPN-App erforderlich).

- **Typ** und **Server**. Für IKEv2 außerdem die **Remote-Identität** (die Serveridentität, leer bedeutet die Serveradresse) und die **Lokale Identität**, die die Variablen $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$ und $UDID$ enthalten kann.
- **Authentifizierung** des Geräts: ein Zertifikat (von der Seite „Zertifikate“, das Zertifikat des Gerätebenutzers oder von einem SCEP-Server angefordert), ein gemeinsames Geheimnis (mit dem optionalen Gruppennamen für IPSec) oder keine für IKEv2-Server, die nur Benutzername und Passwort prüfen.
- **Vertrauenswürdige Zertifikate**: die CA-Zertifikate Ihres VPN-Servers, die mit dem VPN installiert werden. Für IKEv2 können Sie auch den erwarteten Aussteller und Namen des Serverzertifikats festlegen.
- **Benutzername und Passwort**: Der Benutzer authentifiziert sich zusätzlich mit einem Benutzernamen (Variablen erlaubt) und einem Passwort (EAP für IKEv2, XAuth für IPSec). Lassen Sie das Passwort leer, damit der Benutzer es auf dem Gerät eingeben kann.
- **VPN-Name** (in den Einstellungen angezeigt) und **Gilt für**.

Verbindung

- **Der Benutzer verbindet sich in den Einstellungen**: Das VPN wird installiert und der Benutzer aktiviert es bei Bedarf.
- **Bei Bedarf**: Das Gerät verbindet das VPN automatisch. Mit **außer in vertrauenswürdigem Wi-Fi** wird das VPN nicht in den von Ihnen aufgeführten Wi-Fi-Netzwerken verwendet, zum Beispiel im Büronetzwerk.
- **Immer an** (nur IKEv2, überwachte iPhones und iPads): Der gesamte Datenverkehr läuft über Mobilfunk und Wi-Fi durch das VPN, und der Benutzer kann es nicht deaktivieren. Andere Geräte erhalten dieses VPN nicht. Wenn das VPN einen Benutzernamen verwendet, muss das Passwort in der Richtlinie festgelegt werden.
- **VPN pro App**: Nur einige Apps verwenden das VPN. Wählen Sie das VPN für jede App im Abschnitt **App-Verwaltung** (Feld **VPN** der App, auf dem Mac nicht verfügbar), und führen Sie optional Safari-Domains auf, die es verwenden.

> Testen Sie ein Immer-an- oder Bei-Bedarf-VPN zuerst auf einem Testgerät: Wenn der Server nicht erreichbar ist, hat das Gerät möglicherweise keine Verbindung.

Globaler Proxy, verschlüsseltes DNS und Webinhaltsfilter

Diese Einstellungen gelten für den gesamten Datenverkehr des Geräts. Aktivieren Sie sie mit ihrem Schalter.

- **Globaler HTTP-Proxy** (überwachte iPhones und iPads, Mac): Der gesamte HTTP-Datenverkehr läuft in jedem Netzwerk über den Proxy. Legen Sie Server und Port (mit optionalem Benutzernamen und Passwort) oder eine automatische Konfiguration fest (PAC-Datei-URL oder leer, um sie im Netzwerk zu finden). **Wi-Fi-Anmeldeseiten erlauben** ermöglicht dem Benutzer, sich ohne den Proxy bei öffentlichen Wi-Fi-Netzwerken anzumelden.
- **Verschlüsseltes DNS**: Das Gerät löst Namen mit Ihrem DNS-Server über DNS over HTTPS (Server-URL) oder DNS over TLS (Servername) auf, optional nur für bestimmte Domains. Auf überwachten Geräten können Sie verhindern, dass der Benutzer es deaktiviert.
- **Webinhaltsfilter** (überwachte iPhones und iPads): Der in iOS integrierte Filter beschränkt Websites für Erwachsene, mit Listen von Websites, die immer erlaubt oder immer blockiert sind, oder erlaubt nur eine Liste von Websites, die in Safari als Lesezeichen angezeigt werden.

