datomo®
MOBILE
DEVICE MANAGEMENT

Linux-Geräteeinschreibung

Version 03.03.2026 – Aktualisiert 06.03.2026

Übersicht

1 Überblick

datomo MDM für Linux ist eine Verwaltungslösung, die es Administratoren ermöglicht, Linux-Computer und -Server über dieselbe zentrale Konsole zu überwachen und zu steuern, die auch für Android- und iOS-Geräte verwendet wird.

Das System funktioniert über einen leichtgewichtigen Agenten, der als Systemdienst installiert wird und im Hintergrund läuft. Dieser Agent kommuniziert mit dem MDM-Server, indem er regelmäßig nach neuen Aufgaben, Sicherheitsrichtlinien oder Anwendungsaktualisierungen sucht. Da der Agent mit Administratorrechten betrieben wird, kann er Verwaltungsbefehle ausführen, Einschränkungen anwenden und Telemetriedaten für alle Benutzerkonten des gesamten Systems erfassen.

Hinweis:

Der Agent legt einen dedizierten Systembenutzer essentials-mdm mit vollständigen Administratorrechten an. Dies ermöglicht dem Agenten, Verwaltungsaufgaben für alle Benutzerkonten auf dem System auszuführen.

Dieses Dokument konzentriert sich ausschließlich auf Linux-spezifische Funktionen und deren Betrieb. Es beschreibt nicht den vollständigen Schritt-für-Schritt-Prozess zum Hinzufügen neuer Anwendungen oder Konfigurationen. Ausführliche Anleitungen zu diesen Prozessen finden Sie in unseren anderen Dokumentationen.

2 Voraussetzungen

Verwaltete Geräte müssen bestimmte Anforderungen an Distribution und Hardware erfüllen, um die vollständige Kompatibilität mit dem MDM-Agenten sicherzustellen.

2.1 Unterstützte Distributionen und Architekturen

Die folgende Tabelle gibt Auskunft über die unterstützten Umgebungen auf Basis der Entwicklerspezifikationen, des Legacy-Status und der verifizierten Ergebnisse aus aktuellen Prüfungen.

Distribution	Version	Paketformat	Architekturen
Ubuntu	20.04 LTS (Focal) bis 25	.deb	x86_64, arm64, armhf*
Debian	11 (Bullseye) bis 13	.deb	x86_64, arm64, armhf*
Fedora	38 und neuer	.rpm	x86_64, aarch64
Enterprise Linux	RHEL 8 / CentOS 9 / RHEL 10	.rpm	x86_64, aarch64*

Für die Ubuntu-Familie beginnt die Unterstützung ab Version 20.04 LTS, der ältesten noch aktiven LTS-Version, und erstreckt sich bis zu den neuesten verifizierten Versionen wie 24.04 LTS und 25.

Ebenso wird die Debian-Familie ab Version 11 unterstützt, mit erfolgreich verifizierten Tests auf der neueren Version 13.

Red Hat-basierte Systeme einschließlich RHEL 8 und CentOS Stream 9 werden offiziell unterstützt, und Tests mit RHEL 10 bestätigen ebenfalls die korrekte Funktion auf diesen Systemen.

Die Fedora-Kompatibilität wird ab Version 38 aufrechterhalten, da ältere Versionen das Ende ihres Lebenszyklus erreicht haben. Die erfolgreiche Testung wurde insbesondere für Fedora 43 bestätigt.

Der Agent unterstützt 64-Bit-Intel/AMD-Systeme, wobei die Begriffe x86_64 und amd64 dieselbe Architektur bezeichnen.

2.2 Netzwerkanforderungen

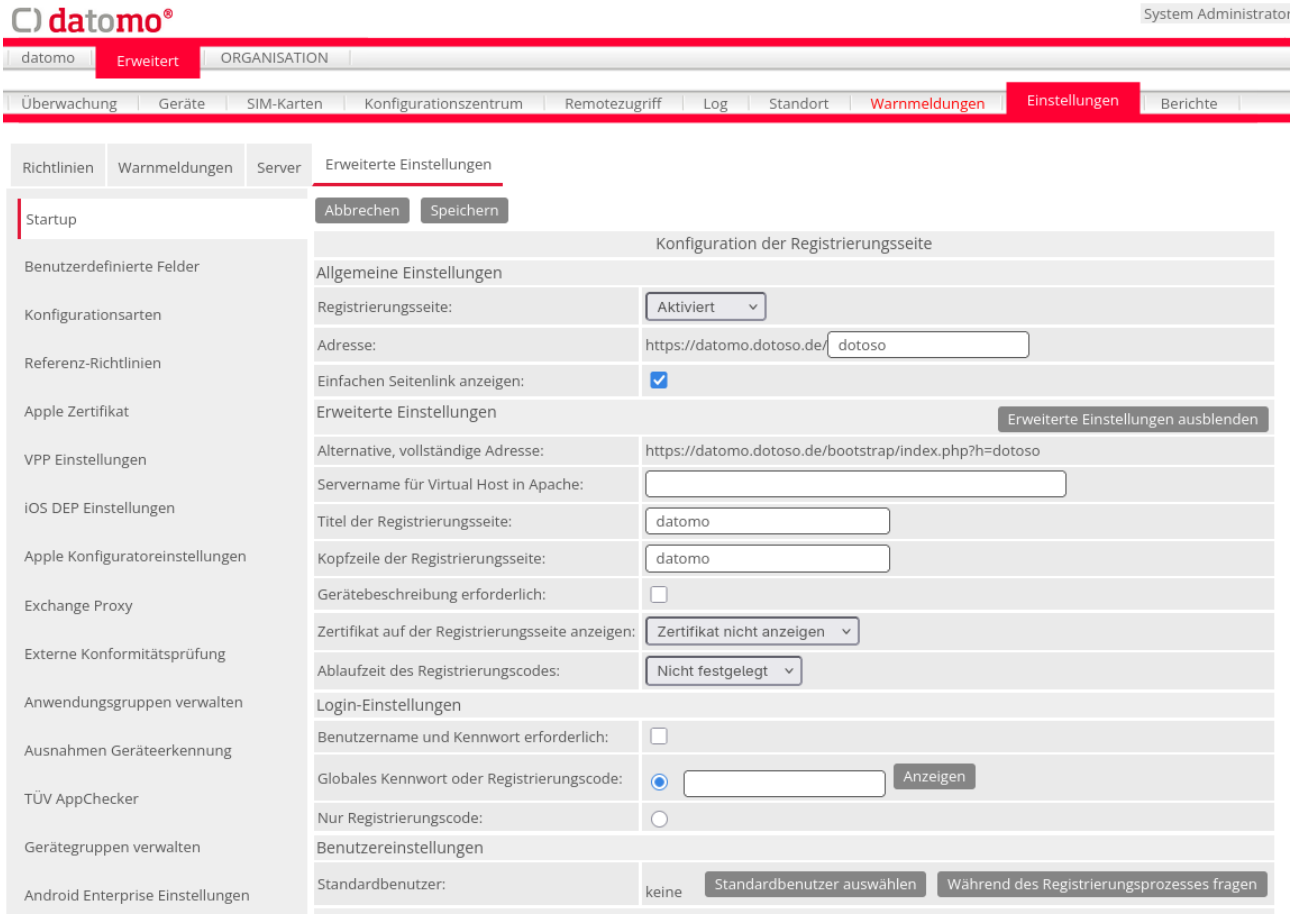
Zu den Netzwerkanforderungen gehört ausgehender Zugriff auf die LiveKit Cloud, um die Funktion des Remote-Terminals zu ermöglichen. Sollten Ihre Geräte Einschränkungen bei ausgehenden Verbindungen haben, Fragen Sie bitte bei unserem Support das entsprechende Dokument zur Konfiguration an.

3 Registrierungsprozess

Das Hinzufügen eines einzelnen Linux-Geräts zum MDM-System erfolgt über eine Registrierungs-Bootstrap-Seite, die in den Organisationseinstellungen konfiguriert wird.

Administratoren können diesen Bootstrap-Link aktivieren, indem sie zur Erweiterten Benutzeroberfläche navigieren, dann zu Einstellungen, gefolgt von Erweiterte Einstellungen und Start, und die Option „Erweiterte Einstellungen“ auswählen.

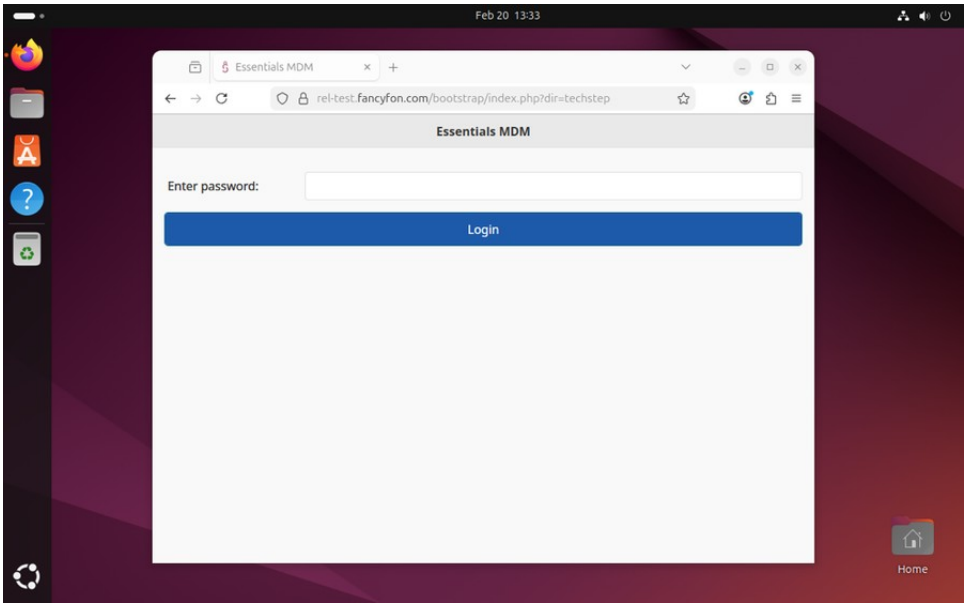
Selektieren Sie „Einfachen Seitenlink anzeigen“



