Druckversion der Relution-Dokumentation

Relution-Handbuch

Für Version 26.4.0

Zuletzt aktualisiert: 2026-10-21 14:00 UTC

Online verfügbar unter hub.relution.io

Inhaltsverzeichnis

1. Relution Cloud
2. On Premises Installation
    1. Installation
    2. Objektspeicher
    3. Nach der Installation
    4. Knowledge Base
3. Produktinformationen
4. Erste Schritte
5. Allgemein
    1. Dashboard
    2. Relution Apps
    3. App-Verwaltung
    4. Benutzerverwaltung
    5. Geräteverwaltung
    6. Apple-Verwaltung
6. Apple iOS
    1. Geräte einschreiben
    2. Supervision
    3. Aktionen
    4. Einstellungen
    5. Richtlinien
    6. Knowledge Base
7. Apple tvOS
    1. Geräte einschreiben
    2. Aktionen
    3. Richtlinien
    4. Wissensdatenbank

Für Version 26.4.0

8. Apple macOS
    1. Geräte einschreiben
    2. Aktionen
    3. Richtlinien
    4. Wissensdatenbank
9. Apple visionOS
    1. Geräte einschreiben
    2. Aktionen
    3. Richtlinien
10. Apple watchOS
    1. Geräte einschreiben
    2. Aktionen
    3. Richtlinien
11. Bildung
    1. Apple im Bildungsbereich
12. Android Enterprise
    1. Geräte einschreiben
    2. Aktionen
    3. Richtlinien
    4. Knowledge Base
13. Android Classic
    1. Geräte einschreiben
    2. Aktionen
    3. Richtlinien
    4. Knowledge Base
14. Whiteboards
    1. Android Classic
    2. Android Enterprise
15. Windows
    1. Geräte einschreiben
    2. Aktionen
    3. Richtlinien
    4. Windows Apps
    5. opsi
    6. Knowledge Base
16. Linux
17. Einstellungen
    1. Lizenzen
    2. TeamViewer
    3. Bedingter Zugriff

Für Version 26.4.0

Relution Cloud

Relution bietet ein leistungsstarkes Cloud-Angebot, das den Betrieb der Software als virtualisierte Cloud-Serverlösung umfasst. Dieses Hosting erfolgt in einer DSGVO-konformen Cloud-Umgebung und gewährleistet die Sicherheit und den Schutz aller verarbeiteten Daten. Durch automatisches Einspielen von Updates bleibt die Software stets aktuell und sicher. Zudem wird durch die Infrastruktur eine hohe Verfügbarkeit der Relution-Plattform von 99,5 % außerhalb des Wartungsfensters sichergestellt, sodass eine zuverlässige Nutzung jederzeit gewährleistet ist.

Allgemeine Informationen

Für den Betrieb der Relution-Cloud gelten die folgenden allgemeinen Hinweise.

Wartungsfenster

Die Wartung der Relution-Cloud-Server findet von montags 17:00 Uhr bis dienstags 4:00 Uhr CE(S)T statt. Während dieser Zeit kann es zu temporären Einschränkungen kommen.

Relution-Updates

Relution-Updates werden vorab über den Newsletter → angekündigt und am jeweils angekündigten Tag zwischen 16:00 Uhr und 19:00 Uhr CE(S)T durchgeführt. Während der Updates kommt es zu keiner Downtime.

Für Version 26.4.0

E-Mail-Empfang

Sicherstellen, dass E-Mails von `no-reply@relution.io` und `no-reply@mail.relution.io` empfangen werden können. Diese Adressen werden als Absender für den Mailverkehr der Cloud-Server verwendet.

Gateway IP-Adressen

Die Gateway-Adressen, unter denen die Relution-Cloud-Server Anfragen versenden, sind auf zwei Wegen verfügbar:

1. Per DNS: Die IP-Adressen sind als DNS-A-Records unter dem FQDN `gateway.<Cluster-Name>.relution.io` hinterlegt, z. B. `gateway.eu.relution.io` für den `eu`-Cluster. In Firewalls, die FQDN-basierte Regeln unterstützen, kann dieser Hostname direkt in der Freischaltung verwendet werden.
2. Als JSON-Liste: Unter https://repo.relution.io/other/relution-cloud-gateways.json werden die Adressen zusätzlich in maschinenlesbarer Form veröffentlicht.

Beide Quellen werden regelmäßig automatisiert aktualisiert. Falls eine IP-basierte Freischaltung für Zugriff auf z. B. LDAP notwendig ist, muss die jeweilige Quelle regelmäßig abgefragt und die Freischaltung aktualisiert werden; empfohlen ist eine automatisierte Lösung oder die Verwendung FQDN-basierter Firewall-Regeln.

Limits und Quotas

Siehe Artikel Limits und Quotas →.

Varianten des Relution Cloud-Angebots

Das Cloud-Angebot von Relution wird in zwei Varianten bereitgestellt, um flexibel auf unterschiedliche Anforderungen einzugehen:

Für Version 26.4.0

Shared Hosting auf live.relution.io

Im `Shared Hosting`-Modell steht eine Organisation auf `live.relution.io` innerhalb eines gemeinsam genutzten Servers zur Verfügung. Diese Variante bietet eine kosteneffiziente Lösung für Organisationen mit weniger komplexen Anforderungen. Ein Testzugang kann direkt über die "Preise und Demo"-Übersicht auf der relution.io-Webseite → angelegt werden.

Dedicated Server

Für Organisationen, die maximale Kontrolle und Individualisierung benötigen, steht ein exklusiv betriebener `Dedicated Server` zur Verfügung. Dieser erlaubt eine eigene Infrastruktur und Erweiterungsmöglichkeiten, die an spezifische Unternehmensbedürfnisse angepasst werden können. Diese Server werden unter einer URL nach dem Schema `<Server-Name>.<Cluster-Name>.relution.io` bereitgestellt, zum Beispiel `acme.eu.relution.io`.

Der `<Server-Name>` unterliegt den folgenden Einschränkungen:

- Maximal 20 Zeichen
- Nur alphanumerische Zeichen (Kleinbuchstaben) oder '-'
- Muss mit einem Buchstaben beginnen
- Muss mit einem alphanumerischen Zeichen enden

Ersteinrichtung

Für die Ersteinrichtung werden die folgenden Daten benötigt:

- Gewünschter Servername, ergibt die Domain `<Server-Name>.<Cluster-Name>.relution.io`
- Ungefähre Anzahl der Geräte, die auf dem Server verwaltet werden sollen
- Name und E-Mail-Adresse des anzulegenden System-Administrator-Accounts

Ablauf der Ersteinrichtung:

1. Relution-Vertrieb beantragt das Anlegen des Servers mit den beschriebenen Daten
2. Server wird im entsprechenden Relution-SaaS-Cluster angelegt
3. Benachrichtigung wird an die kundenseitige Kontaktadresse verschickt
4. Durchführung eines Passwort-Resets für den System-Administrator-Account durch auf das Mail-Konto Zugriffsberechtigte
5. Login und Akzeptieren des Endbenutzer-Lizenzvertrags (EULA)
6. Digitales Unterzeichnen des Auftragsverarbeitunsvertrags (AVV) im Rahmen der Datenschutzgrundverordnung (DSGVO) im Relution-Portal
7. Dringende Empfehlung: Einrichten von Multi-Faktor-Authentifizierung (MFA) → für den System-Administrator

Optional kann anschließend ein Zugang für den Relution-Support → eingerichtet werden.

Eigene Domain für Dedicated Server

Auf Wunsch kann bei der Dedicated-Server-Variante auch eine eigene Domain verwendet werden. Dafür muss ein entsprechender DNS-CNAME-Eintrag für die Domain auf `<Server-Name>.<Cluster-Name>.relution.io` gesetzt werden. Die eigene Domain (z. B. `relution.kundenname.de`) verweist dann auf die Relution Cloud-Instanz (z. B. `kundenname.eu.relution.io`).

Site-to-Site-VPN-Add-on für Dedicated Server

Für die Dedicated-Server-Variante ist zudem das Site-to-Site-VPN-Add-on verfügbar, welches einen sicheren Zugriff auf kundenspezifische Infrastrukturen wie Intranet-Dienste ermöglicht. Dieses Add-on bietet folgende Funktionen:

- Anbindung von Intranet-Diensten an den Dedicated-Cloud-Server
- Bis zu 10 GB Traffic pro Monat
- Sicherstellung der Erreichbarkeit von 99,5 %

Voraussetzung für die Einrichtung ist, dass die kundenseitige Gegenstelle (VPN-Gateway) IPSec IKEv2 mit EAP-PSK unterstützt.

Für Version 26.4.0

Durch diese Optionen können Organisationen ihre IT-Infrastruktur individuell erweitern und sich vollständig auf ihre spezifischen Anforderungen ausrichten.

Relution Shield im SaaS-Betrieb

Als weiteres Add-on für Dedicated Server bietet Relution mit Relution Shield → eine leistungsstarke Erweiterung im SaaS-Betrieb an. Mit Relution Shield kann ein Road-Warrior-Setup für Endgeräte realisiert werden, das eine sichere und flexible Lösung für den Zugriff auf interne Ressourcen ermöglicht. Dieses Add-on umfasst unter anderem:

- Zertifikatsbasierte Zugriffskontrolle, die hohe Sicherheit bei Endgeräte-Verbindungen garantiert
- Konformitätscheck zur Überprüfung der Sicherheitsparameter von verbundenen Geräten
- Nutzung des Site-to-Site-Tunnels, um auf interne Organisationsressourcen zuzugreifen

Dieses Add-on ist ideal für mobile und remote arbeitende Nutzer, die mit hoher Sicherheit Zugang zur internen Infrastruktur benötigen.

Limits und Quotas

Dieses Kapitel beschreibt die Standardquotas und Limits für das Relution-Cloud-Angebot. Die Werte gelten, sofern nicht anders vereinbart, für alle Mandanten und Bereitstellungsformen.

Kategorie	Shared (`live.relution.io`)	Dedicated Server
Maximale Upload-Größe	1 GB pro Datei	1 GB pro Datei
Storage-Limit	10 GB pro Mandant	100 GB pro Server
Aktionen pro Gerät pro Tag	50 Aktionen (7-Tages-Durchschnitt)	50 Aktionen (7-Tages-Durchschnitt)

Upload-Größe

Für Version 26.4.0

Die maximale Upload-Größe definiert, wie groß eine einzelne Datei sein darf, die in die Cloud hochgeladen wird.

- Auf Shared (`live.relution.io`) beträgt das Limit 1 GB.
- Auf Dedicated Servern beträgt das Limit ebenfalls 1 GB. Auf Anfrage kann dieses Limit erhöht werden.

Überschreitet eine Datei diese Grenze, wird der Upload abgelehnt.

Storage-Limit

Das Storage-Limit definiert die maximal verfügbare Speichermenge für Organisationen bzw. Server

- Auf live.relution.io (Shared) steht jedem Mandanten bis zu 10 GB Speicherplatz zur Verfügung.
- Auf Dedicated Servern steht pro Server bis zu 100 GB Speicherplatz zur Verfügung.

Aktions-Limit pro Gerät pro Tag

Zur Sicherstellung der Systemstabilität ist die Anzahl an Aktionen pro Gerät pro Tag begrenzt.

- Es sind maximal 50 Aktionen pro Gerät pro Tag im 7-Tages-Durchschnitt von der Quota abgedeckt.

Wird das Limit dauerhaft überschritten, kann das System temporäre Sperren oder Drosselungen anwenden.

On-Premises zur Cloud migrieren

Relution-Installationen lassen sich unkompliziert in die Relution Cloud überführen.

Für eine erfolgreiche Migration sind lediglich wenige Schritte zu beachten und spezifische Konfigurationen notwendig.

Voraussetzungen

Für die Migration in die Relution Cloud werden folgende Komponenten benötigt:

- Ein aktueller Dump der Relution-Datenbank
- Das S3-Storage-Bucket, sofern dieses in der bestehenden On-Premises-Installation verwendet wird

Beide Komponenten werden in der Cloud durch das Relution-Infrastrukturteam bereitgestellt.

> Die bisher verwendete URL der Relution-Instanz muss auch nach der Migration auf die neue Cloud-Instanz zeigen – in der Regel durch einen DNS-CNAME-Eintrag auf die neue Zieladresse (z. B. `kundenname.eu.relution.io`).

Für Version 26.4.0

Durchführung

Vor der Migration sollte in jedem Fall der Relution Support kontaktiert werden.

Falls die Migration bereits beauftragt wurde, liegt dem Support-Team in der Regel ein entsprechendes Ticket vor – so kann der Prozess gezielt begleitet werden. Zunächst wird ein SQL-Dump der aktuellen Datenbank erstellt und dem Relution Support bereitgestellt. Anschließend wird die neue Cloud-Instanz eingerichtet und die Datenbank importiert.

Die Dauer hängt von der Größe der Datenbank ab und kann mehrere Stunden betragen. Während oder nach dem Import erfolgt die Konfiguration des DNS-CNAME-Eintrags:

Die bisherige URL (z. B. `relution.kundenname.de`) verweist dann auf die neue Relution Cloud-Instanz (z. B. `kundenname.eu.relution.io`).

Hinweis: Die Endgeräte müssen nach der Migration nicht neu eingeschrieben werden. Der Betrieb läuft ohne Unterbrechung weiter – alle MDM-Profile, Apps und Zertifikate bleiben erhalten.

Zusammenfassung: Schritte zur Migration

1. Kontaktaufnahme mit dem Relution Support
2. Terminvereinbarung für Backup und Umstellung
3. Bereitstellung der Datenbank (und ggf. des S3-Buckets) in Abstimmung mit dem Support. Dieser Schritt kann mit dem Relution Support gemeinsam umgesetzt werden.
4. Konfiguration des DNS-CNAME-Eintrags zur neuen Cloud-Instanz

Backups & Wiederherstellung

Dieser Artikel beschreibt die Backup- und Wiederherstellungs-Maßnahmen für von Relution betriebene Dedicated → Cloud-Instanzen.

> Für selbst gehostete Instanzen liegt die Verantwortung für Backups beim jeweiligen Betreiber.

Relution setzt ein mehrstufiges Sicherungskonzept ein, um die Verfügbarkeit und Integrität der Kundendaten zu gewährleisten. Alle Maßnahmen werden regelmäßig überprüft und weiterentwickelt.

Datenbank

Die Relution-Datenbank wird in einer hochverfügbaren Konfiguration mit automatischer Replikation betrieben. Dadurch ist beim Ausfall einer einzelnen Datenbankinstanz kein Datenverlust zu erwarten. Weitere technische Maßnahmen erkennen und beheben Probleme auf Hardware-Ebene, bevor diese zu Datenverlust führen können.

Darüber hinaus werden Datenbankänderungen kontinuierlich extern gesichert und regelmäßig durch Vollsicherungen ergänzt. Dadurch ist eine Wiederherstellung zu einem beliebigen Zeitpunkt (Point-in-Time Recovery) innerhalb des Aufbewahrungszeitraums von bis zu 90 Tagen möglich.

Nach dem 3-2-1-Prinzip werden die Sicherungen mit zwei voneinander unabhängigen Backup-Methoden erstellt, wobei eine Kopie bei einem unabhängigen Anbieter an einem geografisch getrennten Standort gespeichert wird. Alle Daten werden mit kundenspezifischen Schlüsseln verschlüsselt gespeichert.

Für Version 26.4.0

Objektspeicher

Die Daten im Objektspeicher sind versioniert und können zusammen mit der Datenbank wiederhergestellt werden.

RPO und RTO

Kennzahl	Wert	Erläuterung
RPO (Recovery Point Objective)	≤ 5 Minuten	Im ungünstigsten Fall können bis zu 5 Minuten an Datenbankänderungen verloren gehen.
RTO (Recovery Time Objective)	≤ 3 Stunden (innerhalb der Geschäftszeiten)	Zielzeit für die Wiederherstellung des Dienstes nach einem Ausfall.

Werden Backups getrennt aufbewahrt?

Ja. Die Datenbanksicherungen folgen dem 3-2-1-Prinzip; eine Kopie wird verschlüsselt bei einem unabhängigen Anbieter an einem geografisch getrennten Standort gespeichert.

Kann ich als Kunde eine individuelle Wiederherstellung anfordern?

Für eine Wiederherstellung bitte den Relution Support kontaktieren. Auf Wunsch ist auch eine Wiederherstellung zu einem bestimmten Zeitpunkt (Point-in-Time Recovery) innerhalb des Aufbewahrungszeitraums möglich. Eine Wiederherstellung auf Kundenwunsch ist kostenpflichtig.

