datomo Essentials MDM Versionshinweise 5.36

Inhaltsverzeichnis

Hinweise....2
Auslaufender CentOS 7-Support....2
Funktionsänderungen Fortgeschrittenen-UI....2
Mögliche Aktualisierung der MySQL-Datenbank....2
Neue Funktionen....3
Android....3
Apple....4
Verbesserungen der Weboberfläche....5
Geräteliste / Details....5
Richtlinien....5
Kampagnen....6
Verwaltete Konfigurationen....7
Intelligente Gruppen....7
Ansicht Einstellungen....7
Weitere Funktionen und Verbesserungen....7
Serververbesserungen....9
Fehlerbehebungen....9
Android....9
Apple....10
Sonstiges Fehlerbehebungen / Verwaltungskonsole....10
Plug&Play 1.16.0 Fehlerbehebungen....11
Neue Gerätemodelle....11
Neue Plattformen....12
Versionshistorie....13

Hinweise

Auslaufender CentOS 7-Support

datomo MDM 5.36 ist die letzte Version mit CentOS 7-Unterstützung. Weitere Aktualisierungen und

Verbesserungen werden in Zukunft nicht für diese Plattform verfügbar sein. Was bedeutet das für den Systembetrieb für On-Premise Kunden?

Das System läuft mit der aktuellen Version weiter, wir empfehlen jedoch die Migration auf eine der Plattformen mit Langzeitunterstützung: Oracle Linux 8, RHEL 8 oder Rocky Linux 8.

Als On-Premise Kunde sollten Sie zur Migration bereits Dokumente erhalten haben. Für weitere Unterstützung stehen wir Ihnen selbstverständlich zur Seite.

Funktionsänderungen Fortgeschrittenen-UI

Um Funktionalitäten schneller entwickeln und erweitern zu können, werden wir in der nächsten datomo MDM-Version einige der Funktionen, welche bereits im Management UI verfügbar sind, deaktivieren:

- Konfiguration > Registerkarte „Anwendung“ wird auf die Registerkarte „Anwendung“ der Management UI umgeleitet
- Die Registerkarte Organisation > Benutzer wird auf die Registerkarte Benutzer der Management UI umgeleitet (der Import von Benutzerdateien ist weiterhin über die Registerkarte Organisation > Importe verfügbar)
- Organisation > Benutzerdetails leitet zur Registerkarte Profil der Management-Oberfläche weiter
- Die Registerkarten Konfigurationszentrum > Packages und Set of Packages werden deaktiviert.

Mögliche Aktualisierung der MySQL-Datenbank

Nach der Aktualisierung des MDMs auf Version 5.36 haben Sie die Möglichkeit auf MySQL 8.0.36 zu aktualisieren. Dazu nutzen Sie auf dem Applikationsserver den Befehl:

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

Die Aktualisierung wird spätestens für datomo MDM 5.37 benötigt werden. Erstellen Sie wie bei anderen Updates auch vor der Durchführung ein Backup. Auf CentOS 7 ist diese Aktualisierung nicht notwendig, da datomo MDM 5.37 nicht auf dieser Plattform unterstützt werden wird.