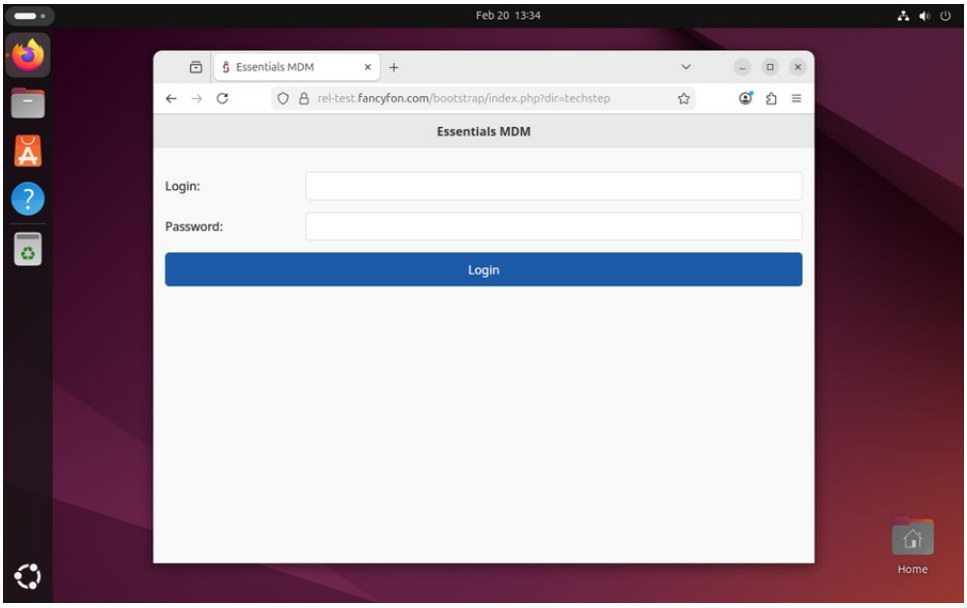
Es ist möglich, einen dedizierten Link zur Bootstrap-Seite zu konfigurieren, den Autorisierungsmodus festzulegen, den Ablaufzeitraum einzustellen, den Seitentitel anzugeben und andere auf dem obigen Bildschirm verfügbare Optionen anzupassen.

Beim Öffnen der Bootstrap-Seite ist eine Autorisierung gemäß der zuvor festgelegten Konfiguration erforderlich. Das Erscheinungsbild auf der Geräteseite variiert je nach den ausgewählten Autorisierungseinstellungen:

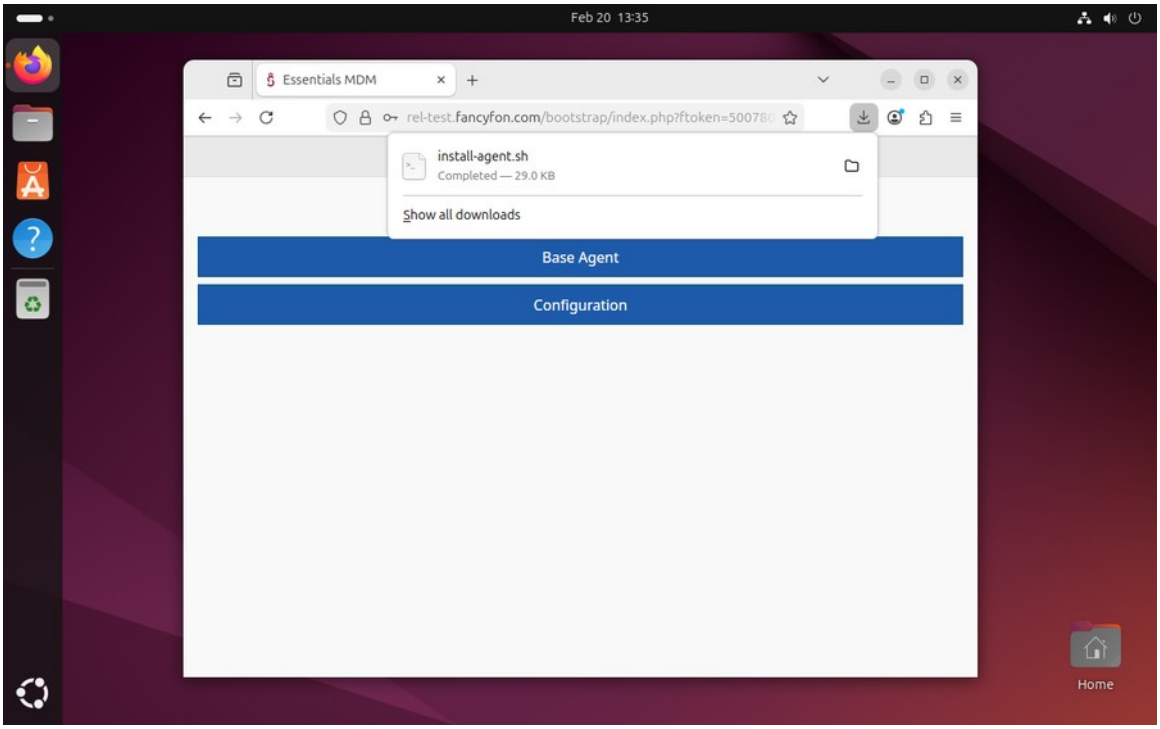
- Globales Passwort oder Bootstrap-Code



- Benutzerautorisierung



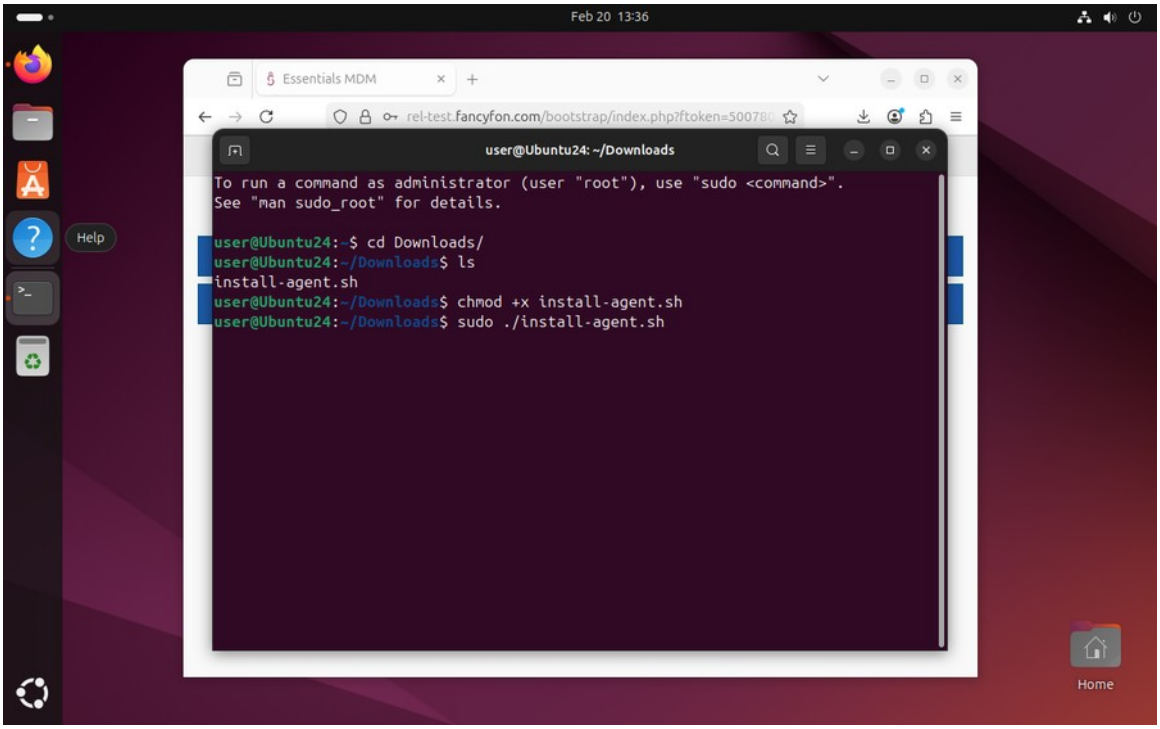
In diesem Szenario erfolgt die Registrierung mit einem globalen Passwort. Nach der Eingabe des Passworts wählen Sie die Schaltfläche Basis-Agent, um das Installationsskript (install-agent.sh) auf das System herunterzuladen.



Nach dem Herunterladen des Skripts öffnen Sie ein Terminal und navigieren Sie zu dem Verzeichnis, in dem sich die Datei befindet. Erteilen Sie dem Skript die Ausführungsberechtigung und führen Sie es mit Administratorrechten mittels sudo aus.

Führen Sie dazu die folgenden Befehle aus:

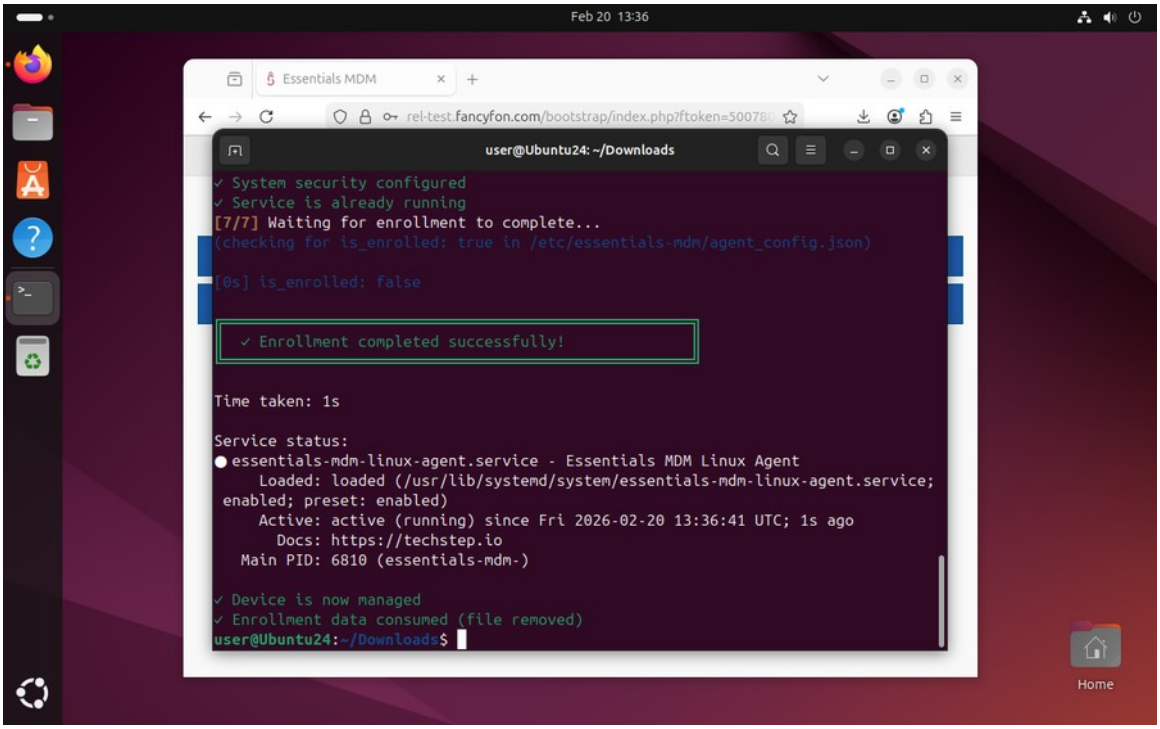
```
$ chmod +x install-agent.sh
$ sudo ./install-agent.sh
```



