Empfehlungen zur Geräteregistrierung bei Apple

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 im ASM 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. Erforderlich ist nur eine Verbindung ins Internet. 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, was aber für private Endgeräte nicht sinnvoll ist.

Diese Art der Geräteregistrierung findet man typischerweise bei Geräten, die sich im Eigentum der Schule befinden. Betreute Geräte bieten die umfangreichsten Möglichkeiten zur Gerätekonfiguration. Entscheidet sich die Schule für diese Art der Geräteregistrierung, verhalten sich die privaten Endgeräte wie schuleigene Endgeräte. Es ist durch administrative Eingriffe sicherzustellen, dass das Gerät außerhalb der Schule vollumfänglich genutzt wird (z. B. zeitliche Befristung der Profile).

Da die Geräte von der Schule zentral verwaltet wird, ist eine Einwilligung der Erziehungsberechtigen notwendig. Die Erziehungsberechtigen sollten auch explizit darauf hingewiesen werden, dass die Geräte beim Verlassen der MDM-Lösung vollständig zurückgesetzt werden. Deswegen müssen die persönlichen Daten vorher gesichert werden. Allerdings werden auch einige Serviceleistungen durch die Schule erbracht (z. B. Lizenzierung von Apps, Sicherstellung von Updates). Bei Anmeldung mit einer privaten Apple ID auf dem

Gerät, können die Erziehungsberechtigen die Bildschirmzeit selbst verwalten, sofern eine entsprechende Familiengruppe eingerichtet wurde.

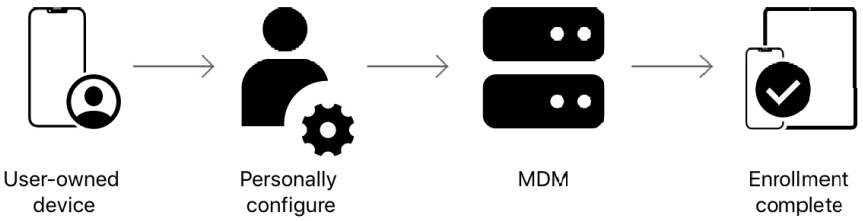
PROBLEMATIK BEI NICHT SCHULEIGENEN GERÄTEN

BYOD Geräte sind im ersten Moment 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 und gerätebasierte Registrierung

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 (VERWALTETE 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. schule.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.

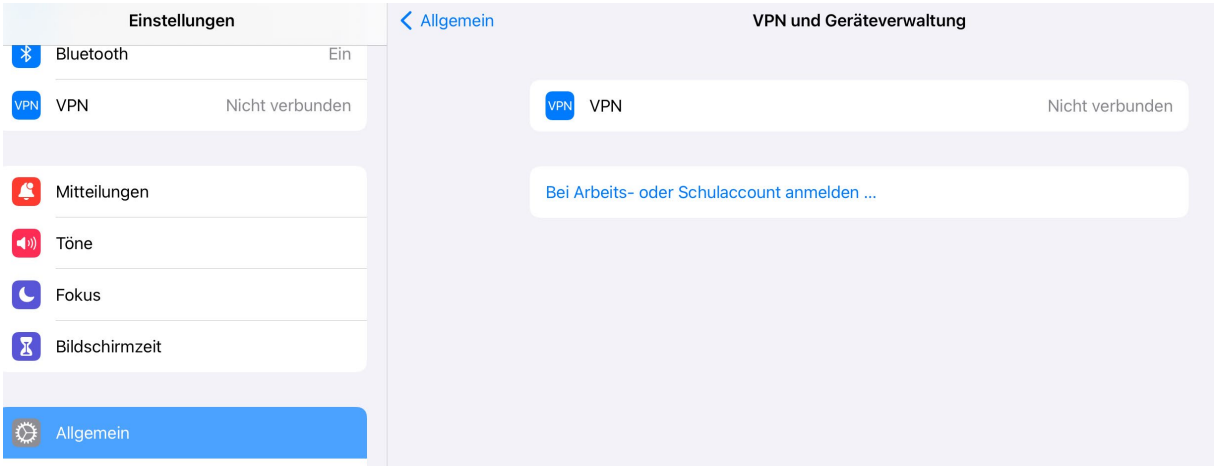
[1] SCIM bezeichnet einen Dienst zur verknüpften Authentifizierung. Typische Authentifizierungsdienste wären hier Microsoft Azure oder Google Workplace.

