

Enterprise Mobility Management

Was leisten Managementlösungen heute?

Inhalt

1 Enterprise Mobility Management (EMM)	03
2 Sicherheit automatisiert gewährleisten	04
2.1 Enrollment	04
2.2 Inventarisierung	05
2.3 Passwortschutz erzwingen	06
2.4 Remote sperren und löschen	06
2.5 Aktualisierung der Firmware	07
2.6 Apps sperren oder freigeben	07
2.7 App-Konfiguration	08
2.8 Sicherheit durch Zertifikate, Verteilung und Enterprise Wi-Fi	08
2.9 IT-Richtlinien prüfen	09
2.10 Self-Service anbieten	09
2.11 Apple Volume Purchase Program bzw. Android Enterprise App-Distribution	09
3 Umfassend, effizient und einfach	10
3.1 Integriert vs. Standalone: Was eignet sich für wen?	10
3.2 Implementierungsaufwand und Bedienbarkeit	10
3.3 Herausforderung der Plattformvielfalt	10
3.4 Transparentes Management in Echtzeit	11
4 Checkliste wichtiger Funktionen	12
5 Fazit	13



1 Enterprise Mobility Management (EMM)

Während der Markt zu Unified Endpoint Management (UEM) migriert, bleibt Enterprise Mobility Management (EMM) die Basis für die sichere Verwaltung mobiler Geräte. Bring-Your-Own-Device (BYOD) ist in Unternehmen zum Standard geworden: Mitarbeiter möchten private Notebooks, Tablets oder Smartphones für den Zugriff auf Firmendaten nutzen. Das bringt Vorteile wie Flexibilität und Produktivität, doch IT-Verantwortliche müssen sich der Risiken bewusst sein. Effektiver Schutz, Inventarisierung und Automatisierung sind Voraussetzung – idealerweise integriert in eine moderne UEM-Lösung.

Smartphones, Tablets und PCs sind ähnlichen Cyberbedrohungen ausgesetzt: In den vergangenen Jahren stiegen gezielte Angriffe und Malware-Varianten auf Rekordhöhe. Unternehmen sollten sich daher entsprechend absichern.

Wichtige Fragen helfen, die passende EMM- oder UEM-Lösung zu finden:

- ➔ Wie einfach lassen sich Mobilgeräte in die Management-Lösung integrieren und inventarisieren?
- ➔ Unterstützt die Lösung Gerätekonfiguration und umfassende Sicherheitsfunktionen?
- ➔ Bietet sie plattformspezifische Features wie Apple Business Manager oder Android Enterprise?
- ➔ Integriert vs. Standalone: Welche Variante passt zum IT-Umfeld?
- ➔ Wie userfreundlich ist die Bedienung?

Daraus entsteht eine maßgeschneiderte Anforderungsliste für die Vorauswahl von Anbietern. Deren Lösungen sollten in der Praxis getestet und bewertet werden.

2 Sicherheit automatisiert gewährleisten

In diesem Kapitel erfahren Sie, wie EMM-/UEM-Systeme Geräte automatisiert einbinden und absichern – von Enrollment-Modellen bis hin zu Compliance, App-Management und zentralen Updates.

2.1 Enrollment

Damit mobile Geräte verwaltet werden können, müssen sie zunächst in die EMM-Lösung eingebunden und beim Managementserver registriert werden. Dabei stehen verschiedene Optionen zur Verfügung:

- Aufnahme als vollverwaltetes Unternehmensgerät (COBO)
- Aufnahme als Unternehmensgerät mit privater Nutzung (COPE)
- Aufnahme als Privatgerät mit Zugriff auf Unternehmensdaten (BYOD)
- Aufnahme als zweckbestimmtes Gerät (COSU)

iOS-Aktivierung mit DEP



2.1.1 Firmengeräte nur für Unternehmenszwecke (COBO)

Corporate Owned Business Only (COBO)-Geräte erlauben keinerlei private Nutzung und enthalten daher auch keine privaten Daten. Sie lassen sich durch strenge Richtlinien so weit einschränken, dass eine versehentliche Privatnutzung verhindert wird. Das gewährleistet höchste Sicherheit, kann aber die Bedienung umständlich machen – Nutzer greifen daher oft auf private Geräte zurück.