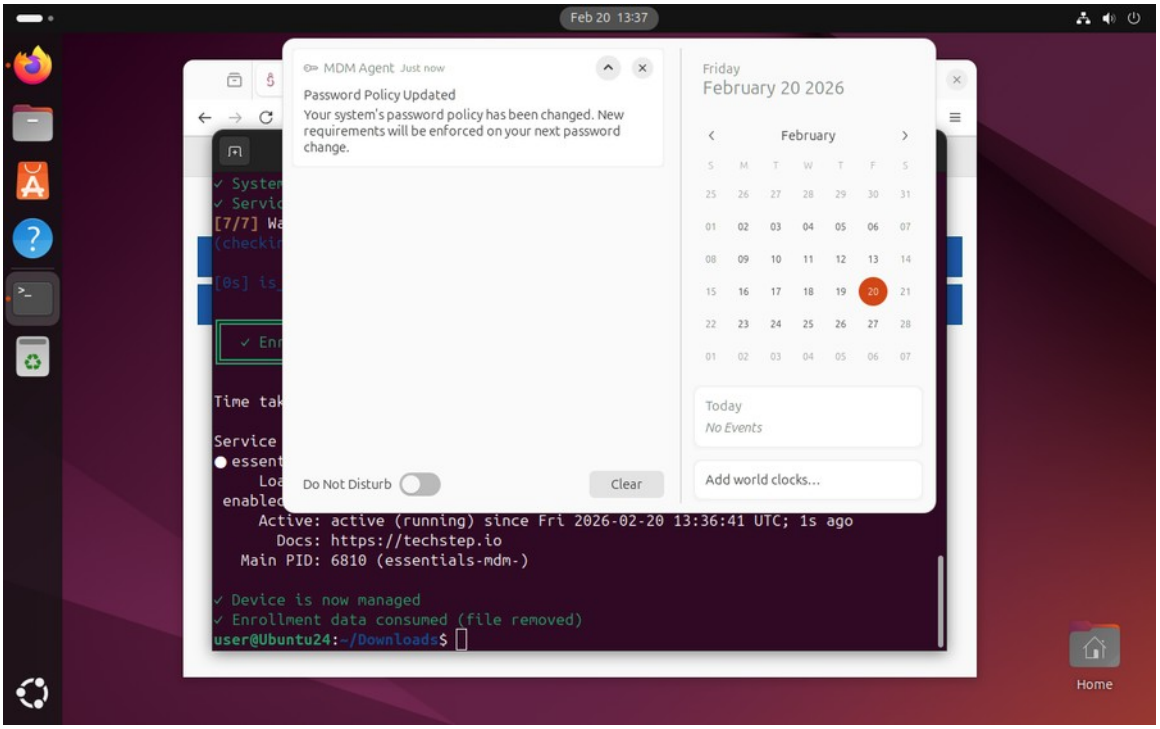
Zusätzlich unterstützt das Installationsskript folgende optionale Parameter:

- --help, -h – zeigt das Hilfemenü an
- --force, -f – erzwingt die Installation (verwendet für Neuinstallation oder Downgrade)
- --re-enroll – erzwingt die erneute Geräteregistrierung

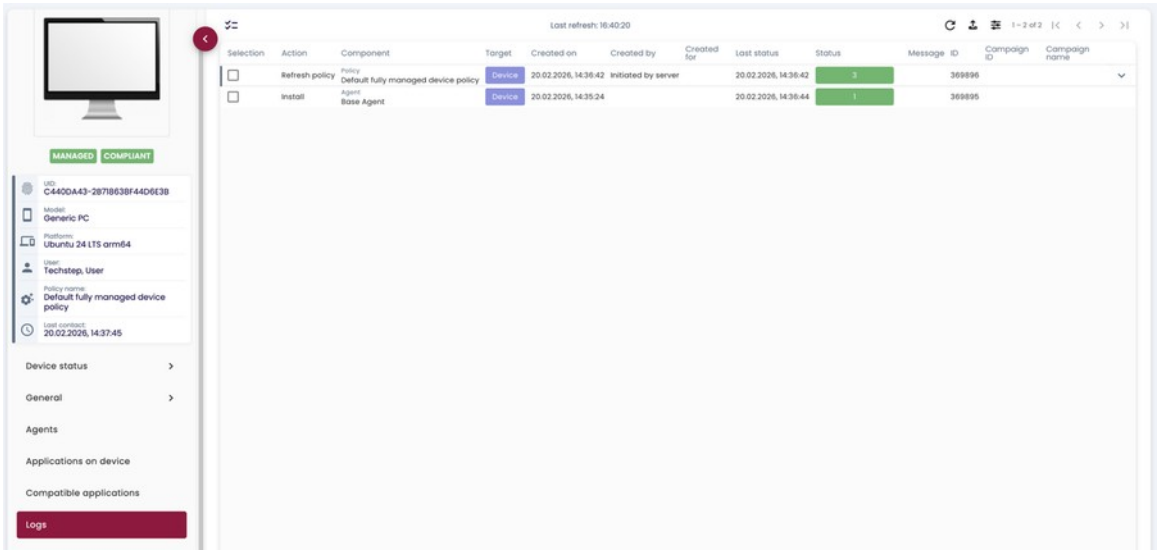
Nach der Ausführung des Skripts werden Echtzeit-Protokolle im Terminalfenster angezeigt. Der Vorgang ist abgeschlossen, wenn der Status als „registriert" angezeigt wird und die aktuelle Agentenversion erscheint.

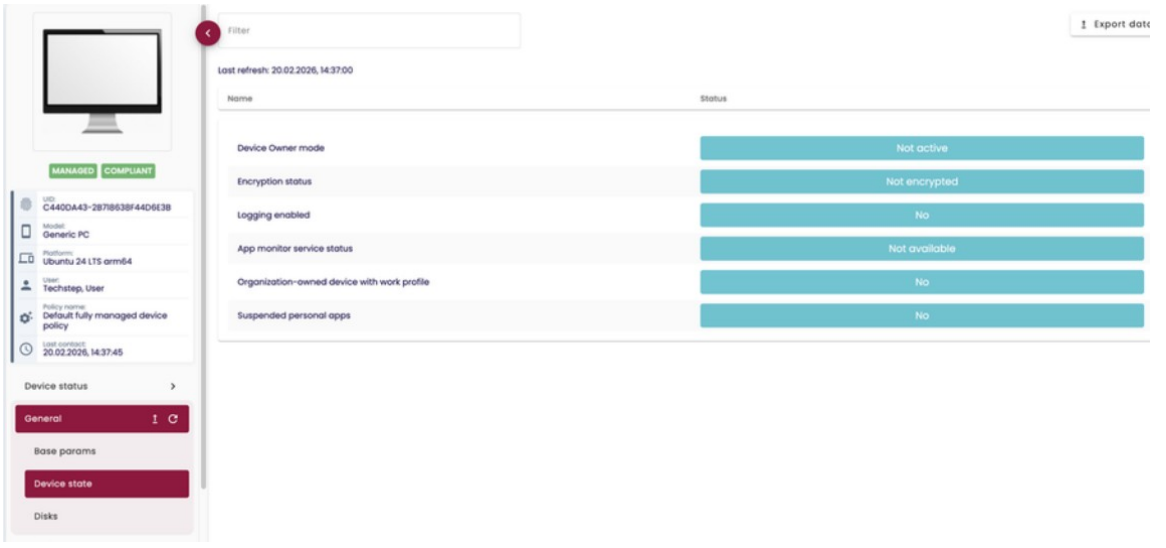


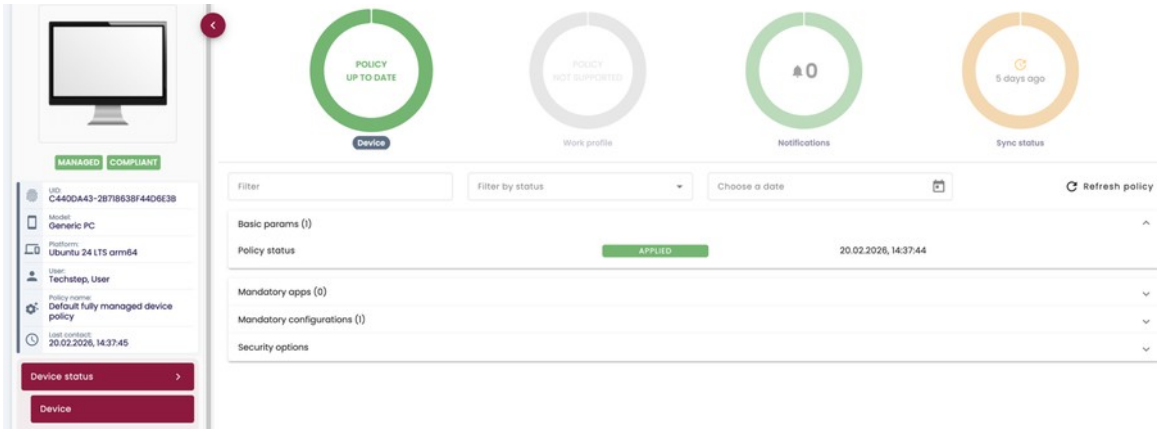
Wie bereits erwähnt, läuft der MDM-Agent als Systemdienst und bleibt für den Benutzer unsichtbar. Seine Aktionen sind jedoch beobachtbar. Wenn beispielsweise Kennwortrichtlinienbeschränkungen konfiguriert sind, werden diese auf das System angewendet und im Benachrichtigungs-Tab angezeigt.



Aus der Administratorperspektive erscheint das Gerät nach vollständiger Registrierung in der Geräteliste, mit detaillierten Informationen, die auf die gleiche Weise wie bei anderen Gerätetypen verfügbar sind, wie unten dargestellt.