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.



Bei der **profilbasierten Registrierung** wird ein Registrierungsprofil auf das Gerät gespielt und manuell durch den Benutzer 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. In diesem Szenario kann nur eine Apple ID gleichzeitig auf dem Gerät angemeldet sein.

Beide Arten der Geräteregistrierung bieten nicht die umfangreichen Möglichkeiten der automatisierten Geräteregistrierung.

3. Empfehlung an Schulen:

Eine Verwaltung von schülereigenen Geräten stellt einen Eingriff in das Privateigentum der Erziehungsberechtigten dar. Je nach Umfang der Verwaltung durch die Schule, sind diese umfassender oder weniger umfassend. Bei allen drei Szenarien (automatische Geräteregistrierung, profilbasierte Registrierung und Benutzerregistrierung) ist eine informierte Einwilligung der Erziehungsberechtigten notwendig. In dieser Einwilligung sollte darüber informiert werden, wie das Gerät verwaltet wird und welche Einschränkungen während der Unterrichtszeit greifen.

Für die technische IT-Betreuung ergibt sich durch die Registrierung der Geräte bei der schulischen MDM-Lösung die einfache Möglichkeit der Verteilung von Apps und Lizenzen an die Geräte. Zudem können entsprechende Einschränkungen oder Komfortangebote (z. B. WLAN-Profil) einfach an die Geräte verteilt werden.

Apple empfiehlt für BYOD-Geräte die Benutzerregistrierung, da hier eine echte Trennung von privaten und schulischen Daten erfolgt. Generell sind aber alle drei

Registrierungsmöglichkeiten denkbar. Die Schule sollte für sich abwägen, was die richtige Vorgehensweise ist.

Für den Praxiseinsatz wenig tauglich ist die Verwendung von Dummy Accounts (z. B. eine verwaltete Apple-ID für alle Geräte), da hier die Cloud-Synchronisierung datenschutzrechtlich sehr problematisch zu sehen ist und es auch in anderen Kontexten (z. B. Classroom App) zu unüberwindbaren Problemen kommt.

4. Gegenüberstellung der Szenarien

Für die bessere Übersicht sollen die verschiedenen Registrierungsarten anhand verschiedener Aspekte gegenübergestellt werden.

	Automatische Geräteregistrierung	**Benutzerregistrierung**	**Gerätebasierte Registrierung**
Gerätestatus	Betreut	Nicht betreut (BYOD)	Nicht betreut
zentralisiert Updates einspielen	Ja	Nein	Ja
Registrierung beim MDM	Automatisch über ASM	Manuell durch Benutzer mit verwalteter Apple-ID	Manuelle Profilinstallation
Anmeldung mit	Privater oder verwalteter Apple-ID	Privater und verwalteter Apple-ID	Privater oder verwalteter Apple-ID
Trennung in Schul- und private Daten	Nein	Ja	Nein
App-Installation über ein MDM	Ja	Ja	Ja
(Zeitgesteuerte)[2] Konfigurationsprofile	Ja	Ja	Ja
Restriktions-möglichkeiten	Hoch	Niedrig - Mittel	Mittel
Anpassung des Hintergrunds	Ja	Nein	Nein
Zurücksetzung notwendig bei Verlassen des MDM	Ja	Nein	Nein
Backup der privaten Daten bei Verlassen der MDM-Lösung	notwendig	nicht notwendig	nicht notwendig

[2] Zeitsteuerung ist abhängig vom verwendeten MDM.

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 Lehrkräfte 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.

Die entsprechenden Konfigurationsprofile können auch lokal (ohne MDM) bereitgestellt werden und z. B. über einen QR-Code den Schülern zur Installation zur Verfügung gestellt werden. Das Profil kann dann manuell von den Schülern deinstalliert werden. Dabei wird die Verantwortlichkeit an die Schülerinnen und Schüler übergeben, dass das Gerät sich in dem vorher festgelegten Zustand (z. B. installiertes WLAN-Profil) befindet.