Kann der Aufbewahrungszeitraum angepasst werden?

Ja. Der Aufbewahrungszeitraum kann je nach Bedarf (gegen Aufpreis) angepasst werden. Dazu bitte den Relution Support kontaktieren.

Für Version 26.4.0

Welche Daten sind vom Backup abgedeckt?

Die Sicherung umfasst alle persistenten Daten der eigenen Relution-Instanz.

Systemanforderungen

Die folgende Hardware ist für den Betrieb eines Relution-Servers erforderlich:

- 2 CPU Kerne
- 4 GB RAM
- 1 Netzwerkkarte
- 10 GB HDD/SSD
- Zusätzlicher Speicherplatz für Benutzerdaten, Betriebssystem und weitere Anwendungen und Programme

Externer Objektspeicher

Wir empfehlen generell die Verwendung eines externen Ressourcen-Speichers, insbesondere dann wenn:

- Installation und Verwaltung von nativen Apps auf Windows-Geräten
- Bei einer größeren Anzahl nativer Apps oder nativen Apps größer als 50 MB
- Für Server mit mehr als 5.000 Geräten

Relution bietet hierfür die Möglichkeit, einen S3-kompatiblen Objektspeicher anzubinden. Weitere Informationen unter Objektspeicher →

Für Version 26.4.0

Empfohlene Hardware

Je nach Anzahl der verwalteten Geräte empfehlen wir die folgende Hardware Ausstattung:

- Bis zu 150 Geräte
- 150 bis 1.000 Geräte
- 1.000 bis 5.000 Geräte
- 5.000 bis 10.000 Geräte
- 10.000 bis 30.000 Geräte
- 30.000 bis 50.000 Geräte
- 50.000 bis 100.000 Geräte
- 100.000 bis 200.000 Geräte

Betriebssystem

Die folgenden Betriebssysteme werden unterstützt:

- Alma Linux oder Rocky Linux Version 9 oder 10
- Red Hat Enterprise Linux (RHEL) Version 9 und neuer
- Ubuntu Server in der aktuellen LTS-Version

Docker Installation (empfohlen)

- Aktuelle Versionen von Docker und Docker Compose

Native Installation

Die folgende Software wird für den Betrieb eines Relution Servers empfohlen:

- Java 21
  - Empfohlen wird AdoptOpenJDK 21
- NGINX 1.8 oder neuer
- Ein unterstützter Datenbank-Server

Für Version 26.4.0

Unterstützte Datenbanken

Relution unterstützt folgende Datenbank Server:

- PostgreSQL 14.0 oder neuer
- Deprecated: MariaDB 10.11 LTS oder eine neuere LTS Version
  - MariaDB wird noch bis Ende 2027 unterstützt, wir empfehlen die Verwendung von PostgreSQL

Für die Nutzung des Relution Web-Portals ist einer der folgenden Browser in der neuesten Version erforderlich:

- Chrome
- Firefox
- Safari

Verwaltete Geräte und Plattformen

Die folgenden Betriebssystemversionen werden von Relution offiziell unterstützt. Ältere Versionen werden hinsichtlich ihrer Funktionsweise nicht geprüft, und Funktionen und Apps können dort nicht zur Verfügung stehen.

Betriebssystemversionen in End-Of-Life (EOL): Aus Sicherheitsgründen unterstützt Relution generell keine Betriebssystemversionen, die bereits ihr End-Of-Life (EOL) erreicht haben, da dort keine Sicherheitspatches mehr vom Hersteller zur Verfügung gestellt werden.

- Android 10 oder höher
- iOS 18 oder neuer
- iPadOS 18 oder neuer
- tvOS 18 oder neuer
- macOS 14 oder neuer
- visionOS 26 oder neuer
- watchOS 26 oder neuer
- Windows 10 Professional/Education oder neuer

Netzwerk

- Direkte Internetverbindung
- Kein Proxyserver zwischen Relution und dem Internet
- Ein SSL-Zertifikat von einer vertrauenswürdigen CA
  - Traefik bezieht in der Relution Standardkonfiguration ein Lets Encrypt Zertifikat über Port 80

Internetzugang

Für Version 26.4.0

Die folgenden Ports müssen auf der Firewall für eingehende und ausgehende Verbindungen vom/zum Internet geöffnet werden.

Port	Typ	Richtung	Quelle	Erforderlich	Beschreibung
80	TCP	Eingehend	Alle	Ja	Umleitung zu HTTPS
443	TCP	Eingehend	Alle	Ja	Für Internetzugang und Client-zu-Server-Kommunikation
7800	TCP	Ein-/Ausgehend	Cluster-Knoten	Ja	Notwendig für die Kommunikation zwischen den Cluster Knoten
8099	TCP	Eingehend	Lokales Netzwerk	Nein	Notwendig für Health Status Monitoring
2197	TCP	Ein-/Ausgehend	Verbunden/Eingerichtet	Nein[1]	Apple Push Notification Services (APNS)
443	TCP	Ausgehend	-	Ja	z.B. SMS-Service, Lizenz-Server, VPP, DEP, …
123	UDP	Ausgehend	-	Ja	NTP (Zeitserver)

[1] Benötigt zur Kommunikation zwischen iOS Geräten und den Apple Push Notification Services (APNS) bis zu Relution 4.70. In späteren Versionen als Fallback benötigt.

Apple Netzwerk Anforderungen

Firewall Unterstützt die Firewall Hostnamen, können die meisten der oben genannten Apple-Dienste über ausgehende Verbindungen zu `*.apple.com` freigegeben werden. Lässt sich die Firewall nur über IP-Adressen konfigurieren, sind je nach IP-Version ausgehende Verbindungen zu den folgenden IP-Adressbereichen von Apple freizugeben.

```
Für IPv4: ausgehende Verbindungen zu 17.0.0.0/8.
Für IPv6: ausgehende Verbindungen zu diesen Netzbereichen:
2403:300::/32
2620:149::/32
2a01:b740::/32
```

HTTP-Proxy Apple-Dienste können über einen Proxy genutzt werden, wenn Paket-Inspektion und Authentifizierung für den Datenverkehr von und zu den aufgeführten Hosts deaktiviert sind. Ausnahmen davon sind oben vermerkt. Versuche, verschlüsselte Kommunikation zwischen Apple-Geräten und Apple-Diensten per Content-Inspektion zu analysieren, führen zum Abbruch der Verbindung, um Plattformsicherheit und Datenschutz zu wahren.

Apple Netzwerk Anforderungen →

Für Version 26.4.0

Google Netzwerk Anforderung

Google Netzwerk Anforderung →

Microsoft Windows WNS Firewall Anforderung

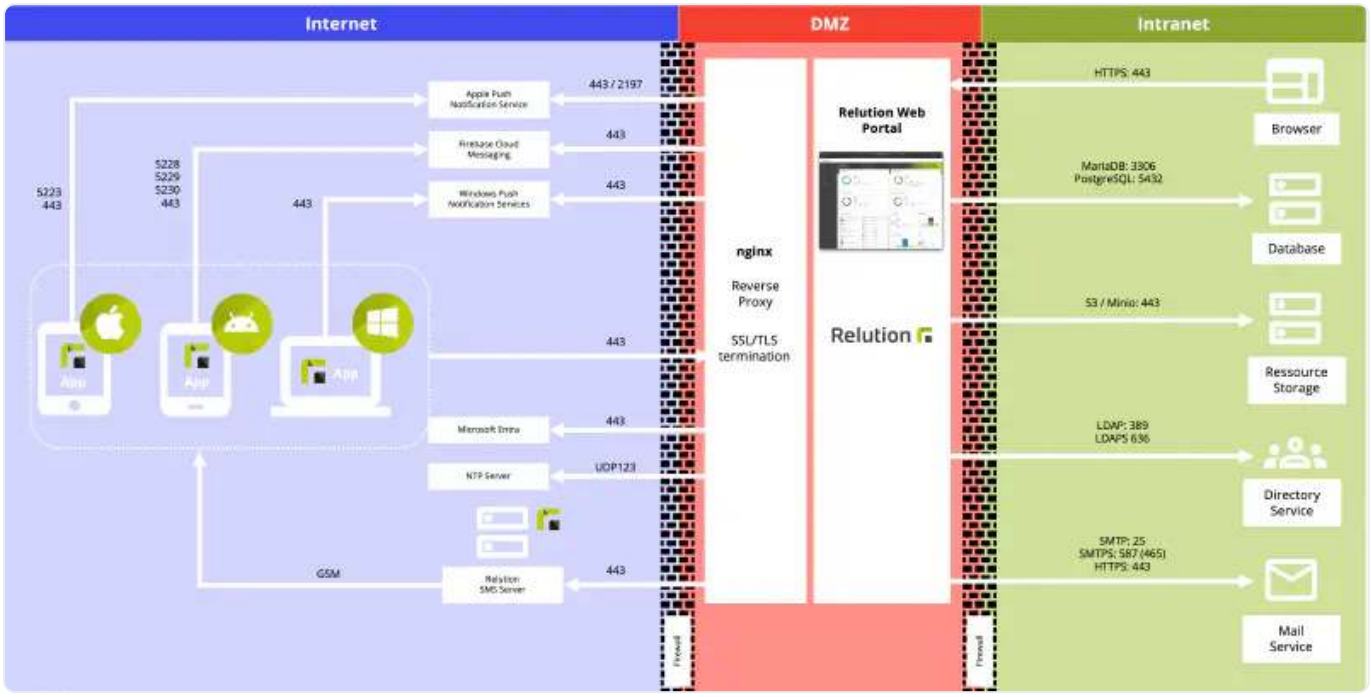
Windows WNS Anforderung →

Internes Netzwerk

Der Relution Dienst verwendet diese Ports zur Kommunikation mit externen Diensten (Datenbank, Verzeichnisdienst, Mail-Server). Die genaue Konfiguration hängt davon ab, welche Dienste verwendet werden und ob die Dienste auf separaten Servern laufen (empfohlen).

Wenn sich die Server im selben Netzwerk befinden, sollte keine zusätzliche Firewall-Konfiguration erforderlich sein. Alle Ports sind TCP.

Port	Beschreibung
25	Mail-Server (SMTP)
389	Verzeichnisdienst (LDAP)
587	Mail Server (SMTPS)
636	Verzeichnisdienst (LDAPS)
3306	MariaDB/MySQL
5432	PostgreSQL



Mobile Geräte

Wenn mobile Geräte mit einem internen Netzwerk verbunden sind, müssen *zusätzliche* eingehende und ausgehende Ports geöffnet werden, damit die Geräte eine Verbindung zu den Apple-, Microsoft- oder Google-Servern aufbauen können, um Push-Nachrichten zu empfangen. Für die Kommunikation mit Relution ist der Standard-HTTPS-Port 443 erforderlich. Je nach Funktionsumfang, das auf den Geräten verwendet wird, sind weitere Ports notwendig, die in der Dokumentation des Herstellers vorgegeben sind. Wenn die Geräte mit mobilen Daten verbunden sind, sollte keine zusätzliche Konfiguration erforderlich sein.

Weiterführende Links:

- Apple-Produkte in Unternehmensnetzwerken verwenden →
- Von Apple-Softwareprodukten verwendete TCP- und UDP-Ports →
- Apple technotes →
- Apple Classroom →
- Firebase Cloud Messaging →
- Firebase Cloud Messaging ASN of 15169 →

Port	Typ	Richtung	Beschreibung
443	TCP	Ausgehend	HTTPS, z.B. Relution, Google FCM, Microsoft WNS, Apple Push Notification Service,…
443	UDP	Ausgehend	QUIC, z.B. iCloud Private Relay, Google services
5223	TCP	Eingehend/Ausgehend	Apple Push Notification Service[1]
5228-5230	TCP	Ausgehend	Google Firebase Cloud - Firebase Cloud Messaging (FCM)
3283	TCP	Eingehend/Ausgehend	Apple Remote Desktop (z.B. Apple Classroom App)
3283	UDP	Eingehend/Ausgehend	Apple Remote Desktop (z.B. Apple Classroom App)
3284	TCP	Eingehend/Ausgehend	Apple Classroom Document Sharing
3285	TCP	Eingehend/Ausgehend	Apple Classroom App

Für ve

Vor der Installation

Vor Beginn der Installation empfiehlt es sich, diese Checkliste durchzugehen, um zu überprüfen, ob die eigene Infrastruktur die Mindestanforderungen erfüllt und korrekt konfiguriert ist.

Es ist es möglich, mehrere Dienste auf einem Rechner zu hosten (aus Sicherheitsgründen empfehlen wir, jeden Dienst auf einem separaten Server zu hosten).
Zum Beispiel: Wenn Relution und der Reverse Proxy `nginx` auf demselben Rechner installiert sind, beziehen sich `der Server, auf dem Relution läuft` und `der Server, auf dem nginx` auf denselben physischen Rechner. In diesem Fall muss der Server die Anforderungen beider Dienste erfüllen.

Hardware

Der Server, auf dem Relution läuft, erfüllt oder übertrifft die folgenden Mindestanforderungen →.

Betriebssystem

Der Server, auf dem Relution läuft, verwendet ein empfohlenes Betriebssystem → und die Version des Betriebssystems entspricht oder übertrifft die minimal unterstützte Version.

Für Version 26.4.0

Datenbank

Der Server, auf dem Relution läuft, hat Netzwerkzugang zu einem unterstützten Datenbank-Server →.
Diese Anleitung enthält Anweisungen zur Installation von MariaDB, falls ein neuer Datenbankserver installiert werden muss.

Netzwerkinfrastruktur

Der Server, auf dem der Reverse-Proxy `nginx` läuft, ist so eingerichtet, dass er einen im Internet verfügbaren Dienst hosten kann. Er hat eine öffentliche IP-Adresse und einen öffentlichen DNS Namen z. B. `mdm.example.com`. Wenn Dienste auf mehreren internen Servern gehostet werden, können sie ihre Hostnamen gegenseitig auflösen.

Die öffentliche IP-Adresse muss statisch sein. Dynamische IP-Adressen werden nicht unterstützt. Ausnahmen: Der Server wird von einem Cloud-Anbieter gehostet, wie Amazon Web Services (AWS) oder Microsoft Azure, die die notwendige DNS-Infrastruktur bereitstellen.

Anforderung

- Server hat direkten Zugriff ins Internet
- Server hat eine statische IP Adresse
- Server hat einen öffentlichen DNS Namen
- Das interne DNS ist richtig konfiguriert und funktioniert.

Firewall Konfiguration

Die Firewall ist so eingerichtet, dass sie eingehende HTTP(S)-Anfragen von mobilen Geräten und Webbrowsern entgegennimmt.

