datomo®
MOBILE
DEVICE MANAGEMENT

datomo MDM Verwaltung im BYOD- und WPC Modus

Version 19. Jul. 2024 – Aktualisiert 12. Dez. 2024

Übersicht

1. Verwaltung von Android BYOD / WPC-Geräten

Bei Android-Geräten wird das BYOD-Konzept (Bring Your Own Device) für private Geräte mit Arbeitsprofil verwendet, welches die Speicherung von Arbeitsanwendungen und Daten in einem einem separaten, abgeschlossenen Bereich innerhalb eines Geräts erlaubt. Ein Mitarbeiter kann weiterhin sein Gerät wie gewohnt nutzen. Alle persönlichen Apps und Daten verbleiben auf dem primären Profil des Geräts.

Das Unternehmen des Mitarbeiters hat die volle Managementkontrolle über die Anwendungen, Daten und Einstellungen im Arbeitsprofil des Geräts, hat aber keinen Einblick oder Zugriff auf das persönliche Profil des Geräts. Diese klare Trennung gibt Unternehmen die Kontrolle über Unternehmensdaten und -sicherheit, ohne die Privatsphäre der Mitarbeiter zu gefährden.

Das Arbeitsprofil kann auch verwendet werden, um eine gemischte berufliche und private Nutzung auf unternehmenseigenen Geräten (WPC) zu ermöglichen. Wie bei einem Gerät, das dem Unternehmen gehört, haben Unternehmen die volle Verwaltungskontrolle über die Anwendungen, Daten und Einstellungen in einem Arbeitsprofil. Mit einem unternehmenseigenen Gerät können Unternehmen außerdem viele geräteübergreifende Richtlinien durchsetzen (z. B. Wi-Fi-Einstellungen konfigurieren, USB-Dateiübertragungen blockieren) Dateiübertragungen blockieren) und Einschränkungen, die für das persönliche Profil eines Geräts gelten (z. B. bestimmte Apps).

Diese zusätzlichen Verwaltungsfunktionen ermöglichen es Unternehmen, die unternehmenseigenen Geräte mit den IT-Richtlinien konform zu halten und gleichzeitig die Privatsphäre der Mitarbeiter zu respektieren. Das persönliche Profil eines firmeneigenen Geräts, einschließlich Apps, Daten und Nutzung, sind für Unternehmen nicht sichtbar oder zugänglich.

2. Verwaltung von Apple BYOD-Geräten

Bei Apple-Geräten ist das BYOD-Konzept (Bring Your Own Device) vorhanden, bei dem der Benutzer und nicht die Organisation Eigentümer des Geräts ist. Die Benutzerregistrierung erfordert verwaltete Apple IDs. Diese sind Eigentum der Organisation und werden durch diese verwaltet. Sie ermöglichen Mitarbeitern den Zugang zu bestimmten Apple-Diensten.

Wenn ein Benutzer ein Anmeldeprofil entfernt, werden alle Konfigurationsprofile, dessen Einstellungen und verwaltete Apps, die auf diesem Anmeldeprofil basieren, mit entfernt.

Die Benutzerregistrierung ist mit verwalteten Apple IDs integriert, um eine Benutzeridentität auf dem Gerät zu etablieren. Der Benutzer muss sich erfolgreich authentifizieren, damit die Registrierung abgeschlossen werden kann. Die verwaltete Apple ID kann neben der persönlichen Apple ID verwendet werden, mit welcher sich der Benutzer bereits angemeldet hat. Die beiden interagieren nicht miteinander.

Wenn die Benutzerregistrierung abgeschlossen ist, werden automatisch separate Verschlüsselungsschlüssel auf dem Gerät erstellt. Wenn das Gerät vom Benutzer abgemeldet wird, werden diese Verschlüsselungsschlüssel sicher zerstört. Die Schlüssel werden verwendet, um die unten aufgeführten verwalteten Daten kryptografisch zu trennen:

- App-Datencontainer (iPhone, iPad, Mac)
- Kalender (iPhone, iPad, Mac) - ab iOS, iPadOS 16.1, macOS 13
- Schlüsselbund-Elemente (iPhone, iPad, Mac)
- Mail-Anhänge und Text der Mail-Nachricht (iPhone, iPad, Mac)
- Notizen (iPhone, iPad, Mac)
- Erinnerungen (iPhone, iPad, Mac) - ab iOS, iPadOS 17, macOS 14

Wenn ein Benutzer mit einer persönlichen Apple ID und einer verwalteten Apple ID angemeldet ist, wird automatisch die Anmeldung mit verwalteter Apple ID für verwaltete Apps und die persönliche Apple ID für nicht verwaltete Apps verwendet werden.

Bei Verwendung eines Anmeldevorgangs in Safari oder SafariWebView innerhalb einer verwalteten App, kann der Benutzer seine verwaltete Apple ID auswählen und eingeben, um die Anmeldung mit seinem Arbeitskonto zu verknüpfen.