2.1.1.1 Apple Automated Device Enrollment (ADE)

Apple bietet mit Automated Device Enrollment (ADE), einem Bestandteil des Apple Business Managers, eine effiziente Möglichkeit, iOS-, iPadOS- und macOS-Geräte schnell und sicher in EMM- oder UEM-Systeme zu integrieren. Administratoren können den Prozess zentral steuern und Richtlinien vordefinieren, während Endnutzer von einer automatisierten und vereinfachten Aktivierung profitieren. Dadurch bleiben alle Firmengeräte dauerhaft verwaltet und geschützt.

2.1.1.2 Android Enterprise Zero-Touch Enrollment

Google stellt für Android Enterprise-Geräte mit Zero-Touch Enrollment eine vergleichbare Option bereit. Damit können Android-Geräte automatisch beim ersten Einschalten in die UEM-Lösung eingebunden und mit vordefinierten Richtlinien, Apps und Zertifikaten versehen werden. Auch hier ist kein manueller Eingriff der Administratoren nötig. Unternehmen profitieren von Skalierbarkeit, Konsistenz und einer sofortigen Absicherung aller unternehmenseigenen Geräte.

2.1.2 Firmengeräte mit Privatnutzung (COPE)

Corporate Owned Personally Enabled (COPE)-Geräte gehören dem Unternehmen, dürfen aber von dem Nutzenden auch privat genutzt werden. Durch die Kombination aus zentralem Management und getrennter Datenhaltung können IT-Abteilungen Unternehmensrichtlinien durchsetzen, ohne die Privatsphäre der Mitarbeitenden zu verletzen.

- **iOS / iPadOS:** User Enrollment trennt automatisch geschäftliche und private Bereiche.
- **Android Enterprise:** Work Profile on Company Owned Device ermöglicht eine sichere logische Trennung zwischen Arbeits- und Privatprofil, einschließlich differenzierter Richtlinien.

2.1.3 Privatgeräte mit Unternehmensnutzung (BYOD)

Bring Your Own Device (BYOD) erlaubt die Nutzung privater Geräte im Unternehmensumfeld. Eine klare Trennung von privaten und geschäftlichen Daten muss jedoch sichergestellt werden, um Datenschutz und Compliance sicherzustellen.

- **iOS / iPadOS:** User Enrollment schützt Nutzer-Privatsphäre, während Unternehmensdaten isoliert verwaltet werden.
- **Android Enterprise:** Work Profile erstellt einen separaten geschäftlichen Bereich, der zentral verwaltet, aber vom privaten Bereich vollständig abgeschottet ist.

2.1.4 Zweckbestimmte Endgeräte (COSU)

Corporate Owned Single Use-Geräte (COSU) sind ausschließlich auf einen speziellen Einsatzzweck konfiguriert, etwa als Barcode-Scanner oder Kassensystem. Sie führen lediglich vordefinierte Apps aus und erfordern keine Nutzeridentifikation. Ideal für Szenarien, in denen Geräte flexibel zwischen mehreren Mitarbeitern geteilt werden. Sowohl Apple (über den Kiosk Mode) als auch Android Enterprise (über Dedicated Device Mode) bieten hierfür native Verwaltungsmöglichkeiten.

