datomo MDM
Versionshinweise 5.37

Wichtiger Hinweis!
datomo MDM 5.36 war die letzte Version, welche CentOS 7 unterstützt hat. Wenn Sie noch CentOS 7 verwenden, können Sie nicht auf diese Version aktualisieren

Übersicht

Wichtige Hinweise

CentOS 7

Support Status:

- datomo MDM 5.36 war die letzte Version, die CentOS 7 unterstützte
- Es wird keine weiteren Funktions-Upgrades oder Releases für diese Plattform geben

Was bedeutet das für den Betrieb des Systems?

- Das System arbeitet mit der aktuellen Version normal weiter
- 5.37.0 und höher können nicht auf diesem System installiert werden

Migrationspfad:

- Planung der Migration zu einer der langfristig unterstützten Plattformen:
  - RHEL 8
  - Oracle Linux 8
  - Rocky Linux 8

Wenn Sie Hilfe benötigen, wenden Sie sich bitte an den Support: mdm@dotoso.de

Update benötigt: MySQL Datenbank 8.0.36

Das Update auf die Version 5.37 wird nicht gestartet werden, wenn die MySQL-Version niedriger als 8.0.36 ist. Um die Aktualisierung durchzuführen, führen Sie folgenden Befehl auf dem Applikationsserver aus, bevor Sie das MDM aktualisieren:

```
essentials-mdm-config upgrade:database-server
```

Hinweis:

Eine Aktualisierung der Datenbank ist auf CentOS 7 möglich, dies ermöglicht jedoch nicht die Installation von datomo MDM 5.37.

Neue Funktionen

Android

- Unterstützung der Plattform Android 15
  - datomo MDM Base Agent, Fernzugriff, Nutzungs-Monitor und Launcher-Apps wurden in der neuesten Beta-Version von Android 15 getestet.
- Nutzungsmonitor bei dedizierten Geräten
  - Die Aktivierung des Accessibility-Services ist erforderlich, damit der Nutzungsmonitor Daten ordnungsgemäß erfassen kann.
  - Das Administrator-Passwort ist nicht mehr erforderlich für die Aktivierung des Nutzungsmonitors auf bereits angemeldeten Geräten und bei neu eingeschriebenen Geräten
- Implementierung komplexer Passwörter ohne PIN-Auswahl (Android 12+)
- Ziel-SDK-Upgrade auf 28 für die datomo MDM-Addon-Anwendung
- Verbesserung des Wiederherstellungsvorgangs von Kontakten
  - Nach erfolgreicher Entschlüsselung der Wiederherstellungsdatei oder nach dem dritten fehlgeschlagenen Versuch wird der Benutzer nun über das Ergebnis der Wiederherstellung der Kontakte informiert.
- Verbesserung der KNOX-Lizenzverwaltung
  - Der datomo MDM-Server sendet die KNOX-Lizenzaktivierungsoperation erneut, wenn der Agent feststellt, dass die KNOX-Lizenz nicht vom Benutzer aktiviert wurde.
- Verbesserung der Anmeldeseite des Android Base Agent
  - Nach dem Herunterladen des Agenten von Google Play oder nach dem Wiederherstellungsmodus ist die Option Autokorrektur im Anmeldefeld deaktiviert.
- Zusätzliche Motorola Kamera-Apps wurden der Liste der aktivierten System-Apps für WPC-Geräte hinzugefügt.
- Verbesserte Handhabung beim Anwenden von Konfigurationen mit ähnlichen vom Benutzer festgelegten WLANs
  - Fehlercode wird an die Admin-Konsole gesendet, wenn eine Netzwerkänderung über das MDM nicht möglich ist

Verloren-Modus

  - Möglichkeit, Android Geräte als verloren zu markieren, ähnlich der Implementierung des Verloren-Modus in iOS

- Wenn die Funktion aktiviert ist, wird eine Reihe von Operationen erstellt:
  1. Änderung des Sperrcodes (auf den im Vorgang angegebenen temporären Sperrcode)
  2. Standortüberwachung aktivieren (falls sie deaktiviert war)
  3. Aktuellen Standort abrufen
  4. Gerät mit verlorenen Modus-Nachricht sperren (Nachricht und Telefonnummer können in der Operation festgelegt werden)