>

> Ein falscher Proxy- oder DNS-Server kann die Geräte ohne Verbindung zurücklassen: Testen Sie die Einstellungen zuerst auf einem Testgerät.

Zertifikate

Klicken Sie auf **Zertifikat hinzufügen**, um ein Zertifikat separat zu installieren: eine Zertifizierungsstelle, der Safari und die Apps vertrauen müssen, oder eine von Apps verwendete Identität. Die Zertifikate eines Wi-Fi-Netzwerks oder eines VPNs müssen hier nicht hinzugefügt werden.

Zertifikatoptionen

- **Ein Zertifikat der Seite „Zertifikate“**: dasselbe Zertifikat auf jedem Gerät. Klicken Sie auf **Zertifikat auswählen**, um es auszuwählen.
- **Das Zertifikat des Gerätebenutzers**: Jedes Gerät erhält das mit seinem Benutzer verknüpfte Client-Zertifikat. Geräte, deren Benutzer kein Zertifikat hat, erhalten es nicht. Wenn Sie dem Benutzer ein anderes Zertifikat zuordnen, werden die Geräte aktualisiert.
- **Von einem SCEP-Server angefordert**: Jedes Gerät fordert sein eigenes Zertifikat von Ihrem SCEP-Server an (zum Beispiel Microsoft NDES), sodass der private Schlüssel das Gerät nie verlässt. Legen Sie die Server-URL, die Challenge, falls der Server eine verlangt, den Betreff (zum Beispiel CN=$EMAIL$), die alternativen Namen, die Schlüsselgröße und die Schlüsselverwendung fest.

> Client-Zertifikate (.p12), die mit der alten RC2-Verschlüsselung geschützt sind, können nicht auf Apple-Geräten installiert werden. Exportieren Sie sie vor dem Importieren erneut mit 3DES- oder AES-Verschlüsselung.

Sicherheit

Profile, die Passwörter oder private Schlüssel enthalten, werden nur an das Gerät gesendet, für das sie erstellt wurden: Das Gerät muss seine Anforderung mit seinem Verwaltungszertifikat signieren. Passwörter und Zertifikate werden nicht in den Protokollen geschrieben.

Softwareupdates

Der Bereich **Softwareupdates** des Apple-Richtlinieneditors hält die Geräte auf dem neuesten Stand: Er kann eine bestimmte OS-Version bis zu einer Frist verlangen und steuern, wie die Geräte Updates herunterladen und installieren.

Erforderliche OS-Updates

Klicken Sie auf **Erforderliches Update hinzufügen**, um eine OS-Version zu verlangen. Das Gerät lädt das Update herunter, informiert den Benutzer über die Frist und installiert es bei Fristablauf, falls der Benutzer es nicht vorher erledigt hat. Geräte, die diese Version oder eine neuere bereits ausführen, ignorieren es. Erfordert iOS und iPadOS 17 oder macOS 14.

- **Gilt für** (erforderlich): iPhone und iPad oder Mac. Jedes OS hat eigene Versionsnummern, daher fügen Sie für jedes ein erforderliches Update hinzu.
- **OS-Version**: die zu installierende Version, zum Beispiel 18.5 oder 15.4.1.
- **Build** (optional): ein bestimmter Build, zum Beispiel eine Beta oder eine Background Security Improvement.
- **Installieren bis**: die Frist, in der Ortszeit jedes Geräts. Ein Datum in der Vergangenheit bewirkt, dass die Geräte das Update so bald wie möglich installieren.
- **Details-URL** (optional): eine Webseite über das Update, die dem Benutzer angezeigt wird.

> Das Gerät meldet den Fortschritt des Updates (Download, Installation, Fehler) im Bereich **Gerätestatus** der Geräteseite.

