datomo®
MOBILE
DEVICE MANAGEMENT

Versionshinweise

datomo MDM 5.41

März 2026

Übersicht

1 Hinweise

Als Teil der in Version datomo MDM 5.41 eingeführten Verbesserungen bei der Authentifizierung müssen die im Bulk generierten QR-Codes aus Version 5.40 neu erstellt werden. Laden Sie bitte die aktualisierten QR-Codes vom Server herunter, um volle Kompatibilität und Sicherheit zu gewährleisten.

1.1 On-Premise Installationen

Diese Version von datomo MDM aktualisiert das System während des Updates auf PHP 8.2.

Das Konfigurationstool *famoc-config* wird durch *essentials-mdm-config* mit der Aktualisierung ersetzt werden. Ein Teil der Konfigurationen wird nun in der Webkonsole vorgenommen. Weitere Hinweise zu dieser Änderung finden Sie im Abschnitt „Server“ dieses Dokuments.

2 Neue Funktionen

2.1 Linux-Unterstützung

datomo MDM unterstützt jetzt Linux als verwaltete Plattform erster Klasse– und bringt damit leistungsstarke Sicherheit, Automatisierung sowie Fernoperationen zu den Geräten Ihrer Linux-Flotte.

Die Linux-Unterstützung bietet:

- Sichere Verbindung mit einem gehärteten Agent-Server-Protokoll
- Automatisierte Updates & Patch-Management über native Paketverwaltungsprogramme
- Fernzugriffaktionen, darunter Befehlsausführung, App-Steuerung, Dateiübertragung, Sperren und Löschen von Geräten
- Vollständige Richtlinienumsetzung für Sicherheit, Konnektivität und Gerätebeschränkungen
- Remote-Terminalzugriff für schnelle Fehlerbehebung

- Einfache Registrierung mit automatischem Installationsstart und skriptbasierter Einbindung
- Tiefgehende Transparenz durch Geräteinformationen, Protokolle und Überwachung
- IP-basierte Standortbestimmung, weitere Hardware-Methoden sind in Vorbereitung
- Läuft im Hintergrund als stummer Dienst

Die Verwaltung von Linux-Geräten wird für folgende Distributionen unterstützt:

- Ubuntu 20.04 LTS bis 25
- Debian 11 bis 13.2
- Fedora 38+
- Red Hat 8, CentOS 9, RHEL 10

Weitere Informationen zu den unterstützten Plattformen finden Sie im Downloadbereich unter Geräteeinschreibungen – Linux-Geräte.

2.2 Android

Neuorganisation der Basis-Agenten-Ansicht

und Verschiebung der Protokolle vom Tab Benachrichtigungen in einen separaten Tab namens „Operationen“ mit Option zur Filterung nach Status oder Aktionsart. Zudem wird angezeigt, wer die Aktion ausgelöst hat.

Geräteprotokolle abrufen mit Android-Fehlerbericht für COBO-/COSU-Geräte

Die Operation zum Abrufen von Geräteprotokollen kann nun einen Android-Fehlerbericht erstellen, der zusammen mit den Agent-Protokollen an den Server gesendet werden kann.

Heartbeat-Option

Das Heartbeat-Feature bietet eine beinahe Echtzeit-Ansicht des Online-Status der Geräte (aktiv/inaktiv) in der Benutzeroberfläche. Die Funktion kann in der Richtlinie aktiviert werden, indem der Schalter „Geräte-Online-Status aktivieren“ eingeschaltet und ein passendes Intervall eingestellt wird.

Sobald dies aktiviert ist, wird der Online-Status aller der Richtlinie zugewiesenen Geräte sowohl in der Geräteliste (Spalte Status) als auch in den Geräteinformationen unter dem Geräte-Symbol sichtbar.

Änderungen bei Play Integrity

Während des Einschreibens wird, wenn die Play Integrity-Prüfung durchgeführt wird, unser Agent auf dem Setup-Bildschirm bleiben und der Endnutzer über den Fortschritt der Integritätsprüfung informiert werden.