Anforderung

- Der Reverse-Proxy ist über HTTP (80) aus dem Internet erreichbar
- Der Reverse-Proxy ist über HTTPS (443) aus dem Internet erreichbar
- Relution kann sich mit dem Internet verbinden (80, 443, 5223, UDP 123)
- Relution kann sich mit dem SMTP-Server verbinden
- Relution kann sich mit dem Datenbankserver verbinden
  Optional:
- Relution kann sich mit LDAP über Port 389 oder 636 verbinden

Für Version 26.4.0

Zertifikate

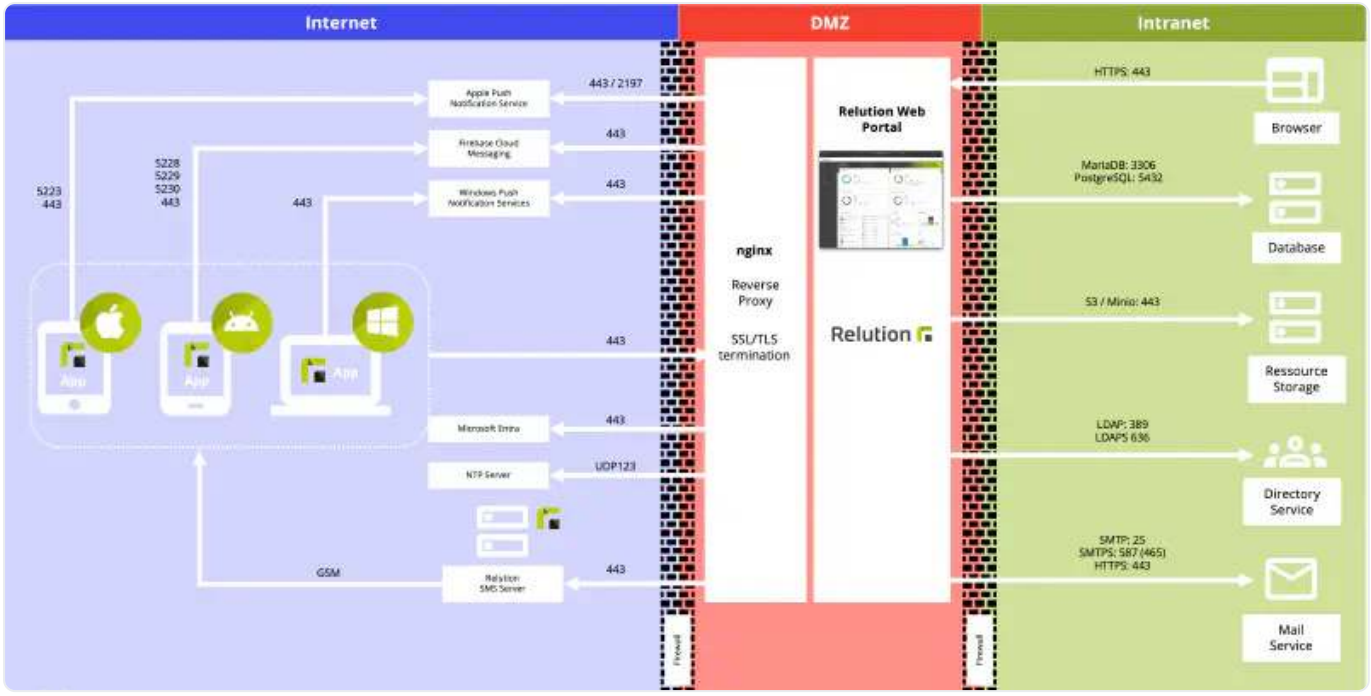
Für HTTPS wird ein gültiges SSL-Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle (CA) benötigt.

- Selbstsignierte Zertifikate funktionieren nicht, weil mobile Geräte ihnen im Allgemeinen nicht trauen.
- Zertifikate von Let's Encrypt → funktionieren und sind kostenlos

Auf W3Techs → findet sich eine Liste bekannter Zertifizierungsstellen auf der Grundlage von Marktanteil und Nutzung.

Anforderung	Erfüllt
Ein gültiges SSL-Zertifikat und ein gültiger Schlüssel liegen vor	

Relution wird mit einem gültigen APNS-Zertifikat ausgeliefert, dass verwendet wird. In diesem Fall wird das Zertifikat mit dem Update von Relution ebenfalls aktualisiert. Die automatische Aktualisierung findet bei der Nutzung eigener APNS-Zertifikate nicht statt und muss selbstständig verantwortet werden.



Für Version 26.4.0

Docker (empfohlen)

Die Anleitung gilt für Rocky / Alma Linux 9 und 10 sowie Ubuntu Server (aktuelle LTS-Version).
Wir empfehlen die Verwendung von Linux für das Hostsystem.

Diese Anleitung behandelt die Installation und Konfiguration einer grundlegenden Relution Instanz, die in Docker-Containern ausgeführt wird.

Voraussetzungen

Vor dem Beginn sicherstellen, dass folgende Punkte erfüllt sind:

- Der Host-Rechner sich mit dem Internet verbinden kann.
- Über `root` oder `sudo` Rechte verfügen.
- Optional: Ein gültiges SSL Zertifikat für die URL.

> Selbst signierte Zertifikate funktionieren nicht, da mobile Geräte ihnen nicht vertrauen. Das manuelle Installieren des Root-Zertifikats auf einem Gerät ist zwar möglich, aufgrund des hohen Aufwands aber nicht empfohlen. Zertifikate von Let's Encrypt → sind getestet und funktionieren.

Für Version 26.4.0

Vorbereitung

Bei Vertrautheit mit `vim` lässt sich dieser als Standardeditor festlegen. Bei Verwendung des Standardeditors kann dieser Abschnitt übersprungen werden.

```
sudo dnf install -y vim
sudo update-alternatives --install /usr/bin/editor editor /usr/bin/vim 100
```

Ablauf der Installation

Die Installation gliedert sich in folgende Hauptschritte:

1. Docker und Docker Compose installieren.
2. Container konfigurieren.
3. Traefik oder nginx konfigurieren.

Docker und Docker Compose installieren

Um Relution in einem Docker Container zu betreiben, müssen vorher `Docker` und `docker compose` installiert werden.

Docker installieren

Für Alma / Rocky Linux gelten folgende Befehle:

```
dnf install -y dnf-utils wget
yum-config-manager --add-repo https://download.docker.com/linux/centos/docker-ce.repo
dnf install -y docker-ce docker-ce-cli containerd.io docker-compose-plugin
```

Für Ubuntu Server gelten folgende Befehle (Docker-Repository laut Docker-Dokumentation →):

```
apt-get update
apt-get install -y ca-certificates curl
install -m 0755 -d /etc/apt/keyrings
curl -fsSL https://download.docker.com/linux/ubuntu/gpg -o /etc/apt/keyrings/docker.asc
chmod a+r /etc/apt/keyrings/docker.asc
echo "deb [arch=$(dpkg --print-architecture) signed-by=/etc/apt/keyrings/docker.asc]
https://download.docker.com/linux/ubuntu $(. /etc/os-release && echo
"$VERSION_CODENAME") stable" > /etc/apt/sources.list.d/docker.list
apt-get update
apt-get install -y docker-ce docker-ce-cli containerd.io docker-compose-plugin
```

Sicherstellen, dass der Docker-Dienst nach der Installation gestartet und aktiviert wird, damit er nach einem Systemneustart verfügbar ist.

```
systemctl enable docker
systemctl start docker
```

Auf den Minimal- und Cloud-Images von RHEL, AlmaLinux und Rocky Linux 10 (EL10) fehlt das Paket `kernel-modules-extra`, wodurch der Docker-Dienst nicht startet. In diesem Fall vor dem ersten Start von Docker die Schritte unter Docker startet nicht auf EL10 → ausführen. Auf EL9 ist dies nicht erforderlich.

Container konfigurieren

Ein Verzeichnis für Relution-Konfigurationsdateien erstellen, z.b. für `docker compose`.

```
mkdir -p /opt/relution
mkdir /opt/relution/secrets
```

Vorbereitung Passwörter

Für die Passwörter sichere Zufallspasswörter verwenden (z. B. mit `pwgen -snc 48 1`).

Die folgenden Dateien erzeugen:

Platzhalter	Inhalt
`/opt/relution/secrets/postgres_password`	Das Passwort des Relution-Datenbank-Benutzers
`/opt/relution/secrets/system_admin_password`	Das initiale Passwort des Systemadministrator. Nach dem ersten Login ändern.

compose.yaml

Die Datei herunterladen:

```
compose.yaml
```

```
wget https://raw.githubusercontent.com/relution-io/relution-setup/master/docker/Linux/opt/relution/compose.yaml \
    --directory-prefix=/opt/relution
```

Die Compose-Datei definiert drei Dienste: `database`, `relution` und `traefik`.

application.yml

Die Datei herunterladen:

```
application.yml
```

```
wget https://raw.githubusercontent.com/relution-io/relution-setup/master/docker/Linux/opt/relution/application.yml \
    --directory-prefix=/opt/relution
```

Die Datei bearbeiten:

```
vim /opt/relution/application.yml
```

Die Datei an die eigene Umgebung anpassen. Dabei müssen die folgenden Platzhalter ersetzt werden:

Version 26.4.0

Platzhalter	Beschreibung
`%EXT_HOSTNAME_URL%`	Die externe Adresse des Relution-Servers, z.B. `https://mdm.example.com`
`%SYSTEM_ADMIN_EMAIL%`	Die Mailadresse des Systemadministrators

Die Standard Konfiguration bildet die Datenverzeichnisse von PostgreSQL auf das Host System ab. Relution speichert alle seine Daten in der Datenbank, so dass keine zusätzliche Konfiguration erforderlich ist. Sicherstellen, dass PostgreSQL in die eigene Backup-Strategie einbezogen wird.

Konfiguration von Traefik (Reverse Proxy)

Traefik wird als Reverse Proxy verwendet, um den Zugriff auf Relution zu ermöglichen und gleichzeitig SSL/TLS-Verschlüsselung bereitzustellen. Ohne Traefik oder einen ähnlichen Proxy ist der Zugriff auf Relution nur lokal über localhost möglich.

Automatische Zertifikatserstellung (Let’s Encrypt)

Die Traefik-Konfigurationsdatei herunterladen und an die eigene Umgebung anpassen:

relution.yaml

```
wget https://raw.githubusercontent.com/relution-io/relution-
setup/master/docker/Linux/opt/relution/relution.yaml \
    --directory-prefix=/opt/relution/configs/traefik
```

In der Datei `/opt/relution/configs/traefik/relution.yaml` muss der Platzhalter `external.url` durch die tatsächliche externe URL ersetzt werden:

```
vim /opt/relution/configs/traefik/relution.yaml
```

relution.yaml

```yaml
http:
  routers:
    relution:
      rule: Host(`external.url`) # Platzhalter ersetzen
```

Die Angabe der External URL erfolgt hier, anders als in der application.yml, ohne vorangeführtem `https://`.

Optional

- Traefik - statische Zertifikate
- Nginx alternativ zu Traefik (Reverse Proxy)

Relution starten

In das Relution-Verzeichnis wechseln und die Docker-Container starten:

```
cd /opt/relution/
docker compose up -d
```

Dadurch werden die Images heruntergeladen und die Dienste gestartet. Es kann einige Zeit dauern, bis die Dienste verfügbar sind.

Um die Log-Ausgabe eines bestimmten Containers zu sehen (z.B. Relution):

```
docker logs -f <container_name> # Beispiel: docker logs -f relution
```

Für Version 26.4.0

SSL Zertifikate - Certbot

Certbot ist eine kostenlose Lösung zur Ausstellung von SSL/TLS-Zertifikaten über Let's Encrypt, die eine sichere HTTPS-Verbindung für Websites ermöglicht. Im Vergleich zu kostenpflichtigen Anbietern, die oft zusätzliche Verwaltungsaufwände und wiederkehrende Kosten mit sich bringen, bietet Certbot eine automatisierte, kostenlose Alternative, die die Verwaltung von Zertifikaten vereinfacht und laufende Erneuerungen übernimmt.

Einrichtung

Es wird empfohlen Certbot → nativ auf dem Host zu installieren, einmalig Zertifikate darüber zu beziehen und als Volume in den nginx-Container einzubinden.

1. Certbot installieren

Voraussetzung
→ ALMA / Rocky Linux oder Ubuntu Server als Host
→ Docker nach Anleitung installiert
→ Relution nach Anleitung konfiguriert

Certbot wird unter Alma / Rocky Linux mit folgendem Befehl installiert:

Version 26.4.0

```
sudo dnf install epel-release -y
sudo dnf install certbot -y
```

Unter Ubuntu Server:

```
sudo apt-get update
sudo apt-get install -y certbot
```

2. Nginx stoppen

Nginx muss temporär gestoppt werden, da Certbot im `--standalone` Modus kurzzeitig einen eigenen Webserver auf Port 80 startet.

```
docker stop docker_nginx
```

3. Zertifikat erstellen

Certbot starten und dem Assistenen folgen.

```
sudo certbot certonly --standalone -d example.com
```

4. Zertifikat Pfad anpassen

In der `docker-compose.yml` muss der Pfad zu den erstellten SSL Zertifikaten angepasst werden.

```
services:
  nginx:
    …
    volumes:
     - '/etc/letsencrypt/live/<example.com>/fullchain.pem:/etc/nginx/server.pem'
     - '/etc/letsencrypt/live/<example.com>/privkey.pem:/etc/nginx/server.key'
```

Wenn Nginx mit den Volumes (Pfad zu den Zertifikaten) in der docker-compose.yml gestartet wurde und die Zertifikate nicht vorhanden sind, erstellt Docker Ordner anstelle der Dateien. Diese Ordner müssen gelöscht werden, damit die Zertifikate beim Start von Docker erstellt werden können.

Für Version 26

5. Docker Container starten

Sind die Zertifikate erfolgreich erstellt können alle Container gestartet und geprüft werden

```
docker compose up --detach
docker ps
```

6. Pre- und Post-Hooks

Für die Erneuerung können im Certbot Pre- und Post-Hooks konfiguriert werden, die den nginx-Container stoppen und danach wieder starten. Die Hooks werden nur ausgeführt, wenn Certbot beim Renwal-Aufruf feststellt, dass die Zertifikate tatsächlich ausgetauscht werden müssen. Certbot ist üblicherweise so konfiguriert, dass es zweimal am Tag läuft und prüft, ob ein Austausch notwendig ist. Die Zertifikate sind 90 Tage lang gültig.

Je nach Hostsystem sollte Certbot bereits automatisch eine Erneuerung einrichten (z.B. als systemd Service + Timer). Der Aufruf dort kann dann entsprechend um diese Hooks erweitert werden, z.B.

```
ExecStart=/usr/bin/certbot [--dry-run] -q renew --pre-hook "…" --post-hook "…"
```

Pre- und Post-Hook wären dann entsprechend:

```
--pre-hook "/usr/bin/docker compose -f /opt/relution/docker-compose.yml down nginx"
--post-hook "/usr/bin/docker compose -f /opt/relution/docker-compose.yml up --detach
nginx"
```

Die Hooks können auch auf Skriptdateien verweisen, die den eigentlichen Aufruf enthalten, was in der Regel übersichtlicher ist.

Beim ersten Ausprobieren sollte immer `--dry-run` verwendet werden, damit Let's Encrypt nicht durch zu viele Fehlversuche für mehrere Tage blockiert wird. Im produktiven Betrieb muss das natürlich weg, sonst gibt es kein Zertifikat.

Für Version 26.4.0

Docker - 1000 bis 5000 Geräte

Für eine Geräteanzahl im Bereich von 1000 bis 5000 wird empholen, den Applikations- und den Datenbankserver separat zu betreiben.

Die grundlegende Einrichtung der Server sowie die Installation der erforderlichen Softwarepakete sind detailliert in der Allgemeinen Docker Installationsanleitung → beschrieben.

Diese Anleitung beschreibt die notwendigen Konfigurationsdateien mit erläuternden Kommentaren, die die Anpassung erleichtern, und ist ergänzend zur allgemeinen Docker Installationsanleitung.

Hardware Anforderung und Aufbau

1x Anwendungsserver

- 2 CPU Kerne
- 4 GB RAM
- Etwa 30 GB SSD Speicherplatz

1x Datenbankserver

- 4 CPU Kerne
- 8 GB RAM
- Etwa 100 GB SSD Speicherplatz

Für Version 26.4.0

App Server

Für den Anwendungsserver werden die folgenden beiden Dateien benötigt.

compose.yaml

```yaml
services:
  relution:
    image: relution/relution:latest
    restart: unless-stopped
    container_name: relution
    environment:
      TZ: "Europe/Berlin"
    expose:
      - "8080"
      - "8099"
    ports: # Extern freigegebener Port der Applikation zum testen // deaktivieren
sobald der Server unter der URL erreichbar ist
      - "8080:8080" # Extern freigegebener Port der Applikation zum testen //
deaktivieren sobald der Server unter der URL erreichbar ist
    volumes:
      - "./application.yml:/opt/relution/application.yml"

networks:
  relution-network:
```

application.yml

Für Version 26.

```yaml
relution:
  system:
    admin:
      password: $Platzhalter # Initiales Passwort hier setzen und nach der ersten
Anmeldung im Portal ändern !
      email: $Platzhalter # Alternative zum Benutzernamen "Admin" und zum zurücksetzen
des Passworts
  server:
    externalURL: https://$Platzhalter # Ersetzen durch die URL unter der der Server
erreichbar sein wird. Beginnt immer mit https://
  database:
    type: postgresql
    url: jdbc:postgresql://$Platzhalter:5432/relution?currentSchema=public # IP, FQDN
oder URL des Datenbankservers mit Portangabe. Der Port wird auf DB Seite  weiter in der
Anleitung konfiguriert.
    username: relution # Benutzername der Datenbank
    password: $Platzhalter # Passwort der relution Datenbank = POSTGRES_PASSWORD
```

Das Passwort aus der application.yml wird folgend noch einmal bei der Datenbank Konfiguration in der compose.yaml benötigt.