Systemadministratoren können nur die Accounts, Einstellungen und Informationen einer Organisation verwalten und Informationen verwalten, die mit datomo MDM bereitgestellt wurden, niemals die des persönlichen Kontos. Die gleichen Funktionen, die für die Sicherheit der Daten in unternehmenseigenen verwalteten Apps sorgen, schützen auch die persönlichen Inhalte eines Benutzers davor, in den Unternehmensdatenstrom gelangen.

Das MDM kann:

- Konten konfigurieren
- Auf das Inventar von verwalteten Apps zugreifen
- Nur verwaltete Daten entfernen
- Apps installieren und konfigurieren
- Einen Passcode erfodern
- Bestimmte Einschränkungen erzwingen
- Ein VPN per App konfigurieren

Das MDM kann nicht:

- Persönliche Informationen, Nutzungsdaten oder Protokolle einsehen
- auf das Inventar der persönlichen Apps zugreifen
- Persönliche Daten entfernen
- die Verwaltung einer persönlichen App übernehmen
- einen komplexen Passcode oder ein Passwort verlangen

  Für iPhone und iPad können Administratoren Passwörter mit mindestens sechs Zeichen festlegen und verhindern, dass Benutzer einfache Passwörter wie „123456“ oder ‚abcdef‘ verwenden. Es können aber keine komplexen Zeichen oder Passwörter vorausgesetzt werden.

- auf den Standort des Geräts zugreifen
- auf eine eindeutige Gerätekennungen zugreifen
- das gesamte Gerät aus der Ferne löschen
- die Aktivierungssperre verwalten
- Zugriff auf den Roaming-Status erhalten
- den Verloren-Modus einschalten

3. Anwendungsfälle

Ideal für hybride Arbeitsmodelle - denken Sie an Geschäftsteams und Führungskräfte, die persönliche Geräte für den Zugriff auf Arbeitsanwendungen und Tools verwenden wollen, um im Büro oder unterwegs produktiv zu bleiben. Geeignet sowohl für Bring Your Own Device (BYOD) als auch für Company Owned Personally Enabled (WPC) Richtlinien.

4. Vorteile

Berufliche und private Daten bleiben sicher und getrennt, so dass die Privatsphäre der Nutzer gewahrt bleibt. Die Mitarbeiter können ihr vertrautes, bevorzugtes Gerät verwenden, während die IT-Administratoren die Kontrolle über die Arbeitsdaten behält und diese sicher hält.

Unternehmen müssen kein Geld für neue Unternehmensgeräte ausgeben, sind aber dennoch in der Lage Unternehmensanwendungen, Daten und Berechtigungen sicher zu verwalten. Außerdem sind die Mitarbeiter in der Lage, Arbeitsbenachrichtigungen am Ende des Tages abzuschalten, was dazu beiträgt Burnout zu verhindern und die Work-Life-Balance zu verbessern.

5. Erwägungen

Einige Sicherheitsmerkmale können von den Sicherheitsanforderungen des Unternehmens abhängen. Dies erfordert ggf., dass die Mitarbeiter die Unternehmensrichtlinien für die persönliche Gerätenutzung befolgen.

6. Hauptmerkmale (Android)

(Die Hauptfunktionen von Apple wurden bereits in Kapitel 2 erwähnt)

6.1 Geräte-Einschreibung

- **Verwaltungs-App**

  Laden Sie den datomo MDM-Agent (Essentials) von Google Play herunter, um die Einrichtung von BYOD-Geräten zu starten.

- **QR-Code**

  Scannen Sie einen in der MDM-Konsole bereitgestellten QR-Code, um ein Gerät über den Einrichtungsassistenten eines Geräts (WPC) zu registrieren.

- **Zero-Touch-Registrierung**

  Vorkonfiguration von Geräten über das Zero-Touch-Enrollment-Portal, registrieren Sie Geräte in großer Anzahl (WPC).

6.2 Gerätesicherheit

- **Festlegen von Einschränkungen für den Sperrbildschirm**

  Festlegen und Erzwingen der Art des Passcodes (z. B. PIN/Muster/Passwort) der zum Entsperren eines Geräts erforderlich ist. Darüber hinaus können Sie die Qualität, Länge und die Komplexität des Kennworts

- **Festlegen von Einschränkungen für den Sperrbildschirm des Arbeitsprofils**

  Legen Sie den Typ des Passcodes (z. B. PIN/Muster/Passwort) fest, der zum Entsperren eines Arbeitsprofils erforderlich ist. Außerdem können Sie die Qualität, die Länge und Komplexität des Passcodes festlegen.

- **Löschen und Sperren von Arbeitsdaten**

  Sperren und Löschen eines Arbeitsprofils aus der Ferne.

- **Überprüfung der Geräteintegrität**

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

- **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.