Softwareupdate-Einstellungen

Aktivieren Sie **Softwareupdate-Einstellungen für iPhone und iPad** oder **Softwareupdate-Einstellungen für Mac**, um die Updates auf diesen Geräten zu steuern. Wenn ein Schalter ausgeschaltet ist, behalten die Geräte ihre eigenen Einstellungen. Erfordert iOS und iPadOS 18 oder macOS 15: Ältere Geräte ignorieren diese Einstellungen.

- **Updates verzögern**: Neue Updates werden dem Benutzer erst nach der angegebenen Anzahl von Tagen angezeigt (1 bis 90). Auf einem Mac können Sie unterschiedliche Zeiträume für Hauptupdates, Nebenupdates und andere Systemupdates festlegen.

- **Dem Benutzer angezeigte Updates** (iPhone und iPad): Wenn mehr als ein Update verfügbar ist, zeigen Sie alle an, nur das älteste Nebenupdate oder nur das neueste.
- **Standardbenutzer können Updates installieren** (Mac): Benutzer ohne Administratorrechte können macOS-Updates installieren.
- **Benutzer über erforderliche Updates benachrichtigen**: die Benachrichtigungen über die erforderlichen Updates und ihre Frist anzeigen.
- **Automatischer Download**, **Automatische Installation** und **Automatische Sicherheitsupdates**: Lassen Sie den Benutzer entscheiden (Apple-Standard) oder halten Sie sie immer eingeschaltet oder immer ausgeschaltet.
- **Background Security Improvements**: Bieten Sie dem Benutzer die schnellen Sicherheitskorrekturen von Apple an und wählen Sie, ob der Benutzer sie entfernen kann.
- **Beta-Programme**: Lassen Sie den Benutzer Apple-Beta-Programmen beitreten oder entfernen Sie das Gerät daraus und blockieren Sie sie (nur auf überwachten iPhones und iPads).

Ein Update von der Geräteseite aus installieren

Der Bereich **Gerätestatus** eines Geräts listet die dafür verfügbaren Updates auf. Verwenden Sie **Nach Updates suchen**, um die Liste vom Gerät anzufordern, und **Installieren**, um ein Update jetzt zu installieren oder es herunterzuladen und den Benutzer installieren zu lassen. Dies funktioniert auf überwachten iPhones und iPads sowie auf Macs. Apple entfernt diese Befehle in iOS, iPadOS und macOS 27: Verwenden Sie in diesen Versionen die erforderlichen Updates der Richtlinie.

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.

Standort und Geofences

Der Abschnitt **Standort und Geofences** des Apple-Richtlinieneditors definiert Bereiche, zum Beispiel einen Standort oder ein Lager. iPhones und iPads mit der Cerberus Enterprise-App melden, wenn sie einen dieser Bereiche betreten oder verlassen, und Ereignisregeln können darauf reagieren: eine E-Mail senden, das Gerät sperren oder deaktivieren oder es wieder aktivieren. Macs verwenden keine Geofences.

Geofence-Felder

Verwenden Sie **Geofence hinzufügen**, um einen neuen Eintrag zu erstellen. Eine Richtlinie kann bis zu **10 Geofences** enthalten, und ihre Namen müssen innerhalb der Richtlinie eindeutig sein. Jeder Geofence enthält diese Felder:

- **Name**: erforderlich und eindeutig.
- **Breitengrad** und **Längengrad**: der Mittelpunkt des Bereichs. Sie können ihn auch durch Klicken auf die Karte festlegen.
- **Radius (m)**: erforderlich, von **200** bis **10000** Metern.
- **Beschreibung**: optionale Hinweise für Administratoren.
- **Betreten melden** und **Verlassen melden**: Wählen Sie aus, welche Ereignisse erzeugt werden. Mindestens eine Option muss aktiviert bleiben.
- **Aktiv**: aktiviert oder deaktiviert den Geofence, ohne ihn zu löschen.

Jeder Geofence hat eine Kartenvorschau. Mittelpunkt und Radius eines gespeicherten Geofence sind gesperrt: Verwenden Sie die Sperrschaltfläche auf der Karte, um sie zu ändern. Die anderen Schaltflächen zentrieren die Karte auf den Bereich oder auf Ihren aktuellen Standort.