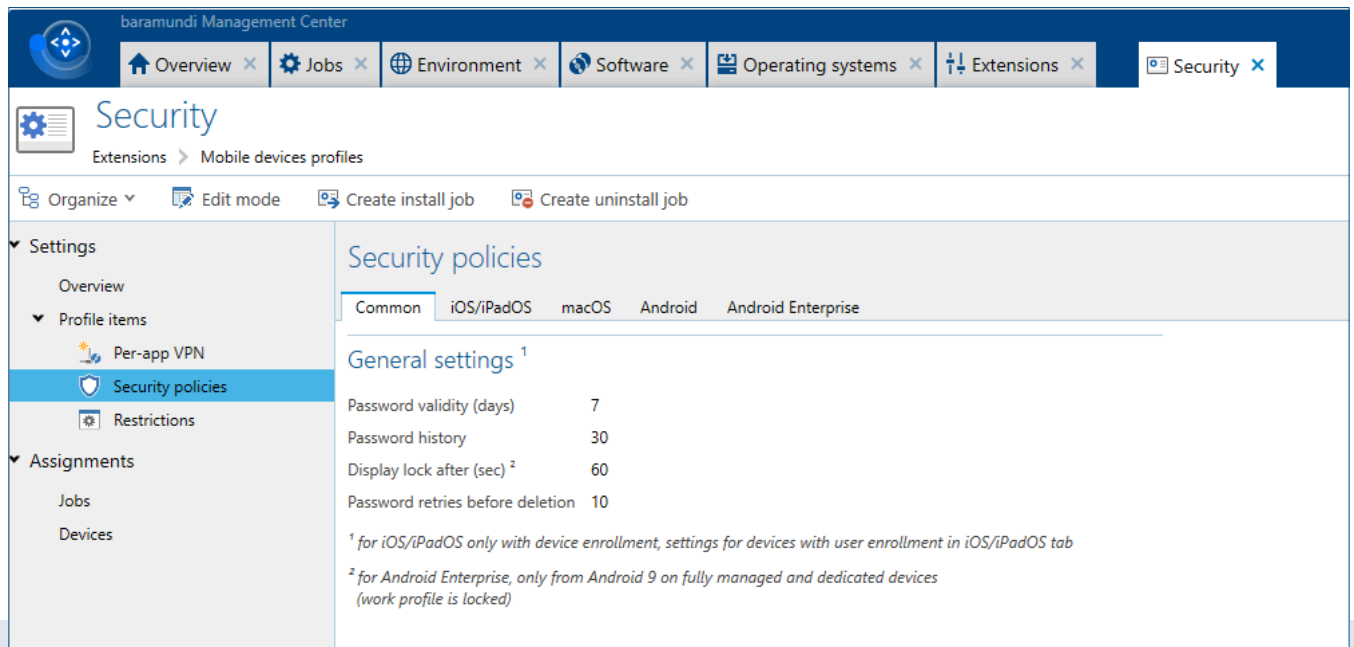
2.2 Inventarisierung

Ein EMM-/UEM-System sollte eine umfassende Übersicht über alle registrierten Geräte und deren Zustand bieten. Dazu zählen Hardwareinformationen, Betriebssystemversionen, installierte Apps, Sicherheitsrichtlinien und Zertifikate – unabhängig davon, ob es sich um ein iOS-, iPadOS-, macOS- oder Android-Gerät handelt.

So behalten Administratoren jederzeit den Überblick über die Geräteflotte, Compliance und Sicherheitsstatus.

2.3 Passwortschutz erzwingen

Um wertvolle Unternehmensdaten vor unbefugtem Zugriff zu schützen, lassen sich Passwortrichtlinien plattformübergreifend erzwingen. EMM- und UEM-Systeme erlauben die zentrale Vorgabe von Passwortkomplexität und -länge sowie die Aktivierung weiterer Schutzmaßnahmen wie Geräteverschlüsselung und biometrischer Verifizierung. So können Sicherheitsrichtlinien im gesamten Unternehmen einheitlich durchgesetzt werden.



Konfiguration eines Sicherheitsprofils

2.4 Remote sperren und löschen

Bei Verlust oder Diebstahl kann das Gerät je nach Plattform aus der Ferne gesperrt, gelöscht und geortet werden. Vergessene Passwörter kann der Admin aus der Ferne zurücksetzen, das Gerät in den Lost Mode (Apple) bzw. Lockdown Mode (Android) versetzen oder biometrische Entsperrung vorübergehend deaktivieren.

2.5 Aktualisierung der Firmware

Ebenso wichtig wie das Unterbinden von Manipulationen ist das zeitnahe Aktualisieren der Firmware. Diese bringt nicht nur neue Funktionen, sondern beseitigt auch Schwachstellen. Ein gutes EMM ist in der Lage, Firmware-Updates zentral zu verteilen und bei Bedarf, um einen definierten Zeitraum zu verzögern, etwa um die Funktion selbstentwickelter Spezial-Apps testen zu können.