Unterstützung für WPA3-WLAN-Konfigurationen

Es gibt eine neue Option – „WPA3 erzwingen“ – in der WLAN-WPA-PSK-Konfiguration für Android-Geräte

Aktualisierung der Android Agent API

Neue API-Funktionen in dieser Version:

- actions.sendDebugReport
- actions.message
- app.clearData
- app.getInstalledApp
- app.install
- app.start

- app.stop
- app.hide
- app.updateInBackground
- android.startActivityForResult
- android.createFileContentUri
- device.wifi.*

Die vollständige Dokumentation kann auf datomo MDM-Server unter

https://fqdn/docs/agent-api/

eingesehen werden.

Aktualisierung der für Fernzugriff verwendeten LiveKit-Bibliotheken

Die Bibliotheken wurden auf den aktuellsten Stand aktualisiert.

2.3 Apple

Neuer iOS Agent 5.6.0

Inklusive der Aktualisierung der für Fernzugriff verwendeten LiveKit-Bibliotheken

Neue Plattformen

iOS, iPadOS, macOS, tvOS 26.3

Unterstützung für mehrere APN-Profile auf iOS-Geräten

Es ist nun möglich, Standard-APN, Daten-APN oder beides gleichzeitig im selben Payload zu definieren.

2.4 Mobiler Bedrohungsschutz

Wir haben den Mobilen Bedrohungsschutz mit neuer Sichtbarkeit, optimierten Arbeitsabläufen und stärkerer automatisierter Schutzmaßnahmen erweitert.

Die Neuerungen im Detail:

- Neue Spalten in der Geräteliste: Status Mobiler Bedrohungsschutz sowie Compliance-Status
- Richtlinien-Duplizierung umfasst nun alle MTD-Einstellungen
- Übersichtlichere Richtlinienstruktur mit neu organisierten Abschnitten für Bedrohungsregeln und Scan-Optionen
- Scan-Intervalle für URL-Überwachung und App-Bedrohungserkennung werden nun auf Richtlinienebene festgelegt
- Vereinfachte Virenwarnmeldungen – ohne Angabe des Warnlevels
- Neue automatische Behebungsmaßnahmen:
  - Gerät sperren
  - Arbeitsprofil deaktivieren
  - Bluetooth blockieren
  - NFC blockieren
  - VPN blockieren
  - Anwendung entfernen

2.5 Verwaltungskonsole

2FA-Authentifizierung für Super-/Semi-Admin-Konto

Auf dem Formular zur Erstellung eines Semi-Admins gibt es nun einen neuen Schalter – Zwei-Faktor-Authentifizierung aktivieren. Ist dieser gesetzt, können Semi-Admins die 2FA-Authentifizierung nutzen (nur SMS-Methode verfügbar)

Voraussetzungen: Der SMS-Gateway muss auf dem Server konfiguriert sein und in der config.php muss {{$cons_twofactor_sms_available = true;}} gesetzt sein.

Automatische Behebungsaktionen für Checkpoint MTD-Integration

Es ist nun möglich, automatische Behebungsaktionen festzulegen, wenn Checkpoint dem Server spezifische Risiken auf einem Gerät meldet.

Das Panel für Risiken und Behebungen ist im Bereich der Checkpoint-Integrations-Einstellungen verfügbar.

Bestätigungsschritt vor Aktivierung der Auto-Import-Option bei Samsung KME-Bulk-Registrierung

Der Administrator muss die Auswahl der Auto-Import-Option bestätigen, bevor sich die Änderung auf die gesamte Samsung-KME-Integration auswirkt.

Verbesserungen der Mobile-Threat-Defense-Integration

- Neue Spalten in der Geräteliste: „Mobiler Bedrohungsschutz Status“ und „Compliance-Status“
- Die Duplikation einer Richtlinie dupliziert nun auch alle MTD-Einstellungen.
- Umstrukturierung der MTD-Abschnitte in der Richtlinie zu:
  - System- & Netzwerkbedrohungsregeln
  - Anwendungsbedrohungsregeln
  - Aktivierung der Malware-/Virusprüfung für Anwendungen
  - Aktivierung der kategorisierten URL-Überwachung.
- Die Intervalle für die kategorisierte URL-Überwachung und Anwendungsbedrohungsprüfungen wurden in die Richtliniendetails verschoben und können nun auf Richtlinienebene (nicht mehr Organisationsebene) eingestellt werden.
- Der Alarm-Level wurde aus der Viruswarnmeldung entfernt.