Nachrichtenformat:

- Die auf dem Sperrbildschirm angezeigte Nachricht hat folgendes Format: Dieses Gerät gehört zu %message% %phone%, wobei der Text „Dieses Gerät gehört zu“ ein fester Wert ist.
- Beispiel: „$Name_des_Unternehmens. Bitte anrufen: “
- Darüber hinaus wird beim Aktivieren des verlorenen Modus eine Benachrichtigung generiert, die informiert, dass das verlorene Gerät mit dem Server verbunden ist. Mit dieser Benachrichtigung kann der Administrator den Zeitpunkt der Verbindung einsehen (erster und letzter), zu der das verlorene Gerät mit dem Server verbunden war.

Deaktivierungsprozess:

- Während der Deaktivierung des verlorenen Modus wird der datomo MDM-Server die folgenden Operationen senden:
  - Sperrcode entfernen
  - Standortüberwachung deaktivieren (falls diese nicht in der Gerätestrategie aktiviert ist)
  - Nachricht des verlorenen Modus vom Sperrbildschirm entfernen

Apple

- iOS-Agent-Aktualisierungen (v5.2.1), SDK wurde auf Version 18 aktualisiert
- Gerätefeldzuordnung in der benutzerdefinierten SSL-VPN-Anbieter-Konfiguration für iOS-Geräte
  - Es ist jetzt möglich, Gerätefelder in der benutzerdefinierten SSL-VPN-Konfiguration auszuwählen.
- Verbesserungen im Umgang mit Apple APNs-Token:
  - Detaillierte Antwortnachricht und Code, wenn das APN-Token widerrufen wird

    - Wenn der APNs-Token auf dem Apple-Server widerrufen wird, wird die Sichtbarkeit des Tokens in den MDM-Einstellungen geändert (der Token wird als widerrufen angezeigt).
- Der Code zur Umgehung der Aktivierungssperre wird jetzt in der Benutzeroberfläche auf der Seite mit den Gerätedetails angezeigt - Registerkarte Allgemein > Basisparameter
- Informationen über die Deinstallation der App durch den Benutzer
    - Wenn der Endbenutzer die App auf dem Gerät deinstalliert, wird eine entsprechende Operation in der MDM-Konsole erstellt.
    - Dies funktioniert nur für Apps, die über das MDM installiert wurden (sowohl von der Administrationskonsole als auch aus dem Unternehmensstore).
- Möglichkeit, die Deinstallation einer einzelnen Anwendung auf iOS-Geräten zu blockieren.
    - Die Option wird der Richtlinie > Sicherheitsoptionen > Apple-Anwendungsrichtlinie mit der ausgewählten Option hinzugefügt: Anwendungen aus der Liste zulassen.
    - In der Liste der zulässigen Bundle-IDs gibt es einen zusätzlichen Schalter - Deinstallationssperre. Wenn diese Option aktiviert ist, ist die Deinstallation der ausgewählten Anwendung nicht möglich.

Aktualisierungen zu Einschränkungen

- Funktionen, welche von Apple als veraltet (deprecated) markiert wurden:
    - Foto-Stream blockieren
    - Sprachwahl blockieren, wenn das Gerät mit einem Passwort gesperrt ist
    - Den Benutzer zwingen, sein iTunes-Passwort für jede Transaktion einzugeben
- Neue Netzwerk-Beschränkungen:
    - Übertragen einer eSIM auf ein anderes Gerät verhindern (iOS 18.0+)
- Neue Hardware-Beschränkungen:
    - iPhone-Mirroring deaktivieren

      Wenn diese Einstellung auf macOS verwendet wird, verhindert sie, dass der Mac ein iPhone spiegelt. Wird sie auf iOS verwendet, verhindert sie das Spiegeln des iPhones auf einen Mac. (iOS 18.0+, macOS 15+)
    - Deaktivieren der automatischen Dimmung auf iPad-Geräten mit OLED-Display (iOS 17.4+)
- Neue Anwendungsbeschränkungen
    - Verteilung von Web-Apps untersagen (iOS 17.5+)

- Das Erstellen neuer Genmoji verbieten (iOS 18.0+)
- Image Playground deaktivieren (iOS 18.0+, macOS 15+)
- Image Wand deaktivieren (iOS 18.0+)
- Verhindern, dass das System Text in der Handschrift des Benutzers erzeugt (iOS 18.0+)

Verbesserungen der Verwaltungsoberfläche

Kampagnen

- Neuer Kampagnentyp - Konfiguration anwenden

  Der Administrator kann Kampagnen mit einem Zeitplan für die Installation der Konfiguration erstellen. Es gibt die Möglichkeit, eine vorhandene Konfiguration auszuwählen oder eine neue zu erstellen (in einem neuen Fenster).

