

## Auftaktveranstaltung am 11.06.2024 | Fragen und Antworten

### „Verwaltung von schülereigenen Endgeräten“

In der Digitalen Schule der Zukunft kann, in Absprache mit dem Schulaufwandsträger, als schulspezifisches technisches Mindestkriterium festgelegt werden, dass die mobilen Endgeräte der Schülerinnen und Schüler in einem schulischen Mobile Device Management zentral verwaltet werden. Auf eine zentrale Verwaltung kann auch verzichtet werden. Bei der Entscheidung sind die personellen Ressourcen und die verfolgten Ziele und Zwecke zu berücksichtigen.

Um Sie bestmöglich im Entscheidungsprozess und bei der Umsetzung zu unterstützen können Sie auf folgende Angebote zurückgreifen:

- Zentrale Fortbildungen zu verschiedenen Themen, wie z. B. der Auswahl und Administration von MDM-Systemen, IT-Infrastruktur im digitalen Klassenzimmer, Netzwerkinfrastruktur (s. <https://schulnetz.alp.dillingen.de>)
- Unterstützungsmaterialien bei der Einrichtung und Verwaltung der mobilen Endgeräte (aktuell im Aufbau, s. <https://schulnetz.alp.dillingen.de/dsdz.php>)
- Regelmäßige Techniksprechstunden (s. <https://links.alp.dillingen.de/dsdzsprechstunde>)
- Beratung digitale Bildung (s. <https://mebis.bycs.de/bdb>)

### Verwaltung von schülereigenen Endgeräten ohne MDM-System

#### **Wie kann Software ohne MDM verteilt werden?**

Die Schule stellt eine Liste an verwendeter und zu installierender Software zur Verfügung. Optimalerweise wird dabei auf die Auswahl von kostenpflichtigen Apps verzichtet, sofern es hierfür kostenlose Alternativen gibt. Die Installation der Anwendungen wird anschließend eigenständig oder zusammen, z. B. im Rahmen eines Elternabends, durchgeführt. Zur Unterstützung der Erziehungsberechtigten bieten sich entsprechende Anleitungen an.

#### **Welche Möglichkeiten zur Gerätesteuerung (z. B. durch Erziehungsberechtigte) ohne MDM gibt es?**

Moderne Betriebssysteme verfügen inzwischen über verschiedene Funktionalitäten (z. B. Bildschirmzeit, Digitales Wohlbefinden o. ä.) zur Regulierung der Nutzung des Endgeräts. So können maximale Nutzungszeiten für ausgewählte Anwendungen (z. B. Social Media) festgelegt werden. Erziehungsberechtigte können sich auch die tägliche oder wöchentliche Nutzungszeiten der verschiedenen Apps anzeigen lassen. Zur besseren Fokussierung können Mitteilungen des Betriebssystems oder von Anwendungen für eine gewisse Zeit unterdrückt und so ein konzentriertes Arbeiten gewährleistet werden.

Die Cloud-Accounts der Betriebssystemhersteller bieten die Möglichkeit der Verbindung der Accounts der Erziehungsberechtigten und deren Kinder. Dadurch können die Erziehungsberechtigten nachvollziehen welche Anwendungen ausgeführt worden sind. Zur Gewährleistung des Jugendschutzes können auch Inhaltsfilter für Webinhalte über den gemeinsamen Account von den Erziehungsberechtigten aktiviert werden. Suchmaschinen bieten inzwischen auch sog. Safe-Search Funktionalitäten, wodurch unangemessene Suchergebnisse herausgefiltert werden.

Ausführliche weitergehende Informationen zu diesem Themenkomplex finden Sie unter [https://mebis.bycs.de/beitrag/jugendschutz\\_und\\_sicherheitseinstellungen](https://mebis.bycs.de/beitrag/jugendschutz_und_sicherheitseinstellungen). Dort finden sich auch Anleitungen für Erziehungsberechtigte zur Einrichtung der vorgestellten Möglichkeiten.