DB Server

Für den Datenbankserver wird eine eigene Compose-Datei verwendet.

compose.yaml

```yaml
services:
  database:
    image: postgres:18
    restart: unless-stopped
    container_name: database
    environment:
      TZ: "Europe/Berlin"
      POSTGRES_DB: "relution"
      POSTGRES_USER: "relution"
      POSTGRES_PASSWORD: "$Platzhalter" # Passwort der relution Datenbank
    expose:
      - "5432"
    ports: # extern freigegebener Port der Datenbank, der Applikation Server muss diese
erreichen können
      - "5432:5432" # extern freigegebener Port der Datenbank, der Applikation Server
muss diese erreichen können
    volumes:
      - 'postgresql:/var/lib/postgresql'

volumes:
  postgresql:

networks:
  relution-network:
```

Monitoring mit Grafana

Relution bietet eine Vielzahl von Metriken, die mittels Grafana visualisiert werden können. Im Folgenden haben wir eine Basiskonfiguration für ein Docker-Setup sowie zwei Dashboards bereitgestellt. Diese Konfigurationen können nach eigenen Bedürfnissen angepasst werden.

Prometheus, Grafana und die einzelnen Dashboards werden nicht vom Relution-Support betreut.

Prometheus-Metriken in Relution aktivieren

Seit Relution 26.4 stellt Relution aus Sicherheitsgründen standardmäßig nur den Health-Endpoint bereit; der Prometheus-Endpoint (`/actuator/prometheus`) ist deaktiviert. Damit die Metriken abgerufen werden können, muss die Konfigurationsdatei `application.yml` des Relution-Servers um folgenden Abschnitt ergänzt werden:

```
management:
  endpoints:
    web:
      exposure:
        include:
          - health
          - prometheus
```

Nach der Anpassung ist ein Neustart des Relution-Servers erforderlich, damit die Änderung wirksam wird.

Konfiguration lokaler Service

Diese Konfiguration implementiert Prometheus und Grafana in ein on Premises betriebenes Relution Setup in einer Docker Umgebung. Soll ein Server überwacht werden, auf den beispielsweise kein direkter Zugriff besteht, ist die Konfiguration weiter unten zu finden.

Notwendige Dateien und Verzeichnisse

Wie erwähnt, sind die Konfigurationen verfügbar und können hier → heruntergeladen und verwendet werden.

Dateien

- `docker-compose.yml`
  - Beinhaltet die Konfigurationen der Docker Container `Prometheus` und `Grafana`.
- `prometheus.yml`
  - Beinhaltet die Konfiguration von `Prometheus`.
- `.env`
  - Hier sind die Variablen `GF_SECURITY_ADMIN_USER` und `GF_SECURITY_ADMIN_PASSWORD` enthalten. Für den Produktivbetrieb ist es empfehlenswert, das Passwort zu ändern.

Subfolder

- Dashboards Beispieldashboards: Die Konfigurationsdateien für zwei Beispieldashboards sind enthalten. Diese Dashboards werden automatisch in den Grafana Docker Container importiert.

- Provisioning Basiskonfigurationen: Die Konfigurationsdateien für die Datenquelle Prometheus und die beiden Beispieldashboards sind enthalten. Diese Konfigurationen können nach Bedarf angepasst werden.

Einbindung der docker-compose.yml

Die hier beschriebene `docker-compose.yml` kann auf zwei Arten verwendet werden:

- Standalone Die Datei kann als eigenständige Datei benutzt werden.

- Inhaltlich Der Inhalt der Datei kann in eine bestehende `docker-compose.yml` eingebunden werden.

Für Version 26.4.0

In unserem Beispiel wird der Inhalt der Datei in die bestehende `docker-compose.yml` eingebunden. In diesem Fall ist es wichtig, dass die Dateien und Verzeichnisse der Volumes an der entsprechenden Stelle liegen und die korrekten Berechtigungen haben. In unserer verwendeten `docker-compose.yml` sind die Container `mariadb`, `relution` und `nginx` vorhanden, deshalb sind die Zeilen zwei bis vier lediglich zur Orientierung eingefügt worden.

> Vollständiges Konfigurationsbeispiel anzeigen

In der `docker-compose.yml` sind die Ports für Prometheus und Grafana auf 9090 bzw. 3000 festgelegt. Dieser Abschnitt kann für das Beispiel in die vorhandene `docker-compose.yml` eingefügt werden.

Anpassung der .env Datei

Für die Sicherheit ist es empfehlenswert, den Parameter für das Kennwort anzupassen.

```
GF_SECURITY_ADMIN_USER=admin
GF_SECURITY_ADMIN_PASSWORD=password
```

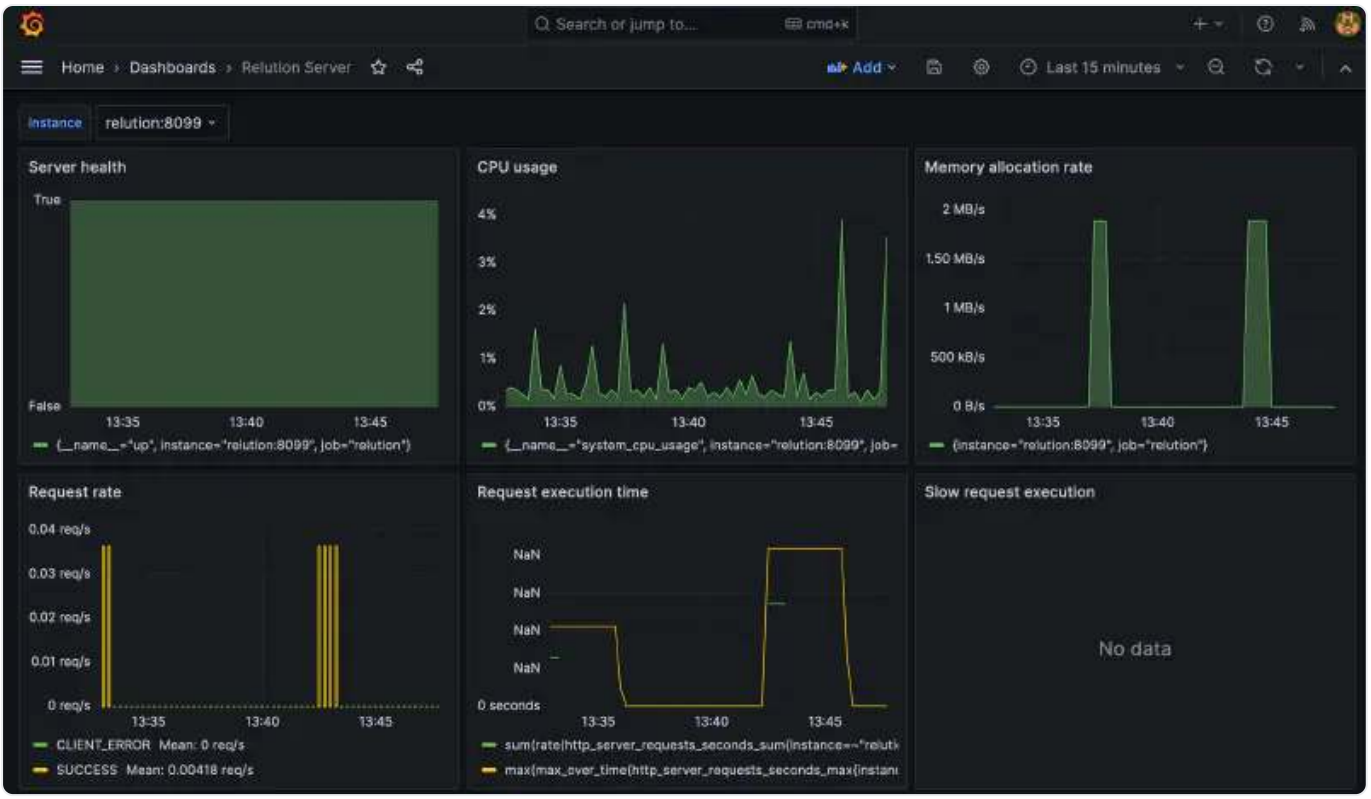
Anpassungen der prometheus.yml Datei

```
global:
 # Default scrape interval
  scrape_interval: 15s

scrape_configs:
 # Job to scrape Prometheus metrics
  - job_name: "prometheus"
    scrape_interval: 5s
    static_configs:
      - targets: ["localhost:9090"]

  - job_name: "relution"
 # Job to scrape application metrics
    metrics_path: "/actuator/prometheus"
    scrape_interval: 5s
    static_configs:
 # Call the docker host inside container
      - targets: ["relution:8099"]
```

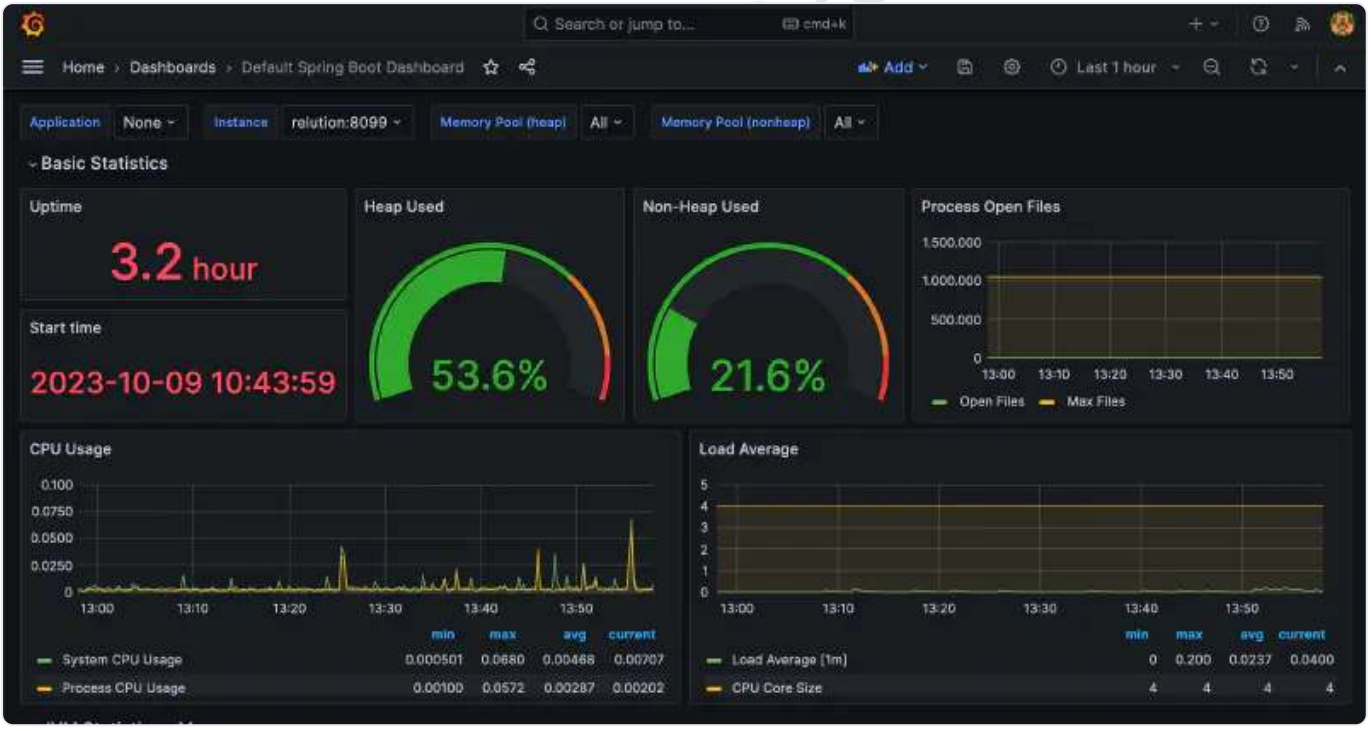
In unserem konkreten Setup müssen in der letzten Zeile der Name und der Port des Containers, in diesem Fall `relution:8099`, stehen. Mit dem Befehl `docker ps` kann der Name und der Port des genutzten Containers geprüft und anschließend bei Bedarf angepasst werden. Wenn die Container mit `docker compose down` bzw. `docker compose up -d` heruntergefahren und gestartet werden, ist die Grafana UI unter der IP des Servers auf Port 3000 erreichbar. Es stehen nun zwei Dashboards zur Verfügung.

Dashboards

Relution Server Dashboard:



Standard Spring Boot Dashboard:



Konfiguration für Remote-Server

Grafana wird in diesem Szenario ebenfalls in einem Docker-Container betrieben. Um Metriken korrekt auslesen zu können, sind spezifische Anpassungen notwendig. Der wesentliche Unterschied zur lokalen Konfiguration besteht darin, dass dieses Setup über HTTPS mit der Relution-Instanz kommuniziert.

Vorbereitung in Relution

Bevor die Container gestartet werden, muss ein entsprechender Benutzer in Relution existieren:

- Organisation: Der User muss zwingend in der Global Organisation angelegt werden.
- Berechtigung: Dem User die Berechtigung Health Check (bzw. Systemzustand) zuweisen.
- Authentifizierung: Der Zugriff muss über Basic Authentication erfolgen.
- Benutzerkonten mit OIDC (Single Sign-On) funktionieren für diesen Zweck nicht.
- Multi-Faktor-Authentifizierung (MFA) muss für diesen Account deaktiviert sein.

Download und Entpacken

Die vorbereiteten Konfigurationsdateien herunterladen:
Grafana Setup herunterladen →

Das Archiv in ein Verzeichnis der eigenen Wahl auf dem Zielserver entpacken.

Für Version 26.4.0

Anpassung der Konfigurationsdateien

Datei: compose.yml

Die Umgebungsvariablen für den administrativen Zugriff auf die Grafana-Oberfläche anpassen:

- `GF_SECURITY_ADMIN_USER`: Gewünschter Administrator-Benutzername.
- `GF_SECURITY_ADMIN_PASSWORD`: Ein sicheres Passwort für den Grafana-Login.

Datei: prometheus.yml

In dieser Datei wird die Verbindung zur Relution-Schnittstelle definiert. Die Platzhalter durch die spezifischen Daten ersetzen:

Parameter	Beschreibung
`$SERVER_URL`	Die externe URL des Relution-Servers (wichtig: ohne das Präfix `https://`).
`username`	Der Benutzername des unter Vorbereitung in Relution erstellten Users.
`password`	Das zugehörige Passwort des Users.

Deployment

Sobald die Konfiguration abgeschlossen ist, können die Container gestartet werden. Dazu folgenden Befehl im Verzeichnis ausführen:

```
docker compose up -d
```

Hinweise zum Zugriff:

- Grafana ist standardmäßig über den Port 3000 erreichbar.
- Der Zugriff kann je nach Server-Härtung direkt über die IP/Domain oder gesichert über einen SSH-Tunnel erfolgen.

Um den Zugriff auf Grafana sicher über einen SSH-Tunnel zu realisieren, kann die Port-Weiterleitung genutzt werden. Dies ist besonders sinnvoll, wenn Port 3000 in der Firewall des Servers nach außen hin geschlossen ist.

SSH-Tunnel aufbauen

Den folgenden Befehl im lokalen Terminal (Windows PowerShell, macOS oder Linux) ausführen:

```
ssh -L 3000:localhost:3000 benutzername@ihr-server-ip
```

Erläuterung der Parameter:

- `-L 3000:localhost:3000`: Dies leitet den Port 3000 des lokalen Rechners an den Port 3000 des Remote-Servers weiter.
- `benutzername`: SSH-User auf dem Server.
- `ihr-server-ip`: Die IP-Adresse oder der Hostname des Remote-Servers.

Zugriff auf die Oberfläche

1. Das Terminalfenster mit der aktiven SSH-Verbindung geöffnet lassen.
2. Den Webbrowser öffnen.
3. In die Adresszeile eingeben: `http://localhost:3000`
4. Sich mit den Zugangsdaten anmelden, die in der `compose.yml` unter `GF_SECURITY_ADMIN_USER` und `GF_SECURITY_ADMIN_PASSWORD` definiert wurden.

Relution Files Bridge

Die App Relution Files für iOS und Android kann auf SMB- und WebDAV Freigaben zugreifen. Die Relution Files Bridge bietet die Möglichkeit SMB bzw. DFS Freigaben als WebDAV bereit zu stellen. Die Relution Files Bridge kann bequem als Docker Container betrieben werden.