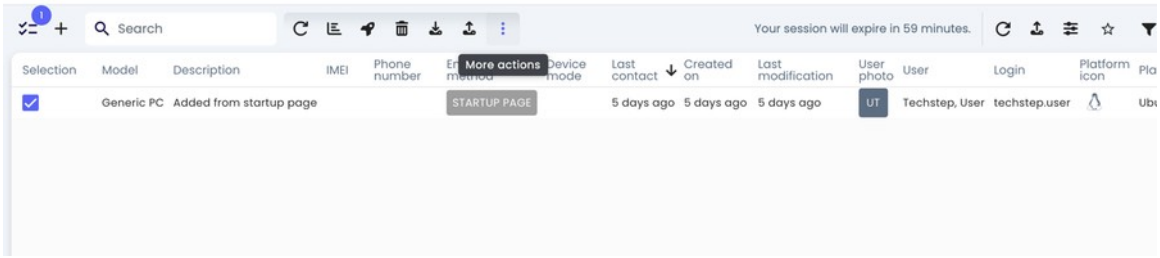


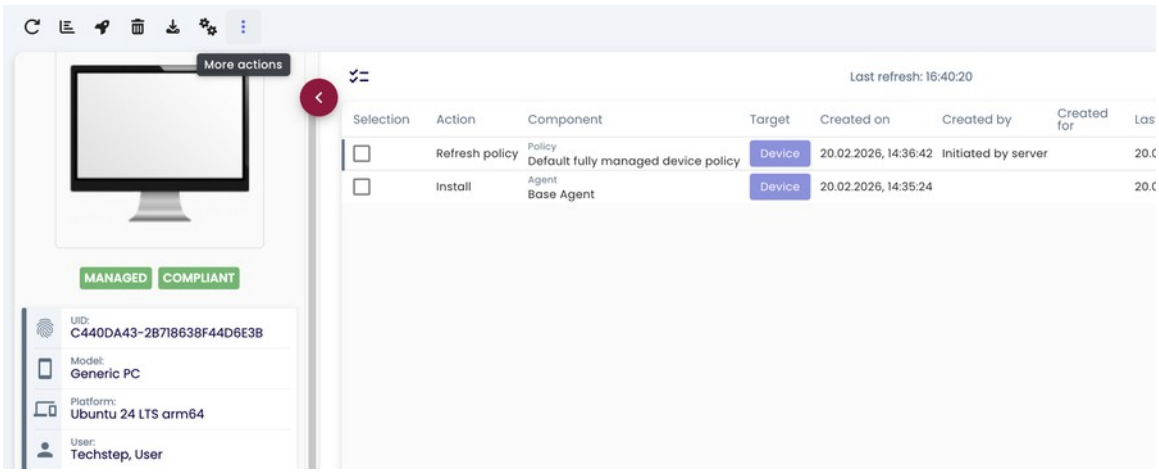



MANAGED
COMPLIANT
UID:
C440DA43-2B718638F44D6E38
Model:
Generic PC
Platform:
Ubuntu 24 LTS arm64
User:
Techstep, User
Policy name:
Default fully managed device policy
Last contact:
20.02.2026, 14:37:45
Device status
Device
POLICY UP TO DATE
Device
POLICY NOT SUPPORTED
Work profile
0
Notifications
5 days ago
Sync status
Filter
Filter by status
Choose a date
Refresh policy
Basic params (1)
Policy status
APPLIED
20.02.2026, 14:37:44
Mandatory apps (0)
Mandatory configurations (1)
Security options

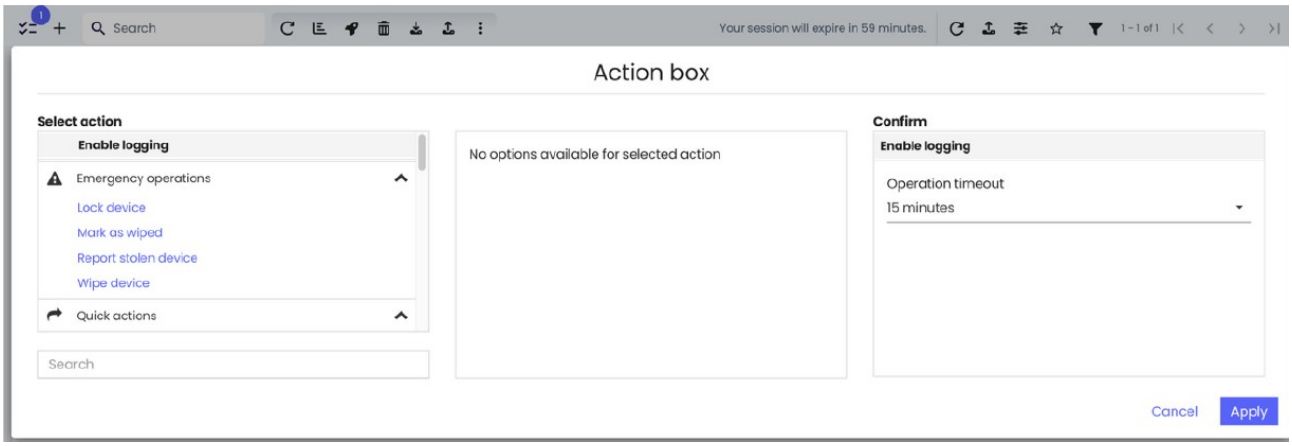
4 Operationen

Sofortige Verwaltungsaktionen werden über die Aktionsbox ausgelöst, die sich in der Gerätedetailansicht oder direkt in den Gerätedetails befindet.





Die Aktionsbox mit allen unterstützten Operationen wird dann angezeigt. Um Operationen auszuführen, wählen Sie diese aus der Liste und klicken Sie auf die Schaltfläche Übernehmen.



4.1 Unterstützte Operationen

4.1.1 Gerät zurücksetzen

Der Vorgang „Gerät zurücksetzen" ermöglicht die Fernlöschung sensibler Informationen und wird als kritische Sicherheitsmaßnahme eingestuft. Dieser Prozess löscht Benutzerverzeichnisse, Shell-Historien, Verschlüsselungsschlüssel und Browserdaten auf verschiedenen Plattformen. Das System löscht außerdem Systemprotokolle und temporäre Dateien, bevor ein abschließender Systemneustart eingeleitet wird.

Hinweis: Es ist wichtig zu beachten, dass dieser Vorgang nicht rückgängig gemacht werden kann und zur Entfernung des MDM-Agenten führt, wodurch jede zukünftige Verwaltung des Geräts beendet wird.

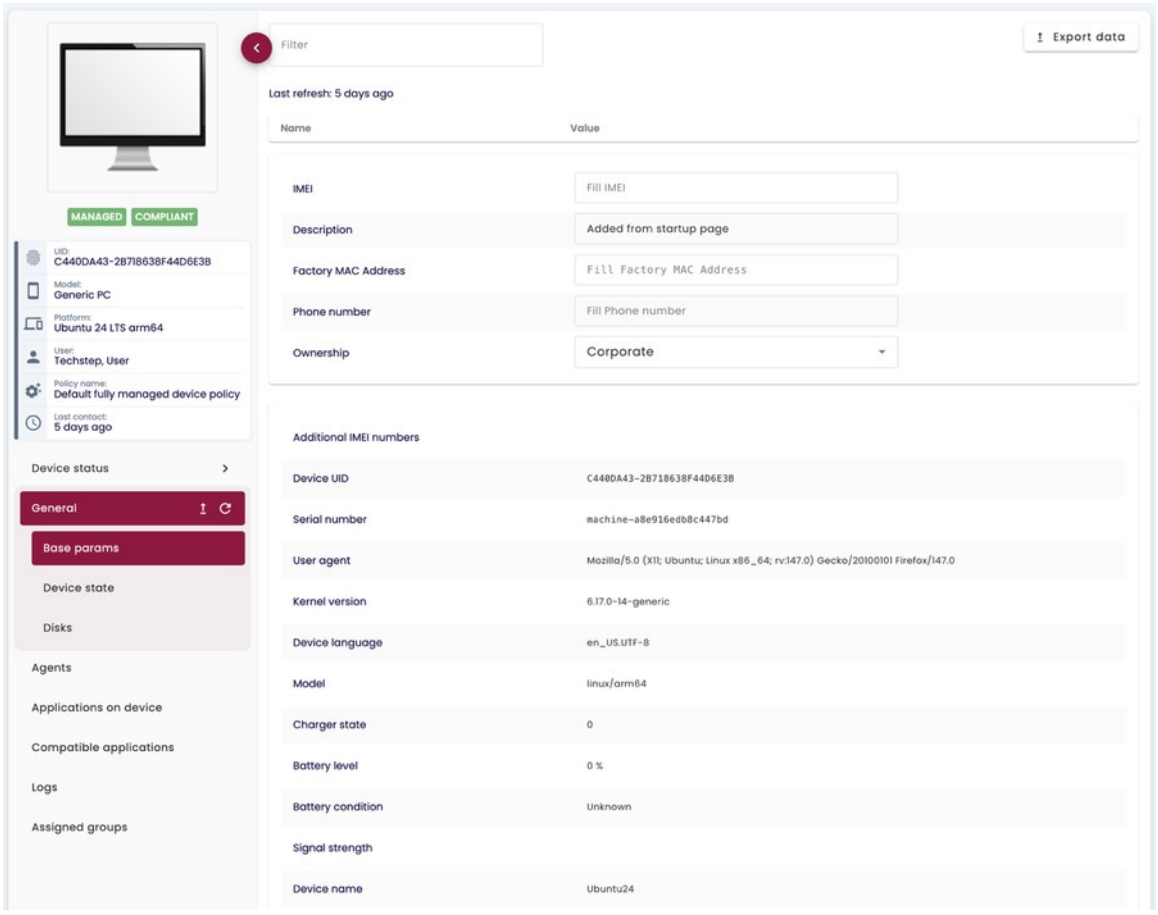
4.1.2 Gerät sperren

Der Vorgang „Gerät sperren" dient dazu, das Terminal sofort zu sichern, indem alle aktiven Zugriffe beendet werden. Der Agent trennt aktuelle SSH-Verbindungen, stoppt alle Prozesse der angemeldeten Benutzer und nutzt Mechanismen, um den Abmeldevorgang zu finalisieren. Nach der Ausführung kehrt das Gerät in einen standardmäßigen Anmeldezustand zurück, von dem aus ein Benutzer mit gültigen lokalen Anmeldeinformationen wieder auf das Gerät zugreifen kann.