Richtlinienverwaltung

- Option zum Löschen von Richtlinien (nur verfügbar, wenn der Richtlinie keine Geräte zugewiesen sind)
  - Option zum Duplizieren einer Richtlinie aus der Richtlinienliste

    Wenn die Option verwendet wird, öffnet sich die Ansicht der Einzelheiten der neuen Richtlinie, wobei der Name der Richtlinie auf: „alter_Richtlinien_Name (DUPLIKAT)“ geändert wird.

Benutzerseite

- Neue Registerkarte auf der Seite Benutzerdetails - Geräte

  Anzeige der Liste von Geräten, die dem ausgewählten Benutzer zugewiesen sind

Geräteansichten

Geräteliste

- Neuer Filter für das Sicherheits-Patch-Datum

  Administratoren können Geräte nach dem gemeldeten Sicherheits-Patch-Datum filtern. Das Datum kann innerhalb eines Bereichs festgelegt werden.
- Filterung nach OS-Version

Administratoren können Geräte nach der gemeldeten OS-Version filtern, z. B. iOS 17.0.3)

- Verbesserte „Alles auswählen“ Funktionalität

  Das obere Kontrollkästchen, das für die Auswahl aller Aktionen verwendet wird, ist jetzt inaktiv, und zwei Optionen 'Alle auswählen' und 'Alle, die den Filtern entsprechen, zur Auswahl hinzufügen' werden angezeigt, wenn einige Filter angewendet sind.

  Zusätzlich wird angezeigt, wie viele Geräte ausgewählt werden, nachdem die Optionen 'Alle auswählen' oder 'Zur Auswahl hinzufügen' angewendet wurden.

- Möglichkeit, alle Filter in der Tabellenansicht zu entfernen

  Es gibt jetzt einen „x“-Schaltfläche neben der Filter-Schaltfläche. Damit werden alle angewendeten Filter entfernt.

Geräteverwaltung

- Anzeige des Namens der angewandten Richtlinie in der Seitenleiste der Gerätedetails
- Option „Alle Pins aus der Karte ausblenden“ auf der Registerkarte „Standort“.

  Es ist jetzt möglich, alle Pins aus der Karte auszublenden. Es gibt eine spezielle Schaltfläche (oben rechts in der Karte).

- Zeitfilteroptionen für die Einzelauswahl in der Ansicht Aktivitätsprotokolle:
  - Letztes Jahr (Standard)
  - Letzter Monat
  - Letzte Woche
  - Letzter Tag
- Seitenaufteilung für den Benutzerfilter in der Ansicht der Aktivitätsprotokolle

  Der Benutzerfilter in der Ansicht der Aktivitätsprotokolle unterstützt eine Seitenaufteilung, wenn mehr als 25 Optionen zur Auswahl stehen

Weitere Neuerungen

- Der Name der Microsoft Azure AD-Integration wurde in Microsoft Entra ID geändert
- Aktion zur erneuten Anwendung der verwalteten Konfiguration
  - Aktion zur erneuten Anwendung der verwalteten Konfiguration in der Anwendungsübersicht > Schnellaktionsleiste mit der Möglichkeit, die verwaltete Konfiguration aller ausgewählten Apps gleichzeitig an mehrere Geräte zu senden.
- Benachrichtigungen über Lizenzprobleme für Systemadministratoren, wenn es ein Problem mit der Serverlizenz gibt

- Die Aktion „Anwendung entfernen“ enthält jetzt zusätzliche Informationen, wenn die Anwendung über MDM installiert wurde
- Verbesserungen bei der LDAP/AD-Synchronisierung
  - Warnungen bei Erreichen der Zeitüberschreitung/Bindung und beim Entfernen eines AD-Benutzers
  - Die Verbindungszeitüberschreitung wurde auf 5 Sekunden geändert
  - Wenn die erste LDAP-Synchronisierung der Liste fehlschlägt, wird die nächste aus der Liste synchronisiert
- Erhöhte Details bei der Protokollierung beim Senden der App-Konfiguration an ein Gerät

weitere Verbesserungen

- Web Services
  - In den Filterparametern können Gerätegruppen-Ids (deviceGroupIds-Knoten mit groupdId-Knoten) festgelegt werden.

