

# Versionshinweise

## datomo MDM 5.41.1

*April 2026*

Alle Rechte vorbehalten. Die Veröffentlichung kann Marken und Produktnamen enthalten, die Marken oder eingetragene Marken der jeweiligen Eigentümer sind.

SPEZIFIKATIONEN UND INFORMATIONEN ZU DEN IN DIESEM HANDBUCH EINGEFÜHRTEN PRODUKTEN UND DIENSTLEISTUNGEN KÖNNEN ÄNDERUNGEN UNTERLIEGEN. ALLE IN DIESEM DOKUMENT ENTHALTENEN INFORMATIONEN UND EMPFEHLUNGEN SIND RELEVANT, JEDOCH LIEGT DIE VERANTWORTUNG FÜR DIE IMPLEMENTIERUNG UND NUTZUNG DER PRODUKTE UND DIENSTLEISTUNGEN BEI DEN ANWENDERN.

## Übersicht

1	Neue Funktionen.....	3
1.1	Android.....	3
1.2	Apple.....	3
1.3	Mobiler Bedrohungsschutz.....	3
1.4	Verwaltungskonsole.....	4
1.5	Sicherheitsaktualisierungen.....	5
2	Fehlerbehebungen.....	6
2.1	Android.....	6
2.2	Apple.....	7
2.3	Admin-Konsole und sonstige.....	8
3	Versionshistorie.....	9

# 1 Neue Funktionen

## 1.1 Android

### Option „Bildschirm anlassen“ für dedizierte Geräte (COSU)

Neuer Schalter in der Richtlinie für dedizierte Geräte bei Allgemeinen Einstellungen im KIOSK-Modus.

Wenn aktiviert, bleibt der Bildschirm des Geräts dauerhaft eingeschaltet. Verfügbar ab Android 9+ für Samsung und Nicht-Samsung-Geräte, einschließlich Multi-Profil-Anmeldebildschirmen und Sperrbildschirmen.

## 1.2 Apple

### Account-gesteuerte Benutzerregistrierung für BYOD

Benutzer können nun persönliche iOS-Geräte in das MDM registrieren, indem sie sich mit ihrer verwalteten Apple-ID über Einstellungen > Anmeldung bei Arbeits- oder Schulkonto anmelden. Die Registrierung nutzt Apples Standard-Discovery-Mechanismus und die Authentifizierung über eine WebView, was eine sichere, benutzergesteuerte Registrierung ohne manuellen Profil-Download ermöglicht.

## 1.3 Mobiler Bedrohungsschutz

### MTD-Logfilter im Abschnitt „Operationen“

Ein neuer Filter ermöglicht es Administratoren, Mobile Threat Defense-Vorgänge im Hauptreiter „Protokolle“ und im Protokollreiter des einzelnen Geräts anzuzeigen oder auszublenden, wodurch die Protokollanzeige übersichtlicher wird.

## **Behebungsmaßnahmen im Reiter „Mobiler Bedrohungsschutz“**

Umkehrbare Behebungsmaßnahmen (Bluetooth blockieren, VPN blockieren, NFC blockierung, Arbeitsprofil deaktivieren) können nun zusätzlich zum bestehenden Protokollreiter direkt über Gerätestatus > Mobiler Bedrohungsschutz ausgelöst werden.

## **Neue vordefinierte Berichte für Mobilen Bedrohungsschutz**

Fünf neue Berichte wurden unter der Kategorie Mobiler Bedrohungsschutz hinzugefügt:

- Anzahl der Geräte mit aktivem MTD
- Geräte gruppiert nach erkannter Bedrohungskategorie
- Geräte gruppiert nach erkanntem Bedrohungstyp
- Anzahl der Geräte mit erkannten Bedrohungen
- Anzahl der Geräte ohne erkannte Bedrohungen

# **1.4 Verwaltungskonsole**

## **Benutzerdefinierte Felder in benutzerdefinierten Berichten**

Benutzerdefinierte Felder (Text, Datum, Nummer, Wörterbuch) für Geräte, Benutzer und SIM-Karten stehen nun als Datenquellen im Abfrageerstellungstool für benutzerdefinierte Berichte zur Verfügung. Benutzerdefinierte Felder vom Typ Passwort werden vom Berichtsinhalt ausgeschlossen.