4.1.3 Gerätemonitordaten abrufen

Der Vorgang „Gerätemonitordaten abrufen" erfasst einen umfassenden Satz von Telemetriedatensätzen, die für die Systemprüfung und Bestandsverwaltung wesentlich sind. Dieser Vorgang aggregiert Hardwarespezifikationen wie Hersteller, Modell, Seriennummer, CPU-Architektur sowie gesamte und verfügbare RAM-Kapazität. Er meldet auch Betriebssystemdetails einschließlich der spezifischen Distributionsversion, Kernelversion und der aktuellen Systemsprache. Netzwerkparameter wie lokale IP-Adressen und MAC-Adressen für drahtlose und kabelgebundene Schnittstellen werden erfasst, zusammen mit hardware-spezifischen Daten wie Akkuzustand, BIOS-Versionen und LUKS-Festplattenverschlüsselungsstatus. Darüber hinaus enthält der Monitor-Datensatz eine vollständige Liste aller installierten Softwarepakete und aktiven Systemprozesse.

Alle vom Gerätemonitor gesammelten Informationen werden im Bereich Gerätedetails der Administratorkonsole angezeigt, wie unten dargestellt.



4.1.4 Gerät neu starten

Der Vorgang Gerät neu starten führt einen Remote-Systemneustart des verwalteten Geräts durch.

4.1.5 Richtlinie aktualisieren

Der Vorgang „Richtlinie aktualisieren“ zwingt den Agenten, seine lokalen Sicherheitseinstellungen sofort mit dem MDM-Server zu synchronisieren. Der Agent ruft die aktuelle Konfiguration ab, analysiert Änderungen an den Einschränkungen und führt die entsprechenden Durchsetzungsskripte aus, um sicherzustellen, dass das Gerät der zugewiesenen Richtlinie entspricht.

4.1.6 Protokollierung aktivieren / Protokollierung deaktivieren

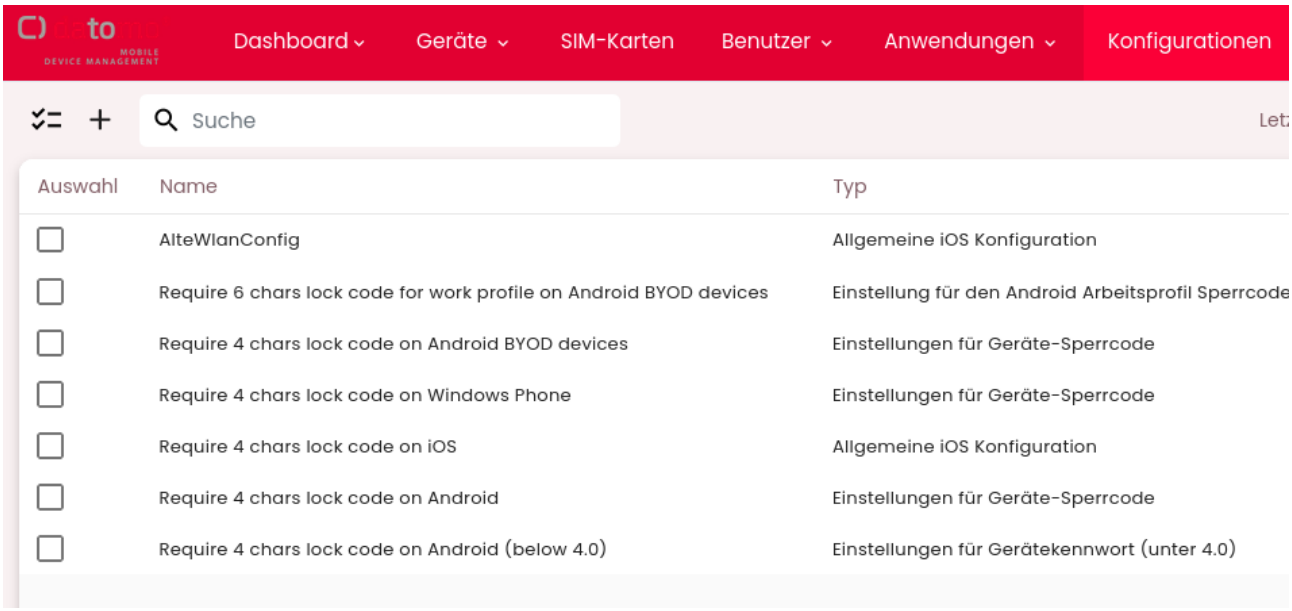
Die Vorgänge Protokollierung aktivieren oder Protokollierung deaktivieren steuern die Ausführlichkeit der Diagnosedatensätze des Agenten. Das Aktivieren der Protokollierung schaltet den Agenten auf die DEBUG-Ebene um, was detaillierte Informationen zur internen Kommunikation und Skriptausführung liefert. Diese Einstellung bleibt aktiv, bis eine Deaktivierungsaktion gesendet wird, die die Protokollierung auf die Standard-INFO-Ebene zurücksetzt, um die Festplattennutzung zu minimieren.

4.1.7 Geräteprotokolle abrufen

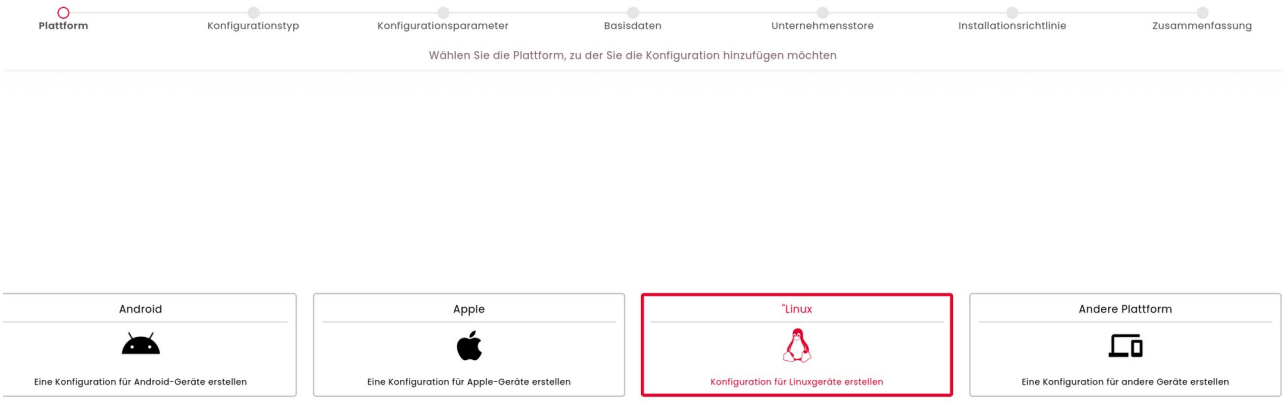
Der Vorgang „Geräteprotokolle abrufen" ermöglicht das Fernlesen der internen Aktivitätsaufzeichnungen des Agenten. Diese Aktion komprimiert die aktuellen Agentenprotokolle in ein ZIP-Archiv und lädt sie auf den Server hoch. Nach einem erfolgreichen Upload führt der Agent eine Protokollrotation durch, indem er die aktive Protokolldatei leert und frühere Einträge archiviert. Um die Festplatteneffizienz zu gewährleisten, löscht das System automatisch archivierte Protokolle, die älter als zehn Tage sind.

5 Konfigurationen

Konfigurationen ermöglichen die Durchsetzung dauerhafter Systemeinstellungen auf verwalteten Linux-Geräten. Diese Einstellungen werden in der Verwaltungskonsole definiert und an den Agenten übermittelt, um die kontinuierliche Einhaltung der Organisationsstandards zu gewährleisten. Um eine Konfiguration hinzuzufügen, navigiert der Administrator zum Tab Konfigurationen und klickt auf die Plus-Schaltfläche.



Anschließend wird die Plattform Linux ausgewählt.



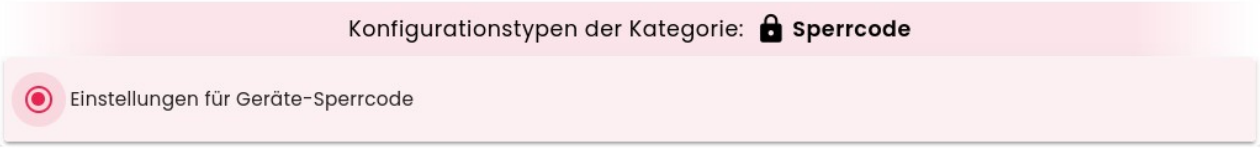
Es werden derzeit zwei Konfigurationen unterstützt: Shell-Skript ausführen und Gerätesperrcode-Einstellungen.

5.1 Unterstützte Konfigurationen

5.1.1 Einstellungen für den Gerätesperrcode

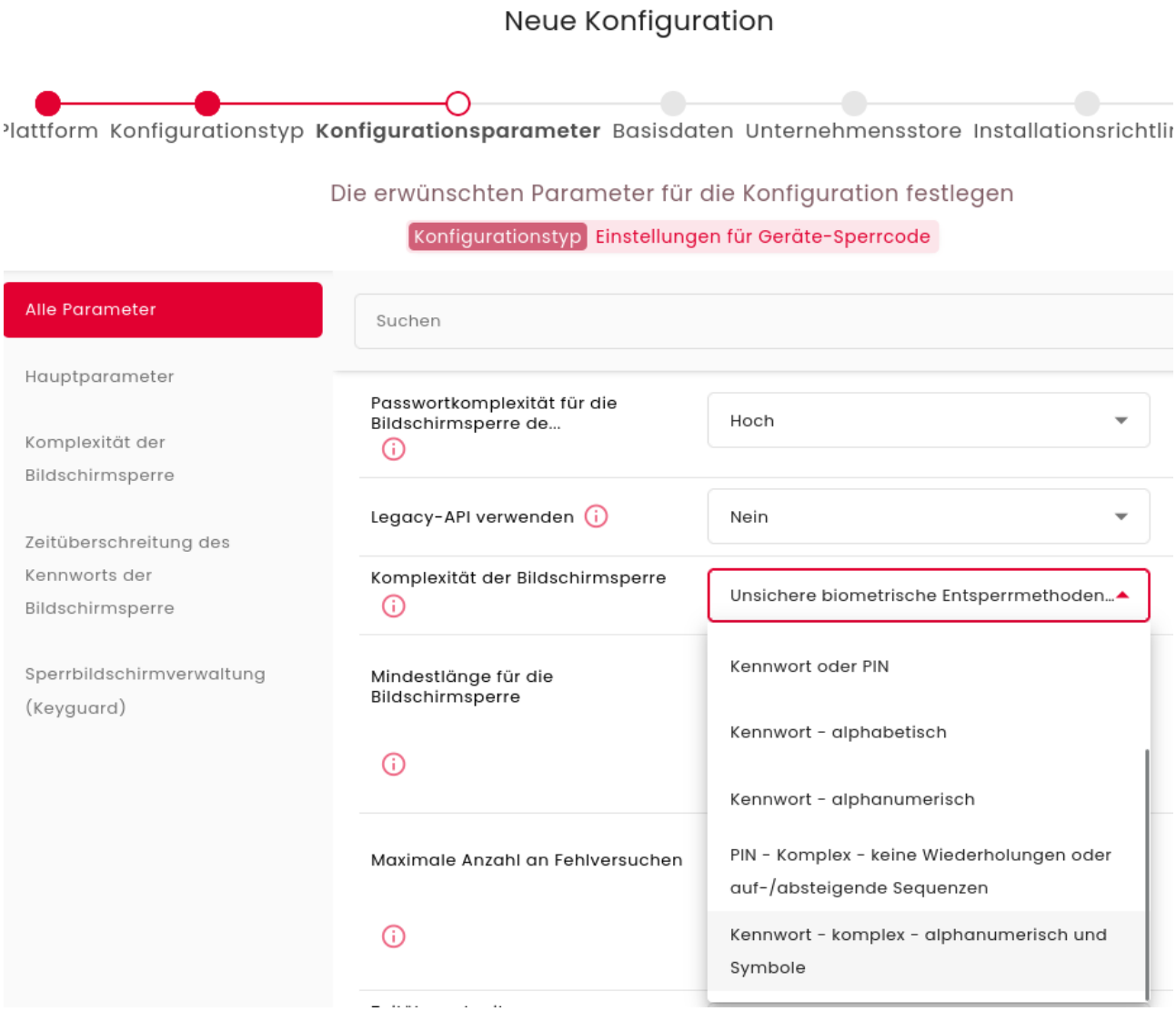
Diese Konfiguration verwaltet die Anforderungen an die Passwortkomplexität. Sie ermöglicht Administratoren, spezifische Sicherheitsstandards für lokale Benutzerkonten durchzusetzen.