    Der Webdienst gibt nur Geräte aus den angegebenen Gerätegruppen aus
  - In der Ergebnisliste wird die Gesamtanzahl der Geräte angezeigt
  - Das Geräteobjekt gibt zusätzliche Felder zurück:
    - PlatformSystem - mit Werten wie z.B. Android, Apple
    - SecurityPatchDate - Datum der letzten Sicherheitsaktualisierung

- Gerätegruppenanzeige:
  - Neuer Eingabeparameter - loadDevices (standardmäßig auf aktiv gesetzt) - wenn nicht auf aktiv gesetzt, wird die Liste der Geräte nicht in der Liste der Gruppen zurückgegeben
  - In der Ergebnisliste wird die Gesamtanzahl der Geräte angezeigt

- Serverkonfiguration
  - Unterstützung der disablereuse-Direktive für die ProxyPass-Direktive in der Apache-Konfiguration in /etc/httpd/conf.d/mdm-apps.conf auf Proxy-Servern

    Diese Direktive ist notwendig für den korrekten Betrieb von Proxies, die sich nach fqdn mit dem geografischen Backend-Cluster verbinden.

    Die Option wurde in famoc-config hinzugefügt (nur bei Proxy-Servern):

famoc-config > System configuration > Additional HTTP Server Settings: Disable proxy connection reuse

- Möglichkeit APK-Apps in den AWS S3-Speicher zu replizieren und sie über CloudFront CDN bereitstellen

  Weitere Informationen zur Einrichtung von AWS S3-Speicher finden Sie in der Dokumentation AWS-CDN-Integration-Guide

Änderungen für die Erweiterte Benutzeroberfläche

Um die Funktionen schneller entwickeln und erweitern zu können, werden wir in der nächsten datomo MDM-Version einige der Funktionen deaktivieren, die bereits in der Verwaltungsoberfläche verfügbar sind:

- Konfiguration > Anwendungstab wird zum Anwendungstab der Verwaltungsoberfläche weitergeleitet
- Organisation > Benutzertab wird zum Benutzertab der Verwaltungsoberfläche weitergeleitet (der Datei-Benutzerimport ist weiterhin über Organisation > Importtab verfügbar)
- Organisation > Benutzerdetails leitet zur Registerkarte Profil der Verwaltungsoberfläche weiter
- Konfigurationszentrum > Pakete und Paketsets-Registerkarten werden deaktiviert.

Fehlerbehebungen

Android

- Benutzerdefinierte Felder werden auf speziellen Geräten nicht in der benutzerdefinierten Leiste angezeigt
- Neue verwaltete Konfiguration der Anwendung aus der Richtlinie wird nicht auf das Gerät angewendet, wenn die Richtlinie des Geräts geändert wird
- Der Fernzugriff unter Android 8 funktioniert nicht
- Die Samsung KSP-Konfiguration wird bei der Richtlinienaktualisierung nicht automatisch auf das Gerät angewendet
- Wenn eine Nachricht als Popup oder Vollbildnachricht gesendet wird, erscheint sie nicht in dieser Form auf dem Gerät
- Das IMEI-Nummernfeld wird nicht aktualisiert, wenn das Gerät mit einer anderen Variablen (meid) verbunden ist.
- Die Strongswan-VPN-Verbindung auf Abruf sollte für WPC-Geräte deaktiviert werden
- Das Ausschalten des WLANs ändert nicht das WLAN-Statussymbol im Kioskmodus (vollständig verwaltetes Gerät mit Kioskmodus-Konfiguration)
- Die Optionen ‚Nicht festgelegt' in der verwalteten Konfiguration werden nach der Parametrierungssynchronisierung in ‚Aus' geändert.
- Die Schaltflächen in der Android Base Agent-Anwendung passen nicht auf den Bildschirm

