# Empfehlungen zur Geräteregistrierung

## 1. Automatische Registrierung (Automated Device Enrollment, „DEP“)


Sofern Geräte bei einem autorisierten Händler oder direkt bei Apple gekauft werden, erscheinen die Geräte automatisch im entsprechenden schulischen Apple School Manager (ASM). Voraussetzung hierfür ist, dass die Schule sich unter https://school.apple.com registriert hat und die Händler-ID im ASM unter *Einstellungen/MDM-Server*-Zuweisung hinterlegt wurde. Gleichzeitig muss die in den *Registrierungsinformationen* befindliche Organisations-ID dem entsprechenden Händler mitgeteilt werden, damit dieser die Zuordnung der Geräte durchführen kann.

Es bietet sich an, dass Gerätetypen (z. B. iPad) einem Mobile Device Management (MDM) automatisch zugewiesen werden. Dadurch werden die entsprechenden Geräte automatisiert bei der entsprechenden MDM-Lösung registriert und erscheinen dort im Bereich *automatisierte Geräteregistrierung bzw. DEP.* Der Gerätebenutzer muss dazu beim ersten Start des Geräts nicht eingreifen, es ist von Seiten der Schule keine Vorbereitung notwendig. Diese Registrierungsart ist gut skalierbar und sehr zuverlässig: Endbenutzer haben unmittelbar nach der Aktivierung Zugriff auf vorgegebene Konteneinstellungen, Apps, Bücher und Services (Mailkonten, Speicherkonten).

Die Geräte sind vollständig von der Schule betreut (supervised) und es kann verhindert werden, dass der Endbenutzer die Geräteverwaltung verlässt. In diesem Szenario können die Geräte auch als geteiltes Gerät („geteiltes iPad“) konfiguriert werden.

Diese Art der Geräteregistrierung findet man typischerweise bei Geräten, die sich im Eigentum der Schule befinden. Betreute Geräte bieten die umfangreichsten Möglichkeiten zur Gerätekonfiguration.

### PROBLEMATIK BEI NICHT SCHULEIGENEN GERÄTEN

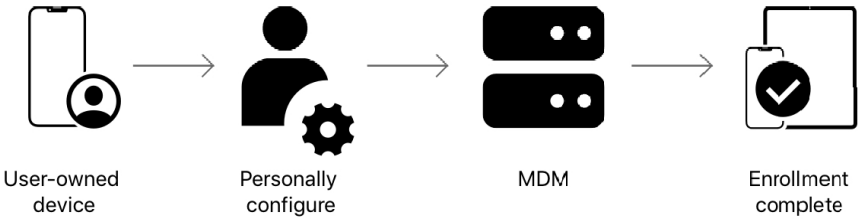
BYOD Geräte sind eigentlich nicht für die automatische Registrierung vorgesehen, da diese voraussetzt, dass

- Geräte mit dem ASM registriert sind und dem zugehörigen MDM zugewiesen sind,
- Geräte von Apple Authorized Resellern gekauft werden, der die Geräte beim schulischen ASM registriert,
- Gebrauchte Geräte (z.B. aus Spenden oder gesponsort vom Elternbeirat) manuell im ASM registriert werden.

- Geräte, die nicht bei autorisierten Händlern gekauft wurden (z. B. im Einzelhandel) manuell mit dem Apple Configurator 2 dem schulischen ASM zugewiesen werden. Eine entsprechende Anleitung hierfür findet sich in den Materialien.

## 2. Benutzerregistrierung

Verwendet ein Schüler sein privates Endgerät in der Schule (BYOD Szenario), so kann er trotzdem Ressourcen und Services der Schule nutzen (Zugang zu WIFI, Mailaccounts, Gruppenkalender), deren Voreinstellungen und Konfiguration die Schule bereitstellen kann über ein MDM. Prädestiniert ist hier z.B. der vorkonfigurierte Zugriff auf das WLAN der Schule.




Bei der Benutzerregistrierung werden Daten aus schuleigenen Apps strikt von Daten aus privaten Apps getrennt verwaltet. Die Daten des Benutzers werden nicht mit den Daten(strömen) der Schule bzw. Organisation gemischt (u.a. durch eigene verschlüsselte Speicherbereiche auf dem Gerät und eine eigene Verschlüsselung der Kommunikation).

### MANAGED APPLE IDS

Die Benutzerregistrierung erzwingt die Verwendung von verwalteten Konten (Managed Apple IDs), welche die Schule bereitstellt und besitzt. Diese Konten müssen den Endgerätebenutzern eindeutig zugeordnet werden können. Die Schule sollte hierfür eine Domäne (z. B. alp.dillingen.de) im ASM registrieren und diese für die Generierung der Benutzernamen verwenden. Eine Anonymisierung ist genauso möglich wie die Verwendung von SCIM[1].

Die Benutzerregistrierung des Geräts erzeugt auf dem Gerät eine eigene Useridentität (ein zweites Konto neben der privat verwendeten Apple ID). Diese ist ein Teil des Benutzerregistrierungsprofils und die Registrierung ist erst abgeschlossen, wenn sich die verwaltete Apple ID mindestens einmal erfolgreich angemeldet hat.

