datomo®
MOBILE
DEVICE MANAGEMENT

Versionshinweise

datomo MDM 5.42

Juli 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

1.1 Android

App-Pinning für dedizierte Geräte (COSU)

Neue Option in der dedizierten Geräte-Richtlinie unter COSU-Einstellungen. Bei Aktivierung können Administratoren Benutzern erlauben, Launcher-Apps zu pinnen und das Gerät gesperrt zu halten, bis die App aus der Benachrichtigungsleiste entfernt wird.

Desktop-unterstützte COBO- und COSU-Registrierung

Das neue Desktop-Registrierungstool ermöglicht die Bereitstellung von Android-Geräten in COBO- und COSU-Modi direkt von einem Computer aus. Es erstellt die erforderliche Registrierungs-Konfiguration und führt den Administrator durch einen ADB-basierten Einrichtungsablauf.

Diese Methode ist ideal, wenn eine herkömmliche Massenregistrierung nicht verfügbar ist oder Geräte in einem geschlossenen Netzwerk mit eingeschränktem oder keinem Internetzugang betrieben werden. Bei Interesse an diesem Tool kontaktieren Sie bitte den Support unter mdm@dotoso.de.

Benutzerdefinierte Zuordnung von Hardware-Tasten

Der Basis-Agent kann Hardware-Tasten-Ereignisse über den Barrierefreien-Dienst erfassen und erkannte Tasten-Codes protokollieren. Das erleichtert Administratoren das Zuordnen eigener Tasten, z. B. PTT-Tasten, auf unterstützten Android-Geräten.

Neue Option zur „Intent senden"-Konfiguration – *Bei Tastendruck ausführen*

Administratoron können den Tasten-Code festlegen (abhängig vom Hersteller, z. B. bei Crosscall-Geräten – 416, 417, 423, 424 oder bei Zebra-Geräten – 104, 105).

Legacy-API-Option für Work-Profile-Pin-Code

Neue Option „Legacy-API verwenden" in der Android-Work-Profile-Pin-Code Konfiguration.

Administratoren können die Legacy-Pin-Code-Verarbeitung für Android 12+ Work-Profile-Geräte auswählen, wenn das Geräteverhalten dies erfordert.

Standard-Nachrichten-App-Konfiguration
Neue Android-Richtlinien-Option, mit welcher Administratoren die Standard-Nachrichten-App per Paketname festlegen können. Die Angabe eines leeren Paketnamens setzt die Standard-App-Blockierung zurück.

Die Option ist in vollständig verwalteten (COBO) und COSU-Richtlinien im Reiter „Allgemeine Einstellungen“ verfügbar.

WPC-Richtlinie – aktivierte Anwendungen nach Paketname
Administratoren können nun benutzerdefinierte Paketnamen zur Liste der aktivierten Anwendungen für WPC-Richtlinien hinzufügen.

Benutzerdefinierte DNS-Konfiguration
Neue Android-Einstellung, mit welcher Administratoren den privaten DNS-Modus für COBO- und COSU-Geräte ab Android 10 setzen können. Unterstützt wird der automatische Modus (empfohlen) sowie ein privater DNS-Provider-Hostname (in diesem Modus kann nur ein Hostname, keine IP-Adresse, angegeben werden).

Mobile-Daten-Registrierungsoption
Android-QR-Registrierung unterstützt jetzt eine Mobile-Daten-Option. Administratoren können Registrierungs-QR-Codes erzeugen, die Geräte über mobile Daten statt WLAN provisionieren.

Automatische Bereinigung des Usage-Monitors
Der Usage-Monitor entfernt nun automatisch alte lokale Daten, nachdem sie an den Server gesendet wurden. Der voreingestellte Schwellenwert beträgt 5 Tage.

Unterstützung für 16 KB-Speicherseiten bei Android 16
Der Basis-Agent unterstützt nun Android-Geräte, die 16 KB-Speicherseiten verwenden. Zentrale Funktionen des Agenten wurden angepasst, um mit den neueren Anforderungen von Android-Geräten kompatibel zu bleiben.