Installation

Auf dem Server, der als Relution Files Bridge genutzt werden soll, im Verzeichnis `/opt/rfb` eine `compose.yaml`-Datei anlegen und folgenden Inhalt einfügen

```
services:
  relution-smb-bridge:
 # Aktuelle Versionsnummer auf https://hub.docker.com prüfen
    image: relution/relution-smb-bridge:1.0.1
    restart: unless-stopped
    ports:
      - '8080:8080'
    environment:
      TZ: "Europe/Berlin"
```

Betrieb mit https

Soll die Verbindung zudem über https hergestellt werden, lässt sich ein Reverse Proxy vor die Files Bridge stellen. Diese kann ebenfalls über die gleiche `compose.yaml`-Datei betrieben werden. Im Beispiel wird ein Traefik verwendet.

Die Datei müsste in diesem Fall so aussehen:

> Vollständiges Konfigurationsbeispiel anzeigen

Als Konfigurationsdatei für den Traefik die gleiche Datei wie für den Relution-Betrieb nutzen und entsprechend anpassen:

```
wget https://raw.githubusercontent.com/relution-io/relution-
setup/master/docker/Linux/opt/relution/relution.yaml \
    --directory-prefix=/opt/rfb/configs/traefik
```

Zeile 4 mit der externen Adresse und Zeile 15 mit dem Namen des Containers `relution-smb-bridge` entsprechend anpassen.

Start und Betrieb

Die Container starten mit:

```
docker compose up -d
```

Zugriff auf die Freigabe

Hat die DFS Freigabe einen Pfad genutzt, der `smb://mein-fileserver.intra/data` hatte, muss in Relution Files die Konfiguration wie folgt aussehen:

1. Name: Frei wählbar
2. Protokoll: WebDAV
3. Pfad: https://adresse-des-relution-files-bridge-servers/mein-fileserver.intra/data
4. Benutzername: Domäne\Username
5. Passwort

Die Relution Files Bridge wird dann die Anfrage, die als WebDAV Anfrage eingeht, als SMB- / DFS-Anfrage an den Server weiterleiten.

Für Version 26.4.0

HA Cluster (Advanced)

Die Installation von Relution in einer hochverfügbaren Konfiguration ermöglicht es, einen Cluster einzurichten. In diesem Cluster werden mehrere Relution-Instanzen (Applikationsknoten) gestartet, die sich alle mit derselben Datenbank verbinden. Ein Loadbalancer verteilt den Datenverkehr auf diese Knoten mithilfe des Round-Robin-Verfahrens.

Die Konfiguration eines hochverfügbaren Clusters sollte nur von erfahrenen Administratoren durchgeführt werden.

Voraussetzungen

Um einen Cluster einzurichten, müssen alle Relution-Instanzen im gleichen Netzwerk sein. Die Knoten müssen über ihre Hostnamen und den TCP-Port 7800 miteinander kommunizieren können. Weitere Informationen dazu sind unter Netzwerkanforderungen → zu finden.

Alle Relution-Instanzen müssen dieselben Konfigurationsdateien (z.B. `application.yml`) oder dieselben Umgebungsvariablen verwenden. Die einzige Ausnahme besteht darin, dass bei nicht ermittelbarem Hostnamen die Umgebungsvariable `EXTERNAL_IP` verwendet werden kann, um die IP-Adresse der Instanz festzulegen, über die andere Relution-Instanzen auf diese Instanz zugreifen können.

Für Version 26.4.0

Funktionsweise

Beim Start einer Relution-Instanz verbindet sich dieser mit der Datenbank und trägt ihren Hostnamen in die Tabelle `JGROUPSPING` ein. Anschließend werden alle Einträge aus der Tabelle geladen, und die Instanz stellt eine Verbindung zu den anderen Instanzen über den TCP-Port 7800 her. Der Zustand des Clusters wird regelmäßig anhand der Datenbanktabelle überwacht. Wenn eine Instanz nicht erreichbar ist, werden ihre Einträge aus der Datenbank entfernt.

Überprüfung des Clusterstatus

Es gibt verschiedene Möglichkeiten, den Status des Clusters zu überprüfen:

1. System Portal

Für eine Clusterumgebung wird empfohlen, das System Portal zu aktivieren. Das System Portal bietet eine Übersicht über die registrierten Knoten im Cluster. Eine volle Funktionsweise setzt die Kommunikation zwischen den Knoten über Port `8099` voraus. Zur Aktivierung und Freischaltung der Actuator-Endpoints siehe Aktivierung des System-Portals →.

2. Metrik-Endpunkt

Über den API-Endpunkt für Prometheus `https://127.0.0.1:8099/actuator/prometheus` lässt sich die Metrik `counter_cluster_size_total` überprüfen, um herauszufinden, wie viele Knoten im Cluster erfolgreich registriert sind. Seit Relution 26.4 erfordert dieser Endpunkt die Freischaltung in der `application.yml` unter `management.endpoints.web.exposure.include` (z. B. `prometheus` oder `metrics`), siehe Freischaltung der Actuator-Endpoints →.

Für Version 26.4.0

Relution Shield (Add-on)

Relution Shield ermöglicht einen sicheren Zugriff vom Internet auf das organisationsinterne Intranet und kombiniert Virtual Private Network (VPN), Public Key Infrastructure (PKI) und UEM - MDM. Weitere Informationen: Relution Shield →.

Für das Upgrade von Relution Shield 1.x siehe Upgrade von 1.x zu 2.x →

Voraussetzungen

Die Installation von Relution Shield ist anspruchsvoll und erfordert Aufmerksamkeit und Zeit. Befehle und Konfigurationen vor dem Speichern sorgfältig prüfen – besonders auf Variablen achten, die gesetzt werden müssen.

Relution Applikation Server

Der bestehende Relution Applikation Server, auf dem Relution Shield konfiguriert und die VPN-Profile für die Endgeräte verwaltet werden.

1. Relution-Server (Version 5.26+)
2. Eine Zielorganisation auf dem Server mit Relution Shield-Lizenz

Für Version 26.4.0

Relution Shield Server

Ein separater Server, auf dem Relution Shield als VPN-Komponente installiert wird.

- Ubuntu 22.04+
  - Version prüfen: `lsb_release -a`
- UDP Port 500 und 4500 müssen frei und von außen erreichbar sein
  - Wird bei der Firewall-Einrichtung freigegeben (`ufw allow 500,4500/udp`)
    Status prüfen: `sudo ufw status verbose`
- Ausgehender Datenverkehr zu allen Zielen, die durch Relution Shield geschützt werden sollen
- Ausgehender Datenverkehr via HTTPS zum Relution Server
- Der Server muss vom Internet aus erreichbar sein
- Empfohlen: Öffentlicher DNS-Eintrag
  - z.B. `vpn.meinedomain.de`

Anlegen eines technischen Users und API-Access-Tokens

Neu in 26.5

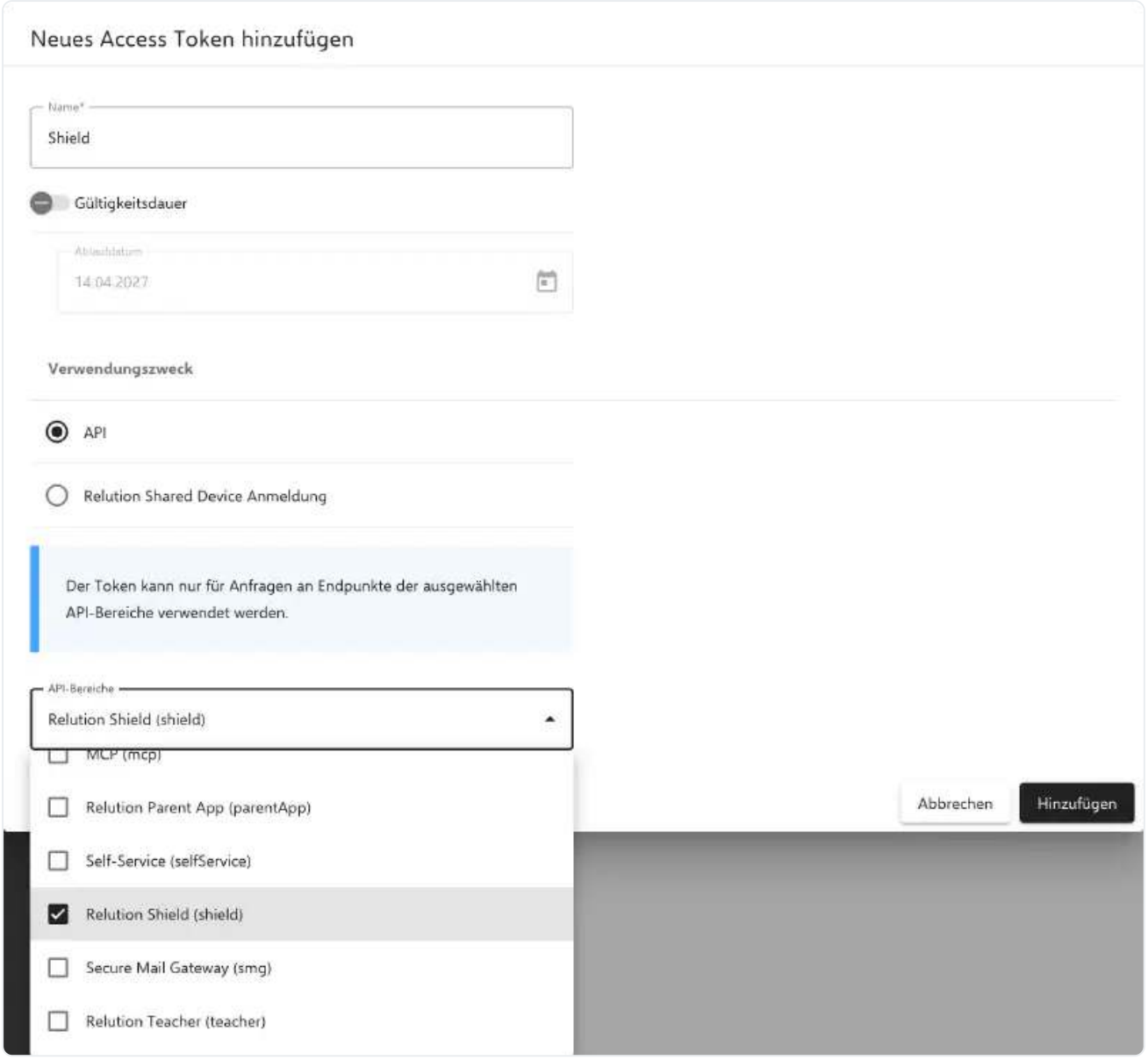
1. Neue Berechtigung mit der Rolle Relution Shield Zugangsprüfung erstellen: unter `Home` → `Benutzer` → `Berechtigungen` → `Hinzufügen` im Abschnitt Geräte den Punkt `Relution Shield Zugangsprüfung` aktivieren

2. Neuen Benutzer ohne Passwort (Passwortbasierte Authentifizierung deaktivieren) in der Zielorganisation erstellen

> Wird der Benutzer in der `Global`-Organisation angelegt, kann Relution Shield Zugriffschecks für alle Organisationen auf dem Relution Server durchführen (Benötigt Relution Shield 2.0 oder neuer).

3. Dem Benutzer die neu erstellte Berechtigung zuweisen

4. API-Access-Token für den Benutzer erstellen und Gültigkeitsdauer deaktivieren: unter Verwendungszweck die Option API wählen und im Feld API-Bereiche den Eintrag Relution Shield (shield) aktivieren



5. Benutzer speichern

Ab Relution 26.5 gilt ein API-Access-Token nur für die ausgewählten API-Bereiche. Relution Shield benötigt ausschließlich den Bereich Relution Shield (shield). Fehlt er, lehnt der Relution-Server die Zugriffsprüfung ab. Relution Shield behandelt das wie einen nicht erreichbaren Server: Mit dem Standardwert `RELUTION_SERVER_NOT_REACHABLE_ALLOW_DEVICE=true` werden Geräte mit gültigem Zertifikat ohne Zugriffsprüfung zugelassen, im Log erscheint `Relution: Could not retrieve status, temporarily accepting …`.

API-Access-Tokens, die vor dem Update auf Relution 26.5 erstellt wurden, erhalten beim Update automatisch alle API-Bereiche und funktionieren unverändert weiter.

Erforderliche Parameter

1. Relution Host: Hostname des Relution-Servers
   z.B. `mdm.meinedomain.de`
2. Relution API Token: API-Access-Token mit dem API-Bereich Relution Shield (shield), siehe vorheriger Schritt
   Anlegen eines technischen Users und API-Access-Tokens →
3. VPN CIDR: Der private IP-Adressbereich, aus dem Relution Shield den verbundenen Geräten eine interne IP-Adresse zuweist, z.B. `10.1.0.0/16`. Dieser Bereich darf sich nicht mit dem bestehenden Netzwerk überschneiden.
4. Network interface: Name der Netzwerkschnittstelle, die der Relution Shield Server verwendet, z.B. `eth0` – prüfen via `ip a`
5. Relution Shield Host: Hostname von Relution Shield
   z.B. `vpn.meinedomain.de`
6. DNS-Server: Die IP-Adressen der internen DNS-Server des Netzwerks, z.B. `10.1.0.1,10.1.0.2`. Diese werden den verbundenen Geräten mitgeteilt, damit interne Hostnamen (z.B. Intranet-Ressourcen) aufgelöst werden können.

Für Version 26.4.0

Installation

1. Folgenden Befehl ausführen:

```
sudo apt update && sudo apt upgrade
```

2. Docker inklusive docker-compose installieren (nicht via `snap`)
   Docker Installationsanleitung →

3. Installationsverzeichnis und Compliance-Verzeichnis erstellen:

```
mkdir -p /opt/relution-shield/compliance
```

4. Umgebungsdatei `/opt/relution-shield/.env` erstellen:

```
touch /opt/relution-shield/.env
vi /opt/relution-shield/.env
```

   Den Platzhalter `<%Relution Host%>` durch den tatsächlichen Hostnamen ersetzen, z.B. `RELUTION_HOSTNAME=mdm.meinedomain.de`

```
RELUTION_HOSTNAME=<%Relution Host%>
RELUTION_REST_API_ACCESS_TOKEN=<%Relution API Token%>
```

   Wenn das API-Access-Token zu einem Benutzer aus der `Global`-Organisation gehört, muss der globale Scope für den Zugriffscheck aktiviert werden
   (Benötigt Relution Shield 2.0 oder neuer):

```
RELUTION_ACCESS_CHECK_SCOPE=global
```

5. Ubuntu-Firewall `ufw`

Für Version 26.4.0

1. Standard-Weiterleitungsrichtlinie in `/etc/default/ufw` auf `DEFAULT_FORWARD_POLICY="ACCEPT"` setzen:

```
vi /etc/default/ufw
```

```
DEFAULT_FORWARD_POLICY="ACCEPT"
```

2. SSH und die erforderlichen IPSec UDP-Ports freigeben:

```
ufw allow ssh
ufw allow 500,4500/udp
```

3. Folgende Zeilen am Anfang der Datei `/etc/ufw/before.rules` einfügen – vor den erforderlichen Zeilen, die `*filter` enthalten:

```
vi /etc/ufw/before.rules
```

```
# Relution Shield additional rules
*nat
-A POSTROUTING -s <%VPN CIDR%> -o <%Network interface%> -m policy --pol ipsec
--dir out -j ACCEPT
-A POSTROUTING -s <%VPN CIDR%> -o <%Network interface%> -j MASQUERADE
COMMIT

*mangle
-A FORWARD --match policy --pol ipsec --dir in -s <%VPN CIDR%> -o <%Network
interface%> -p tcp -m tcp --tcp-flags SYN,RST SYN -m tcpmss --mss 1361:1536 -j
TCPMSS --set-mss 1360
COMMIT
```

```
# Don't delete these required lines, otherwise there will be errors
*filter
...
```

`<%VPN CIDR%>` und `<%Network interface%>` an den drei Stellen ersetzen.

```
#
# rules.before
#
# Rules that should be run before the ufw command line added rules. Custom
# rules should be added to one of these chains:
#   ufw-before-input
#   ufw-before-output
#   ufw-before-forward
#

# Relution Shield additional rules
*nat
-A POSTROUTING -s 10.10.10.0/24 -o eth0 -m policy --pol ipsec --dir out -j ACCEPT
-A POSTROUTING -s 10.10.10.0/24 -o eth0 -j MASQUERADE
COMMIT

*mangle
-A FORWARD --match policy --pol ipsec --dir in -s 10.10.10.0/24 -o eth0 -p tcp -m tcp --tcp-flags SYN,RST SYN -m tcpmss --mss 1361:1536 -j TCP
MSS --set-mss 1360
COMMIT


# Don't delete these required lines, otherwise there will be errors
*filter
:ufw-before-input - [0:0]
:ufw-before-output - [0:0]
:ufw-before-forward - [0:0]
:ufw-not-local - [0:0]
# End required lines


# Relution Shield additional rules
-A ufw-before-forward --match policy --pol ipsec --dir in --proto esp -s 10.10.10.0/24 -j ACCEPT
-A ufw-before-forward --match policy --pol ipsec --dir out --proto esp -d 10.10.10.0/24 -j ACCEPT
```