Neue Funktionen

Android

- Unterstützung für zwei IMEI-Nummern, wenn das Gerät eine Verbindung zum Server herstellt
  - Unabhängig davon, in welchem Slot sich die SIM-Karte befindet, wird das Gerät den Server korrekt kontaktieren.
- Möglichkeit, Systemanwendungen im privaten Teil von WPC zu sperren (firmeneigene mit privatem Teil aktivierte) Geräte
  - Die Option ist verfügbar unter BYOD-/WPC-Richtliniendetails > Gerätesicherheitsoptionen > Anwendungs-Einschränkungen > Anwendungsrichtlinie auf WPC-Geräten
- Die Meldung „Bildschirm sperren“ zeigt jetzt den Wert aus dem Feld „Auf dem Gerät angezeigter Organisationsname“ aus der Richtlinie an
- Neue Konfiguration - Aktivieren von mobilen Daten
  - Die Konfiguration ist für Geräte im Kioskmodus (dedizierte Geräte) verfügbar.
  - Die Konfiguration ermöglicht es, die Einstellungsansicht aufzurufen und mobile Daten zu aktivieren.
  - Nach dem angegebenen Zeitlimit wird die Einstellungsansicht deaktiviert und der Vorgang wird als fehlgeschlagen markiert.
- Neue Konfigurationen - Sprache auf dem Gerät ändern
  - Die Konfiguration ist auf Android-Geräten mit signierter Addon-Anwendung verfügbar.
  - Die Konfiguration der Sprachänderung erfordert einen gültigen Sprachnamen wie en_US, de_DE, fr_FR
- Meldung der MEID-Nummer an die Verwaltungskonsole (falls auf dem Gerät vorhanden)
- Remote Access (6.10) Agent mit geändertem Symbol
- Ziel-SDK der Launcher-App wurde auf Version 31 (Android 12) aktualisiert
- Badge für geänderte Dateien innerhalb des Ordners in der FileViewer-Anwendung
  - In früheren Versionen gab es einen Badge für Änderungen an Dateien oder Ordnern.
  - Auf dem Gerät konnte der Benutzer sehen, dass es eine Änderung im Ordner gibt, aber beim betreten des Ordners konnte der Benutzer nicht feststellen, welche Datei geändert wurde.
  - In der aktuellen Version werden neue Dateien in Ordnern mit einer entsprechenden Anzeige versehen. Diese Funktion erfordert eine spezielle Geräterichtlinie mit aktivierten Produktivitätsanwendungen und FileViewer-Anwendung mit eingestelltem FTP-Sync.

Produktivitätsanwendungen können in einer Organisation nur aktiviert werden, wenn eine zusätzliche Lizenz vorhanden ist. Bitte wenden Sie sich für diese Option an Ihren Dienstanbieter.

- Plug&Play (1.16.12) und FileViewer (1.8.4): Verbesserungen bei der Speicherung von Protokollen
- Das Ziel-SDK für die Plug&Play-App wurde auf 34 (Android 14) aktualisiert
- Neue Icons für die Plug&Play- und FileViewer-Apps.

Apple

Apple-Funktionen und Verbesserungen (einschließlich iOS-Agent 5.2.0 und macOS-Agent 5.0.0):

- Unterstützung mehrerer VPP-Integrationen
  - Mit der Version 5.36 kann der Administrator mehr als eine VPP-Integration in der Organisation zu definieren.
  - Verfügbar bei der Registerkarte Einstellungen > Apple > VPP-Integration, wo die Liste der VPP-Integrationen angezeigt wird. Um eine neue Integration (neues Token) hinzuzufügen, klicken Sie auf die Plus-Taste.
- [macOS/iOS] Unterstützung der Datei-Upload-Konfiguration sowohl für iOS- als auch für macOS-Agenten
  - Es ist jetzt möglich, die Datei-Upload-Konfiguration auf iOS- und macOS-Geräten zu verwenden. Es werden URL- und Dateiquellentypen unterstützt.
  - Das Pfadfeld in der Konfiguration wird aufgrund der Apple-Richtlinien übersprungen.
  - Alle Dateien werden unter macOS und iOS in den Ordner „Dokumente“ heruntergeladen.
  - Unter iOS finden Sie die heruntergeladenen Dateien in der Anwendung Dateien (integriert) -> Auf meinem iPhone in dem Verzeichnis namens Essentials MDM.
  - Der Administrator ist für die korrekte Benennung der Dateien mit Erweiterungen verantwortlich.
- [macOS/iOS] Möglichkeit, Agentenprotokolle basierend auf der Richtlinieneinstellung zu löschen
  - Es gibt eine neue Richtlinieneinstellung - Agent Operation History period - die es erlaubt, die historischen Protokolle nach einem bestimmten Zeitraum (1 Tag bis 3 Monate) vom Gerät zu entfernen.
- [iOS] Sicherung von Kontakten im iOS-Agent
  - Aktionen zum Sichern/Wiederherstellen von Kontakten können über das Aktionsfeld in der Management UI aufgerufen werden.