Für Linux-Geräte ist die empfohlene Option für die Festlegung der Passwortkomplexität Passwort – Komplex – Alphanumerisch mit Sonderzeichen. Andere Konfigurationen haben Einschränkungen und decken die unterstützten Restriktionen nicht vollständig ab.



Unterstützte Komplexitätsparameter umfassen:

- Mindestlänge des Passworts: Legt die erforderliche Anzahl an Zeichen fest.
- Mindestanzahl an Ziffern: Gibt die erforderliche Anzahl numerischer Zeichen (0–9) an.
- Mindestanzahl an Kleinbuchstaben: Gibt die erforderliche Anzahl kleiner Buchstaben (a–z) an.
- Mindestanzahl an Großbuchstaben: Gibt die erforderliche Anzahl großer Buchstaben (A–Z) an.
- Mindestanzahl an Sonderzeichen: Gibt die erforderliche Anzahl von Sonderzeichen (z. B. !, @, #) an.



Neben den oben genannten Einstellungen gibt es eine weitere Einstellung namens Passwortänderung erzwingen überspringen, die in der gesamten Konfiguration unterstützt wird. Wenn diese Option aktiviert ist, wird der Benutzer gezwungen, sein Passwort zu ändern, um der in der Konfiguration definierten Passwortrichtlinie zu entsprechen.

Bekannte Probleme und Anforderungen:

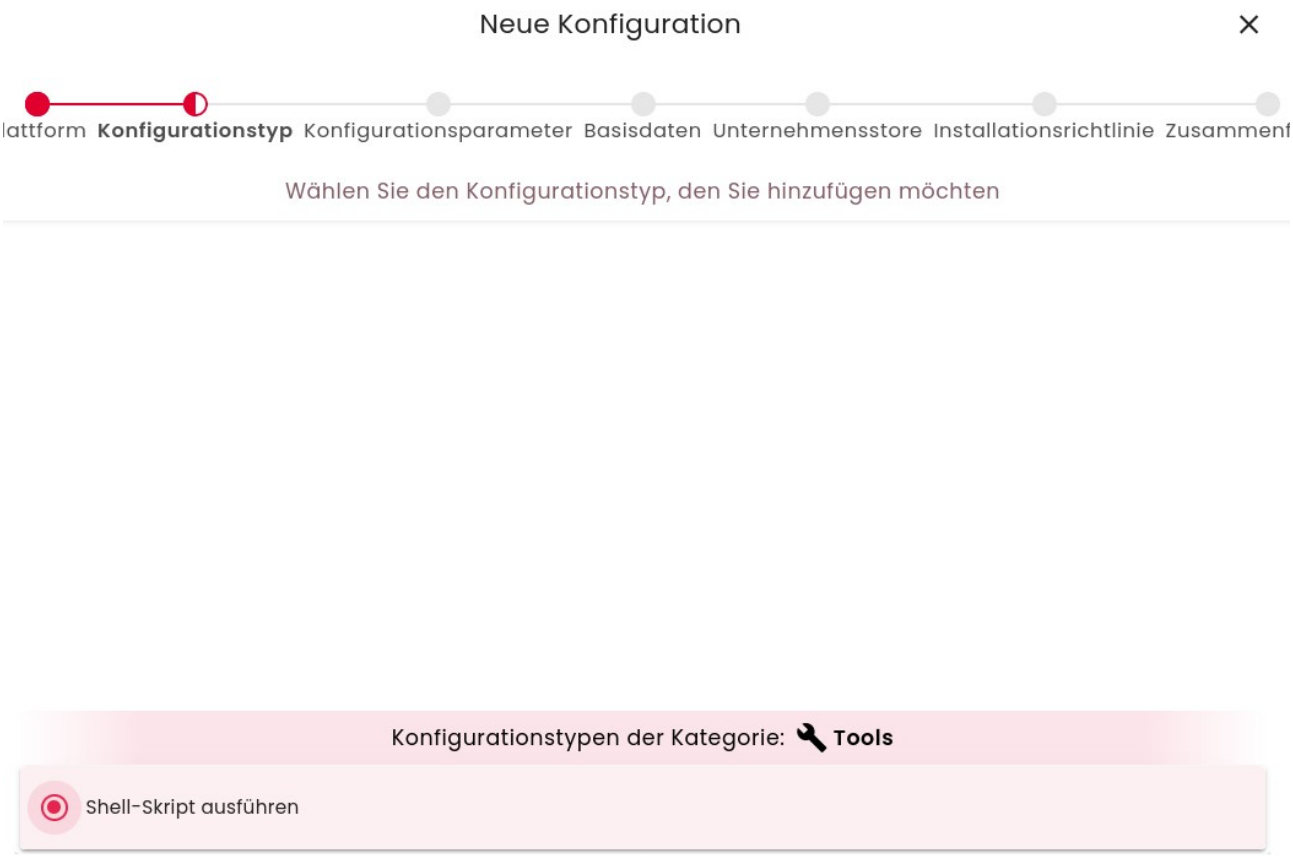
- Passwortänderungen über die grafische KDE-Oberfläche sind derzeit aufgrund umgebungsspezifischer Einschränkungen blockiert.
- Auf Fedora-Systemen kann der Bildschirm zur Passwortänderung beim nächsten Login einfrieren, wenn „Erzwingung überspringen" auf „Falsch" gesetzt ist und eine

Passwortänderung nach dem Abmelden erzwungen wird; möglicherweise ist ein manueller Systemneustart erforderlich.

- Passwortänderungen in der grafischen GNOME-Oberfläche erfordern eine Mindestpasswortlänge von 8 Zeichen.
- Das Entfernen der Passwortrichtlinienkonfiguration entfernt möglicherweise nicht die angewendeten GNOME-Einstellungen.
- Die Durchsetzung der Passwortänderung kann auch dann ausgelöst werden, wenn das aktuelle Passwort die konfigurierten Anforderungen erfüllt.

5.1.2 Shell-Skript ausführen

Diese Konfiguration dient als vielseitiges Werkzeug zur Systemautomatisierung und ermöglicht die Remote-Bereitstellung und -Ausführung benutzerdefinierter Skripte.



Konfigurationsparameter:

Operationstitel: Eine optionale Bezeichnung zur Identifizierung der jeweiligen Skriptausführung in den Protokollen.

Code: Der primäre Textbereich, in dem der Skriptinhalt angegeben wird. Der Agent erkennt automatisch den geeigneten Interpreter anhand der Shebang-Zeile am Anfang des Codes. Während /bin/bash der Standard ist, wenn kein Shebang angegeben wurde, unterstützt das System ausdrücklich andere Interpreter wie #!/bin/sh, #!/usr/bin/python3 oder #!/usr/bin/env python.

Für jede Ausführung erstellt der Agent ein eindeutiges temporäres Verzeichnis im /tmp/-Ordner des Systems (z. B. /tmp/essentials_{zufälliger_name}). Das Skript wird in diesem Verzeichnis mit eingeschränkten Berechtigungen gespeichert, um den Zugriff durch andere lokale Benutzer zu verhindern. Nach Abschluss des Skripts werden das temporäre Verzeichnis und sein Inhalt automatisch vom System entfernt.

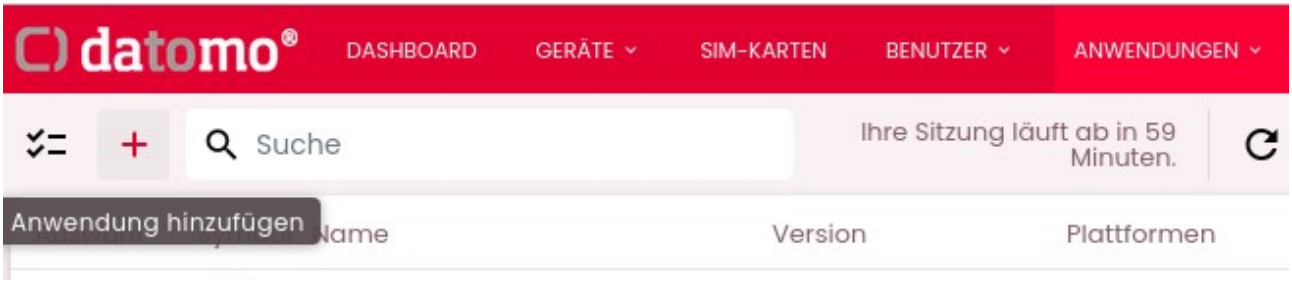
Skript-Argumente: Eine dynamische Liste, mit der Administratoren bestimmte Variablen oder Flags an das Skript während der Ausführung übergeben können.

Ergebnis zurückgeben: Ein Dropdown-Menü, das bestimmt, ob die Skriptausgabe (Standardausgabe und Fehler) an den MDM-Server zurückgesendet werden soll. Wenn auf „Ja" eingestellt, können Administratoren die Ausführungsergebnisse direkt in der Konsole im Konfigurationsausführungsprotokoll einsehen, was sehr nützlich ist, um den erfolgreichen Abschluss zu überprüfen oder Fehler zu diagnostizieren.