## **KME-Spalten in benutzerdefinierten Berichten**

Die Felder „KME-Integrationsname“ und „Admin-E-Mail“ sind nun in benutzerdefinierten Berichten für Geräte verfügbar, die über die neue Samsung Knox Mobile Enrollment-Integrationsmethode registriert wurden.

**Geschwindigkeitsfeld in Standortberichten** Ein Geschwindigkeitsfeld wurde zu den vordefinierten Berichten „Letzter Standort des Geräts“ und „Standorte der Geräte in...“ hinzugefügt.

## **Mehrere Entra ID-Integrationen**

Organisationen können nun mehrere Entra ID (Azure AD)-Integrationen gleichzeitig konfigurieren. Benutzer eines bestimmten Entra-Tenants sind serverweit auf eine Integration beschränkt, während Gruppen organisationsweit festgeschrieben werden, um Synchronisierungskonflikte zu vermeiden.

## **Standortfilter nach Benutzer- und Gerätegruppen**

Der Reiter „Standorte“ unterstützt nun die Filterung der angezeigten Geräte nach Benutzergruppen und Gerätegruppen.

## **Getrennte Berechtigungen für Schnellaktionen in der Geräteliste und den Gerätedetails**

Geräteverwaltungsaktionen sind nun in zwei Berechtigungsarten unterteilt:

- Massenaktionen aus der Gerätelistenansicht und
- Einzelgeräteaktionen aus der Gerätedetailansicht.

Dies ermöglicht es Administratoren, Massenoperationen (z. B. Massenlöschung) einzuschränken, während die Verwaltung einzelner Geräte weiterhin zulässig bleibt.

## **1.5 Sicherheitsaktualisierungen**

Folgende Frontend-Bibliotheken wurden aktualisiert um Sicherheitslücken zu beheben, welche bei Penetrationstests identifiziert wurden:

- jQuery aktualisiert (vorher 1.12.4)
- jQuery-UI aktualisiert (vorher 1.12.1)
- lodash aktualisiert (vorher 4.6.1)

## 2 Fehlerbehebungen

### 2.1 Android

#### **Audio-Routing bleibt nach einer Remote-Access-Sitzung im Hörer-Modus hängen**

Ein Problem wurde behoben, bei dem Geräte nach Beendigung einer Remote-Access-Sitzung in einem Anruf-ähnlichen Audiostatus verblieben, was dazu führte, dass alle Töne über den Hörer ausgegeben wurden.

#### **Webview-Ladebildschirm bleibt während der Registrierung hängen**

Ein Problem wurde behoben, bei dem der Webview-Ladebildschirm des Base Agents während der SSO/COSU-Registrierung hängen bleiben konnte, was zeitweise zu doppelten Bootstrap-Aufrufen führte. Die Aktualisierung der Warteschlange wird nun während der Registrierung ordnungsgemäß verwaltet, und die Übergänge zwischen den Registrierungsschritten sind vorhersehbarer.

#### **Protokollierung schaltet sich auf Geräten unerwartet aus**

Ein Regressionsfehler wurde behoben, bei dem die Geräteprotokollierung nach der Registrierung stillschweigend deaktiviert wurde, sodass nur noch Nachrichten der Ebenen WARN und ERROR verblieben.

#### **Wallpaper-Anwendung schlägt während der ersten COBO-Richtlinien-Einrichtung fehl**

Ein Regressionsfehler wurde behoben, bei dem das Festlegen eines Hintergrundbilds als Teil der ersten Richtlinienanwendung auf COBO-Geräten aufgrund fehlender Berechtigungen fehlschlug. Nachfolgende Richtlinienaktualisierungen wendeten das Hintergrundbild korrekt an; die initiale Anwendung funktioniert nun wie erwartet.

#### **Heartbeat stoppt nach Agenten-Upgrade auf Work Profile-Geräten**

Ein Regressionsfehler wurde behoben, bei dem der MQTT-basierte Heartbeat nach der Neuinstallation des Basis Agenten auf Work Profile-Geräten nicht mehr funktionierte. Zuvor war eine manuelle Richtlinienaktualisierung erforderlich, um die Konnektivität wiederherzustellen.