Please define which OS versions are allowed for certain device types

Note: The lines will be checked from top to bottom. As soon as a matching hardware configuration for a device is found, it will be checked if the OS version is in the allowed version range. Patch levels are taken into account for iOS and macOS devices only.

Platform	Manufacturer	Model	Category	Owner	min. ver	min. patch level	max. ver	max. patch level
iOS/iPadOS	*	*	*	*	13.6	*	*	*
Android	Google	Pixel 7a	*	*	15.2	*	*	*
macOS	Apple	iPhone 11 P...	*	*	25.4	*	*	*

Up Down Remove condition

Next > Cancel

Auf Apple-Geräten (iOS/macOS) erfolgt dies über Managed Software Updates mit Enforcement und Deferrals bis 90 Tage. Auf Android Enterprise überwachen Compliance Policies OS-Versionen und triggern Updates automatisch. Auf allen Plattformen ermöglicht eine Inventur mit Regeln dem Admin jederzeit Fernüberblick über Firmware-Stände.

Prüfregel für Betriebssystemversionen

2.6 Apps sperren oder freigeben

Das EMM sollte die Sperrung bzw. Freigabe von Apps unterstützen, um zu verhindern, dass gefährliche Apps ausgeführt werden bzw. nur vertrauenswürdige Apps installiert werden können. So kann der Admin auf den verwalteten Mobilgeräten die Installation bzw. Ausführung unerwünschter Apps unterbinden. Umgekehrt ermöglicht der Freigabeansatz, explizit erlaubte Apps zu definieren. Alle nicht freigegebenen Apps werden dann an der Installation bzw. Ausführung gehindert. Je nach Anwendungssituation kann entweder ein Freigabe- oder Sperransatz für ein jeweiliges Endgerät genutzt werden.

baramundi Management Center

testItalyWhite

Software > App management > Lists

Organize Edit mode New Add to new profile

Settings

Overview

Apps

Display system apps Filter entries

	Name	Platform	Identifier
1	baramundi Management Center	Android	com.baramundi.android.bcenter
2	baramunditaly	Android	com.google.enterprise.webapp.xdfebb96c92795eb4
3	Google Chrome	Android	com.android.chrome
4	Microsoft Authenticator	Android	com.azure.authenticator
5	Microsoft Outlook	Android	com.microsoft.office.outlook
6	OpenVPN Connect - OpenVPN App	Android	net.openvpn.openvpn

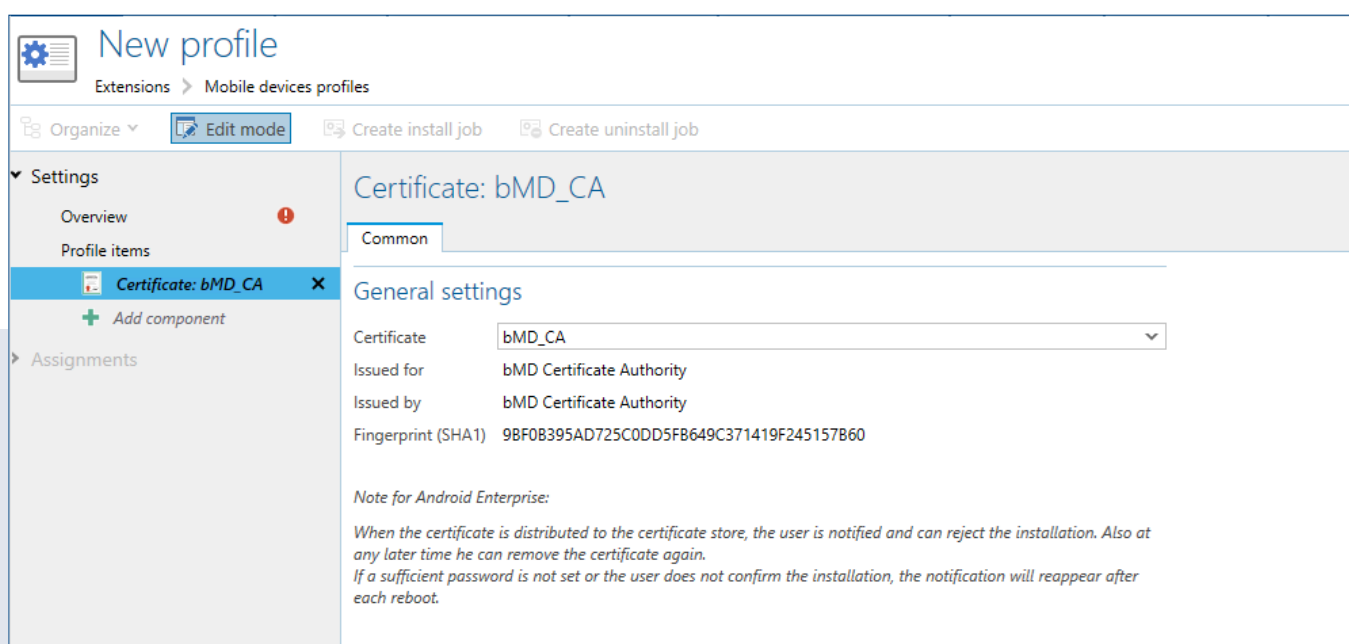
App-Auswahl für Sperr- oder Freigabelisten