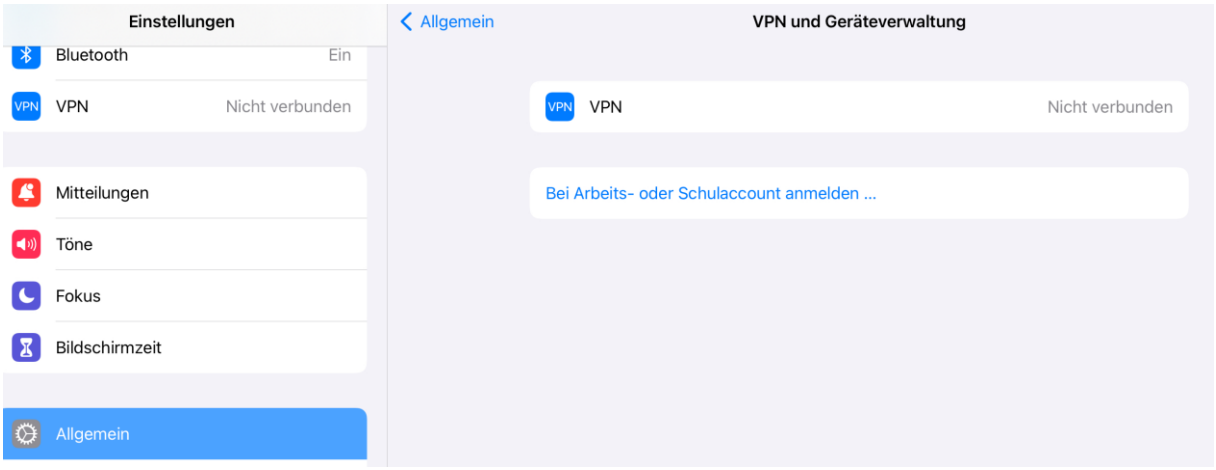
Die private Apple ID und die verwaltete Apple ID können ohne Konflikte gleichzeitig auf dem Apple Gerät verwendet werden.

### ACCOUNT BASED USER ENROLLMENT UND PROFILE BASED ENROLLMENT

Die **Benutzerregistrierung** kann entweder über den Dialog in den Einstellungen des Geräts vorgenommen werden (Einstellungen – Allgemein – VPN und Geräteverwaltung – Bei Arbeits- oder Schulaccount anmelden) oder bei einigen Anbietern (z. B. Jamf) über eine Webseite, welche auf dem betreffenden Gerät im Browser aufgerufen werden muss.

Bei der Verwendung von SCIM oder anderen föderierten Anmeldeverfahren, wird man zur Authentifizierung auf die Dialoge der authentifizierenden Provider umgeleitet.

[1] SCIM bezeichnet ein Protokoll zur verknüpften Authentifizierung. Typische Authentifizierungsdienste wären hier Microsoft Azure oder Google Workplace.




Bei der **profilbasierten Registrierung** wird ein Konfigurationsprofil auf das Gerät gespielt und manuell installiert. Hier findet keine Trennung zwischen Organisations- und Schuldaten statt. Das Gerät erscheint als nicht-betreutes Gerät in der MDM-Lösung. Es können anschließend Apps, Richtlinienprofile und Bücher an das Gerät verteilt werden.

Beide Arten der Geräteregistrierung bieten nicht die umfangreichen Möglichkeiten der Gerätekonfiguration wie die automatisierte Geräteregistrierung.

## 3. Empfehlung an Schulen:

Da es sich um Endgeräte handelt, die sich nicht im Eigentum der Schule befinden, ist eine automatische Registrierung von Apple eigentlich nicht vorgesehen. Möchte man diese verwenden, so muss das im Einverständnis mit den Gerätebesitzern geschehen und eventuell auch Alternativen angeboten werden.

Die empfohlene Vorgehensweise, die auch von Apple unterstützt wird, ist die Benutzerregistrierung über verwaltete Apple IDs.

Datenschutzrechtlich und im Praxiseinsatz sehr problematisch ist das Verwenden der Geräte mit Dummy Accounts (dieselbe Apple ID auf jedem Gerät). Hier stellt die Synchronisierung der Geräte über die Apple Cloud eine fast unüberwindliche Hürde dar.

**Alternativen mit oder ohne MDM**

Generell sollte man sich überlegen, ob sich der Aufwand für das Einrichten der verwalteten Apple IDs im Zusammenspiel mit einem MDM für die Schule überhaupt lohnt.

Apple Geräte bieten mit dem „geführten Zugang“ und dem Tool „Bildschirmzeit“ auch reizvolle und unkomplizierte Möglichkeiten, wie Erziehungsberechtigte und Lehrer die Geräte auch ohne zentrale Verwaltung verwenden können. Entscheidend wird hier sein, wie viele Apps die Schule den Eltern zur Verfügung stellen möchte, denn die Verteilung der verbilligten Apps aus dem Education Store für Schulen ist an verwaltete Konten gebunden. Eine Einbindung der Erziehungsberechtigten in die nicht zentrale Verwaltung der Geräte erscheint als gangbarer Lösungswerg.