Wenn Sie die Richtlinie speichern, fordert Cerberus Enterprise die iPhones und iPads der Richtlinie auf, die neuen Geofences abzurufen. Dies dauert normalerweise einige Minuten, aber iOS kann es verzögern, zum Beispiel im Energiesparmodus oder ohne Netzwerkverbindung. Die Geräteseite zeigt an, wenn die App die neuesten Geofences noch nicht angewendet hat.

Voraussetzungen

Geofences funktionieren auf iPhones und iPads mit der Cerberus Enterprise App. Macs ignorieren sie. Auf dem Gerät:

- die Cerberus Enterprise App ist installiert (Cerberus installiert sie) und der Benutzer hat sie mindestens einmal geöffnet;
- der Standortzugriff für die App ist auf **Immer** gesetzt;
- **Präziser Standort** ist für die App aktiviert;
- **Hintergrundaktualisierung** ist aktiviert.

> **Standort und Geofences auf persönlichen Geräten**, oben im Abschnitt, ist standardmäßig deaktiviert. Solange es deaktiviert ist, erfasst Cerberus den Standort persönlicher Geräte (User Enrollment) nicht, ihre Geofence-Ereignisse werden nicht erzeugt, und ihre Geräteseite bietet weder „Standort ermitteln“ noch Live-Tracking an. Wenn Sie es aktivieren, teilen persönliche Geräte der Richtlinie ihren Standort und ihre Geofence-Ereignisse wie Firmengeräte, jedoch nur, wenn der Benutzer den Standort für die Cerberus Enterprise App erlaubt; die App erklärt dies dem Benutzer, bevor iOS fragt. Ihre Organisation ist dafür verantwortlich, Benutzer zu informieren und lokale Vorschriften zum Mitarbeiterstandort einzuhalten. Der Modus „Verloren“ und die MDM-Standortanfrage sind auf persönlichen Geräten nie verfügbar (Apple erlaubt sie nicht).

Im **Energiesparmodus** funktionieren Geofences weiterhin, aber iOS meldet das Verlassen eines Bereichs später und mit einem weniger präzisen Standort und kann das Abrufen neuer Geofences nach einer Richtlinienänderung um Stunden verzögern, bis die App erneut ausgeführt wird (zum Beispiel beim nächsten Übertritt oder wenn der Benutzer sie öffnet).

Wie Ereignisse eintreffen

iOS überwacht die Bereiche für die App und weckt sie, wenn das Gerät eine Grenze überschreitet, auch wenn die App nicht geöffnet ist. Ereignisse können einige Minuten nach dem Übertritt eintreffen, und ein kleiner Bereich oder ein kurzer Besuch kann verpasst werden: iOS benötigt eine gewisse Strecke, die das Gerät über die Grenze hinaus zurücklegt, und einen längeren Aufenthalt dort.

Wenn die App nicht ausgeführt werden kann, zum Beispiel nach einem Neustart, bevor das Gerät entsperrt ist, erkennt auch der Server den Übertritt später anhand der von der App gesendeten Standorte. Jeder Übertritt löst die Ereignisregeln einmal aus, unabhängig davon, ob die App oder der Server ihn erkennt.

Wenn die App den Server mehrere Stunden lang nicht kontaktiert hat, bittet der Server iOS, sie zu wecken, damit sie ihre Geofences erneut prüfen kann. iOS garantiert diese Anforderungen nicht.

Geräteseite

Auf der Geräteseite zeigt die Registerkarte **Geofence** des Bedienfelds **Standortkarte** die Übertritte des Geräts an. Wenn die Richtlinie aktive Geofences enthält, teilt eine Statuszeile mit, ob die Geofence-Funktion auf dem Gerät funktioniert oder warum nicht: Die App hat den Server nicht kontaktiert oder muss aktualisiert werden, der Standortzugriff ist nicht auf **Immer** gesetzt, **Präziser Standort** oder **Hintergrundaktualisierung** ist deaktiviert, der **Energiesparmodus** war aktiviert, als die App ihre Einstellungen zuletzt gemeldet hat, oder die App hat die neuesten Geofences noch nicht angewendet.