Für Version 26.4.0

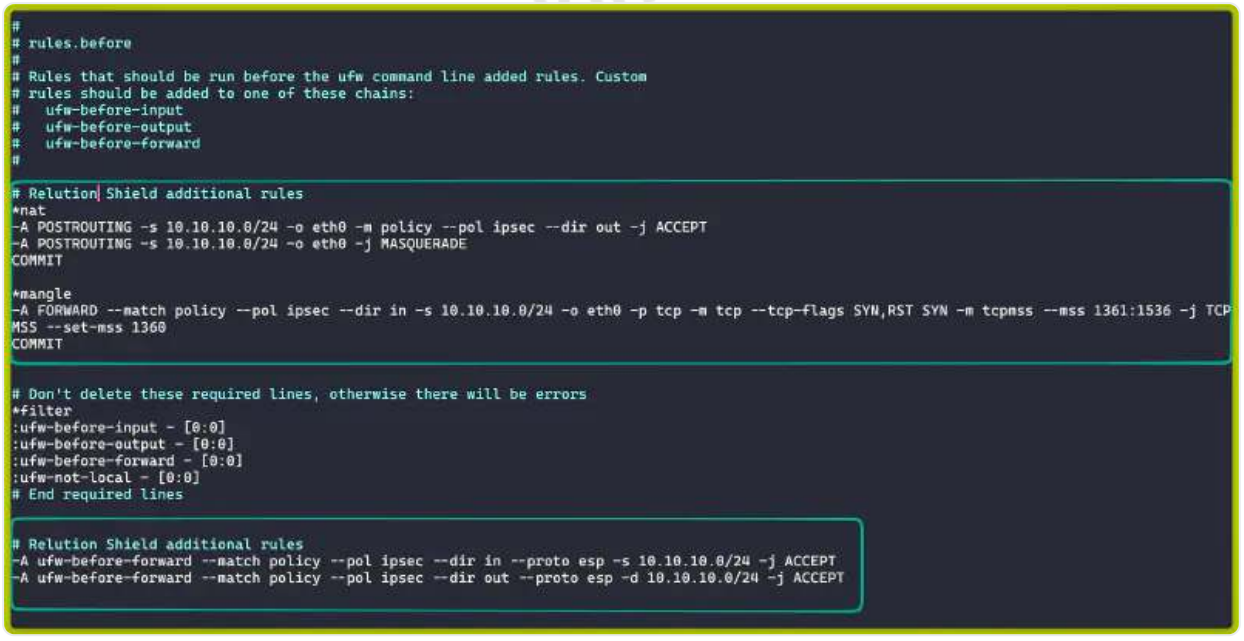
1. Folgende Zeilen am Ende der Datei `/etc/ufw/before.rules` einfügen – nach den erforderlichen Zeilen, die `*filter` enthalten:

```
vi /etc/ufw/before.rules
```

```
...
# End required lines
```

```
# Relution Shield additional rules
-A ufw-before-forward --match policy --pol ipsec --dir in --proto esp -s <%VPN
CIDR%> -j ACCEPT
-A ufw-before-forward --match policy --pol ipsec --dir out --proto esp -d
<%VPN CIDR%> -j ACCEPT
```

`<%VPN CIDR%>` an zwei Stellen ersetzen.



2. Folgende Zeilen am Ende der Datei `/etc/ufw/sysctl.conf` einfügen:

```
vi /etc/ufw/sysctl.conf
```

```
# Relution Shield IPv4 forwarding kernel configuration
net/ipv4/ip_forward=1
net/ipv4/conf/all/accept_redirects=0
net/ipv4/conf/all/send_redirects=0
net/ipv4/ip_no_pmtu_disc=1
```

3. Ubuntu-Firewall neu starten:

```
ufw disable && ufw enable
```

Für Version 26.4.0

6. Konfiguration von Relution Shield vorbereiten:

Für Version 26.4.0

1. Erforderliche Zertifikate und Schlüssel erstellen:

```
cd /opt/relution-shield
# Create mounted directories
mkdir -v -p pki/{cacerts,certs,private}
docker run -ti --volume "$(pwd)/pki:/opt/pki" relution/relution-shield:2-
latest bash
```

```
# Now in docker container
cd /opt
```

```
# Create CA private key
pki --gen --type rsa --size 4096 --outform pem > pki/private/ca-key.pem
```

Es wird eine Zeile im Terminal angezeigt plugin 'tpm': failed to load…, die auf ein fehlendes TPM Plugin hinweist. Diese Meldung kann ignoriert werden. Es handelt sich dabei nicht um einen Fehler.

Den Platzhalter `<%Relution Shield Host%>` ersetzen, z.B. `"CN=ca.vpn.meinedomain.de"`:

Für Version 26.4.0

```
# Create certificate
pki --self --ca --lifetime 3650 --in pki/private/ca-key.pem \
    --type rsa --dn "CN=ca.<%Relution Shield Host%>" --outform pem >
pki/cacerts/ca-cert.pem
```

```
# Generate server key, signed by the CA
pki --gen --type rsa --size 4096 --outform pem > pki/private/server-key.pem
```

```
# Generate certificate, signed by the CA
pki --pub --in pki/private/server-key.pem --type rsa \
    | pki --issue --lifetime 1825 \
        --cacert pki/cacerts/ca-cert.pem \
        --cakey pki/private/ca-key.pem \
        --dn "CN=<%Relution Shield Host%>" --san "<%Relution Shield Host%>" \
        --flag serverAuth --flag ikeIntermediate --outform pem \
    >  pki/certs/server-cert.pem
```

Folgende TPM-Fehlermeldung kann ignoriert werden:

```
plugin 'tpm': failed to load - tpm_plugin_create not found and no plugin file
available
```

```
# Prepare Key Pair archive, will be needed for Relution later
openssl pkcs12 -export -out "pki/ca.<%Relution Shield Host%>.p12" -inkey
pki/private/ca-key.pem -in pki/cacerts/ca-cert.pem
```

```
# Exit the docker container
exit
```

Der private Schlüssel der Zertifizierungsstelle (CA) muss sicher aufbewahrt werden, da im Falle des Diebstahls die Sicherheit der VPN Public Key Infrastructure (PKI) kompromitiert ist.

2. Zertifikatsdateien an die entsprechenden Orte verschieben:

```
mkdir -v -p /opt/relution-shield/etc/swanctl/{x509,x509ca,private}
mv pki/cacerts/ca-cert.pem /opt/relution-shield/etc/swanctl/x509ca/ca-cert.pem
mv pki/private/server-key.pem /opt/relution-shield/etc/swanctl/private/server-
key.pem
mv pki/certs/server-cert.pem /opt/relution-shield/etc/swanctl/x509/server-
cert.pem
```

3. Konfigurationsdatei `/opt/relution-shield/etc/strongswan.conf` erstellen und folgenden Inhalt einfügen:

```
vi /opt/relution-shield/etc/strongswan.conf
```

Vollständiges Konfigurationsbeispiel anzeigen

1. Konfigurationsdatei `/opt/relution-shield/etc/swanctl/swanctl.conf` erstellen:

```
vi /opt/relution-shield/etc/swanctl/swanctl.conf
```

Die Platzhalter `<%Relution Shield Host%>`, `<%VPN CIDR%>`, `<%Relution Host%>` und `<%DNS Servers%>` ersetzen:

Vollständiges Konfigurationsbeispiel anzeigen

Für Version 26.4.0

1. Relution Shield mit Docker installieren:

Für Version 26.4.0

1. Datei `/opt/relution-shield/compose.yml` erstellen und folgenden Inhalt einfügen. Die Platzhalter müssen hier nicht mehr angepasst werden, da sie bereits in der `.env`-Datei definiert wurden.

```
vi /opt/relution-shield/compose.yml
```

```yaml
services:
  relution-shield:
    image: relution/relution-shield:2-latest
    restart: unless-stopped
    privileged: true
    cap_add:
      - NET_ADMIN
      - NET_RAW
      - SYS_MODULE
    network_mode: host
    ports:
      - "500:500/udp"
      - "4500:4500/udp"
    environment:
      RELUTION_HOSTNAME: ${RELUTION_HOSTNAME}
      RELUTION_REST_API_ACCESS_TOKEN: ${RELUTION_REST_API_ACCESS_TOKEN}
      RELUTION_ACCESS_CHECK_SCOPE: ${RELUTION_ACCESS_CHECK_SCOPE}
    volumes:
      - "./etc/swanctl:/etc/swanctl:ro"
      - "./etc/strongswan.conf:/etc/strongswan.conf:ro"
      - "./compliance:/opt/strongswan/compliance"
```

Falls Relution Shield 1.x verwendet wird, muss `RELUTION_REST_API_ACCESS_TOKEN` durch `REST_API_ACCESS_TOKEN` ersetzt werden.

2. Relution Shield starten:

```
cd /opt/relution-shield && docker compose up -d
```

3. Relution Shield Auto-Start einrichten – folgende Datei erstellen und öffnen:

```
vi /etc/systemd/system/relution-shield-networkd-post-restarter.service
```

Folgenden Inhalt einfügen und speichern:

```
[Unit]
Requires=systemd-networkd.service
After=systemd-networkd.service network-online.target

[Service]
Type=oneshot
ExecStart=docker compose -f /opt/relution-shield/compose.yml restart
RemainAfterExit=yes

[Install]
WantedBy=multi-user.target
```

4. Dienst mit folgendem Befehl aktivieren:

```
systemctl enable relution-shield-networkd-post-restarter --now
```

Umgebungsvariablen

Die folgenden Umgebungsvariablen können verwendet werden, um Relution Shield zu konfigurieren.

Variablenname	Beschreibung	Werte	erforderlich	Benötigte Relution-Shield-Version
`RELUTION_HOSTNAME`	Hostname des Relution-Servers, z.B. `mdm.meinedomain.de`		ja	1.0.0
`RELUTION_REST_API_ACCESS_TOKEN`	API-Token für den Zugriff auf den Relution-Server (Bei Relution Shield 1.x.y: `REST_API_ACCESS_TOKEN`)		ja	2.0.0
`RELUTION_ACCESS_CHECK_SCOPE`	Scope für den Access-Check	`global` / `local`	nein (Standardwert: `local`)	2.0.0
`RELUTION_SERVER_NOT_REACHABLE_ALLOW_DEVICE`	Verbindung mit gültigem Zertifikat erlauben wenn der Relution-Server für den Konformitätscheck nicht erreicht werden kann	`true` / `false`	nein (Standardwert: `true`)	26.0.0
`DEVICE_STATE_CACHE_DURATION_MINUTES`	Dauer, die der einmal geladene Konformitätsstatus lokal gecacht wird, bevor erneut beim Relution-Server nachgefragt wird	Numerischer Wert	nein (Standardwert: `1`)	1.0.0

Für Versi

Zertifikats-Einrichtung

1. Zertifikate in die Zielorganisation importieren:

    1. Navigieren zu `Einstellungen` → `Zertifikate`

    2. Zertifikat `ca-cert.pem` vom Relution Shield Server `/opt/relution-shield/etc/swanctl/x509ca/ca-cert.pem` herunterladen, in `<%Relution Shield Host%> CA-Zertifikat` umbenennen und im Relution Applikation Server unter `Einstellungen` → `Zertifikate` → `CA-Zertifikat` hochladen

    3. Zertifikat `server-cert.pem` vom Relution Shield Server `/opt/relution-shield/etc/swanctl/x509/server-cert.pem` herunterladen, in `<%Relution Shield Host%> Server-Zertifikat` umbenennen und im Relution Applikation Server unter `Einstellungen` → `Zertifikate` → `Server-Zertifikat` hochladen

    4. PKCS12-Schlüsselpaar vom Relution Shield Server `/opt/relution-shield/pki/ca.<%Relution Shield Host%>.p12` herunterladen, in `<%Relution Shield Host%> CA-Schlüsselpaar` umbenennen und im Relution Applikation Server unter `Einstellungen` → `Zertifikate` → `CA-Schlüsselpaar` hochladen

    5. Inhalt von `/opt/relution-shield/pki/` extern sichern und das Verzeichnis anschließend entfernen

2. Zertifizierungsstelle und Zertifikatsvorlage erstellen:

    1. Navigieren zu `Einstellungen` → `Zertifizierungsstellen`

    2. Neue Zertifizierungsstelle vom Typ `Built In` hinzufügen und das zuvor hochgeladene Zertifikat `<%Relution Shield Host%> CA-Schlüsselpaar` auswählen

    3. Navigieren zu `Einstellungen` → `Zertifikatsvorlagen`

    4. Neue Zertifikatsvorlage hinzufügen:

        1. Zuvor erstellte Zertifizierungsstelle auswählen
        2. `Name des Inhabers` auf `CN=${device.uuid}@<%Relution Host%>` setzen (das `CN=` am Anfang beachten)
        3. Im Feld `Verwendung von Zertifikatsschlüsseln` `Signatur` und `Schlüsselverschlüsselung` aktivieren
        4. `Subject Alternative Name` vom Typ `Email` mit `${device.uuid}@<%Relution Host%>` hinzufügen (kein `CN=` am Anfang)
           Eingabe mit Enter bestätigen
        5. `Automatische Verlängerung` aktivieren und passende Werte setzen, z.B. 60 oder 180 Tage

Für Version 26.4.0

Home > Einstellungen > Zertifikatsvorlagen >

Bearbeiten

Bearbeiten

Allgemein

Name *

Shield

Vorlagentyp des Zertifikats

Zertifikat

Beschreibung

1

Zertifizierungsstelle *

Auswählen

Shield

2

Name des Inhabers *

CN=${device.uuid}@support.relution.io

3

Subject Alternative Name

Verzeichnis-Name +

E-Mail | ${device.uuid}@support.relution.io

Länge des Schlüssels *

4096

4

Verwendung von Zertifikatsschlüsseln

Signatur, Schlüsselverschlüsselung

Erweiterte Schlüsselverwendungen von Zertifikaten

5

Automatische Verlängerung aktivieren

Automatische Verlängerung (in Tagen)

60

Verhalten bei der Zertifikatserneuerung

Alte Zertifikate behalten ihre Gültigkeit

Beispiel iOS-Konfiguration

1. Neue iOS-Richtlinie erstellen oder bestehende erweitern
2. VPN-Konfiguration hinzufügen:
    1. Typ `IKEv2` auswählen
    2. `Per App und Konto-VPN` aktivieren (siehe auch Relution Hub Docs →)
    3. `Server` und `Entfernte ID` auf den Wert von `<%Relution Shield Host%>` setzen
    4. `Lokale ID` auf `${device.uuid}@<%Relution Host%>` setzen
    5. `Authentifizierungsmethode` auf `Zertifikat` setzen und die zuvor erstellte Zertifikatsvorlage auswählen
    6. `Erweiterte Authentifizierung (EAP)` aktivieren
    7. IKE SA-Parameter und Untergeordnete SA-Parameter auf `AES-256`, `SHA2-256`, `DH-Gruppe 16: 4096-Bit-Gruppe`, `1440` Minuten setzen
    8. Optional: Test-Domain unter `Safari-Domänen` hinzufügen, um die VPN-Verbindung automatisch zu aktivieren, wenn die Domain über Safari aufgerufen wird
3. `Zertifikat`-Konfiguration zur Richtlinie hinzufügen und das zuvor hochgeladene `<%Relution Shield Host%> CA-Zertifikat` auswählen
4. Optional: `App zu VPN Mapping`-Konfiguration hinzufügen, die zuvor erstellte VPN-Konfiguration sowie eine Browser-App wie Firefox oder Chrome auswählen, um den VPN-Zugang zu testen. Empfohlen: App-Konformität hinzufügen, damit sichergestellt ist, dass die App installiert ist.
5. Richtlinie veröffentlichen und einem Gerät zuweisen. Die VPN-Verbindung lässt sich anschließend manuell über `Einstellungen` → `Allgemein` → `VPN & Geräteverwaltung` → `VPN` aktivieren. Relution Shield verbindet sich auch automatisch, wenn die in Safari konfigurierten Domains aufgerufen oder die Browser-App geöffnet wird.
6. Konfiguration anpassen, um die Konten, Apps und Domains einzuschließen, die nur über Relution Shield zugänglich sein sollen.