1.2 Apple

Apple 26.6-Plattform-Support

Unterstützung für iOS, iPadOS, macOS und tvOS 26.6 hinzugefügt.

Apple 27-Plattform-Support

Unterstützung für iOS, iPadOS, macOS und tvOS 27 hinzugefügt.

Apple-Firmware-Update Kampagne

Neuer Kampagnentyp „Apple Firmware Update“ für iOS-, iPadOS- und macOS-Geräte. Die Kampagne nutzt die verfügbaren Betriebssystem-Versionen der Geräte und unterstützt die Planung von Updates über den Apple-Software-Update-Prozess.

iOS Unternehmens-Portal im Agent

Der iOS-Agent enthält nun Unternehmens-Portal-Funktionen, um zugewiesene Ressourcen und Geräteinformationen direkt im Agent anzuzeigen. Damit wird die Grundlage für verwaltete Apps, Richtlinien-Vorschau und konfigurierbare Agent-Ansichten geschaffen, darunter:

- Ansicht „Verwaltete Apps“ im iOS-Agent
  Die neue Ansicht „Verwaltete Apps“ zeigt Anwendungen an, die per Richtlinie bereitgestellt wurden. Die Liste enthält App-Symbol, Name, Bundle-Identifier, Version, Aktualisierungsaktion, Suchfunktion und, wo unterstützt, eine „Öffnen“-Aktion.

- Richtlinien-Vorschau im iOS-Agent
  Eine neue schreibgeschützte Richtlinien-Vorschau zeigt die angewandten Richtlinieneinstellungen innerhalb des iOS-Agents an. Einstellungen werden in Abschnitte gruppiert und mit übersetzten Beschriftungen, Werten und Sichtbarkeits-Status dargestellt.

1.3 Mobiler Bedrohungsschutz

Android-kategorisiertes URL-Monitoring

Neue Mobile-Threat-Defense-Richtlinien-Option, welche Android-Geräte veranlasst, geöffnete Links über den Basis-Agenten für kategorisierte URL-Prüfungen zu leiten. Wird eine schadhafte

URL erkannt, wird der Link blockiert und eine Server-Benachrichtigung erzeugt.
Hinweis: Damit diese Funktion vollständig funktioniert, muss der Basis Agent als Standard-Browser festgelegt sein. Wenn der Nutzer dies nicht tut, bleibt eine permanente Benachrichtigung bestehen, um die Einstellung später abzuschließen.

Installations- und Upgrade-App-Scanning
Mobile Threat Defense kann nun Anwendungen unmittelbar nach der Installation oder dem Upgrade scannen. Der Scan wird für Apps aus dem Google Play-Store, APK-Dateien und unterstützten Anbieter-Stores ausgelöst.

1.3.1 Neue Behebungen

Verwalte-Apps ausblenden
Versteckt alle verwalteten Anwendungen, sobald eine konfigurierte Bedrohung erkannt wird. Gilt für über das MDM installierte Apps und ist für bedrohungsbasierte Behebungs-Regeln verfügbar.

Anwendungs-Ausblendung
Versteckt die Anwendung, die mit einer erkannten Bedrohung verknüpft ist. Verfügbar für globale und pro-Anwendung-Mobile-Threat-Defense-Regeln.

Verlorenen-Modus
Aktiviert den Verlorenen-Modus, wenn eine Bedrohung erkannt wird. Unterstützt auf relevanten Android-Ownership-Modi (COSU, vollständig verwaltet) sowie Apple-Geräten.

Behebung-Rückgangig-Aktion aus der Bedrohungsliste
Rückgängig-Aktionen für unterstützte Behebungen können nun aus der Bedrohungsliste ausgelöst werden, sodass das Umkehren von Behebungen dem jeweiligen Bedrohungs-Aktionsset entspricht.

Behebungen nach Wartungs-Modus
Mobile-Threat-Defense-Scans und Behebungen werden nun mit dem Wartungs-Modus koordiniert; Behebungen werden nach Beendigung des Wartungs-Modus wiederhergestellt.