### Verwaltung von schülereigenen Endgeräten mit einem MDM-System

#### **Welche Unterschiede in der Verwaltung der verschiedenen Betriebssysteme gibt es?**

Grundsätzlich lassen sich alle mobilen Betriebssysteme inzwischen zentral verwalten. Wichtiger sind der richtige konzeptionelle Aufbau und die Organisation des MDM-Systems. Allerdings sind auch hier immer die gewählten Rahmenbedingungen vor Ort hier entscheidend.

### **Welche Arten von MDM-Systemen gibt es?**

Im Bereich der mobilen Endgeräte gibt es drei große Betriebssystemhersteller: Apple (iOS, iPadOS, macOS), Microsoft (Windows 10 und 11) und Google (Android, ChromeOS). Insofern werden MDM-Lösungen in zwei Arten eingeteilt:

- Spezialisierte Lösungen, die nur einen Betriebssystemhersteller unterstützen, wie z. B. Jamf School/Pro für reine Apple-Lösungen oder Samsung Knox Manage und Google Admin Konsole für Android und Chrome OS.
- Generalistische Lösungen, die mehrere Betriebssysteme unterstützen, wie z. B. MS Intune, Rellution, Meraki, VM Ware Workspace One, Baramundi etc.

### **Gibt es Erfahrungen mit MDM bei "Mischsystemen"? (Windows/iPadOS/ChromOS)**

Mischsysteme bzw. generalisierte Systeme können verschiedene Betriebssysteme verwalten. Allerdings unterscheiden sie sich hier sehr im Funktionsumfang. Optimalerweise werden im Vorfeld konkrete Anforderungen (s. u.) definiert und anschließend, zusammen mit dem Schulaufwandsträger und der Beratung digitale Bildung, erörtert und in einer Testumgebung geprüft.

### **Android Enterprise vs. iPads. Gibt es hier Vor- oder Nachteile eines Systems?**

Beide Systeme erfordern die Anlage eines Organisationsaccounts bei Apple (Apple School Manager) und bei Google (Google Workspace), um Zugriff auf die herstellereigenen Stores sowie die Möglichkeit der Verwaltung der mobilen Endgeräte zu erhalten. Beide Systeme unterstützen die automatisierte Geräteersteinrichtung (Android Zero Touch, Automatische Geräteregistrierung) sowie die Möglichkeit die mobilen Endgeräte als persönliche Geräte (Arbeitsprofil und Benutzerregistrierung) bei einer MDM-Lösung zu registrieren. Bei Android Endgeräten empfiehlt sich die Fokussierung auf einen Hersteller, da die unterschiedlichen Anbieter das zu grundlegende Android-Betriebssystem an ihre Bedürfnisse anpassen und das die zentrale Administration erschwert. Zudem unterstützen nicht alle Hersteller über ihre Betriebssysteme die Verwaltungsmöglichkeiten von Android Enterprise. Die Endgeräte sollten auch das Label Android Enterprise tragen, um umfangreich verwaltbar zu sein.

### **Welches der genannten MDM-Systeme ist das Geeignetste?**

Ein MDM-System muss zu den individuellen technischen Rahmenbedingungen der Schule passen. Diese gilt es gemeinsam mit dem Schulaufwandsträger und der Beratung digitale Bildung zu analysieren, um anschließend ein für die Schule passendes System auszuwählen.

Die verschiedenen MDM-Lösungen unterscheiden sich zum Teil erheblich in ihren Funktionalitäten. Die nachfolgenden **Anforderungen** an ein MDM-System sollen bei der Auswahlentscheidung unterstützen:

- ggf. Unterstützung von mehreren Betriebssystemen zur Verwaltung in heterogenen Umgebungen: Hier sollte die aktuelle sowie die geplante Geräteausstattung (z. B. Lehrergeräte, private Schülergeräte sowie Schülerleihgeräte) der Schule bei der Entscheidung berücksichtigt werden
- Möglichkeit der Registrierung von persönlichen und schulischen Endgeräten im MDM-System: Alle Betriebssysteme bieten die Möglichkeit, dass ein Endgerät als persönliches Endgerät in einer MDM-Lösung registriert wird. Das erleichtert beispielsweise die strikte Trennung von privaten und schulischen Daten erheblich. Privat installierte Apps sind in diesem Szenario über das MDM auf

dem Endgerät nicht sichtbar. Für die erfolgreiche Integration in das MDM-System sind i. d. R. schulische Konten notwendig, die anschließend parallel zu den privaten Konten genutzt werden können.