- Die Funktion zur Sicherung von Kontakten sollte wie unter Android funktionieren. Der einzige Unterschied ist, dass Android für Sicherung- und Wiederherstellungsvorgänge ein Passwort für einen bestimmten Zeitraum im IT-Kontrollpanel des Agenten festlegt werden kann, wohingegen unter iOS ein Kennwort für jeden Sicherungsvorgang festgelegt werden kann.
- Die meisten Felder werden von vCard 3.0 unterstützt.
- Bei der Sicherung/Wiederherstellung wird nach Abschluss des Vorgangs ein Hinweis angezeigt.

- [macOS] Gerätemonitor-Operation, die Prozessor-, RAM- und Modellattribute von macOS-Geräten meldet

Verbesserungen der Weboberfläche

Geräteliste / Details

- Neuer Filter in der Geräteliste - OS Version
  - Die Liste der Geräte kann jetzt nach der gemeldeten OS-Version gefiltert werden.
- Option „Aktuelle Auswahl anzeigen“ im Auswahlmenü
  - Administratoren können nun alle ausgewählten Elemente anzeigen (wenn viele Filter ausgewählt oder Suchen durchgeführt wurden).
  - Alle ausgewählten Geräte werden am Anfang der Liste angezeigt.
- Neue Spalte „Erstinstallation“ der Anwendung auf der Registerkarte „Anwendungen auf dem Gerät“.
- Alle Sicherheitseinschränkungen, die in der Richtlinie festgelegt sind, werden jetzt auf der Registerkarte „Gerätestatus“ angezeigt

Richtlinien

- Es gibt eine neue Registerkarte in der Detailansicht der Richtlinie - Historie der Änderungen.
  - In dieser Ansicht werden Revisionen angezeigt, die zeigen, wer und was in der Richtlinie geändert wurde.
  - HINWEIS: Die erste Berechnung des Änderungsverlaufs der Richtlinie betrifft den Zeitpunkt der Installation des 5.36-Updates und kann daher ein wenig länger dauern.
- Regelbasierte Sicherheitsoptionen und Standardsicherheitsoptionen in den Richtliniendetails werden jetzt Seite an Seite angezeigt

- Regelbasierte Sicherheitsoptionen in dedizierten Geräterichtlinien
  - Es ist jetzt möglich, regelbasierte Sicherheitsoptionen in der dedizierten Geräterichtlinie zu aktivieren.
  - Der Mechanismus funktioniert genauso wie bei vollständig verwalteten Geräterichtlinien.
- Regelbasierte Sicherheitsoptionen im Modal zum Ändern der Richtlinieneinstellungen
  - Die regelbasierten Sicherheitsoptionen können mit der Aktion Einstellungen ändern sowohl für vollständig verwaltete Richtlinien und dedizierte Geräterichtlinien geändert werden.
- Die Spalte „Verfügbarkeit“ auf der Registerkarte „Sicherheitseinschränkung“ enthält jetzt nur noch Plattformsymbole.
  - Details über die Plattformverfügbarkeit werden als Tooltip angezeigt.
- Einstellungen ändern > FRP-Richtlinie - Überprüfung der angegebenen Werte bei der Option „Entsperren des Gerät mit einem Konto aus der Liste“ ausgewählt wird.
  - Diese Liste lässt nur numerische Werte zu.
- Wenn Sie alle untergeordneten Einschränkungen der WiFi-Sperre aktivieren, können Sie jetzt die Option WiFi-Sperre aktivieren.