> Geofence-Übergänge und Standorte werden **90 Tage** lang aufbewahrt, ältere Daten werden jede Nacht automatisch gelöscht. Der letzte Standort jedes registrierten Geräts bleibt immer erhalten, sodass das Gerät auf den Karten bleibt.

Einschränkungen

- Das Kopieren einer Richtlinie kopiert ihre Geofences nicht: Fügen Sie sie in der Kopie erneut hinzu.
- Geofence-Ereignisse auf iPhones und iPads sind nach bestem Bemühen: iOS entscheidet, wann die App ausgeführt werden kann.

> Um auf Geofence-Ereignisse zu reagieren, erstellen Sie eine Ereignisregel für **Gerät betritt einen Geofence** oder **Gerät verlässt einen Geofence**. Siehe **Ereignisregeln**.

Konten

Der Abschnitt **Konten** des Apple-Richtlinieneditors fügt E-Mail-, Exchange-, Google-, Kalender-, Kontakte- und Verzeichniskonten zu iPhone, iPad und Mac hinzu. Klicken Sie auf **Konto hinzufügen** und wählen Sie den Typ. Der Abschnitt enthält außerdem die Einschränkung **Kontenänderung erlauben** (überwachte Geräte).

> Auf einem Mac (macOS 13 oder höher) werden die Konten in der Sitzung der für die Verwaltung registrierten Benutzer installiert – in der Regel der Benutzer, der den Mac registriert hat –, wenn diese angemeldet sind. Die Geräteseite listet diese Benutzer unter **Mac-Benutzer** mit dem Status ihrer Konten auf. Konten, die die E-Mail-Adresse vom Gerätebenutzer übernehmen, verwenden den in Cerberus Enterprise dem Mac zugewiesenen Benutzer.

Allgemeine Einstellungen

- **Name und E-Mail des Gerätebenutzers** (E-Mail, Exchange, Google): Jedes Gerät verwendet den Namen und die E-Mail-Adresse seines Benutzers, die auf der Seite Benutzer festgelegt wurden (bei Google das Google-Konto des Benutzers). Geräte ohne Benutzer oder deren Benutzer keine E-Mail-Adresse hat, erhalten das Konto nicht. Legen Sie andernfalls eine feste E-Mail-Adresse und einen vollständigen Namen fest.
- **Kontoname** (optional): der Name des Kontos in den Einstellungen und in den Apps.
- **Benutzername** und **Passwort** (optional): Der Benutzername kann die Variablen $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$ und $UDID$ enthalten. Lassen Sie das Passwort leer, damit der Benutzer es auf dem Gerät eingibt, oder lassen Sie beide leer, damit der Benutzer sie eingibt.
- **Gilt für**: Beschränken Sie das Konto auf bestimmte Gerätetypen.

Kontotypen

- **E-Mail-Konto**: IMAP- oder POP-Eingangsserver und Ausgangsserver mit ihren Ports und ihrer Authentifizierung. Der Ausgangsserver kann denselben Benutzernamen und dasselbe Passwort wie der Eingangsserver verwenden.
- **Exchange-Konto** (Exchange ActiveSync): der Server oder leer, um ihn aus der E-Mail-Adresse zu ermitteln. Wählen Sie die Dienste (E-Mail, Kontakte, Kalender, Erinnerungen, Notizen) und ob der Benutzer sie ändern kann. Mit **Moderner Authentifizierung**

(OAuth) meldet sich der Benutzer über die Seite Ihres Identitätsanbieters an, beispielsweise Microsoft 365. Ein **Authentifizierungszertifikat** (iOS 17 oder höher) authentifiziert das Gerät mit einem Zertifikat.
- **Google-Konto**: Der Benutzer meldet sich mit der angegebenen E-Mail-Adresse beim Google-Konto an.
- **Kalenderkonto (CalDAV)** und **Kontakte-Konto (CardDAV)**: Server, Port und Pfad.
- **Verzeichnis (LDAP)**: Server und Port sowie die Suchvorgänge (Suchbasis, Bereich und Beschreibung), die zum Nachschlagen von Kontakten verwendet werden.
- **Abonnierter Kalender**: die URL des Kalenders (https, http oder webcal).