- Neue automatische Behebungsaktionen:
  - Gerät sperren,
  - Arbeitsprofil deaktivieren,
  - BT blockieren,
  - NFC blockieren,
  - VPN blockieren,
  - Anwendung deinstallieren.

Neuer Monitoring-Tab

mit überarbeitetem Layout und Links zum neuen Reports-Tab.

Neuer Reports-Tab

mit Liste vordefinierter Berichte und Möglichkeit zur Erstellung benutzerdefinierter Berichte basierend auf Geräte-, Benutzer- oder SIM-Kartendetails. Der neue Bereich ist unter dem Monitoring-Tab zu finden.

Option, Anwendungsupdates für Android-Geräte über Richtlinienmechanismus aufschieben

Anwendungen, welche als Komponenten in einer Richtlinie hinzugefügt wurden, haben nun die Möglichkeit, deren Update aufzuschieben. Die Option ist in der Richtlinienkomponentenliste verfügbar. Ist sie aktiviert, wird das Upgrade um 90 Tage ab dem Zeitpunkt der Veröffentlichung des Updates im Verwalteten Google Play Store verschoben.

Aktualisierung verwendeter Bibliotheken für Oberflächendarstellung

Bootstrap- und Angular-Bibliotheken aktualisiert

Lizenzänderungen im Fortgeschrittenen-UI

Änderungen an alten Lizenzen werden ermöglicht, selbst wenn die aktuelle Anzahl verwalteter Geräte höher ist als die in der alten Lizenz begrenzte Anzahl.

Möglichkeit zur Nutzung der Security Identifier (SID)-Erweiterung im CSR für MSCA-Integration

Die Verbesserung wurde aufgrund einer Änderung bei den über Microsoft CA generierten Zertifikaten vorgenommen, bei welcher die neue Erweiterung automatisch enthalten ist.

2.6 Server

Datenbankversion

MySQL 8.0.43 ist nun die Mindestversion für Serveraktualisierungen

PHP-Versionen

Aktualisierung der PHP-Bibliotheken auf Version 8.2

Ersatz von *famoc-config*

Die meisten Einstellungen von *famoc-config* können nun mit *essentials-mdm-config* abgerufen werden.

Folgende Optionen sind für Super-Admins über die UI-Konsole im Bereich „Serverkonfiguration“ (neben „Einstellungen“) verfügbar:

Grundlegende Einstellungen

- E-Mail-Adresse des Systems
- Absendername der E-Mail

SMS-Gateway-Konfiguration

- SMS-Gateway-Host
- TCP-Port des SMS-Gateways
- Passwort zur Authentifizierung am SMS-Gateway
- Verschlüsseltes SMS-Gateway-Passwort
- Nummer für Benachrichtigungen bei SIM-Kartenwechsel
- CID (Client ID), die vom SMS-Gateway verwendet wird

Erweiterte Einstellungen

- Ermöglicht Nutzern, sich mit einer E-Mail-Adresse anzumelden
- Standardsprache
- Passwortkomplexität für Nutzer

Push-Benachrichtigungskonfiguration (FCM)

Einstellungen zur Geräteprotokollierung

- Protokolle aktiver Geräte nach einer Anzahl von Tagen löschen
- Protokolle inaktiver Geräte nach einer Anzahl von Tagen löschen

Die restlichen Optionen von *famoc-config* können mit dem *essentials-mdm-config* gesetzt werden.

Weitere Informationen erhalten Sie durch Eingabe von:

essentials-mdm-config -h

2.7 Neue / aktualisierte Gerätemodelle

- Apple iPad 11
- CipherLAB RS36
- CipherLAB RS38

- Crosscall Core T5
- Elotouch EMC-M51
- IIIF150 Action A5 Pro
- Lenovo Idea Tab TB336FU
- Motorola Moto G56 5G
- Motorola Moto G86 5G
- Oppo Reno 13 5G
- Oukitel G2
- Realme 14 Pro+
- Realme Note 60
- Samsung SM-F741 Galaxy Z Flip 6
- Samsung SM-F766 Galaxy Z Flip 7
- Samsung SM-F956 Galaxy Z Fold 6
- Samsung SM-F966 Galaxy Z Fold 7
- Samsung SM-M356B Galaxy M35 5G
- Samsung SM-X356B Galaxy Tab Active 5 Pro 5G
- Samsung SM-X526B Galaxy Tab S10 FE 5G
- Unitech EA660
- Vivo Y22s