Kampagnen

- Neuer Kampagnentyp – Anwendungsinstallation
  - Administratoren können Kampagnen mit einem Zeitplan für die Anwendungsinstallation erstellen.
  - Darüber hinaus verteilt der Server automatisch die Last des Servers, so dass das Versenden vieler Vorgänge auf einmal kein Problem darstellen. Details zur Überwachung der Serverauslastung werden darunter beschrieben.
- Neuer Kampagnentyp - Nachricht senden
  - Administratoren können Kampagnen erstellen, um neue / vordefinierte Nachrichten an Geräte zu senden.
  - Nachrichten können zur einmaligen Ausführung, in einem Zeitfenster oder als wiederkehrende Operation geplant werden.
- Neue Spalte: „Komponente“, die die Firmware-Kennung für Zebra Lifeguard OTA Updates und den Namen der Anwendung für die Anwendungsinstallation enthält.
  - Mit dieser Spalte wird es einfacher sein, den Inhalt der Kampagne in der Liste zu bestimmen.

Verwaltete Konfigurationen

- Textfeld ändern
  - Jetzt gibt es nur noch ein Feld mit der Möglichkeit, es manuell zu füllen oder ein Attribut aus einer Datenquelle auszuwählen.
  - Wenn ein Attribut ausgewählt wird, wird das Token dieses Attributs in das Textfeld eingefügt, so dass es möglich ist, den Wert mit anderen Daten zu kombinieren (manuell ausgefüllt oder aus anderen Attributen).
- Möglichkeit zum Abbrechen der aktuellen Änderungen in der verwalteten Konfiguration
  - Es gibt eine neue Schaltfläche mit dem Namen „Abbrechen und alle Änderungen verwerfen“, die alle nicht gespeicherten Änderungen in der verwalteten Konfiguration verwirft.

Intelligente Gruppen

- Grundlegende Geräteattribute können jetzt als Bedingung für die Zuordnung von Geräten in Intelligenten Gruppen verwendet werden

- Das Datumsfeld für den Sicherheitspfad kann nur mit einem Datum im Format JJJJ-MM-TT gefüllt werden

Ansicht Einstellungen

- Minimierung des linken Fensters in der Ansicht der Organisationseinstellungen
- Zusammenklappbare Symbolleiste in der Ansicht der Organisationseinstellungen
  - Mit beiden Änderungen können die Einstellungsansicht mit z.B. der Liste der Gruppen, der Integrationen, usw. vergrößert dargestellt werden.

Weitere Funktionen und Verbesserungen

- Überarbeitete Cache-Steuerung für eine bessere Leistung der Benutzeroberfläche
  - Statische Dateien, die vom Server ausgeliefert werden - js, png, svg, woff2, ttf, css, ico, jpg, jpeg haben nun „Cache-Control: private, max-age:43200, must-revalidate“ Antwort-Header hinzugefügt.
  - Alle dynamischen Inhalte - rpc json-Anfragen, dynamisch erstellte HTML-Vorlagen - werden mit „Cache Control: no-store, no-cache, must-revalidate“ Antwort-Kopfzeilen.
- Nach der Anmeldung werden Semi-Administrator- und Super-Administrator-Konten auf die Liste der Organisationen umgeleitet, anstatt der zuletzt angesehenen Organisation

- Die Registerkarte im Fortgeschrittenen-UI > Fernzugriff leitet jetzt zur Liste der Geräte der Verwaltungsoberfläche gefiltert nach Geräten mit installiertem Fernzugriff weiter.
- Neuer Webdienst: addDeviceCustomFieldValue
  - Diese Methode ermöglicht es, den Wert des benutzerdefinierten Feldes des Geräts aus der angegebenen Organisation zu füllen. Parameter der Methode:
    - organisationID
    - deviceId
    - customFieldID
    - Wert
    - dictValueId

- Migration von famoc-cli in das Werkzeug essentials-mdm-config, Funktionalität von famoc-cli in essentials-mdm-config integriert
  - auf dem App-Server ist famoc-cli nun mit essentials-mdm-config verlinkt
  - auf dem Proxy-Server ist essentials-mdm-config der Befehl, der die Rolle von famoc-cli übernimmt
  - Aufräumarbeiten / Refaktorierung:
    - Warnungen zur „Verifizierung“ von Zertifikaten entfernt
    - Ausnahme behoben, wenn das Skript ohne Argument aufgerufen wird und kein Pfad in der interaktiven Eingabe „Enter path to Certificate“ eingegeben wurder
    - Das Programm gibt nun exakte OpenSSL-Fehler weiter, wenn ein privater Schlüssel verschlüsselt wurde und ein falsches Passwort angegeben wurde oder ein anderer OpenSSL-Fehler auftrat
    - Optionales Flag hinzufügen, um den Neustart von httpd beim Laden von Zertifikaten zu überspringen
    - Sicherungskopie erstellen, bevor die Dateien proxy.pem und /etc/httpd/ssl cert ersetzt werden
    - wenn HA mit httpd-Ressource erkannt wird, und die wenn Standardoption von httpd-Neustart aufgerufen wird, wird auf Wartungsmodus überprprüft und ein Fehler ausgeben, wenn der Wartungsmodus nicht aktiviert ist
    - wenn die HA httpd-Ressource Heartbeat und nicht systemd-Provider ist, wird httpd -k statt des Neustarts über systemctl aufgerufen

Serververbesserungen

- Um hohe Serverlast besser zu bewältigen, haben wir eine Überwachung der Serverkapazitätswerte eingeführt.
    - Basierend auf den Hintergrundberechnungen kann der Server entscheiden, wie viele Operationen auf einmal gesendet werden können (z. B. das Senden einer App-Installationskampagne an 1000 Geräte).
    - Der Hintergrundüberwachungsdienst sammelt Informationen zur Serverleistung, wie CPU-Last, php-Worker Statistiken, Webserver- und Datenbankverbindungen.
    - Auf der Grundlage der gesammelten Informationen können die internen MDM-Warteschlangen ihre Kapazität dynamisch anpassen, um die Menge der gleichzeitig gesendeten Geräteoperationen zu reduzieren oder zu erhöhen.
    - Eine anpassbare Einstellung in der config.php regelt die Qos-Modi: „$cons_queue_qos_mode“, mit diesen Optionen:
        - off (Standard) - keine Drosselung
        - simple - maximal 100 Slots für Geräte, die aktiv Vorgänge verarbeiten
        - adaptive - dynamische Drosselung der Anzahl der gleichzeitig gesendeten Geräteoperationen basierend auf der System-Last
        - adaptiv-soft - sanftere Variante der adaptiven Drosselung

Der Moduswechsel wird sofort wirksam, ohne dass ein Neustart der Dienste erforderlich ist.

Fehlerbehebungen

Android

- Hinzufügen eines Geräts zum WPC-Modus (Zero-Touch oder QR-Code) mit Anmeldeinformationen funktioniert nicht
- Remote Access-Sitzung wird nicht automatisch gestartet, nachdem die Dateiberechtigung erteilt wurde
- Das Gerät wechselt bei der Anmeldung nicht in den Geofence-Beschränkungsmodus
- Die Einstellungen sind nach dem Neustart des dedizierten Geräts verfügbar
- Lange Wartezeit beim Aktualisieren des Google Play Store auf Geräten

- Die Samsung SDK-Optionen in den Netzwerkrichtlinien (eingehende MMS, SMS, Anrufe blockieren) für dedizierte Geräte funktionieren nicht
- Die Anwendung wird nicht gewechselt, wenn die Option: „Erste Anwendung nach Neustart starten“ in der Richtlinie für dedizierte Geräte
- Problem bei der Installation von verwalteten Google Play-Anwendungen
- Benutzer deaktivierte Standortdienste auf Gerätealarm auf neu hinzugefügten Geräten