S/MIME

E-Mail- und Exchange-Konten können Nachrichten mit S/MIME signieren und verschlüsseln (iOS 17 oder höher). Wählen Sie für jedes Konto das Zertifikat: eines von der Seite Zertifikate, das Zertifikat des Gerätebenutzers oder eines, das von einem SCEP-Server angefordert wird. Sie können dem Benutzer erlauben, es zu deaktivieren, ein anderes Zertifikat zu wählen und für die Verschlüsselung einen Schalter für jede Nachricht anzuzeigen.

Sicherheit

Passwörter und Zertifikate sind nicht Teil der an die Geräte gesendeten Einstellungen: Jedes Gerät lädt seine eigenen Anmeldedaten von Cerberus Enterprise herunter und signiert die Anfrage mit seinem Verwaltungszertifikat. Sie werden nicht in den Protokollen gespeichert.

Compliance-Regeln

Der Abschnitt **Compliance-Regeln** des Apple-Richtlinieneditors legt Anforderungen für die Geräte der Richtlinie fest. Ein Gerät, das eine Regel verletzt, ist sofort nicht konform: Die Geräteseite zeigt unter **Warum das Gerät nicht konform ist** den Grund an, und die Geräteliste zeigt es als nicht konform an. Ein Gerät ist auch dann nicht konform, wenn eine Einstellung der Richtlinie darauf nicht angewendet werden kann.

Regeln

- **Code**: Das Gerät hat einen Code und erfüllt die Codeeinstellungen der Richtlinie.
- **Minimale Betriebssystemversion**: für iPhone und iPad oder für Mac. Um die Geräte zu aktualisieren, fügen Sie ein erforderliches Update in Softwareupdates hinzu.
- **Überwachtes Gerät**: Geräte, die mit dem Registrierungsprofil oder mit User Enrollment registriert wurden, sind nicht überwacht.
- **FileVault aktiviert (Mac)**: Die Festplatte des Macs ist mit FileVault verschlüsselt. Andere Geräte sind nicht betroffen.

Eine Regel wird geprüft, wenn das Gerät seinen Status sendet, wenn die Richtlinie gespeichert wird und jede Stunde. Ein Gerät, dessen Status unbekannt ist (zum Beispiel ein Mac, der FileVault noch nicht gemeldet hat), verletzt die Regel nicht.

Sperren des Geräts

Aktivieren Sie **Das Gerät sperren, wenn es weiterhin nicht konform ist** und legen Sie fest, nach wie vielen Tagen (0 sperrt sofort). Überwachte iPhones und iPads wechseln mit der von Ihnen festgelegten Nachricht in den Modus „Verloren“. Die anderen Geräte werden einmal gesperrt; ein Mac startet neu und fragt nach einer PIN, die in den Details des Befehls im Befehlsverlauf angezeigt wird.

- **Entsperren**: Wenn das Gerät wieder konform ist, wird der Modus „Verloren“ automatisch deaktiviert.
- **Modus „Verloren“ selbst deaktivieren**: Das Gerät wird nicht erneut gesperrt, bis es wieder konform wird und erneut eine Regel verletzt. Verwenden Sie dies, damit der Benutzer das Gerät reparieren kann.

> Um benachrichtigt zu werden oder auf andere Weise zu reagieren, erstellen Sie eine Ereignisregel für **Gerät wird nicht konform**: Sie erhält auch die Begründungen.