datomo®
MOBILE
DEVICE MANAGEMENT

Vollständig verwalteter Geräteverwaltungsmodus

Version 24.07.2024 – Aktualisiert 09.07.2025

Übersicht

1. Übersicht

Vollständig verwaltete Bereitstellungen sind für firmeneigene Geräte vorgesehen, die ausschließlich für Arbeitszwecke genutzt werden. Organisationen können eine vollständige Palette an Verwaltungspolicies durchsetzen, einschließlich gerätebezogener Richtlinien, die für Arbeitsprofile und das BYOD-Konzept nicht verfügbar sind. Um hohe Sicherheitsstandards aufrechtzuerhalten, ist es manchmal notwendig, sehr strenge Sicherheitsrichtlinien umzusetzen. Auch wenn dies streng erscheinen mag, minimiert es das Risiko von Sicherheitsverletzungen.

Zusammenfassend lässt sich sagen, dass ein vollständig verwaltetes Gerät:

- *Nur Arbeits-Apps und -Daten enthält*
- *Für die Organisation sichtbar ist*
- *Von der Organisation verwaltet wird*

Auf Apple-Geräten ist eine Supervision erforderlich, um vollständige Kontrolle über das firmeneigene Gerät zu erhalten. Supervision bedeutet im Allgemeinen, dass das Gerät dem Unternehmen gehört, was zusätzliche Kontrolle über dessen Konfiguration und Einschränkungen ermöglicht. Es gibt verschiedene Methoden, mit denen Organisationen Geräte überwachen können:

- *Automatisierte Supervision durch Seriennummernerkennung*
  iPhone-/iPadOS-Geräte 13+ und macOS-Geräte 10.14.4+ verwenden die automatisierte Geräteregistrierung (DEP im Apple Business Manager), um sich in MDM zu registrieren.
- *Manuelle Supervision mit Apple Configurator*
  Es ist möglich, iPhone- und iPad-Geräte manuell mit Apple Configurator für Mac zu überwachen. Dazu muss das Gerät physisch vorliegen und mit einem Mac verbunden sein, auf dem Apple Configurator ausgeführt wird. Während dieses Prozesses wird das Gerät gelöscht und alle Daten gehen verloren.

2. Anwendungsfälle

Ideal für Branchen mit strengen Vorschriften wie Gesundheits- oder Finanzwesen. Denken Sie an Geräte, die in Kassensystemen, zur Erfassung von Gesundheitsdaten oder in anderen Szenarien verwendet werden, die maximale Sicherheit erfordern.

3. Vorteile

Die Vorteile dieses Verwaltungsmodus liegen darin, dass die IT-Administratoren die Richtlinien und Anforderungen für die Geräte kontrollieren und so sicherstellen können, dass die Unternehmensdaten geschützt bleiben und die Vorschriften eingehalten werden.

4. Überlegungen

Mitarbeiter verlieren einen Teil ihrer persönlichen Freiheit bei der Nutzung des Geräts, und der Schutz der Nutzerdaten hat keine hohe Priorität. Die Einrichtung und Verwaltung einer großen Anzahl von Geräten kann für die IT ressourcenintensiv sein. Da die Geräte vom Unternehmen bereitgestellt werden, können hohe Anfangskosten entstehen, und es könnte Schulungs- oder Unterstützungsbedarf für die Endnutzer bestehen.

5. Hauptmerkmale

5.1. Geräteregistrierung

- ***QR-Code***

  Scannen Sie einen QR-Code, der in der MDM-Konsole bereitgestellt wird, um ein Gerät über den Einrichtungsassistenten des Geräts zu registrieren.

- ***Zero-Touch-Registrierung***

  Vorkonfigurieren Sie Geräte über das Zero-Touch-Registrierungsportal (Android Zero-Touch, Samsung KME, Apple ABM) und registrieren Sie sie in großen Mengen.

5.2. Gerätesicherheit

- ***Sperrbildschirm-Einschränkungen festlegen***

  Legen Sie den Typ des benötigten Sperrcodes fest und erzwingen Sie dessen Verwendung (z. B. PIN, Muster, Passwort), um ein Gerät zu entsperren. Legen Sie außerdem die Qualität, Länge und Komplexität des Passcodes fest und setzen Sie sie durch.

- ***Arbeitendaten löschen und sperren***

  Gerät aus der Ferne sperren und löschen.

- ***Geräteintegritätsprüfung (nur Android)***

  Überprüfen Sie die Geräteintegrität, um festzustellen, ob ein Gerät manipuliert oder verändert wurde.

- ***Externe Datenübertragungen blockieren***

  Sperren von Hardware-Elementen (z. B. NFC-Beam, externe Medien, USB-Speicher), um zu verhindern, dass Benutzer Arbeitsdaten teilen oder übertragen.

- ***Durchsetzung von Google Play Protect (nur Android)***

  Die Funktion „Apps überprüfen“ von Google Play Protect ist standardmäßig aktiviert und prüft Apps vor und nach der Installation auf Malware.

5.3. App-Verwaltung

Auf Android-Geräten ist die Verwendung von Managed Google Play-Konten ein entscheidender Faktor für die einfache Verteilung von Apps.
***Funktionen**:*

- ***App-Katalog anzeigen und verwalten***

  Eine Liste der gekauften, genehmigten und privaten Apps anzeigen

- ***Apps still verteilen***

  Apps still auf einem Gerät installieren, ohne dass eine Benutzerinteraktion erforderlich ist

- ***Verwaltete Konfigurationen festlegen***

  Arbeits-Apps für einzelne Benutzer oder Geräte konfigurieren.