Apple

- leinere visuelle Probleme des iOS-Agenten wie z.B. grauer Hintergrund in der Kopfzeile
- VPP-Code-Synchronisierungsproblem, wenn Essentials MDM-App auf der Liste steht
- iOS Business Kontakte synchronisieren ohne polnische Zeichen auf dem Gerät

Sonstiges Fehlerbehebungen / Verwaltungskonsole

- Status-Spalte auf der Registerkarte „Kampagne“ sollte keine Sortieroption haben
- Der Wert 'Geräte-Limit pro Benutzer' kann im Modal 'Einstellungen ändern' nicht eingestellt werden
- SafetyNET-Attestierung (Play integrity API) ist in neuen Richtlinien immer aktiviert, bei Erstellung über das Management UI
- SmartGroups: Die Auswahl „Plattform zuweisen“ wird bei der Gruppenerstellung nicht beibehalten
- Die Richtlinie kann nicht gespeichert werden, wenn die Konfiguration aus den Richtlinienkomponenten entfernt wird.
- Fehler beim Hinzufügen des Geräts über den Browser, der Benutzer erhält in kurzer Zeit mehrere Registrierungs-E-Mails
- Die Dropdown-Liste „Gerätegruppe“ passt nicht in das Zero-Touch-Modal
- Bei der Auswahl von „Alles auswählen“ in der Liste aller Geräte erscheint ein Bedienungsfehler bei einer großen Anzahl von Datensätzen
- Falsche Meldung beim Trennen der Anwendung von der Richtlinie
- Die zweite Simkartennummer ist in der Verwaltungsoberfläche nicht sichtbar
- Falsche Sprache in der exportierten Datei der Gerätestandorte

- Das Entfernen eines aus dem AD entfernten Benutzers schlägt nach längerer Ausführung fehl
- Falsche Weiterleitung zum Management UI bei der Geräteanmeldung
- Richtlinienänderung ist aufgrund der Zeitüberschreitung nicht möglich
- Problem beim Aktualisieren eines benutzerdefinierten Feldes, das ein Wörterbuch ist
- Cronjob-Fehler '/etc/cron.d/sync_platforms' überflutet /var/spool/mail/root
- Nach dem Löschen von Anwendungsdateien sind diese immer noch im Ordner application-files gespeichert

Plug&Play 1.16.0 Fehlerbehebungen

- Konfiguration wird nicht neu geladen, wenn es kein verwaltetes Google Play Konto gibt
- Fehlende Menütasten, wenn das Gerät verbunden ist
- Manchmal trennt das Gerät die Verbindung

Neue Gerätemodelle

- ADOC T10
- Asus Zenfone 11 Ultra
- Bluebird S20
- Honor X6
- Motorola Edge 30 Ultra
- Motorola Edge 40 Neo
- Motorola Edge 50
- Motorola Edge 50 Neo
- Motorola Moto G14
- Motorola Moto G34
- Motorola Moto G53
- Motorola Moto G54
- Motorola Moto G54 5G
- Motorola Moto G84 5G
- Oppo Reno 11 F

- Oukitel RT2
- Pointmobile PM95
- Realme C67
- Samsung SM-A155 Galaxy A15
- Samsung SM-P625 Galaxy Tab S6 Lite (2024)
- Samsung SM-X216B Galaxy Tab A9+ 5G
- Samsung SM-X306B Galaxy Tab Active 5
- Xiaomi 12 Lite
- Xiaomi Redmi 10 (2022)
- Xiaomi Redmi 12
- Xiaomi Redmi Note 12

Neue Plattformen

- macOS 14.6, 15.0, 15.1
- iOS, iPadOS, tvOS 17.6, 18.0, 18.1

Versionshistorie

MDM Version	Release ID	Wichtige Hinweise[1]
MDM 5.37	tbd	MySQL 8.0.36 erforderlich
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