3 Fehlerbehebungen

Android

- Absturz des Basis-Agenten während BTS-Scans
- Der Geräte-Monitor führt dazu, dass das Streaming stoppt da dieser den Audio-Fokus erhält
- Deaktivierung des *Verloren Modus* – das Löschen von Nachrichten auf dem Sperrbildschirm dauert bei Android 15+ sehr lange
- Die erste App öffnet sich auf COSU-Geräten nicht korrekt, wenn der Benutzer nach einem Geräte-Neustart sich mit dem Profil anmeldet, welches ein Widget enthält
- Problem beim Anmelden im privaten Google Play Store auf einem Gerät ohne *Verwaltetes Google Play*
- Lange Verzögerung oder Timeout während der Systemberechtigungsbestätigung für *All Access Files* bei der ersten Registrierung, wenn die Option *Datei hochladen* als Richtlinienkomponente hinzugefügt wurde
- Nur WARN- und ERROR-Protokolle werden gemeldet, obwohl die Protokollierung aktiviert ist
- Die VPN-Anwendung *Strongswan* aus dem Google Play Store funktioniert nicht im Arbeitsprofil
- Die Launcher-Ansicht wird nach der Entfernung der Launcher-Einstellungen vom COBO-Gerät nicht bereinigt.
- Ein falscher Betriebsstatus wird an den Server gesendet, wenn ein Systemabsturz während des Löschvorgangs auftritt.

Weitere / Admin-Konsole

- Nach dem Hochladen einer neuen APK-Datei wird die Option *„Nur im Arbeitsprofil installieren“* unerwartet deaktiviert.
- Es ist nicht möglich, iOS-App-Daten mit einem Aktualisierungsbutton zu aktualisieren.

- Problem bei der Erstellung einer KME-Integration, wenn das beschreibende Datumsformat aktiviert ist.
- Problem beim Speichern von Benutzerzertifikaten auf der Registerkarte *Benutzer*.
- Kein Schutz vor dem Speichern einer Richtlinie mit demselben Namen aus einem anderen Modus.
- Es ist nicht möglich, Geräte Checkpoint-Gruppen zuzuweisen, während der Modus *„Einzelne Gerätegruppe“* in den Organisationseinstellungen aktiv ist.
- Leistungsprobleme auf der Registerkarte *Protokolle*.
- Manchmal tritt ein interner Fehler *„JSON_RPC“* in der Geräteliste auf.
- Es ist nicht möglich, Elemente zum Basisgruppenfilter in der EntraID-Integration hinzuzufügen.
- Einige Nachrichten gehen verloren, statt in den Protokollen aufgezeichnet zu werden.
- Der Befehl `essentials-mdm-config backup:restore` scheitert beim Wiederherstellen eines Backups.

4 Versionshistorie

MDM Version	Release ID	Wichtige Hinweise[1]
5.41.0	2026-02-15X	Aktualisierung auf PHP 8.2, Ersatz von famoc-config
5.40.0	2025-10-31	MySQL-Aktualisierung auf 8.0.43 möglich
5.39.1	2025-07-30X	
5.39.0	2025-06-30X	
5.38.1	2025-03-25-rel	
5.38.0	2025-03-12-rel	
5.37.0	2024-10-31	MySQL 8.0.36 erforderlich
5.36.0	2024-07-31	MySQL-Aktualisierung auf 8.0.36 möglich, letzte Version mit CentOS 7 Unterstützung
5.35.1	2024-06-18-rel	
5.35.0	2024-05-31X	
5.34.0	2024-02-29X	Firebase; Firewall
5.33.0	2023-11-30X	
5.32.2	2023-10-15-rel	VPP
5.32.1	2023-8-31-rel	MySQL 8
5.32.0	2023-07-31X	
5.31.0	2023-05-31X	
5.30.0	2023-01-31X	

1. Für vollständige Informationen lesen Sie bitte die gesamtem Versionshinweise