2.7 App-Konfiguration

Enterprise Mobility Management umfasst mehrere Teildisziplinen des Managements mobiler Geräte. Die wesentlichen drei Aspekte hierzu sind Mobile Device Management (MDM), Mobile Application Management (MAM) und Mobile Content Management (MCM). Gemeint ist damit das Management des gesamten Geräts, der einzelnen Apps und schließlich der Inhalte.

2.8 Sicherheit durch Zertifikate, Verteilung und Enterprise Wi-Fi

Ferner sollte ein EMM die Verteilung von Client-Unternehmenszertifikaten ermöglichen und die dafür nötigen Vertrauensstellungen gegenüber Unternehmensdiensten unterstützen können. Mittels solcher Zertifikate lassen sich Zugriffe auf Microsoft Exchange absichern oder ein sicheres Enterprise Wi-Fi implementieren. Beides erfolgt per Zertifikat-Authentifizierung statt Benutzeranmeldung.

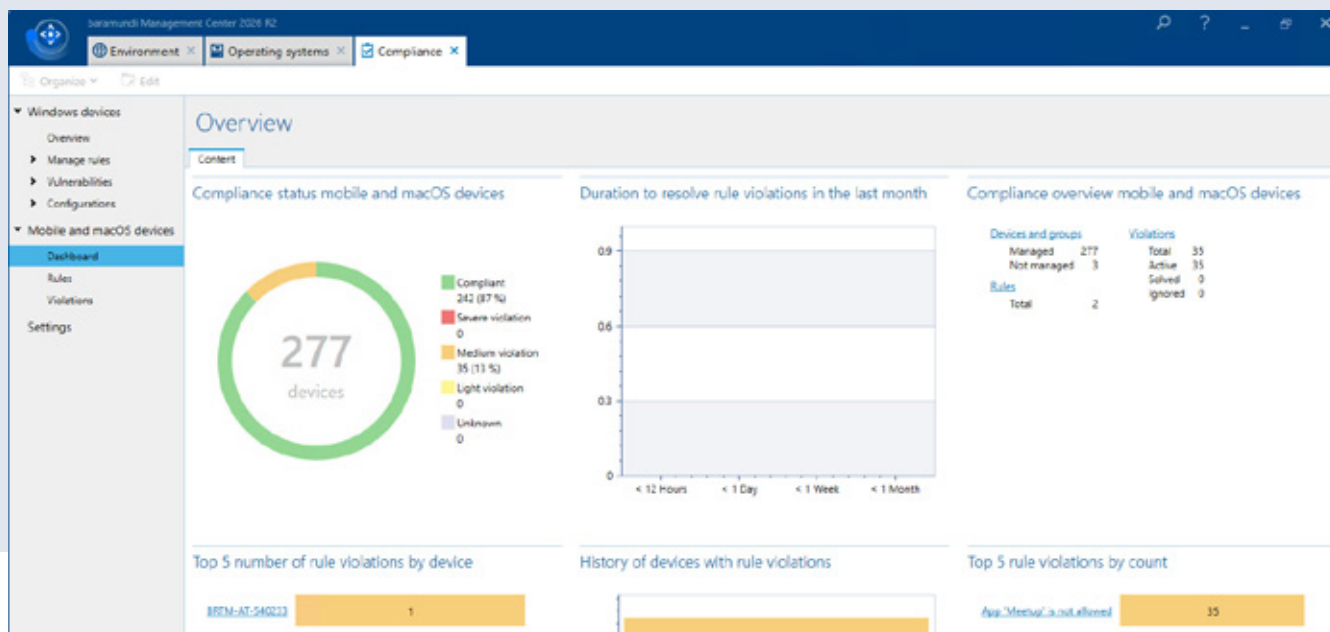


Profilbaustein für Clientzertifikate

2.9 IT-Richtlinien prüfen

Gerade bei mobilen Geräten ist die Einhaltung von Unternehmensrichtlinien von entscheidender Bedeutung. Neben App-Sperr- und Freigabelisten sowie der Erkennung von Manipulationen können fehlende Pflicht-Apps automatisch identifiziert und installiert werden.

Die Compliance-Informationen sollten im Dashboard übersichtlich dargestellt werden – sortiert nach Geräten oder Schweregrad der Verstöße. So erkennt der Admin auf einen Blick, wo Handlungsbedarf besteht. Moderne EMM-Lösungen bieten zudem automatisierte Maßnahmen – von Nutzer-E-Mails bis zur Fernlöschung bei kritischen Verstößen.



Dashboard für IT-Richtlinien

2.10 Self-Service anbieten

Self-Service bietet Nutzern eine elegante Möglichkeit für unmittelbare Unterstützung und reduziert gleichzeitig Supportanfragen erheblich. Vorbereitete Apps, Passwort-Reset-Funktionen und häufige Aufgaben stehen im Portal oder Kiosk-Modus bereit – vollständig ohne Eingriffe der IT.

2.11 Apple Volume Purchase Program bzw. Android Enterprise App-Distribution