Apple

- Endlosschleife beim Laden der iOS-Unternehmensshop-Ansicht auf iPad-Geräten
- Die neuesten Versionen der iOS-Plattform werden nicht automatisch den iOS-Konfigurationen zugeordnet
- Es gibt Optionen für Google-Apps (Richtlinienakzeptanz) auf der Apple-App-Detailseite
- Das Bereitstellen des iPadOS/iOS-Firmware-Updates funktioniert nicht

Verwaltungskonsole / sonstige

- Die Suchkriterien aus der Anwendungsübersicht werden automatisch auf dem Tab für den Installationsstatus auf der Detailseite der Anwendung angewendet.
- Die Tabs „Anwendungen auf dem Gerät“ und „Kompatible Anwendungen“ werden nicht geladen
- Fehlende Übersetzungen für die Spalten 'Persönliche Apps aussetzen' und 'Vom Unternehmen verwaltete Apps mit Arbeitsprofil' in der Geräteliste
- Interner JSON-RPC-Fehler beim Laden der Ansicht 'Von Microsoft Entra erstellte Gruppen' unter Benutzeroberfläche > Einstellungen > Benutzer & Authentifizierung > Microsoft Entra ID-Integrationsansicht
- Problem mit der Darstellung des letzten Standorts auf der Karte bei Verwendung des Datumsfilters
- Es ist nicht möglich, mehr als 50 Benutzer auf einmal zu löschen
- Transformations-Regex und Transformationswert-Optionen werden während der Microsoft Entra ID-Synchronisierung ignoriert
- Beim Speichern einer Richtlinie über die Benutzeroberfläche wird die Benutzersitzung nicht angestoßen
- Nach der Auswahl von Stunden aus der Datumsauswahl, dem Speichern und dem Aktualisieren der Seite sind die angezeigten Stunden anders als die ausgewählten
- Es werden nur 25 Datensätze zurückgegeben, wenn ein Filter im Tab für Geräteorte verwendet wird
- Das Ändern des Benutzers auf mehr als einem Gerät führt dazu, dass die Benutzerliste leer ist.
- Der Protokoll-Tab kann nach dem MySQL-Update auf 8.x weiterhin abstürzen
- Nachdem der 'Dedizierte Anwendungs-TCP-Port' in der famoc-config geändert wurde, verwenden bereits registrierte Geräte weiterhin den alten Port.

Plug & Play 1.16.0 Fehlerbehebungen

- Es wird keine Ansicht gekoppelter Geräte angezeigt, wenn gekoppelte Geräte vorhanden sind

Neue Gerätemodelle

- Apple iPhone 16
- Apple iPhone 16 Plus
- Apple iPhone 16 Pro
- Apple iPhone 16 Pro Max
- Nokia G20
- Realme 12 Pro 5G
- Urovo DT66
- Xiaomi Redmi Note 13 5G

Neue Plattform-Unterstützung

- Android 15
- tvOS 18.1
- macOS 14.7
- iOS / iPadOS 17.7
- iOS 18 / macOS 15

Versionshistorie

MDM Version	Release ID	Wichtige Hinweise[1]
MDM 5.37	2024-10-31	MySQL 8.0.36 erforderlich
		unterstütze Plattformen: RHEL 8, Oracle 8, Rocky 8
MDM 5.36	2024-07-31	MySQL Aktualisierung auf 8.0.36 möglich, letzte Version mit CentOS 7 Unterstützung
MDM 5.35.1	2024-06-18-rel	
MDM 5.35.0	2024-05-31X	
MDM 5.34	2024-02-29X	Firebase; Firewall
MDM 5.33	2023-11-30X	
MDM 5.32.2	2023-10-15-rel	VPP
MDM 5.32.1	2023-8-31-rel	MySQL 8
MDM 5.32.0	2023-07-31X	
MDM 5.31.0	2023-05-31X	
MDM 5.30.0	2023-01-31X	

1: Für vollständige Informationen lesen Sie bitte die gesamtem Versionshinweise