Bring Your Own Device (BYOD) mit Android Enterprise & MobiVisor MDM

In diesem Datenblatt:

1. Voraussetzung für BYOD auf Ihren Android-Geräten
2. Vorteile des BYOD-Modells für Ihr Unternehmen
3. App-Bereitstellung und -Verwaltung
4. Das verwaltete Profil wieder entfernen
5. Mögliche Sicherheitsrichtlinien im Arbeitsprofil

MOBIVISOR

Android Enterprise
Silver partner

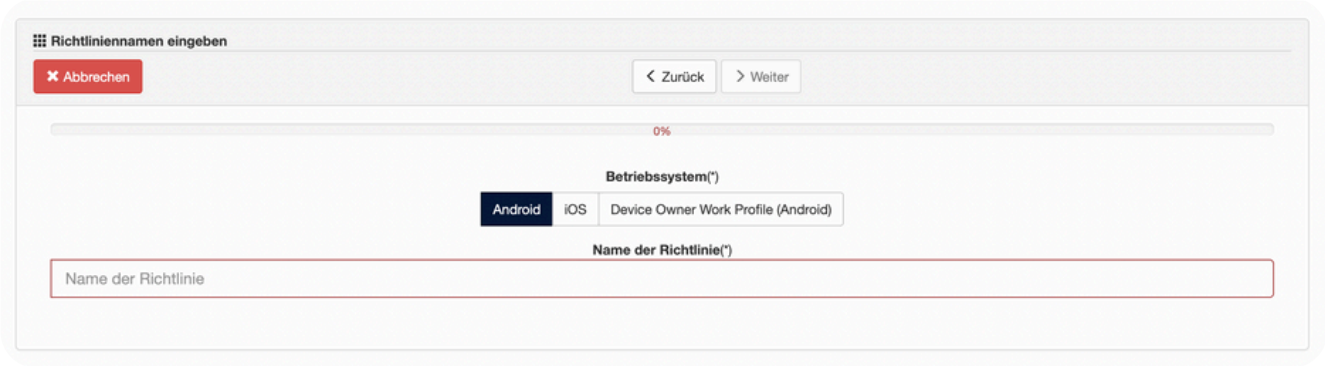
Das Android-Arbeitsprofil mit MobiVisor MDM:
Sicherheit und Flexibilität für Ihre BYOD-Umsetzung

BYOD (Bring Your Own Device) – die Nutzung privater Mitarbeitergeräte für das mobile Arbeiten wird bei IT-Verantwortlichen immer wieder als lohnende Möglichkeit zur Kosteneinsparung beworben. Mit dem Arbeitsprofil von Android wird ein dedizierter, sicherer Bereich auf dem Gerät geschaffen, der alle Unternehmensanwendungen und -daten enthält. Es läuft parallel zum privaten Profil auf dem Gerät, wobei geschäftliche Apps und Benachrichtigungen mit einem Symbol in Form einer Aktentasche gekennzeichnet sind. Das Multitasking zwischen geschäftlichen und privaten Apps ist für Nutzer problemlos möglich, die Daten bleiben dabei jedoch vollständig getrennt.

Voraussetzung für BYOD auf Ihren Geräten

Damit das BYOD-Modell mit Android-Geräten umgesetzt werden kann, ist der Einsatz eines Mobile Device Management Systems (MDM) wie MobiVisor zwingend erforderlich. Nur über ein MDM lässt sich ein sogenanntes **verwaltetes Arbeitsprofil** einrichten, das geschäftliche Daten vom privaten Bereich auf dem Gerät strikt trennt. Das MDM übernimmt dabei die Konfiguration, Vergabe von Richtlinien sowie die laufende Verwaltung des Arbeitsprofils – ohne ein MDM ist die Trennung von privaten und geschäftlichen Inhalten auf BYOD-Geräten nicht möglich.

Um **Android-Geräte im BYOD-Modell (Bring Your Own Device) mit MobiVisor verwalten** zu können, muss zunächst eine passende Richtlinie im System angelegt werden. Dies erfolgt über den Pfad **„Richtlinien > Neu > Android“**. In den Richtlinieneinstellungen finden Sie eine Übersicht aller verfügbaren Funktionen – diese sind in der Spalte **„Unterstützte Versionen“** aufgelistet.



Wichtig: Bei BYOD-Geräten kommen ausschließlich die Funktionen zum Einsatz, die mit dem Hinweis **„Arbeitsprofil“** versehen sind. Das Arbeitsprofil trennt geschäftliche von privaten Daten auf dem Gerät und stellt sicher, dass nur der geschäftliche Bereich durch die IT verwaltet wird – ein zentrales Element für Datenschutz und Nutzerakzeptanz im BYOD-Kontext.

Bitte beachten Sie außerdem, dass bei BYOD-Geräten **keine Samsung-spezifischen Funktionen** genutzt werden können, da die dafür notwendige **Samsung API in diesem Modus nicht aktiv** ist.