- Funktion zur Bildung von (dynamischen) Gerätegruppen: Endgeräte werden zur Verteilung von schulischen Anwendungen und Richtlinien (Profilen) in Gerätegruppen eingruppiert. Die Zuteilung erfolgt optimalerweise automatisiert mit Hilfe von Zuordnungsregeln.
- Anbindungsfunktionalität der entsprechenden Hersteller-Stores: Alle Betriebssystemhersteller bieten eigene Stores zum Erwerb von Anwendungen an. Damit anschließend die gekauften Lizenzen auf die Endgeräte verteilt werden können, muss eine Verbindung zwischen der MDM-Lösung und dem Hersteller-Store hergestellt werden.
- Schnittstelle zu den verschiedenen ID-Provider-Systemen: Auf einem mobilen Endgerät meldet sich i. d. R. ein Benutzer mit einem privaten oder schulischen Account an. Deswegen sollte die Einbindung externer oder interner Verzeichnisdienste per LDAP oder Open-ID-Connect möglich sein.
- Möglichkeit des temporären Ausspiels von Richtlinien (z. B. Einschränkungen) auf das Endgerät während der Unterrichtszeit

Außerhalb der Unterrichtszeit soll eine private Nutzung möglich sein. Aus diesem Grund sind administrative Vorkehrungen zu treffen, damit etwaig vorhandene während der Unterrichtszeit geltende Restriktionen aufgehoben werden. Folgende Möglichkeiten stehen hierfür zur Verfügung (eine ausführliche Erläuterung erfolgt anschließend bei der nächsten Frage):

- zeitgesteuert
- standortbezogen (z. B. per GPS, iBeacon, IP-Range)
- netzwerkbezogen (z. B. im schulischen WLAN)
- benutzerbezogen
- App-gesteuert
- Anfallende Lizenzierungskosten: Bevor ein MDM-System ausgewählt wird, empfiehlt es sich die bisherige Lizenzierung der Schule zu prüfen. Teilweise ist in den gewählten Netzwerkprodukten oder Verwaltungs- sowie Office-Lösungen bereits ein MDM-System enthalten. Bei der Auswahl eines MDM-Systems sollte darauf geachtet werden, welche Arten von Lizenzen angeboten werden (z. B. jährliche, dauerhafte) und ob weitere Kosten (z. B. einmalig anfallende Kosten, Kosten für das Hosting) anfallen. Darüber hinaus müssen ggf. vergaberechtliche Aspekte in Abstimmung mit dem Schulaufwandsträger berücksichtigt werden.
- Möglichkeit der Nutzung einer Testumgebung: Die Verwaltung von mobilen Endgeräten ist eine administrative Tätigkeit, die eine konzeptionelle Vorarbeit erfordert. Die vorher genannten Anforderungen können nur im Rahmen einer Teststellung getestet werden und mit weiteren schulischen Anforderungen überprüft werden. Viele MDM-Anbieter gewähren eine entsprechende Testumgebung, die entweder zeitbegrenzt und/oder nur eine begrenzte Anzahl an registrierten Endgeräten zulässt. Allerdings können hier normalerweise alle Funktionen getestet werden.
- Ggf. optionale Funktionalitäten: Integriertes Ausleihsystem, eigene pädagogische Anwendungen, Verwaltung von weiteren Geräten, wie z. B. Displays, Möglichkeit der Konfiguration von Anwendungen (z. B. Browser)

**Welche Möglichkeit zur Steuerung der unterrichtlichen Restriktionen gibt es?**

Grundsätzlich gibt es die folgenden Möglichkeiten:

- **Zeitfilter:** Hier werden Zeiten und Tage festgelegt, zu denen die entsprechenden Einstellungen auf dem Endgerät aktiv sind. Zu beachten ist dabei, dass der Filter ggf. mit einer gewissen zeitlichen Verzögerung greift, da der Push des MDM-Servers vom Endgerät möglicherweise nicht sofort erhalten wird, und somit entsprechende Pufferzeiten (z. B. 7:30 bei Unterrichtsbeginn 08:00 Uhr) eingeplant werden sollten. Außerdem müssen die Ferien und Feiertage ggf. händisch im MDM-System angelegt werden.
- **Standortbezogen (z. B. per GPS, iBeacon, IP-Bereich):** Über die integrierten aktiven Ortungsfunktion wird bei einer bestehenden Internetverbindung der ungefähre Standort des Endgeräts bestimmt. Sobald sich der Schüler innerhalb der Schule befindet, werden die entsprechenden Richtlinien aktiv. GPS funktioniert jedoch nur bei einer bestehenden Internetverbindung, aktivierten Ortungsdiensten und kann u. U. etwas ungenau sein. Deswegen wird der gewählte Radius durch das MDM-System i. d. R. größer als das Schulhaus gewählt und kann somit auch Gebiete außerhalb des Schulgeländes umfassen und z. B. auch in angrenzenden Wohnungen noch aktiv sein.

Alternativ zu GPS kann auch bei Apple die iBeacon-Technik verwendet werden. iBeacons werden von kleinen Bluetooth-Sendern ausgesendet und vom Endgerät empfangen. Dadurch werden die entsprechenden Richtlinien aktiv. Die iBeacon-Sender werden beispielsweise an den Eingangstüren des Schulhauses befestigt. In einigen MDM-System kann auch ein Standort mit Hilfe eines IP-Bereichs bzw. einer festen öffentlichen IP-Adresse definiert werden.

- **Netzwerkbezogen (z. B. im schulischen WLAN):** Sobald sich das schülereigene Endgerät in das schulische WLAN einwählt, werden die entsprechenden Richtlinien aktiv. Es kann hier notwendig sein, dass auf dem Endgerät eine entsprechende App installiert wird oder eine feste öffentliche IP-Adresse vorhanden ist.
- **Benutzerbezogen:** Restriktionen können auch mit einem Account verbunden werden. Sobald sich der Nutzer mit seinen Zugangsdaten auf dem mobilen Endgerät anmeldet, werden die Einschränkungen aktiv. Zu beachten ist hierbei, dass beim An- und Abmelden mit unterschiedlichen Zugängen es im Hintergrund zu einer Datensynchronisierung kommen kann.
- **Start mit einer App:** Einige MDM-Lösungen bieten einige herstellereigene Apps an, über die die entsprechenden Einschränkungen angestoßen werden. Im Normalfall gibt es bei den Apps eine Lehrer- und eine Schülerversion, die optimalerweise auf den jeweiligen Endgeräten installiert werden. Die Schülerversion muss dabei zwingend auf dem Endgerät vorhanden sein, da ansonsten das Anstoßen der Restriktionen nicht funktioniert. Zudem muss sich der Schüler mit einem schuleigenen Account bei der App anmelden. Im MDM sind Zeiten zu hinterlegen zu denen die Restriktionen der Lehrkräfte automatisch gelöscht werden. Sofern das nicht möglich ist, müssen die Lehrkräfte diese händisch über die App oder eine Weboberfläche nach dem Unterrichtsende aufheben.

**Hinweis:** Je restriktiver ein Endgerät verwaltet wird, desto größer ist der administrative Aufwand, da es zu unerwünschten Nebeneffekten kommen kann, die die pädagogische Arbeit behindern. Außerdem besteht das Risiko einer Fehlkonfiguration. Pädagogische Vorüberlegungen sollten technischen Vorkehrungen vorgezogen werden. Jede dieser Techniken kann durch entsprechende Vorkehrungen (z. B. Deaktivierung der Ortungs-, Bluetooth- oder WLAN-Funktionalität) am Endgerät umgangen werden.

#### **Wer registriert die Endgeräte im schulischen MDM-System?**

Die Registrierung kann automatisch oder manuell erfolgen. Das hängt von der Art der gewählten Implementierung ab: Sofern das Endgerät als persönliches Gerät im MDM verwaltet werden soll, wird

die Registrierung manuell durch den Lernenden bzw. die Erziehungsberechtigten mit Hilfe eines personalisierten schuleigenen Accounts durchgeführt. Alternativ kann das Endgerät auch als vollverwaltetes schuleigenes Gerät im MDM registriert werden. Das kann durch einen Händler oder händisch über eine App oder QR-Code durchgeführt werden. Unabhängig von der Wahl der Registrierungs- methode des Endgeräts ist eine Einverständniserklärung der Erziehungsberechtigten zur zentralen Verwaltung einzuholen.

### **Welche pädagogischen Zusatzlösungen zur Gerätesteuerung bieten MDM-Lösungen?**

Ein MDM dient dazu die Administration der Endgeräte zu vereinfachen. Eine gezielte Gerätesteuerung, wie z. B. Starten von einzelnen Anwendungen, Sperren des Internetzugangs, findet über ein MDM nicht statt. Hierfür bieten sich vorrangig pädagogische Regelungen im Unterricht an, wie z. B. das Umdrehen des mobilen Endgeräts, sobald das Gerät nicht im Unterricht verwendet wird. Einige MDM-Anbieter bieten als weitere Funktionalität zusätzliche Anwendungen hierfür an. Die entsprechende Anwendung wird auf dem Lehrer- und Schülergerät installiert und erhält dadurch weitgehende Eingriffsmöglichkeiten auf das mobile Endgerät. Hierüber sind die Erziehungsberechtigten gesondert zu informieren.

### **Ist ein MDM für Windows Geräte sinnvoll?**

Windows ist, wie andere Betriebssysteme, inzwischen auch über ein MDM grundsätzlich verwaltbar. Es können Richtlinien zur Gerätesteuerung, Updatesteuerung oder Anwendungsinstallation definiert werden. Traditionelle Verfahren (z. B. Imaging) sind bei privaten Endgeräten nicht sinnvoll.

## Allgemeine Fragen

### **Wie können schuleigene Accounts angelegt werden?**

Zentrale Identitätsprovider oder MDM-Systeme bieten i. d. R. die Möglichkeit, dass über eine CSV-Datei eine Vielzahl von Accounts erstellt wird. Alternativ können auch lokale Verzeichnisdienste direkt angebunden werden. Die zentralen Identitätsprovider können miteinander verbunden werden und ein Account unter verschiedenen Anwendungen und Betriebssystemen genutzt werden. Dadurch wird der administrative Aufwand verringert, da nur noch an einer zentralen Stelle die Zugangsdaten gepflegt werden müssen.

### **Kann ein zweiter schuleigener Apple School Manager (ASM) angelegt werden?**

Gemäß der AGB von Apple kann für eine Bildungseinrichtung nur ein ASM angelegt werden. Bei der Registrierung wird von Apple geprüft, ob sich an der Adresse eine berechtigte Einrichtung befindet. Im konkreten Fall würde bei einer weiteren Registrierung diese abgelehnt werden. Stattdessen empfiehlt sich die Arbeit mit unterschiedlichen Standorten in der ASM-Instanz der Schule. Für die verschiedenen Standorte können Apps gekauft werden, Benutzer angelegt werden und unterschiedliche MDM-Systeme verwendet werden, denen die mobilen Endgeräte zugewiesen werden.

### **Welches mobile Betriebssystem sollte gewählt werden?**

Die Wahl des Betriebssystems hängt von den pädagogischen Einsatzszenarien im Unterricht sowie den technischen Rahmenbedingungen der Schule ab. Die schülereigenen Endgeräte sollten zur IT-Infrastruktur der Schule passen. Hier gilt es die vorhandenen Lehrergeräte und Schülerleihgeräte in den Blick zu nehmen. Bei der Arbeit mit browserbasierten Anwendungen (z. B. BayernCloud Schule) spielt das zugrunde liegende Betriebssystem eine untergeordnete Rolle. Unter dem Aspekt der zentralen Verwaltung sind heterogene Betriebssystemumgebungen mit einem größeren administrativen Aufwand verbunden, da unterschiedliche Richtlinien definiert werden, Apps verteilt werden und dif-

ferenzierte Konfigurationen erstellt werden. Weitere Informationen zur Wahl der technischen Mindestkriterien finden sich unter <https://mebis.bycs.de/digitale-schule-der-zukunft/leitfaden/rahmenbedingungen/technische-mindestkriterien-fuer-die-mobilen-endgeraete-definieren> und [https://schulnetz.alp.dillingen.de/materialien/Implementierungsleitfaden\\_1zu1\\_Setting.pdf](https://schulnetz.alp.dillingen.de/materialien/Implementierungsleitfaden_1zu1_Setting.pdf).

### **Welche Bandbreite für das Auspielen von Updates ist notwendig?**

Inwieweit das Auspielen von Updates für Anwendungen und das Betriebssystem über ein zentrales Management durchgeführt wird, sollte vorher geklärt werden, da hierdurch ein nicht unerheblicher Arbeitsaufwand entsteht. Nicht jedes MDM kann Updates automatisch verteilen, sondern erfordert stattdessen ein manuelles Anstoßen des Updateprozesses. Updates können zentral oder u. U. im Betriebssystem selbst zeitlich gesteuert werden, so dass z. B. bis 17 Uhr keine Updates installiert werden. Dadurch wird die Internetbandbreite der Schule geschont. Eine weitere Möglichkeit zur Reduzierung der Bandbreitenbelastung ist die Nutzung eines sog. Cachingserver, der die Updates herunterlädt und dann zentral bereitstellt. Die mobilen Endgeräte laden dann die Updates nicht aus dem Internet, sondern sprechen den lokalen Server an. Die Konfiguration und Verwaltung des Servers erfordert technisches Know-How und sollte von einem Spezialisten eingerichtet werden.

Einige Betriebssysteme bieten auch die Möglichkeit, dass von anderen Geräten im Netzwerk die Updates heruntergeladen werden und Bandbreitenbeschränkungen im Betriebssystem für Updates definiert werden. Auf Netzwerkebene kann ebenfalls die nutzbare Bandbreite für Updates eingeschränkt werden.

### **Wäre ein Terminal Server mit Software, die auf den Endgeräten lauffähig ist, sinnvoll?**

Terminalserver ermöglichen das simultane Arbeiten von verschiedenen Nutzenden auf einem Server und erleichtern die Softwarepflege, da diese nur auf dem Server installiert und gewartet werden muss. Aufgrund der Vielzahl von gleichzeitigen Zugriffen sind aber entsprechende Hardwareressourcen des Servers notwendig, da es ansonsten zu Problemen in der Arbeit kommt. Der Server läuft normalerweise im lokalen Netzwerk und ist von außerhalb nicht oder nur über eine VPN-Verbindung erreichbar. Inzwischen können auch entsprechende Server in Cloud-Infrastrukturen gemietet werden. Im Schulumfeld werden solche Umgebungen gerne für die Verwaltungsarbeit eingesetzt.

Für die Digitale Schule der Zukunft ist dieses Szenario nicht zu empfehlen, da dadurch die technischen Möglichkeiten der mobilen Endgeräte und Betriebssysteme nicht genutzt werden. Außerdem stehen einige Funktionen der Endgeräte in der virtuellen Sitzung nicht zur Verfügung. Somit werden die vielfältigen didaktischen Möglichkeiten der mobilen Endgeräte nicht ausgeschöpft. Es kann auch zu Verzögerungen oder Fehlern bei der Übertragung von Stift- oder Tastatureingaben kommen. Außerdem sind die Terminalserver nicht ohne weiteres von zu Hause nutzbar und die Software steht somit den Schülerinnen und Schülern dort nicht zur Verfügung.