- ***Managed Google Play in der MDM-Konsole (nur Android)***

  Greifen Sie direkt über die MDM-Konsole auf die Managed Google Play-Konsole zu, um Arbeits-Apps zu suchen, zu genehmigen und zu verwalten.

- ***Verwalten und anpassen der Managed Play-Apps der Benutzer (nur Android)***

  Passen Sie das Layout des App-Stores an, das in der Managed Google Play-App auf einem Gerät angezeigt wird.

- ***Unterstützung für von Google gehostete private Apps (nur Android)***

  Veröffentlichen Sie von Google gehostete private Apps aus der MDM-Konsole und verteilen Sie sie auf Geräten.

5.4. Gerätemanagement

- ***Legen Sie die standardmäßigen Laufzeitberechtigungsrichtlinien fest (nur Android)***

  Legen Sie die standardmäßige Antwort (Abfrage, Erlauben oder Ablehnen) auf alle Laufzeitberechtigungsanforderungen von Apps fest.

- ***Legen Sie spezifische Laufzeitberechtigungsrichtlinien fest (nur Android)***

  Legen Sie die standardmäßige Antwort (Abfrage, Erlauben oder Ablehnen) auf spezifische Laufzeitberechtigungsanforderungen von Apps fest.

- ***WLAN-Einstellungen konfigurieren***

  WLAN-Anmeldeeinstellungen (SSID, Passwort) aus der Ferne auf ein Gerät verteilen.

- ***Zertifikat-authentifiziertes WLAN konfigurieren***

  WLAN-Einstellungen aus der Ferne auf ein Gerät verteilen, die Identität, Zertifikate zur Client-Authentifizierung und CA-Zertifikate beinhalten.

- ***Erweiterte Zertifikatsdetails verwalten***

  Zertifikate für bestimmte Apps auswählen und verhindern, dass Benutzer Anmeldeinformationen im verwalteten Keystore ändern.

- ***Always On VPN aktivieren***

  Always On VPN für bestimmte Apps aktivieren, um sicherzustellen, dass sie immer über ein konfiguriertes VPN laufen.

- ***Werkseinstellungen-Berechtigungen einschränken (nur Android)***
- *Geben Sie das/die Konto(s) an, die berechtigt sind, ein Gerät auf die Werkseinstellungen zurückzusetzen.*

- ***Änderungen der WLAN-Einstellungen blockieren***

  Verhindern Sie, dass Benutzer neue WLAN-Konfigurationen erstellen oder bestehende ändern.

- ***Zugang zu autorisierten Konten einschränken***

  Stellen Sie sicher, dass nur autorisierte Unternehmenskonten mit Unternehmensdaten interagieren können, indem Sie verhindern, dass Benutzer Konten hinzufügen oder ändern.

- ***Benutzer daran hindern, Apps zu deinstallieren***

  Verhindern Sie, dass Benutzer Apps deinstallieren oder über die Einstellungen ändern.

- ***Bildschirmaufnahmen deaktivieren***

  Verhindern Sie, dass Benutzer Screenshots machen, während sie Apps verwenden.

- ***Kamera deaktivieren***

  Verhindern Sie, dass Apps die Kameras des Geräts verwenden.

- ***Remote-Neustart***

  Starten Sie ein Gerät aus der Ferne neu.

- ***System-Audioeinstellungen verwalten***

  Steuern Sie die Audiofunktionen des Geräts.

- ***System-Uhrzeit-Einstellungen verwalten***

  Steuern Sie die Uhrzeit- und Zeitzoneneinstellungen des Geräts. Verhindern Sie, dass Benutzer automatische Geräteeinstellungen ändern.

5.5. Gerätebenutzbarkeit

- ***Over-the-Air (OTA) Systemupdates planen***

  Verschieben Sie OTA-Systemupdates und richten Sie regelmäßige Wartungsfenster für Updates ein.

- ***Standard-Apps für bestimmte Aktivitäten festlegen***

  Legen Sie die Standard-App für bestimmte Aktivitäten fest. Zum Beispiel wählen Sie den Standardbrowser zum Öffnen von Weblinks.

- ***Sperrbildschirm-Nachricht und Funktionen anpassen***

  Legen Sie eine Nachricht fest, die auf dem Sperrbildschirm eines Geräts angezeigt wird, und steuern Sie die Funktionen, auf die ein Benutzer vor dem Entsperren des Geräts zugreifen kann.

6. Unterstützte Geräte

Empfohlene Android-Geräte: alle Android 8+ Geräte.

Empfohlene Apple-Geräte:

- *iOS / iPadOS 13+*
- *macOS 10.15+*

***HINWEIS**: Es ist weiterhin möglich, ältere Versionen der oben genannten Plattformen (Android und Apple) zu registrieren, aber diese bieten eingeschränkte Funktionen.*

7. Vollständig verwaltete Geräte-Richtlinienverwaltung

Der nächste Schritt besteht darin, die Möglichkeiten der vollständig verwalteten Geräte-Richtlinie in MDM im Detail zu überprüfen.

*Weitere Informationen finden Sie in der **Dokumentation zur Verwaltung der Richtlinien für vollständig verwaltete Geräte**.*

8. Registrierung vollständig verwalteter Geräte

Bitte entnehmen Sie der separaten Dokumentation, wie Sie vollständig verwaltete Geräte zu MDM hinzufügen:

- Vollständig verwaltetes Android-Gerät
- Vollständig verwaltetes iOS-Gerät

Es ist möglich, vollständig verwaltete Geräte in großen Mengen hinzuzufügen.

Hier finden Sie die allgemeine Dokumentation für Android Zero-Touch, Samsung KME und Apple ABM (DEP):

- Android Zero-Touch-Massenregistrierung
- Samsung KME-Massenregistrierung
- Apple ABM (DEP)