Erneutes Senden von Bedrohungs- und Remediation-Ereignissen
Bedrohungs- und Remediation-Ereignisse werden an den Server gemeldet, sobald das Gerät wieder eine Internetverbindung herstellt.

MTD-Bedrohungsfilter in Gerätedetails
Gerätedetails unterstützen jetzt das Filtern von Mobile-Threat-Defense-Bedrohungen nach auf dem Gerät verfügbaren Werten. Die Liste enthält aktive, beendete und abgebrochene Bedrohungs-Datensätze des Geräts.

Optimierung der Aktualisierung der Bedrohungslisten
Die Bedrohungsliste in den Gerätedetails wird nun aktualisiert, wenn das Gerät eine neue Bedrohung oder einen geänderten Bedrohungs-Status meldet, anstatt konstant zu pollen – dies reduziert den Datenverkehr.

Pradeo-Anwendungsberichte
datomo MDM kann Pradeo-Anwendungsberichte für hochgeladene Apps anfordern und synchronisieren. Berichte werden periodisch aktualisiert, sobald ein neuer Bericht für dieselbe App-Version und denselben Paketnamen verfügbar ist.

Pradeo-Konfigurations-Historie
Änderungen an der Pradeo-Mobile-Threat-Defense-Konfiguration werden nun in der Richtlinien-Historie protokolliert; alle Anpassungen werden bei Aktualisierungen gespeichert.

Berichte zum kategorisierten URL-Monitoring
Neuer vordefinierter Bericht für Geräte, bei denen blockierte Websites auf Android-Geräten festgestellt wurden. Der MTD-Status-Bericht wurde ebenfalls angepasst, um Bedrohungskategorien konsistenter darzustellen.

Verbesserungen im MTD-Richtlinientext
Beschreibungen für das Intervall des kategorisierten URL-Monitorings und die

Batterie-Optimierung wurden überarbeitet. Die Richtlinie erklärt nun klarer das MTD-Reporting und die Anforderungen an den Standard-Browser.

1.4 Verwaltungskonsole

1.4.1 Organisations-Einstellungen

Die Organisations-Einstellungen wurden neu gestaltet. Die Ansicht ist jetzt in die Abschnitte

- Allgemeine Einstellungen,
- Sicherheit und Authentifizierung,
- Android,
- Apple,
- Mobile Threat Defense und
- Benachrichtigungen

unterteilt. Alle Organisations-Details (inkl. benutzerdefinierter Felder) können nun im Reiter Allgemeine Einstellungen festgelegt werden.

1.4.2 Geräte-Compliance-Regeln

Neue Compliance-Regeln ermöglichen Administratoren, Auslöser und Aktionen basierend auf überwachten Geräte-Status-Änderungen zu definieren. Der Compliance-Status und die Regelereignisse werden protokolliert, sodass nachverfolgt werden kann, wann Regeln ausgelöst und gelöst wurden.
Regeln können direkt in der Verwaltungsoberfläche über das Hauptmenü (neue Option zwischen Richtlinien und Kampagnen) erstellt werden.

Unterstützte Auslöser:

- Richtlinien-Status
- MTD-Status
- OS-Version
- Sicherheits-Patch-Datum

Unterstützte automatische Aktionen bei Nicht-Compliance:

- Als nicht-konform markieren
- Server-Alarm auslösen
- Push-Benachrichtigung an das Gerät senden
- Betriebssystem-Upgrade (neueste verfügbare Version)
- Work-Profile blockieren
- Verwaltete Apps ausblenden

Mehrere zeitbasierte Aktionen können definiert werden, die ausgeführt werden, sobald eine Nicht-Compliance-Regel ausgelöst wird.

1.4.3 Verbesserungen der Massenregistrierungen

Massenregistrierung (bulk)

Die Bulk-Registrierung wurde in der Konsole neu gestaltet. Die neue Ansicht behält den bestehenden Registrierungsablauf bei, richtet aber das UI an das aktuelle Konsolen-Design aus.

Zero-Touch-Registrierung (Android)

Die Android-Zero-Touch-Registrierung wurde in der Konsole neu gestaltet. Die Ansicht unterstützt Integrationseinstellungen, Geräteauswahl, Registrierungs-Modus, Autorisierungsmethode, automatischen Import und Zusammenfassungs-Handling.

DEP-Registrierung (Apple)

Die Apple-DEP-Registrierung wurde in der Konsole neu gestaltet. Die Ansicht bietet Token-Verwaltung, Gerätesynchronisation, erforderliche Kontoeinrichtungs-Felder und das alte Basic-Autoriserungs-Verhalten für vorhandene Konfigurationen.

1.4.4 Verbesserung der Berichterstellung

Berichts-Zeitpläne in den Bericht-Details

In den Bericht-Details gibt es nun einen Reiter Ausführungs-Zeitpläne. Administratoren können Zeitpläne hinzufügen, bearbeiten, löschen, aktivieren und deaktivieren.

Bericht-Ausführung-Historie

Ein neuer Reiter Ausführungs-Historie zeigt im Detail an, welche Berichte generiert wurden, ob sie aus einem Zeitplan stammen, wer sie erstellt hat, wann sie erstellt wurden und wohin geplante Berichte gesendet wurden.

Spalte „Aktive Zeitpläne“ in der Berichtsliste

Die Berichtsliste enthält jetzt die Spalte Aktive Zeitpläne, die angibt, wie viele aktive Zeitpläne für jeden Bericht konfiguriert sind und das Sortieren nach dieser Information ermöglicht.

Bestätigung für „Jetzt generieren“ bei geplanten Berichten

Die Aktion Jetzt generieren öffnet nun ein Bestätigungsdialog, wenn der Zeitplan Empfänger hat. Administratoren können wählen, ob nur der Bericht generiert oder gleichzeitig an die konfigurierten Empfänger gesendet wird.

Generierungs-Datum in den Berichtsergebnissen

Ergebnis-Ansichten zeigen nun das vollständige Datum und Uhrzeit des erzeugten Berichts. Diese Änderung gilt für vordefinierte und benutzerdefinierte Berichte.

Leere Berichtsspalten anzeigen

Tabellen und Exporte von Berichtsergebnissen behalten nun Spalten bei, auch wenn sie keine Daten enthalten.

Automatische Berichtserstellung aus dem Monitoring-Tab

Durch Klicken auf Details anzeigen im Monitoring-Tab wird der zugehörige Bericht geöffnet und automatisch generiert, wodurch manuelle Schritte bei der Untersuchung von Monitoring-Ergebnissen entfallen.

Löschen benutzerdefinierter Berichte

Benutzerdefinierte Berichte können jetzt aus der Berichtsliste und den Bericht-Details gelöscht werden. Gelöschte Berichte verschwinden aus allen verfügbaren Ansichten und zugehörige Zeitpläne erzeugen keine Ergebnisse mehr.

Berechtigungen für den Bericht-Tab

Die Rechte im Berechtigung-Baum wurden erweitert. Administratoren können nun separat das Ansehen, Exportieren, Erstellen, Löschen, Detail-Zugriff, Zeitplan-Verwaltung und Zeitplan-Ausführung von Berichten steuern.

Report-Web-Service-Warteschlangen-Migration

Web-Service-Anfragen für Berichte (executeReport, executeReportWithParameters, getReportData) nutzen jetzt die neue Bericht-Warteschlange. Die Ergebnisse entsprechen exakt denen, welche über die Konsole generiert werden.

1.4.5 Weitere Verbesserungen

Intelligente Gruppen bei App- und Konfigurations-Verfügbarkeit

Beim Erstellen oder Bearbeiten von Anwendungen und Konfigurationen können nun intelligente Geräte-Gruppen ausgewählt werden. Die Gruppen stehen im Schritt für die Verfügbarkeit im Corporate Store zur Verfügung.

Mobile-Agent-Ansichtskonfiguration

Neuer Richtlinien-Abschnitt Agenten-Einstellungen (Registerkarte in den Richtliniendetails) erlaubt Administratoren zu bestimmen, welche Ansichten in Android- und iOS-Agenten sichtbar sind. Konfigurierbare Bereiche umfassen: Informationen, Richtlinien, verwaltete Apps, Corporate Store, Operationen, Benachrichtigungen, Remote-Support, IT-Kontrolle und Über-App-Ansichten.

Richtlinien-Statusdaten im Richtlinien-Tab

Der Status von Richtlinien ist jetzt im Konsolen-Richtlinien-Bereich sichtbar. Administratoren können Status-Zähler einsehen und gefilterte Geräteleisten aus den Statusdaten öffnen.

UI-Log-Filterung

Log-Listen in der neuen Konsole unterstützen Filter für Status, Erstellt von, bestimmter Benutzer, Aktion und Operations-Datum. Massen-Abbrechen- und Wiederhol-Aktionen sind sowohl in den globalen Log-Tabs als auch in den Geräte-Log-Tabs verfügbar.

Verbesserungen beim Karten-Filter in der Standort-Ansicht

Der Reiter Standorte unterstützt jetzt erweiterte Karten-Filter für zuletzt gemeldete Standorte. Administratoren können festlegen, wie viele Geräte auf der Karte angezeigt werden, und Standort-Filter mit Benutzer-, Benutzer-Gruppen-, Geräte-Gruppen- und Datums-Filtern kombinieren.

Anzeigeoptionen für Standort-Pfade

Geräte-Standort-Ansichten erlauben nun höhere Grenzwerte für die Anzahl der angezeigten Standorte pro Gerät. Administratoren können umfassendere Pfade für einen ausgewählten Zeitraum darstellen.

Filter für Geräte-Zertifikatslisten

Die Zertifikatslisten (Gerätedetails > Allgemein > Zertifikate) unterstützen jetzt Filter für Status, Typ und fehlendes Datum.

Aktualisierte EULA

Der Standard-EULA-Text wurde für datomo MDM und MTD aktualisiert. Der neue Text wird Nutzern in unterstützten Sprachen angezeigt.

SAML-Datumsformat-Kompatibilität

Das Datumsformat von SAML-Nachrichten wurde für bessere Kompatibilität mit Identity-Providern angepasst.

Erweiterte UI-Deprecations

- Fortgeschrittenen UI > Fortgeschritten > Berichte-Tab leitet jetzt zur neuen Oberfläche > Berichte-Tab weiter.
- Fortgeschrittenen UI > Organisation-Reiter Benutzer, Organisations-Details, Benutzer-Details und Gruppen wurden entfernt; sämtliche Funktionen dieser Tabs stehen nun in der neuen Oberfläche zur Verfügung

1.5 Sicherheitsverbesserungen

Härtung

Zusätzliche Härtungsarbeiten wurden für Befunde aus der Sicherheitsüberprüfung implementiert. Der Schwerpunkt liegt auf der Bereinigung veralteter Bibliotheken (Legacy-Dateien) und auf Bereichen, in denen Server-Konfigurationen potenziell exponiert sein könnten.

MySQL 8.4.9-Unterstützung

datomo MDM unterstützt nun die Aktualisierung des Datenbankservers auf MySQL 8.4.9. Das

Datenbank-Upgrade kann über den dafür vorgesehenen Datenbank-Update-Befehl durchgeführt werden.

1.6 Weitere Verbesserungen

datomo MDM REST-API V1

Neue, kundenorientierte REST-API, die über den bestehenden datomo MDM-SOAP-Web-Services eingesetzt wird. Die API ist versionierbar und wird über OpenAPI-basierte Dokumentation bereitgestellt. Details unter unter https://fqdn/docs/rest-api/v1/ – nur für autorisierte Benutzer zugänglich.

Selbstgehostete MDM-Push-Infrastruktur

datomo MDM enthält nun die grundlegende Infrastruktur für selbstgehostete Push-Auslieferung, ohne ausschließlich auf die Google-Push-Dienste angewiesen zu sein. Die Implementierung ist für große Geräteparks und Online-Auslieferungsszenarien ausgelegt.

2 Fehlerbehebungen

2.1 Android

Samsung-Premium-API-Lizenzhandling

Ein Problem wurde behoben, bei dem eine deaktivierte Samsung-Premium-API-Lizenz dennoch auf Geräte übertragen werden konnte.

Wartungs-Modus-Geste in Multi-Profil-COSU

Die Aktivierung der Wartungs-Modus-Geste funktionierte in Multi-Profil-COSU-Richtlinien nicht korrekt. Die Geste wird jetzt für jedes Launcher-Profil separat aktiviert, sofern sie in den Profileinstellungen eingeschaltet ist.

Samsung Remote Access-Verbindung nach Sitzungsabsturz

Ein Problem wurde behoben, bei dem Samsung Remote Access nach einem vorherigen Sitzungsabsturz keine Verbindung mehr herstellen konnte. Die Konsole erkennt nun den Zustand der Samsung-Screen-Recording-Bibliothek und bietet eine Neustart-Aktion, wenn eine Geräte-Wiederherstellung erforderlich ist.

LiveKit-Warnlog-Spam während Android Remote Access

Exzessive LiveKit-Warnungen wurden während Android-Remote-Access-Sitzungen generiert. Das Logging wurde gestrafft, sodass die Protokolle jetzt leichter zu analysieren sind.

2.2 Apple

iOS Remote Access – Bildschirmübertragung

Ein Problem wurde behoben, bei dem iOS-Geräte während Remote-Access-Sitzungen keine Bildschirmübertragung starteten.

VPP-Lizenz-Synchronisation

Ein Problem wurde behoben, bei dem die VPP-Lizenz-Zähler in datomo MDM von denen im

Apple Business-Portal abwichen. Die Synchronisation importiert jetzt Anwendungen und Lizenz-Zähler korrekt.

2.3 Admin-Konsole

Administrator-Erstellung mit E-Mail-Login

Ein Problem wurde behoben, bei dem das Anlegen eines neuen Administrators fehlschlug, wenn der E-Mail-Login aktiviert war. Semi-Konten können nun korrekt mit E-Mail-Login gespeichert werden.

Zero-Touch-Autorisierungs-Handling

Ein Autorisierungs-Problem in der Android-Zero-Touch-Integration, bei dem Token-Refresh-Fehler die Gerätesynchronisation blockierten, wurde behoben. Der Token-Refresh wird nun dauerhaft gespeichert und erfordert keine manuelle Bereinigung nach ungültigen Autorisierungsantworten.

KME-Integrations-Stabilität

Probleme mit der Samsung Knox Mobile Enrollment-Integration, insbesondere beim Verknüpfen und Token-Refresh, wurden behoben. Neue KME-Integrationen können jetzt erstellt und nach der Synchronisation funktionsfähig bleiben.

Falsche Berechtigungs-Prüfungen

Fehlerhafte Berechtigungs-Checks für Konsolen-Menüs und Geräte-Management-Bereiche wurden korrigiert. Berichte, Standorte, Protokolle, Gruppen und Benachrichtigungen respektieren nun die zugewiesenen Administrator-Privilegien.

2FA-Optionen bei Semi-Admins

2FA-Optionen wurden aus den Profilseiten von Semi-Admins entfernt; diese Benutzer sehen nun keine Kontroll-Elemente, die ihrer Rolle nicht zur Verfügung stehen.

Karten-Zurücksetzen beim Refresh

Beim automatischen Refresh des Standorte-Tabs wurde die aktuelle Karten-Ansicht und die Filter

nicht mehr zurückgesetzt. Position und ausgewählte Filter bleiben beim Aktualisieren der Standort-Daten erhalten.

Unvollständige Geräteliste im Standorte-Screen
Ein Problem, das dazu führte, dass die Haupt-Standorte-Übersicht nur eine unvollständige Geräteliste zeigte, wurde behoben. Die Karte und die Liste zeigen nun die erwarteten Geräte beim Laden und beim Wechseln zwischen Ergebnis-Seiten.

Fehlende Daten im Tab „Allgemeine Standorte“
Fehlende Standort-Daten im Tab „Allgemeine Standorte“ wurden behoben;
Geräte-Standort-Einträge werden nun konsistent geladen.

Log-Export während Live-Updates
Der Export von Protokollen war während eines laufenden Tab-Refresh nicht möglich. Administratoren können nun das aktuell angezeigte Log-Datum auch während Live-Updates exportieren.

Bericht „Installierte Anwendungen“ – Anzeige
Die Aktion „Geräte anzeigen“ im Bericht „Installierte Anwendungen auf Geräten einer bestimmten Benutzergruppe“ wurde korrigiert.

Navigations-Problem im Bericht „Applikations-Nutzung“
Verschachtelte Navigation im Bericht „Anwendungen in Gebrauch für die bestimmte Benutzergruppe“ wurde behoben; Unter-Berichte behalten die Filterung nach Benutzergruppe und kehren zum richtigen übergeordneten Bericht zurück.

Entra ID-Benutzer fälschlich als zu löschen markiert
Benutzer, die von Entra ID synchronisiert wurden, wurden nach einer erfolgreichen Synchronisation fälschlich nicht mehr als zu löschen markiert. Die Bereinigungs-Logik respektiert nun die aktiven Integration-Ergebnisse.

2.4 Sicherheits-Fehlerbehebungen

XSS-Schwachstelle im Autorisierungs-Endpunkt

Eine Cross-Site-Scripting-Lücke, die unauthentifizierten JavaScript-Code über einen Server-Autoriserungs-Endpunkt ausführen ließ, wurde geschlossen. Der Endpunkt prüft jetzt Eingaben korrekt und führt keinen JavaScript-Code mehr aus.

Aktualisierung der Lodash-Bibliothek

Die Lodash-Bibliothek wurde aufgrund bekannter Schwachstellen auf eine sichere Version aktualisiert.

2.5 Weitere Fehlerbehebungen

Enroll-Credential-Fenster mit erlaubten IPs

Ein Problem, bei dem die Konfiguration erlaubter IP-Adressen das Anmeldefenster während der Registrierung blockierte, wurde behoben. Registrierungs-WebViews können nun die erforderliche Anmeldeseite öffnen, während der reguläre Browser-Zugriff weiterhin durch die Erlaubnis-Liste eingeschränkt bleibt.

EAS-CLI-Konfigurations-Reload

Ein Problem, bei dem EAS CLI-Befehle nicht alle Änderungen an Konfigurationsdateien speicherten, wurde behoben. Die Operationen add, edit, mode und remove lösen nun nach dem Absenden der Änderungen einen Konfigurations-Reload aus.

2.6 Neue / Aktualisierte Gerätemodelle

- Apple iPhone 17e
- Apple MacBook Neo
- Crosscall Core-M6

- Crosscall Core-X5
- Crosscall Core-Z5
- Cyrus CM450XA
- Datalogic Memor 17
- Datalogic Memor 35
- Hytera PNC660
- Lenovo Idea Tab K11
- Motorola Signature
- Realme Note 70
- Samsung SM-A175F Galaxy A17
- Samsung SM-S942B Galaxy S26
- Samsung SM-S947B Galaxy S26+
- Samsung SM-S948B Galaxy S26 Ultra
- Samsung SM-X135F Galaxy Tab A11 (LTE)
- Urovo DT610
- Xiaomi Redmi Note 15 5G
- Zebra FR55

3 Versionshistorie

MDM Version	Release ID	Wichtige Hinweise[1]
5.42.0	2026-07-15X	MySQL-Aktualisierung auf 8.4.9 möglich
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