Für Version 26.4.0

Für Version 26.4.0

Home > Richtlinien > Shield >

VPN

VPN

Unterstützt Benutzerregistrierung

Abbrechen | Speichern

Allgemein

Verbindungsname*
ShieldSupport

1

Typ der Verbindung
IKEv2

2

VPN-Verbindung für Apps und Konten

Server*
shield.support.relution.io

Entfernte ID*
shield.support.relution.io

Lokale ID
${device.uuid}@support.relution.io

Authentifizierungsmethode*
Zertifikat

Zertifikat

Benutzerdefiniertes Zertifikat verwenden

Zertifikat wählen

Zertifikat

Auswählen

Shield

Allgemeiner Serverzertifikatname

Allgemeiner Name des Serverzertifikatsausstellers

Zertifikatstyp

3

VPN on demand

Auf-Abruf Regeln

+ Hinzufügen

Aktion	DNS-Domänen	DNS-Server-Adressen	Interface	SSID

Es sind keine Ergebnisse verfügbar

Erweiterte Authentifizierung aktivieren (EAP)

TLS minimum Version

1.0

TLS maximum Version

1.2

Dead Peer-Erkennungsrate

Mobilität und Multihoming deaktivieren

Weiterleitungen deaktivieren

Zertifikat-Widerrufungsprüfung aktivieren

Perfect Forward Secrecy aktivieren

IPv4/IPv6 für interne Teilnetzattribute verwenden

Verbindungstrennung bei Inaktivität aktivieren

Inaktivitätszeit

20

Fallback aktivieren

IKE SA-Parameter

Verschlüsselungsalgorithmus

AES-256

Integritätsalgorithmus

SHA2-256

Diffie-Hellman-Gruppe

DH-Gruppe 16: 4096-Bit Gruppe

Rekey-Intervall (in Minuten)*

1440

Untergeordnete SA-Parameter

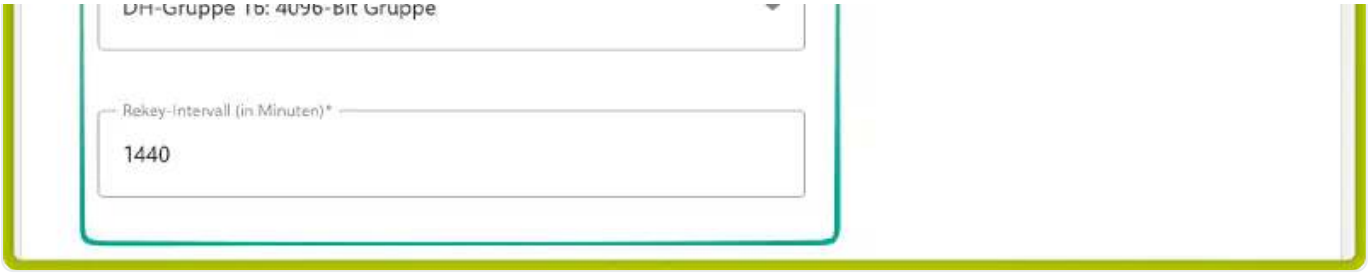
Verschlüsselungsalgorithmus

AES-256

Integritätsalgorithmus

SHA2-256

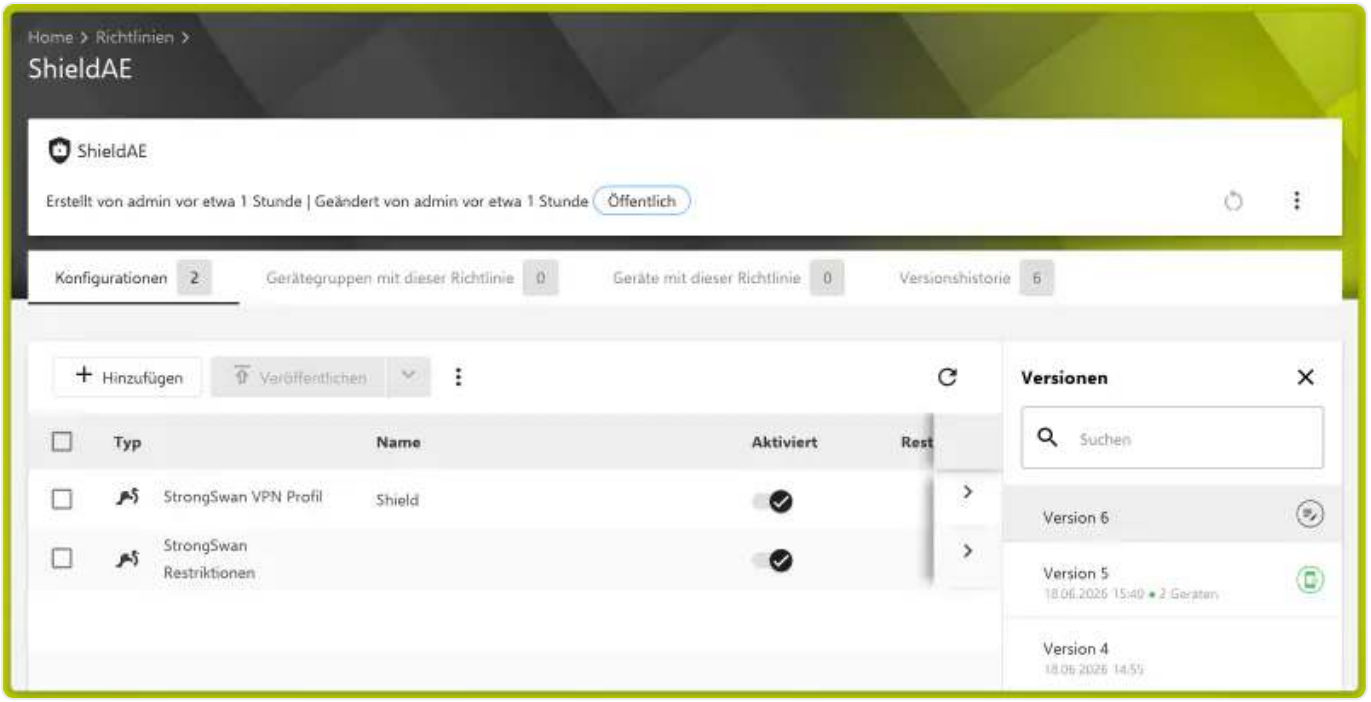
Diffie-Hellman-Gruppe



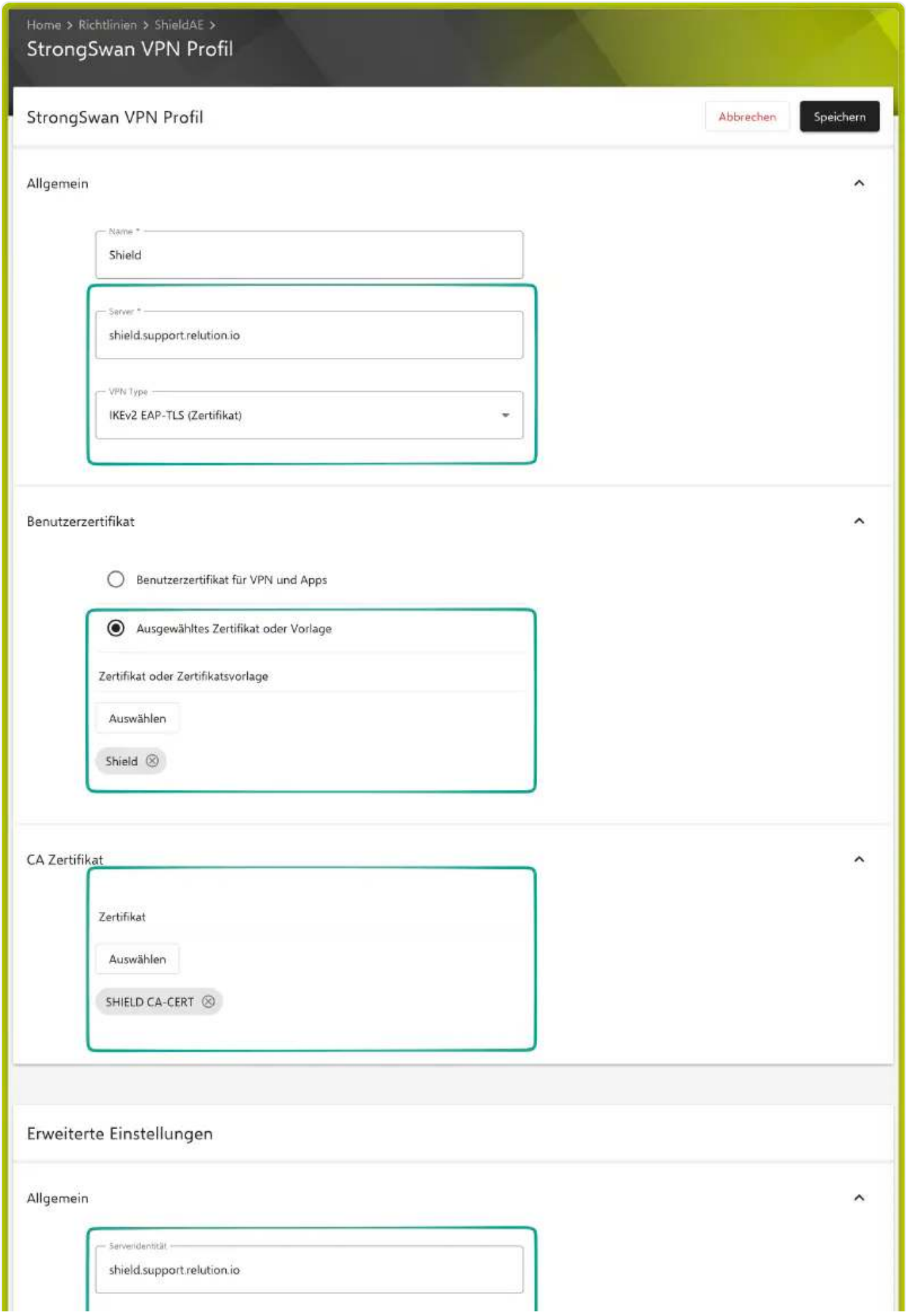
Beispiel Android Enterprise-Konfiguration

1. Neue Android Enterprise-Richtlinie erstellen oder bestehende erweitern
2. `StrongSwan VPN Profil`-Konfiguration hinzufügen:
    1. `IKEv2 EAP-TLS` als `VPN-Typ` auswählen
    2. `Server` und `Server-Identität` auf den Wert von `<%Relution Shield Host%>` setzen
    3. `Benutzerzertifikat` auf die zuvor erstellte Zertifikatsvorlage setzen
    4. `CA-Zertifikat` auf das zuvor hochgeladene `<%Relution Shield Host%> CA-Zertifikat` setzen
    5. `Client-Identität` auf `${device.uuid}@<%Relution Host%>` setzen
    6. `Nur diese Apps verwenden das VPN` auf einen Browser wie Firefox setzen
3. `StrongSwan VPN Einschränkungen`-Konfiguration hinzufügen und das zuvor erstellte VPN-Profil als Standardprofil auswählen
4. Richtlinie veröffentlichen und einem Gerät zuweisen. Die VPN-Verbindung lässt sich anschließend manuell über die StrongSwan-App aktivieren. Relution Shield verbindet sich auch automatisch, wenn die zuvor konfigurierte Browser-App geöffnet wird.
5. Konfiguration anpassen, um die Apps einzuschließen, die nur über Relution Shield zugänglich sein sollen.

Für Version 26.4.0



Für Version 26.4.0


Home > Richtlinien > ShieldAE >
StrongSwan VPN Profil
StrongSwan VPN Profil
Abbrechen
Speichern
Allgemein
Name *
Shield
Server *
shield.support.relution.io
VPN Type
IKEv2 EAP-TLS (Zertifikat)
Benutzerzertifikat
Benutzerzertifikat für VPN und Apps
Ausgewähltes Zertifikat oder Vorlage
Zertifikat oder Zertifikatsvorlage
Auswählen
Shield
CA Zertifikat
Zertifikat
Auswählen
SHIELD CA-CERT
Erweiterte Einstellungen
Allgemein
Serveridentität
shield.support.relution.io

Identität des Kunden

${device.uuid}@support.relution.io

DNS-Server +

MTU des VPN-Tunnelgeräts

0

Port

0

NAT-T Keepalive-Intervall

0

- Zertifikatsanfragen senden
- Verwenden Sie OCSP, um das Zertifikat zu überprüfen
- Verwenden Sie CRLs, um das Zertifikat zu überprüfen
- Strenge Widerrufsprüfung verwenden
- RSA/PSS-Signaturen verwenden
- IPv6-Transportadressen verwenden

Split tunneling

- (●) Der Datenverkehr zu diesen Subnetzen wird nicht über VPN geroutet
- ( ) Nur Datenverkehr zu definierten Subnetzen über VPN routen, alles andere wird so geroutet, als gäbe es kein VPN

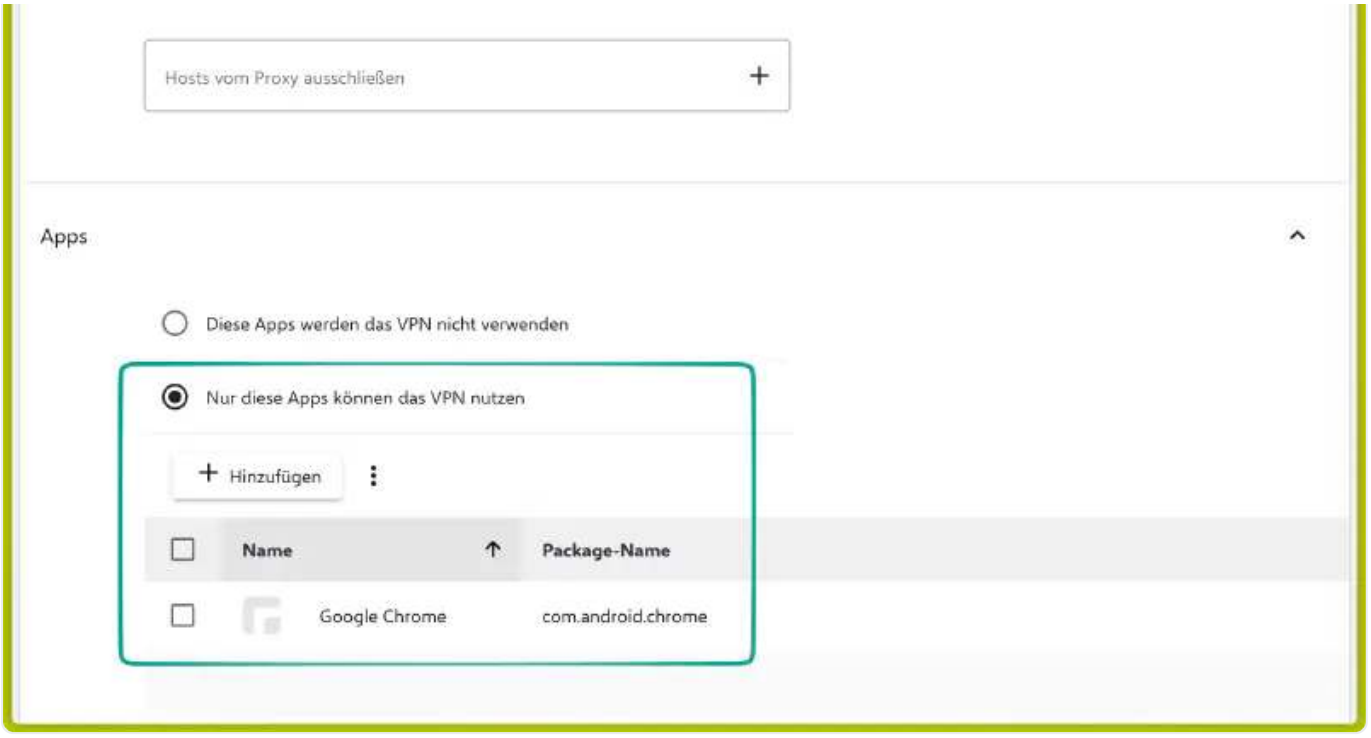
Ausgeschlossene Subnetze +

- IPv4-Verkehr blockieren, der nicht für das VPN bestimmt ist
- IPv6-Verkehr blockieren, der nicht für das VPN bestimmt ist

Proxy

Host-Adresse

Port



Upgrade von 1.x zu 2.x

Ablegen des privaten CA-Schlüssels `/opt/relution-shield/etc/ipsec.d/private/ca-key.pem` an einem sicheren Ort (außerhalb des Servers) falls noch nicht vorhanden.