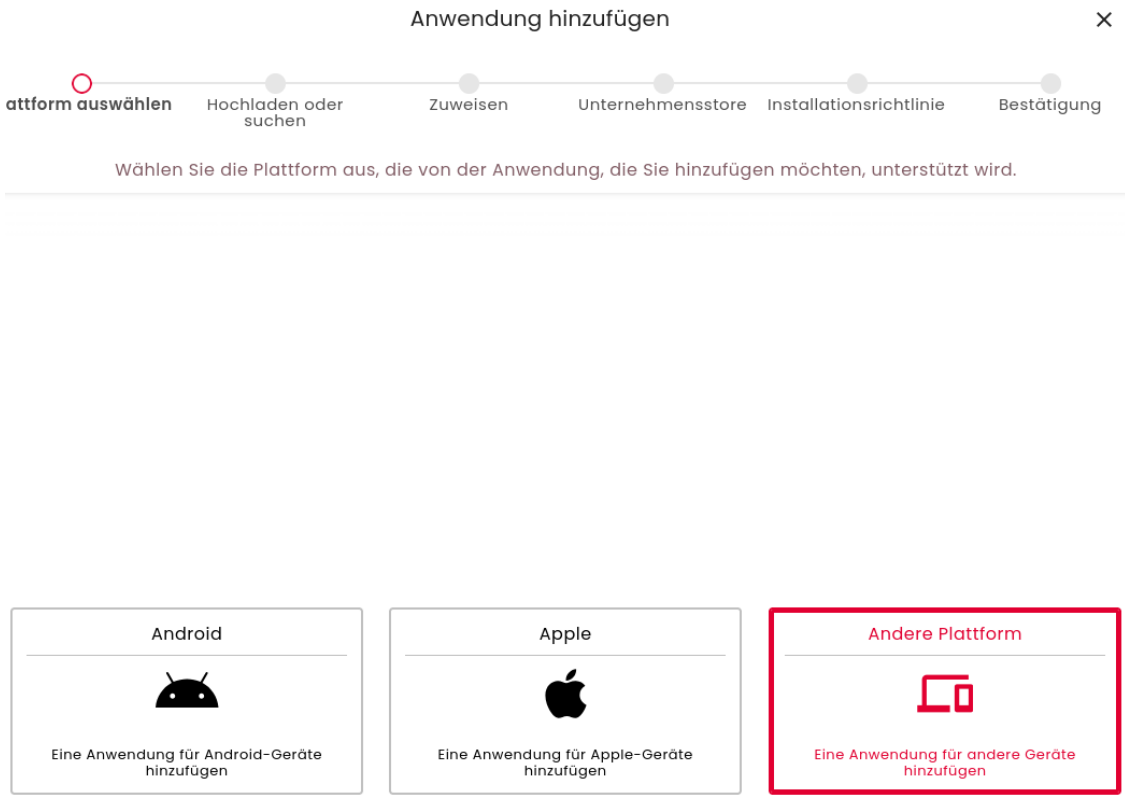
6 Anwendungsinstallation

Die Anwendungsinstallation erfolgt aus der Ferne und erfordert keine Interaktion des Gerätebenutzers. Installationspakete können im Format .deb für Debian- und Ubuntu-Systeme oder im Format .rpm für RHEL- und Fedora-Systeme über den Tab Anwendungen in der Administratorkonsole hochgeladen werden. Um ein Paket hochzuladen, navigieren Sie zur Anwendungsliste:

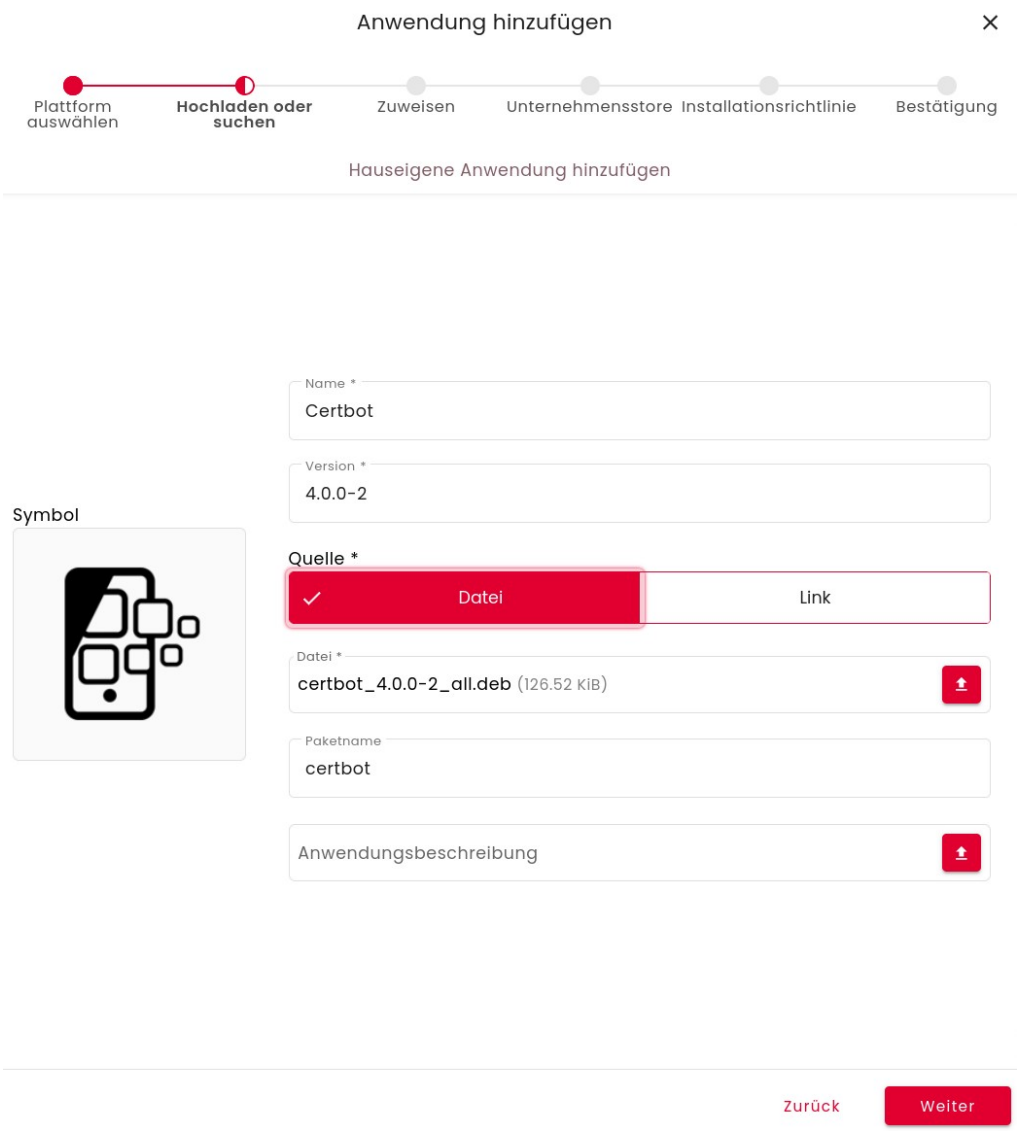
Anschließend wählen Sie die Plus-Schaltfläche.



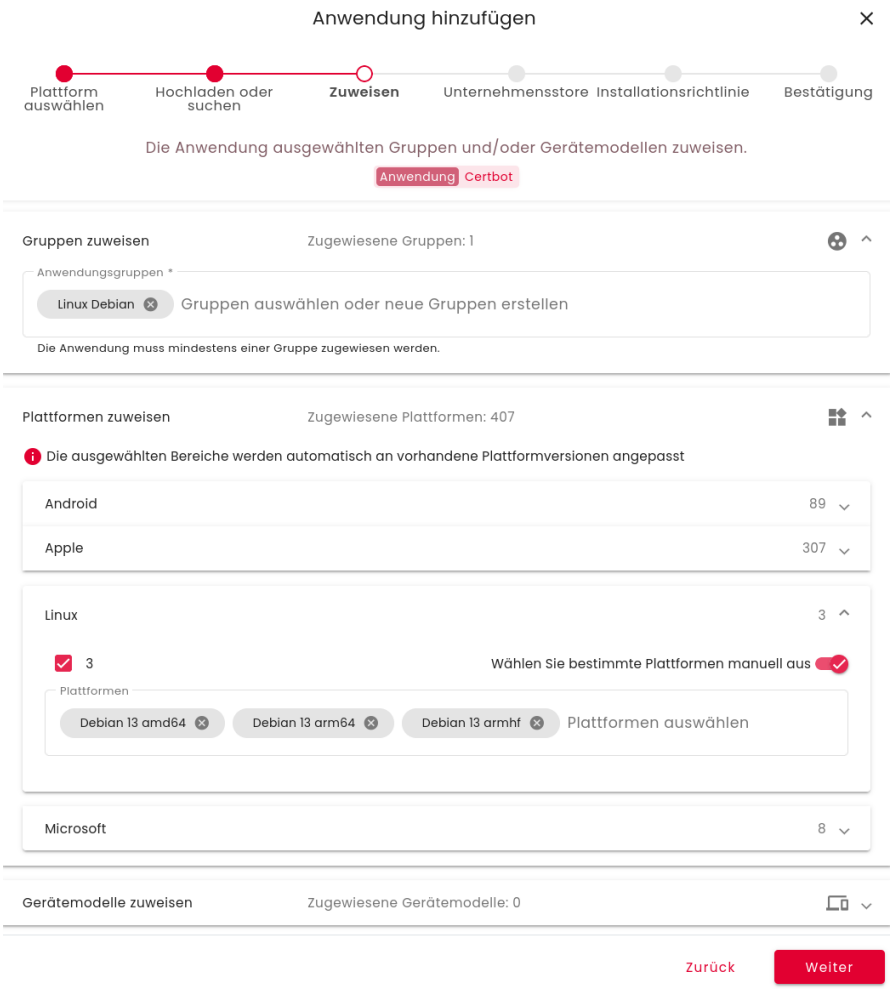
Wählen Sie im ersten Schritt die Schaltfläche Andere Plattform, um ein Linux-Paket hochzuladen.