### **Einstellungen App Monitor Service öffnen sich während der COSU-Registrierung nicht**

Ein Regressionsfehler wurde behoben, bei dem das Tippen auf „OK“ im Berechtigungsdialog des App Monitor Service während der COSU-Registrierung keine Wirkung zeigte, was zum Abbruch des Vorgangs führte. Das Problem stand im Zusammenhang mit dem Schalter „Im Hintergrund aktualisieren“ und betraf spezifische Geratemodelle.

### **Work Profile Laufzeitberechtigungs-Richtlinie schlägt auf Android 15+ fehl**

Ein Problem wurde behoben, bei dem das Anwenden der „Laufzeitberechtigungs-Richtlinie“ mit der Einstellung „Zulassen“ auf Work Profile-Geräten mit Android 15+ zu fehlerhaften Einstellungen in der Benutzeroberfläche führte. Der Base Agent verarbeitet nun SecurityExceptions für eingeschränkte Berechtigungen in verwalteten Profilen korrekt.

### **Bluetooth-Einschränkungen bleiben nach Entfernung der Richtlinie bestehen**

Ein Problem wurde behoben, bei dem Bluetooth auf Geräten auch nach dem Entfernen aller Bluetooth-Einschränkungen aus der Richtlinie blockiert blieb. Der Agent entfernt Einschränkungen nun unter Verwendung aller relevanten APIs, um sicherzustellen, dass zuvor durch nicht genutzte APIs auferlegte Sperren ordnungsgemäß aufgehoben werden.

### **Funktionsumfang Remote Access auf Samsung WPC/BYOD**

Ein Problem wurde behoben, bei dem die Premium-Steuerungsfunktionen der Samsung Remote Access (Mausklicks, Tastatureingabe) auf Work Profile-Geräten mit Android 15+ nicht mehr funktionierten. Die Konfiguration der Samsung Remote Access-Berechtigung wird nun während der App-Installation im WPC-Modus korrekt aufgerufen.

## **2.2 Apple**

### **IMEI wird für iOS 26.0+ Geräte nicht gemeldet**

Ein Problem wurde behoben, bei dem iOS 26.0+ Geräte ihre IMEI-Nummer nicht meldeten. Apple hat das Format der IMEI-Meldung von einem Einzelwert zu einem Array innerhalb von ServiceSubscriptions geändert; der Server analysiert die aktualisierte Struktur nun korrekt.

### **Ausstehende Vorgänge blockieren die Synchronisierung auf Apple-Geräten**

Ein Problem wurde behoben, bei dem fehlerhafte Vorgänge unendlich lange im Status „ausstehend“ verbleiben konnten, was die Gerätesynchronisierung blockierte. Ungültige Vorgangs-Strings werden nun ordnungsgemäß behandelt und als nicht unterstützt markiert, anstatt die Warteschlange zu blockieren.

## **2.3 Admin-Konsole und sonstige**

### **Administrator-Erstellung schlägt über den Organisations-Erstellungsassistenten fehl**

Ein Fehler wurde behoben, bei dem die gleichzeitige Erstellung eines Administrator-Kontos mit einer neuen Organisation mit einer Fehlermeldung fehlschlug, wodurch die Organisation ohne Administrator zurückblieb. Die Organisation wurde erfolgreich erstellt, aber der Administrator-Benutzer musste als Workaround manuell hinzugefügt werden.

### **Apache QoS CLI-Befehl erlaubt leere IP-Adressliste**

Ein Problem wurde behoben, bei dem das Aktivieren von Apache QoS ohne Angabe von IP-Adressen zu einer ungültigen Konfiguration führte, die den Start von httpd verhinderte. Die CLI schließt nun bedingungslos 127.0.0.1 in die Ausschlussliste ein und verhindert, dass diese entfernt oder überschrieben wird.

## 3 Versionshistorie

MDM Version	Release ID	Wichtige Hinweise <sup>1</sup>
5.41.1	2026-03-31X	
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