Für die zentrale Lizenzverwaltung von Apps bieten sowohl Apple als auch Android Enterprise bewährte Lösungen. Das Apple Volume Purchase Program (VPP) sowie die App-Verwaltung über Android Enterprise ermöglichen die zentrale Zuweisung und Wiederverwendung kostenpflichtiger und kostenfreier Anwendungen. Administratoren können Apps wahlweise geräte- oder benutzerbasiert bereitstellen und Lizenzen bei Bedarf wieder entziehen, um sie anderen Geräten oder Nutzern zuzuweisen. Beide Plattformen unterstützen damit eine flexible und effiziente Verwaltung des gesamten App-Lebenszyklus – von der Verteilung über die Aktualisierung bis zur Lizenzrücknahme – und tragen so zur Einhaltung unternehmensweiter Richtlinien und Compliance-Anforderungen bei.

3 Umfassend, effizient und einfach

In diesem Kapitel erfahren Sie, welche Kriterien bei der Auswahl einer EMM-Lösung entscheidend sind und warum eine integrierte, einfach zu bedienende und plattformübergreifende Lösung den größten Mehrwert für IT-Abteilungen bietet.

3.1 Integriert vs. Standalone: Was eignet sich für wen?

Eine grundlegende Entscheidung betrifft die Einbindung der EMM-Lösung in die Unternehmens-IT: integriert in eine Unified Endpoint Management Lösung oder als Standalone EMM. Die integrierte Variante ermöglicht eine zentrale Verwaltung aller Clients über eine Oberfläche hinweg und vollen Überblick für den Admin. Das eignet sich besonders für Unternehmen mit kleinem IT-Team, um Synergieeffekte zu nutzen.

3.2 Implementierungsaufwand und Bedienbarkeit

Bei der Entscheidung für ein EMM sollten Administratoren berücksichtigen, wie hoch der Aufwand für die Implementierung, Inbetriebnahme und Schulung liegt. Die Lösung sollte möglichst einfach in die bestehende IT-Landschaft integriert werden können. Darüber hinaus ist eine intuitive Nutzung mit übersichtlicher Oberfläche wichtig, um neue Kollegen oder eine Vertretung schnell in das Tool einweisen zu können. Umfangreiche Schulungen und damit zusätzliche Kosten entfallen – wichtig für IT-Abteilungen mit knappen Budgets.

3.3 Herausforderung der Plattformvielfalt

Administratoren müssen häufig verschiedene Mobilplattformen unterstützen, d. h. sie bis ins Detail verstehen, einrichten und pflegen. Das ist komplex und zeitaufwändig. Am Beispiel der Exchange-Konfiguration für E-Mail-Services auf Android und iOS zeigt sich, dass identische Parameter (Name, E-Mail-Adresse, Domäne, Server, Verschlüsselung) jeweils in unterschiedlichen Dialogen eingegeben werden müssen.

Cancel Account Done

Email apple.fan@bartoso.de

Server mail.bartoso.de

Domain bartoso.de

Username Apple.Fan

Password Required

Description Apple.Fan

Advanced Settings >

These settings are installed by the profile "apple exchange baustein"

Exchange-Konfiguration auf verschiedenen Mobilplattformen

Der Wunsch nach einem Werkzeug, das eine einheitliche Eingabe für alle verwalteten Geräte ermöglicht, ist daher naheliegend. Ein EMM erlaubt es dem Admin, alle Mobilgeräte über eine zentrale Oberfläche einheitlich zu verwalten.

Exchange account: Exchange

Common iOS/iPadOS macOS Android Android Enterprise

General settings (except macOS) ¹

Component name Exchange

Display name on device {RegisteredUser.Mail}

E-mail address {RegisteredUser.Mail}

User name {RegisteredUser.UserLogonName}

Domain {RegisteredUser.Domain}

Exchange server (FQDN) mail.bartoso.de

Encrypted communication ☒

Certificate selection None

¹ for Android only supported by non Android Enterprise devices with Samsung KNOX or HTC Pro

Plattformübergreifende Exchange-Konfiguration mittels EMM

3.4 Transparentes Management in Echtzeit

Eine leistungsfähige Lösung für Enterprise Mobility Management bietet jederzeit einen klaren Überblick über alle relevanten Daten der verwalteten Mobilgeräte – idealerweise in Echtzeit. Nur wenn Admins schnell auf aktuelle Informationen und Statusmeldungen zugreifen können, lassen sich Sicherheits- und Compliance-Aspekte zuverlässig beurteilen. Eine stets aktuelle Datenbasis bildet zudem die Grundlage, um bei Bedarf aussagekräftige Reports zu erstellen und fundierte Entscheidungen zu treffen.

4 Checkliste wichtiger Funktionen

Softwareverteilung und Konfiguration

- ☐ Verteilung | Verzögerung von Firmware-Updates
- ☐ Unterstützung der nativen Datentrennung
- ☐ Installation von Apps mit | ohne Benutzerbestätigung
- ☐ Deinstallation von Apps mit | ohne Benutzerbestätigung
- ☐ Support für Apple Volume Purchase Program (VPP)
- ☐ Support für Automated Device Enrollment (ADE)
- ☐ Installation | Deinstallation bei deaktiviertem App Store
- ☐ Installation | Deinstallation selbsterstellter Unternehmens-Apps
- ☐ Self-Service-App: Kiosk
- ☐ Installation | Deinstallation von Zertifikaten
- ☐ Parametrisierung von Einstellungen über Variablen
- ☐ Installation von Hyperlinks (iOS: Web-Clip)
- ☐ Deaktivierung der Kamera
- ☐ Konfiguration von Access Points (APN)
- ☐ Sichere Inhaltsverteilung (MCM) mit Verschlüsselung

Inventarisierung

- ☐ Hardwareinformationen
- ☐ Konfigurierte Einschränkungen (z. B. iCloud Sperre)
- ☐ Installierte Profile
- ☐ Installierte Zertifikate
- ☐ SIM-Informationen
- ☐ Roaming Status
- ☐ Sicherheitseinstellungen
- ☐ Letzter Kontakt
- ☐ Gruppierung Geräte
- ☐ App-Nutzungsdaten und Risiko-Scores

Sicherheit

- ☐ Remote Lock | Unlock | Wipe
- ☐ Festlegung PIN-/Passwortabfrage und -komplexität
- ☐ Richtlinien f. Geräteverschlüsselung setzen
- ☐ Unterstützung Allowlist | Blocklist für Apps
- ☐ Deaktivierung von System-Apps
- ☐ Deaktivierung WLAN
- ☐ Deaktivierung Bluetooth
- ☐ Passwort History | Reset | Neues Passwort setzen
- ☐ Zugriff auf SD-Karte zulassen / nicht zulassen
- ☐ Zugriff auf App Stores zulassen / nicht zulassen
- ☐ WLAN auto-connect
- ☐ Erkennung von Jailbreak/Rooting
- ☐ Zero-Trust-Netzwerkzugriff (ZTNA)

Compliance

- ☐ Fehlen von erforderlichen Apps erkennen
- ☐ Installation von unerwünschten Apps erkennen
- ☐ Erkennung falsche Konfiguration
- ☐ Erkennung veralteter Betriebssystemversionen
- ☐ Status und Historie von Regelverstößen
- ☐ Automatisierte Remediation bei Verstößen
- ☐ Audit-Logs und NIS2-Reports

5 Fazit

Bei der Auswahl einer Lösung für Enterprise Mobility Management gibt es nicht die eine „One-Size-fits-all“-Lösung, die für jedes Unternehmen optimal passt. Entscheidend ist eine genaue Definition des Funktionsumfangs, ergänzt durch Praxistests geeigneter Anbieter. Neben der Technik spielen Betriebsmodell und Bedienbarkeit eine zentrale Rolle – ebenso wie die Akzeptanz der Mitarbeitenden. Ohne deren Akzeptanz ist das gesamte Mobility-Projekt zum Scheitern verurteilt. Besonders in Zeiten von NIS2-Compliance, Hybrid Work und KI-gestützter Automatisierung sollten IT-Verantwortliche ein ausgewogenes Verhältnis folgender Elemente priorisieren:

- **Die Sicherheitsanforderungen des Unternehmens**
- **Die Akzeptanz der Mitarbeitenden bei der Nutzung mobiler Geräte**
- **Eine einfache, intuitive Bedienung der Managementoberfläche durch den Admin**

Nur wenn allen drei Punkten Rechnung getragen wird, ist die Einführung einer EMM-Lösung ein Erfolg.

Über die baramundi software GmbH

Die baramundi software GmbH sorgt als Spezialist für Unified Endpoint Management (baramundi Management Suite) und Proactive Endpoint Operations (baramundi Proactive Hub) dafür, dass Unternehmen und Organisationen effizient, sicher und plattformübergreifend Arbeitsumgebungen und digitale Arbeitsplätze managen – On-Prem und in der Cloud. Der Hauptsitz der baramundi software GmbH befindet sich in Augsburg. Die Produkte und Services des im Jahr 2000 gegründeten Unternehmens sind komplett Made in EU. Beim Vertrieb, der Beratung und Betreuung von Kunden arbeitet baramundi weltweit erfolgreich mit Partnerunternehmen zusammen.

www.baramundi.com



Sie möchten mehr über smartes Enterprise Mobility Management mit baramundi erfahren? Melden Sie sich zum Live-Webinar an!

Erleben Sie, wie Sie Smartphones und Tablets genauso einfach und zuverlässig verwalten wie PCs und Notebooks.

<https://www.baramundi.com/de-de/it-training/webinare/>

Kontaktieren Sie uns.

Wir freuen uns auf Sie!



baramundi software GmbH
Forschungsallee 3
86159 Augsburg, Germany
+49 821 56708-380
request@baramundi.com



+48 735 91 44 54
request@baramundi.com



+44 2071 93 28 77
request@baramundi.com



+43 1 928 0136 0010
request@baramundi.com



baramundi software USA, Inc.
30 Speen St, Suite 501
Framingham, MA 01701, USA
+1 508 861 7561
requestUSA@baramundi.com



+41 77 280 49 79
request@baramundi.com



+39 340 8861886
request-italia@baramundi.com



+49 821 56708-390
request@baramundi.com