6.3 App-Verwaltung

Durch die Verwendung von verwalteten Google Play-Konten ist es möglich, Apps im Arbeitsprofil auf BYOD/WPC-Geräte zu verteilen, einschließlich:

- **Anzeigen und Verwalten des App-Katalogs**

  Anzeigen einer Liste von gekauften, genehmigten und privaten Apps.

- **Stille Verteilung von Apps**

  Stille Installation von Apps auf einem Gerät ohne jegliche Benutzerinteraktion.

- **Herunterladen von Apps aus dem verwalteten Google Play**

  Nutzer können Apps installieren und aktualisieren, die für sie über das verwaltete Google Play auf ihren Geräten installieren und aktualisieren.

- **Verwaltete Konfigurationen festlegen**

  Konfigurieren Sie Arbeits-Apps für einzelne Nutzer oder Geräte.

- **Managed Google Play in der datomo MDM-Konsole**

  Zugriff auf verwaltetes Google Play direkt über die datomo MDM-Konsole um nach Arbeits-Apps zu suchen, sie zu genehmigen und zu verwalten.

- **Anpassen des verwalteten Google Play der Nutzer**

  Passen Sie das Layout des App Stores an, das in der verwalteten Google Play App auf dem Gerät angezeigt wird.

- **Unterstützung von bei Google gehosteten privaten Apps**

  Veröffentlichen Sie von Google gehostete private Apps über die datomo MDM Konsole und verteilen Sie diese an das Arbeitsprofil.

6.4 Geräteverwaltung

- **Festlegen von Standardrichtlinien für die Laufzeitberechtigung**

  Legen Sie die Standardantwort (Eingabeaufforderung, Zulassen oder Verweigern) für alle Laufzeitberechtigungs-Anfragen von Anwendungen fest.

- **Festlegen spezifischer Richtlinien für Laufzeitberechtigungen**

  Legen Sie die Standardreaktion (Eingabeaufforderung, Zulassen oder Verweigern) für bestimmte Laufzeit Berechtigungsanfragen von Anwendungen fest.

- **Konfigurieren von Wi-Fi-Einstellungen**

  Verteilen Sie Wi-Fi-Anmeldeeinstellungen (SSID, Kennwort) auf Geräte.

- **Konfigurieren von Zertifikat-authentifiziertem Wi-Fi**

  Verteilen Wi-Fi-Einstellungen auf Geräte, die die Identitäten beinhalten, Zertifikate für die Client-Autorisierung und CA-Zertifikate.

- **Verwalten von erweiterten Zertifikatsdetails**

  Wählen Sie Zertifikate für bestimmte Anwendungen aus, verhindern Sie, dass Benutzer die Anmeldeinformationen im verwalteten Schlüsselspeicher verändern.

- **Aktivieren von Always On VPN**

  Aktivieren Sie Always On VPN für bestimmte Anwendungen im Arbeitsprofil, um sicherzustellen, dass diese immer durch ein konfiguriertes VPN gehen.

- **Beschränken Sie den Zugriff auf autorisierte Konten**

  Stellen Sie sicher, dass nur autorisierte Unternehmenskonten mit den Daten des Arbeitsprofils interagieren können, indem sie das Hinzufügen oder Ändern von Konten durch Benutzer verhindern.

- **Bildschirmfotos deaktivieren**

  Verhindern Sie, dass Benutzer bei der Verwendung von Anwendungen Bildschirmfotos machen können.

6.5 Benutzerfreundlichkeit des Geräts

- **Anpassen von Sperrbildschirmnachrichten und Funktionen**

  Legen Sie eine Nachricht fest, die auf dem Sperrbildschirm eines Geräts angezeigt wird, und steuern Sie die Funktionen, auf die ein Benutzer zugreifen kann, bevor er ein Gerät und ein Arbeitsprofil entsperrt.

- **Festlegen von Standardanwendungen für bestimmte Aktivitäten**

  Legen Sie die Standardanwendung für bestimmte Aktivitäten fest. Wählen Sie zum Beispiel den Standard Browser für das Öffnen von Weblinks.

7. Unterstützte Geräte

- Alle Android 8+ Geräte (für BYOD), Android 11+ Geräte für WPC.
- Für Apple-Plattformen iOS / iPadOS 13+ und macOS 10.5.

8. Verwaltung der BYOD-/WPC-Richtlinien

Im nächsten Schritt überprüfen Sie die Möglichkeiten der datomo MDM BYOD / WPC Richtlinien.

Bitte lesen Sie dazu die Dokumentation zur BYOD / WPC Richtlinienverwaltung.

9. BYOD / WPC-Geräte-Registrierung

Zur Einschreibung der Geräte lesen Sie bitte in der separaten Dokumentation nach, wie Sie Apple BYOD und Android BYOD / WPC-Geräte zu datomo MDM hinzufügen: