datomo®
MOBILE
DEVICE MANAGEMENT

Dedizierter Geräteverwaltungsmodus

Version 19.07.2024 – Aktualisiert 13.01.2025

Übersicht

1 . Übersicht....3
2 . Anwendungsfälle....3
3 . Vorteile....4
4 . Überlegungen....4
5 . Hauptmerkmale....4
5.1 . Geräteregistrierung....4
5.2 . Gerätesicherheit....4
5.3 . App-Verwaltung....5
5.4 . Geräteverwaltung....6
5.5 . Gerätebenutzbarkeit....8
6 . Unterstützte Geräte....8
7 . Verwaltung von Richtlinien für dedizierte Geräte....8
8 . Registrierung von dedizierten Geräten....9

1. Übersicht

Dedizierte Geräte (früher als unternehmenseigene Einzweckgeräte oder COSU bezeichnet) sind eine Untergruppe vollständig verwalteter Geräte, die einem bestimmten Zweck dienen. Android bietet eine umfangreiche Palette von Verwaltungsfunktionen, mit denen Organisationen Geräte für alles Mögliche konfigurieren können – von mitarbeiterorientierten Fabrik- und Industrieumgebungen bis hin zu kundenorientierten Beschilderungs- und Kioskanwendungen.

Dedizierte Geräte sind in der Regel auf eine einzelne App oder eine Gruppe von Apps beschränkt. Android ermöglicht eine detaillierte Kontrolle über den Sperrbildschirm, die Statusleiste, die Tastatur und andere wichtige Funktionen des Geräts, um zu verhindern, dass Benutzer andere Apps aktivieren oder andere Aktionen auf dedizierten Geräten ausführen.

2. Anwendungsfälle

Beispielhafte Anwendungsfälle für mitarbeiterorientierte Geräte:

- Bestandsverwaltung
- Außendienstmanagement
- Logistik-Tracking-Geräte
- Robuste Geräte für den Feldeinsatz

Beispielhafte Anwendungsfälle für kundenorientierte Geräte:

- Digitale Beschilderung
- Check-in im Gastgewerbe
- Selbstbedienungskioske
- Einzelhandelsdisplays

3. Vorteile

Die Vorteile dieses Verwaltungsmodus bestehen darin, dass Apps und Funktionen gesperrt sind, wodurch eine versehentliche Fehlbedienung verhindert wird und das Gerät auf seinen Arbeitszweck fokussiert bleibt. Er erhöht die Sicherheit, indem alle Geräteaktionen außerhalb der vorgesehenen Nutzung unterbunden werden, und ermöglicht die Nutzung des Geräts durch mehrere Benutzer und für gemeinsame Erfahrungen.

4. Überlegungen

Die wichtigste Überlegung ist, dass das Gerät über eingeschränkte Funktionen verfügt. Diese Geräte können nicht für persönliche Aufgaben verwendet werden und erfordern möglicherweise spezialisierte Hardware- oder Softwarekonfigurationen.

5. Hauptmerkmale

5.1. Geräteregistrierung

- **QR-Code**

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

- **Zero-Touch-Registrierung**

  Vorkonfigurieren Sie Geräte mithilfe des Zero-Touch-Registrierungsportals und registrieren Sie diese in großen Mengen.

5.2. Gerätesicherheit

- **Sperrbildschirm-Einschränkungen festlegen**

  Legen Sie den Typ des Passcodes fest (z. B. PIN/Muster/Passwort), der erforderlich ist, um ein Gerät zu entsperren. Darüber hinaus legen Sie die Anforderungen an die Qualität, Länge und Komplexität des Passcodes fest und erzwingen diese.

- **Benutzer vom Umgehen gesperrter Geräte blockieren**

  Verhindern Sie, dass Benutzer gesperrte dedizierte Geräte umgehen, um andere Aktionen durchzuführen.

- **Arbeitsdaten löschen und sperren**

  Sperren und löschen Sie ein Gerät aus der Ferne.

- **Geräteintegritätsprüfung**

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

- **Externe Datenübertragungen blockieren**

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

- **Durchsetzung von Google Play Protect**

  Die Funktion 'Apps überprüfen' von Google Play Protect ist standardmäßig aktiviert und scannt Apps vor und nach der Installation auf Malware.

5.3. App-Verwaltung

Durch die Verwendung von verwalteten Google Play-Konten ist es möglich, Apps auf dedizierten Geräten zu verteilen, einschließlich:

- **App-Katalog anzeigen und verwalten**

  Eine Liste der gekauften Apps, genehmigten Apps und privaten Apps anzeigen.

- **Apps lautlos verteilen**
- Installieren Sie Apps auf einem Gerät ohne Benutzerinteraktion.
- **Verwaltete Konfigurationen festlegen**

  Konfigurieren Sie Arbeits-Apps für einzelne Benutzer oder Geräte.

- **Unterstützung für von Google gehostete private Apps**

  Veröffentlichen Sie von Google gehostete private Apps aus der MDM-Konsole und verteilen Sie diese an Geräte.

5.4. Geräteverwaltung

- **Standardrichtlinien für Laufzeitberechtigungen festlegen**

  Legen Sie die Standardantwort (Aufforderung, Zulassen oder Ablehnen) für alle Laufzeitberechtigungsanforderungen von Apps fest.

- **Spezifische Laufzeitberechtigungsrichtlinien festlegen**

  Legen Sie die Standardantwort (Aufforderung, Zulassen oder Ablehnen) für spezifische Laufzeitberechtigungsanforderungen von Apps fest.

- **WLAN-Einstellungen konfigurieren**

  Stellen Sie WLAN-Anmeldeinformationen (SSID, Passwort) aus der Ferne auf einem Gerät bereit.

- **Zertifikat-authentifiziertes WLAN konfigurieren**

  Stellen Sie WLAN-Einstellungen auf einem Gerät bereit, die Identität, Zertifikate für die Client-Autorisierung und CA-Zertifikate beinhalten.

- **Erweiterte Zertifikatsdetails verwalten**

  Wählen Sie Zertifikate für bestimmte Apps aus und verhindern Sie, dass Benutzer Anmeldeinformationen im verwalteten Keystore ändern.

- **Always On VPN aktivieren**

  Aktivieren Sie Always On VPN für bestimmte Apps, um sicherzustellen, dass diese immer über ein konfiguriertes VPN laufen.

- **Berechtigungen für Werkseinstellungen einschränken**

  Legen Sie das/die Konto(s) fest, die berechtigt sind, ein Gerät auf die Werkseinstellungen zurückzusetzen.

- **Erweiterte Funktionen für dedizierte Geräte verwalten**

  Steuern Sie detaillierte Funktionen für dedizierte Geräte, einschließlich der Deaktivierung der Statusleiste und des Sperrbildschirms.

- **Änderung der WLAN-Einstellungen blockieren**

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

- **Zugriff auf autorisierte Konten einschränken**

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

- **Benutzer vom Deinstallieren von Apps blockieren**

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

- **Bildschirmaufnahmen deaktivieren**

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

- **Kamera deaktivieren**

  Verhindern Sie, dass Apps die Gerätekamera verwenden

- **Fernneustart**

  Starten Sie ein Gerät aus der Ferne neu.

- **Systemeinstellungen für Audio verwalten**

  Steuern Sie die Audiofunktionen des Geräts.

- **Systemeinstellungen für die Uhr verwalten**

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

5.5. Gerätebenutzbarkeit

- **App(s) auf dem Bildschirm fixieren**

  Legen Sie eine App (oder mehrere Apps) fest, die auf dem Bildschirm fixiert werden soll, und stellen Sie sicher, dass Benutzer die Apps nicht verlassen können.

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

  Verschieben Sie OTA-Systemupdates um bis zu 30 Tage und richten Sie regelmäßige Wartungsfenster für Updates ein.

- **Standard-Apps für spezifische Aktivitäten festlegen**

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

- **Sperrbildschirmnachricht und -funktionen anpassen**

  Legen Sie eine Nachricht fest, die auf dem Sperrbildschirm eines Geräts angezeigt wird, und steuern Sie die Funktionen, die einem Benutzer vor dem Entsperren des Geräts zugänglich sind.

6. Unterstützte Geräte

Alle Android 8+ Geräte. Einige Funktionen sind ab Android 9 verfügbar. Die empfohlene Mindestversion des Android-Betriebssystems für den Einsatz als dediziertes Gerät ist Android 11.

7. Verwaltung von Richtlinien für dedizierte Geräte

Der nächste Schritt besteht darin, die Möglichkeiten der MDM-Richtlinien für dedizierte Geräte im Detail zu überprüfen.

Weitere Informationen finden Sie in der Dokumentation zur **Verwaltung von Richtlinien für dedizierte Geräte**.

8. Registrierung von dedizierten Geräten

Bitte lesen Sie die separate Dokumentation, um zu erfahren, wie Sie Android-Dedicated-Geräte zu MDM hinzufügen:

- Dediziertes Android-Gerät

Es ist möglich, dedizierte Geräte in großen Mengen hinzuzufügen. Hier finden Sie die allgemeine Dokumentation für Android Zero-Touch und Samsung KME:

- Android Zero-Touch Massenregistrierung
- Samsung KME Massenregistrierung