Vorteile des Arbeitsprofils für Ihr Unternehmen

Schutz vor Datenverlust (DLP-Richtlinien): MobiVisor MDM ermöglicht es Ihnen, eine Reihe von Richtlinien und Einstellungen zum Schutz vor Datenverlust (DLP) auf das Arbeitsprofil anzuwenden. Dazu gehören:

- **Sicherheitscodes für das Arbeitsprofil:** Erzwingen Sie eine minimale Komplexitäts-stufe im Arbeitsprofil mit PIN, Muster, Passwort oder biometrischem Verfahren, um unbefugten Zugriff zu verhindern.
- **Kopier-Kontrolle:** Verhindern Sie, dass Daten aus geschäftlichen Apps kopiert und in private Apps eingefügt werden, um sensible Informationen zu schützen.
- **Teilen zwischen Apps:** Legen Sie fest, bei welchen geschäftlichen Apps Daten mit privaten Apps geteilt werden dürfen, oder blockieren Sie diese Funktion vollständig.
- **VPN-Optionen:** Apps im Arbeitsprofil können über eine Vielzahl von VPN-Optionen im Netzwerk geschützt werden. Sie haben die Möglichkeit, dafür zu sorgen, dass nur Apps im Arbeitsprofil das VPN nutzen können, um den gesamten Geschäftsdatenverkehr zu sichern.

Datenschutz (für Nutzende) und IT-Kontrolle: Bei für geschäftliche Zwecke genutzten Privatgeräten (BYOD) verwalten die IT-Administrator*innen über MobiVisor MDM ausschließlich Unternehmensanwendungen und -daten.

- **Keine Einsicht in private Daten:** Mitarbeitende können ihre eigenen Apps weiterhin im privaten Profil nutzen. Private Apps und Daten können von der IT-Abteilung nicht geprüft oder kontrolliert werden.
- **Selektive Remote-Löschung:** Geschäftliche Apps und Daten können durch den IT-Administrator aus der Ferne gelöscht werden, ohne dass dies Auswirkungen auf private Anwendungen und Daten hat. Dies ist entscheidend bei Verlust, Diebstahl oder Ausscheiden eines Mitarbeiters.

Work-Life-Balance: Das Arbeitsprofil fördert eine gesunde Work-Life-Balance, indem es eine klare Trennung zwischen privaten und beruflichen Inhalten auf demselben Gerät ermöglicht. Geschäftliche Apps, E-Mails und Daten befinden sich ausschließlich im geschützten Arbeitsbereich, während persönliche Inhalte unberührt bleiben. Dadurch können Mitarbeitende außerhalb der Arbeitszeiten bewusst abschalten, ohne berufliche Benachrichtigungen oder Anwendungen im privaten Umfeld zu sehen.

App-Bereitstellung und -Verwaltung
mit MobiVisor MDM und Managed Play Store

Unternehmen müssen Mitarbeiter*innen mit genehmigten Anwendungen ausstatten, von öffentlich verfügbaren Apps bis hin zu privat entwickelter Software. MobiVisor MDM nutzt den Managed Play Store als Standardmöglichkeit für die sichere Bereitstellung von Apps.

- **Sichere App-Bereitstellung:** Mit dem Managed Play Store können Administrator*innen intern entwickelte sowie öffentliche Anwendungen sicher bereitstellen und aus der Ferne konfigurieren.
- **Automatisierte App-Verteilung:** IT-Administrator*innen können Anwendungen im Managed Play Store auf ihre Zulassungsliste setzen oder sie über Push direkt auf den Mitarbeitergeräten bereitstellen. Apps können für bestimmte Mitarbeitende aus der Ferne bereitgestellt und konfiguriert werden, ohne dass Nutzer*innen dabei selbst etwas tun müssen.

Verwaltetes Profil kann jederzeit entfernt werden

Ein zentraler Aspekt der BYOD-Strategie mit Android ist die Freiwilligkeit der Teilnahme.

- Nutzer*innen behalten jederzeit die Kontrolle über ihr Gerät – das verwaltete Arbeitsprofil, das von MobiVisor eingerichtet wurde, kann bei Bedarf auch wieder **selbstständig entfernt** werden.
- Dabei werden alle geschäftlichen Daten und Apps vollständig gelöscht, während **private Inhalte unberührt** bleiben.

Die **Einrichtung** erfolgt ebenfalls durch die Nutzer*innen selbst:

- Sie laden den MobiVisor-Client aus dem Google Play Store herunter und melden sich mit ihren persönlichen Zugangsdaten (Benutzername und Passwort) an.
- Eine **Schritt-für-Schritt-Anleitung zur Einrichtung** finden Sie hier.

Sicherheitsrichtlinien im Arbeitsprofil

Innerhalb des verwalteten Arbeitsprofils können verschiedene Sicherheitsrichtlinien angewendet werden, um den Schutz von Unternehmensdaten zu gewährleisten. Dazu gehören unter anderem:

- Verpflichtende Einrichtung eines sicheren **Sperrcodes**
- **Verschlüsselung** aller im Arbeitsprofil gespeicherten Daten
- Blockieren von **unsicheren Apps**
- **Einschränkung von Dateiübertragungen** zwischen dem privaten und geschäftlichen Bereich