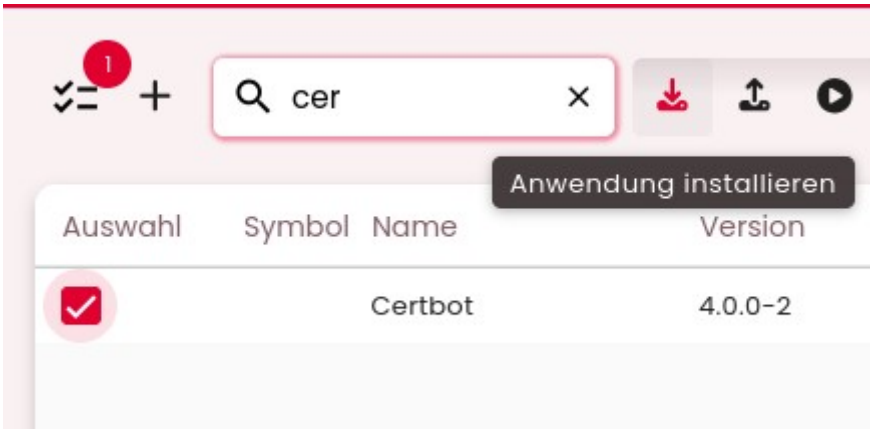
Wählen Sie im Schritt Hochladen das Installationspaket aus, geben Sie dessen Namen und Version an und spezifizieren Sie ggf. den Paketnamen. Ein Anwendungssymbol kann ebenfalls hochgeladen werden. Das Symbol wird in der Administratorkonsole angezeigt.



Stellen Sie im nächsten Schritt sicher, dass die Plattformen korrekt zugewiesen sind. Wählen Sie die entsprechenden Architekturen und Betriebssystemversionen aus, da diese Konfiguration die Gerätekompatibilität bestimmt.



Sobald die Anwendung Plattformen, Richtlinien und eine Corporate-Store-Richtlinie zugewiesen hat und die Konfiguration erfolgreich erstellt wurde, erscheint sie in der Anwendungsliste. Die Anwendung kann dann mit der Aktion Installieren installiert werden, auf die gleiche Weise wie aus den Gerätedetails oder der Geräteliste.

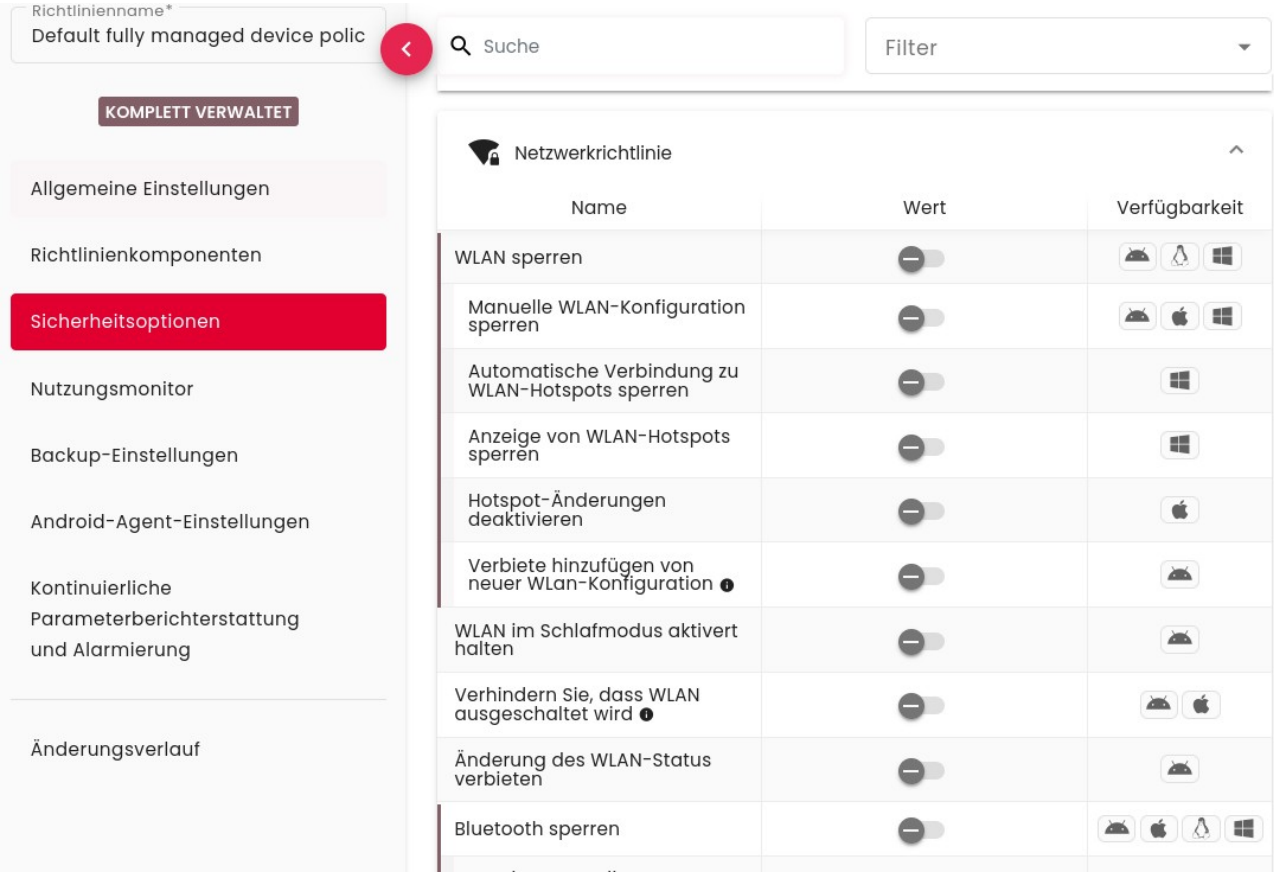


Nachdem der Vorgang an das Gerät gesendet und erfolgreich ausgeführt wurde, wird die Anwendung ohne Benutzerinteraktion auf dem Gerät installiert.

Wichtig: Im Falle eines Installationsfehlers überprüfen Sie, ob die korrekte Architektur hochgeladen wurde (arm64 ist nicht kompatibel mit amd64). Stellen Sie außerdem sicher, dass das Paketformat korrekt ist: .deb-Pakete sind für Debian- und Ubuntu-Systeme bestimmt, während .rpm-Pakete für Red Hat- und Fedora-Systeme vorgesehen sind.

7 Richtlinienbeschränkungen

Mit Linux kompatible Sicherheitsbeschränkungen werden in den MDM-Richtlinien durch ein Pinguin-Symbol gekennzeichnet.



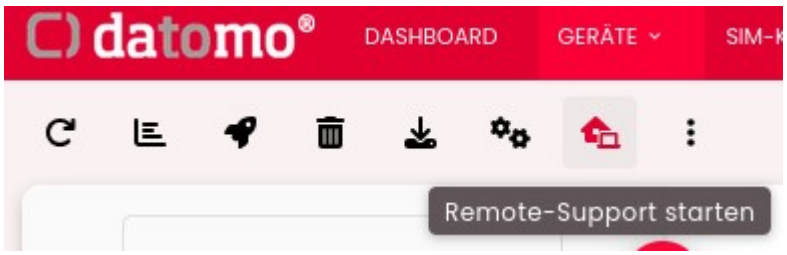
Der Agent ruft diese Einstellungen vom MDM-Server ab und wendet sie systemweit an. Die unterstützten Beschränkungen sind nachfolgend aufgeführt:

- **WLAN-Sperre** – Deaktiviert das drahtlose Funkmodul auf Dienstebene und verhindert, dass der Benutzer es wieder aktiviert.
- **Kamera-Sperre** – Blockiert den gesamten Systemzugriff auf interne und USB-verbundene Kameras und macht sie für Anwendungen nicht verfügbar.

- **Bluetooth-Sperre** – Deaktiviert vollständig die gesamte Bluetooth-Kommunikation und Hardware-Erkennung.
- **USB-Mediaplayer-Sperre** – Verhindert, dass das System externe USB-Massenspeichergeräte einbindet oder darauf zugreift. Diese Beschränkung ist speziell darauf ausgelegt, die Datenübertragung über USB-Speichergeräte zu blockieren, während andere Peripheriegeräte wie Tastaturen oder Mäuse normal funktionieren.
- **Gerät am Standby-Modus hindern** – Stellt sicher, dass das Gerät aktiv bleibt und verhindert automatischen Abmeldevorgang oder Systemsuspendierung.
- **Automatischen Update-Download erzwingen** – Zwingt den lokalen Paketmanager, Sicherheitsupdates automatisch herunterzuladen und zu installieren. Der Agent unterstützt die wichtigsten Paketmanager, darunter APT und YUM.
- **VPN-Einstellungen deaktivieren** – Verhindert, dass Standardbenutzer VPN-Verbindungen konfigurieren oder initiieren.
- **Speicherkartensperre** – Deaktiviert den Zugriff auf interne SD-Kartenleser. Um externe SD-Kartenleser zu deaktivieren, verwenden Sie die USB-Mediaplayer-Sperre.

8 Fernzugriff

Für weitere Funktionen ist eine Verbindung über über eine sichere virtuelle Konsole verfügbar, die direkt im Webbrowser der Administrationskonsole zugänglich ist. Um eine Sitzung zu starten, navigieren Sie zu den Geräteeinstellungen und wählen Sie „Remote Support starten“ aus dem Aktionsmenü – entweder in den Geräteeinstellungen oder in der Geräteliste.



Bevor die Sitzung beginnt, muss das verwaltete Gerät die Sitzungsinformationen vom Server empfangen, was je nach dem nächsten Agenten-Check-in-Zyklus bis zu zwei Minuten dauern kann.

Nach dem Aufbau wird eine sichere Shell-Sitzung über die LiveKit-Cloud-Infrastruktur erstellt, sodass Systembefehle aus der Ferne ausgeführt werden können. Das Terminal läuft mit einem autorisierten Benutzerkonto; jedoch erfordern administrative Aufgaben die Verwendung des sudo-Befehls. Für aktive Remote-Support-Sitzungen ist derzeit keine Zeitbegrenzung festgelegt.

Das Virtuelle Terminal bietet die folgenden Funktionen:

- Manuelle Systemkonfiguration und Serviceanpassungen,
- Echtzeit-Fehlerbehebung und Protokollprüfung,
- On-the-fly-Skripting zur Aufgabenautomatisierung,
- Manuelle Backups und erweitertes Paketmanagement, und mehr...

Alle Kommunikationskanäle sind verschlüsselt, um einen sicheren Zugriff zu gewährleisten. Pro Gerät ist nur eine aktive Sitzung erlaubt. Zusätzliche datomo MDM Administratoren können einer aktiven Sitzung beitreten.

Hinweis: Wenn die Fernzugriffsaktion nicht verfügbar ist, stellen Sie sicher, dass diese Funktion in der zugewiesenen Richtlinie aktiviert ist, wie im folgenden Beispiel dargestellt.