Für Version 26.4.0

1. Relution Shield stoppen:

```
cd /opt/relution-shield && docker compose down
```

Für Version 26.4.0

2. Erstellen bzw. ändern der folgenden Dateien wie in der Installationsanleitung beschrieben:

    1. Erzeugen der neuen Verzeichnisse für Konfigurationsdateien

    ```
    mkdir -v -p /opt/relution-shield/etc/swanctl/{x509,x509ca,private}
    ```

    2. Erstellen von `etc/swanctl/swanctl.conf`
    3. Anpassen von `/opt/relution-shield/compose.yml`
    4. Anpassen von `/opt/relution-shield/.env`
    5. Anpassen von `/opt/relution-shield/etc/strongswan.conf`
    6. Verschieben der folgenden Dateien

Alter Pfad	Neuer Pfad
`/opt/relution-shield/etc/ipsec.d/cacerts/ca-cert.pem`	`/opt/relution-shield/etc/swanctl/x509ca/ca-cert.pem`
`/opt/relution-shield/etc/ipsec.d/certs/server-cert.pem`	`/opt/relution-shield/etc/swanctl/x509/server-cert.pem`
`/opt/relution-shield/etc/ipsec.d/private/server-key.pem`	`/opt/relution-shield/etc/swanctl/private/server-key.pem`

    1. Entfernen des Verzeichnisses `/opt/relution-shield/etc/ipsec.d`
    2. Entfernen von `/opt/relution-shield/etc/ipsec.conf`
    3. Entfernen von `/opt/relution-shield/etc/ipsec.secrets`
    4. Relution Shield starten:

```
cd /opt/relution-shield && docker compose up -d
```

Secure Mail Gateway

Kommt das Secure Mail Gateway zum Einsatz, so ist ab Relution 26.4.0 der Secure Mail Gateway Standalone-Dienst eine Pflichtkomponente. Dieser Artikel beschreibt die Einrichtung für On-Premise-Installationen.

Zur Konfiguration des Secure Mail Gateway in Relution: Secure Mail Gateway →

Technischer Hintergrund

Ist das Secure Mail Gateway unter `Einstellungen` → `Geräteverwaltung` → `Secure Mail Gateway` aktiviert werden eingehende ActiveSync-Verbindungen an den dort konfigurierten Exchange-Server weitergeleitet, vorausgesetzt die Anfrage kommt von einem zulässigen (eingeschriebenen) Gerät.

In Version 26.3.x und älter gehen ActiveSync-Anfragen dazu zunächst an den Relution-Dienst und werden von diesem an den Exchange-Server weitergeleitet. Der Relution-Dienst prüft intern, ob eine Anfrage von einem zulässigen Gerät stammt und weitergeleitet werden darf. Unzulässige Anfragen werden abgelehnt.

Ab Version 26.3.0 kann der Standalone-Dienst wahlweise aktiviert werden, um die Umstellung auf den dedizierten Container vorab testen zu können. Ab Version 26.4.0 und neuer wurde die entsprechende Funktionalität vollständig aus Relution entfernt, so das ActiveSync-Anfragen immer durch den dedizierten Docker Container geleitet werden müssen.

Die dafür notwendige Konfiguration ist im folgenden Artikel beschrieben.

Für Version 26.4.0

Migration – Was ist zu tun?

Installation	Handlungsbedarf
Relution Cloud – Shared Hosting	Kein Handlungsbedarf. Relution übernimmt die Migration des SMG-Dienstes.
Relution Cloud – Dedicated Server (Bestandskunden)	Relution übernimmt das Hosting des SMG-Dienstes. Die Migration wird in Abstimmung mit dem Kunden koordiniert.
Relution Cloud – Dedicated Server (Neukunden)	Der SMG-Dienst muss eigenständig als On-Premise-Komponente betrieben werden. Der Einrichtungsanleitung weiter unten in diesem Artikel folgen.
On-Premise	Der vollständige Einrichtungsablauf ist weiter unten in diesem Artikel beschrieben.

Feature-Toggle für On-Premise-Installationen (26.3)

Neu in 26.3

In Relution 26.3 können On-Premise-Installationen den neuen Modus wahlweise aktivieren. Dazu muss die `application.yaml` des Relution Servers um folgendes Preview-Feature-Toggle ergänzt werden:

application.yaml

```
relution:
  featuretoggle:
    enabledPreviewFeatures:
      - SMG_STANDALONE
```

Zusätzlich muss ein weiterer Docker Container, wie unten beschrieben, in die Dockerumgebung aufgenommen werden.

> Solange der Toggle aktiv ist, wird der neue Standalone-Dienst verwendet. Wird er entfernt, kehrt Relution automatisch zum bisherigen Verhalten zurück. Das macht Relution 26.3 geeignet, um den neuen Dienst vorab in der eigenen Umgebung zu testen, bevor das Update auf 26.4.0 den Wechsel verbindlich macht.

Für Version 26.4.0

Pflichtkomponente ab 26.4.0

Neu in 26.4

Mit Relution 26.4.0 entfällt der Toggle. Das Secure Mail Gateway muss zwangsweise als separater Dienst betrieben werden. Die Komponente wurde vollständig aus Relution entfernt.

Einrichtung

Der Secure Mail Gateway Standalone-Dienst leitet als HTTP-Proxy ActiveSync-Requests von mobilen Geräten an den Exchange-Server und Antworten zurück an das jeweilige mobile Gerät. Dazu muss zunächst entschieden werden, ob ein Request überhaupt weitergeleitet werden darf oder nicht. Damit das Secure Mail Gateway diese Entscheidung treffen kann muss es intern mit dem Relution-Dienst kommunizieren, um prüfen zu können ob eine Anfrage von einem zulässigen Gerät stammt.

Relution

Damit das Secure Mail Gateway mit dem Relution-Dienst kommunizieren kann muss daher zunächst ein technischer Benutzer mit entsprechenden Berechtigungen in Relution angelegt werden

1. Dynamische Rolle in Relution erstellen

Die vorgefertigte Rollenvorlage herunterladen und in der globalen Organisation unter `Einstellungen` → `Benutzerverwaltung` → `Berechtigungen` importieren:

SMG-Rollenvorlage herunterladen →

Alternativ lässt sich die Rolle manuell anlegen:

1. In der globalen Organisation zu `Einstellungen` → `Benutzerverwaltung` → `Berechtigungen` navigieren
2. Eine neue Dynamische Rolle hinzufügen
3. Die Berechtigung Secure Mail Gateway (service account) aktivieren
4. Die Rolle speichern

2. Technischen Benutzer und API-Zugriffsschlüssel anlegen

1. In der globalen Organisation einen neuen Benutzer erstellen und ihm die oben erstellte Dynamische Rolle zuweisen
2. Zur Detailseite des Benutzers navigieren und einen neuen API-Zugriffsschlüssel erstellen
3. Den generierten Schlüssel kopieren – er wird nur einmal angezeigt

---

Secure Mail Gateway Container

Das Secure Mail Gateway muss jetzt als separater Docker Container in die Umgebung aufgenommen und konfiguriert werden. Im Anschluss muss noch der Reverse-Proxy so angepasst werden, das Anfragen an den `/Microsoft-Server-ActiveSync`-Endpunkt zukünftig nicht mehr zum Relution Container sondern zum Secure Mail Gateway Container gesendet werden.

Für Version 26.4.0

1. Dienst bereitstellen

Den folgenden Dienst zur bestehenden `compose.yaml` hinzufügen. Dies ist nur erforderlich, wenn das Secure Mail Gateway verwendet wird.

> Auch wenn auf Docker Hub neuere Versions-Tags erscheinen, empfehlen wir ausdrücklich, `latest` zu behalten. Neue Builds durchlaufen mehrere zusätzliche Quality Gates, bevor sie als `latest` bereitgestellt werden – eine fest eingetragene Versionsnummer kann auf einen Build verweisen, der noch nicht für den Produktiveinsatz freigegeben ist.

```
compose.yaml
```

```yaml
services:
  …
  smg:
    image: relution/relution-smg-standalone:latest
    restart: always
    container_name: smg
    networks:
      - reverse-proxy
    volumes:
      - ./smg/application.yaml:/opt/app/config/application.yaml:ro
    ports:
      - 8093:8093
```

`smg` muss sich wie `relution` und `traefik` im Netzwerk `reverse-proxy` befinden – sonst kann Traefik/nginx nicht zu diesem Dienst weiterleiten.

2. Dienst konfigurieren

Der zuvor in Relution erzeugte API-Zugriffsschlüssel muss in die Konfiguration vom Secure Mail Gateway aufgenommen werden, damit das SMG mit dem Relution-Dienst kommunizieren kann.

Laufen beide Dienste in derselben `compose.yaml` auf einem Server, kommunizieren sie intern über das Docker-Netzwerk.

`smg/application.yaml` neben der `compose.yaml` erstellen:

Für Version 26.4.0

```
smg/application.yaml
```

```yaml
relution:
  server:
    url: http://relution:8080    # Bei gemeinsamer compose.yaml unverändert lassen
    api-key: ihr-api-schluessel   # Zuvor erstellter API-Zugriffsschlüssel
```

URL des Relution-Servers: Laufen Secure Mail Gateway und Relution in derselben `compose.yaml` auf einem Server, bleibt `url: http://relution:8080` unverändert. Der Dienstname `relution` wird dann über das gemeinsame Docker-Netzwerk aufgelöst.

Angepasst wird die URL nur, wenn das SMG nicht im selben Netzwerk wie Relution läuft, z. B. auf einem anderen Server oder in einer eigenen `compose.yaml` mit eigenem Docker-Netzwerk. Dann wird die Adresse eingetragen, unter der Relution vom SMG aus erreichbar ist, z. B. `https://relution.example.com`.

Reverse-Proxy-Konfiguration

Der SMG-Dienst stellt den Endpunkt `/Microsoft-Server-ActiveSync` auf Port `8093` bereit. Die Konfiguration des Reverse-Proxy muss so angepasst werden, dass eingehende Anfragen auf diesen Pfad an den Standalone-SMG-Dienst weitergeleitet werden. Die folgenden Beispiele zeigen die Konfiguration für Traefik und nginx.

Kommt ein anderer, nicht offiziell von uns unterstützter Reverse-Proxy zum Einsatz (z. B. Apache, Sophos, …), muss dessen Konfiguration entsprechend angepasst werden. Die Dokumentation des jeweiligen Produkts gibt Auskunft darüber, wie einzelne Pfade oder Locations an separate Endpunkte weitergeleitet werden.

Hinweis: Die folgenden Beispiele verwenden Hostnamen, die innerhalb des Docker-Netzwerks aufgelöst werden können. Das ist nur möglich, solange Relution, SMG und Traefik/nginx Teil desselben Docker-Netzwerks sind. Liegen Reverse-Proxy oder Dienste in getrennten Netzwerken, sind stattdessen Hostnamen zu verwenden, die der interne DNS-Server auflösen kann.

Traefik

Die folgenden zusätzlichen `smg`-Einträge unterhalb von `routers` und `services` ergänzen. Dabei bleiben bestehende `routers` und `services` wie `relution` erhalten. Siehe auch: Traefik-Konfiguration →

`configs/traefik/relution.yaml`

```yaml
http:
  routers:
    …
    smg:
      rule: Host(`external.url`) && Path(`/Microsoft-Server-ActiveSync`)
      entryPoints:
        - websecure
      tls:
        certResolver: letsencrypt
      service: smg

  services:
    …
    smg:
      loadBalancer:
        servers:
          - url: "http://smg:8093"
```

nginx (Alternative zu Traefik)

Den Block `location ~ /Microsoft-Server-ActiveSync` im bestehenden HTTPS-`server`-Block ergänzen (oder anpassen), damit eingehende Anfragen an das SMG weitergeleitet werden.

`relution-nginx.conf`

```
server {
    listen 0.0.0.0:443 ssl default_server;
    …

    # (NEU) Weiterleitung an das Secure Mail Gateway
    location ~ /Microsoft-Server-ActiveSync {
        proxy_read_timeout 2100;
        proxy_pass http://smg:8093;
    }
}
```

Die Position des Blocks innerhalb des `server`-Blocks ist nicht relevant, da nginx Locations mit regulärem Ausdruck vor der Präfix-Location `/` auswertet. Aus Gründen der Lesbarkeit empfiehlt es sich dennoch, die einzelnen Location-Blöcke beieinander zu halten.

Bei einer Docker-Installation bezeichnet `smg` den Docker-Dienstnamen und ist innerhalb des Docker-Netzwerks erreichbar. Bei einer nativen Linux-Installation `smg:8093` durch `127.0.0.1:8093` ersetzen.

Docker Dienste starten oder neu starten

Version 26.4.0

Damit die Änderungen greifen müssen die Docker Container im Anschluss neu gestartet werden.

```
docker compose up -d
```

Wurden zuvor `relution.smg.*`-Eigenschaften in der Konfiguration des Relution Servers angepasst, müssen diese unverändert in diese Datei übertragen werden – die Eigenschaftsnamen sind identisch.

Erweiterte Konfiguration

Die folgenden Einstellungen sind nur bei spezifischen Umgebungen erforderlich — für interne Certificate Authorities und ausgehende Verbindungen die durch einen Firmenproxy laufen.

(Optional) Vertrauenswürdiges CA-Zertifikat hinterlegen

Präsentiert der Exchange-Server ein Server-Zertifikat, das von einer internen CA ausgestellt wurde (“selbstsigniert”), dann muss das Root-Zertifikat dieser CA als vetrauenswürdiges Zertifikat hinterlegt werden. Dazu kann ein Verzeichnis mit der PEM-kodierten Zertifikatsdatei unter `/opt/app/ca-certs` in den Container gemounted werden. Der Ordner kann bei Bedarf mehr als ein Zertifikat enthalten.

compose.yaml

```yaml
services:
  …
  smg:
    volumes:
      - ./smg/application.yaml:/opt/app/config/application.yaml:ro
      - ./smg/ca-certs:/opt/app/ca-certs:ro
```

Diese Zertifikate werden bei der Kommunikation mit dem Exchange- und Relution-Server verwendet – eine Konfigurationseigenschaft ist dafür nicht erforderlich. Ist nichts gemountet, hat das Feature keine Auswirkung und ausgehendes TLS verhält sich wie zuvor. Zum Hinzufügen, Entfernen oder Ändern eines Zertifikats muss der Container neu gestartet werden; das Verzeichnis wird nur einmal beim Start gelesen.

(Optional) Proxy für ausgehende Verbindungen

Anfragen an Exchange berücksichtigen die Proxy-Systemeigenschaften der JVM. Diese werden über die `JAVA_TOOL_OPTIONS` in der `compose.yaml` für den SMG Container gesetzt. Zusätzlich muss in der `application.yaml` das `honor-proxy-settings`-Flag auf `true` gestellt werden.

sion 26.4.0

compose.yaml

```yaml
services:
  …
  smg:
    environment:
      - JAVA_TOOL_OPTIONS=
        -Dhttp.proxyHost=proxy.example.com
        -Dhttp.proxyPort=3128
        -Dhttps.proxyHost=proxy.example.com
        -Dhttps.proxyPort=3128
        -Dhttp.nonProxyHosts=relution|example.com
```

Mit `-Dhttp.nonProxyHosts` (eine mit `|` getrennte Liste von Host-Mustern, `*`-Platzhalter werden unterstützt) lassen sich bestimmte Hosts vom Proxy ausschließen – typischerweise Exchange selbst, wenn dieser direkt erreichbar ist, ohne über den Unternehmens-Proxy zu gehen.

Standardmäßig werden Anfragen an den Relution Server nicht über den Proxy geleitet – er ist normalerweise direkt erreichbar. Erreicht die eigene Umgebung Relution über denselben Proxy wie Exchange, ist `honor-proxy-settings: true` in `smg/application.yaml` zu setzen:

smg/application.yaml

```
relution:
  server:
    url: https://ihr-relution-server
    api-key: ihr-api-schluessel
    honor-proxy-settings: true   # Standard false; nur erforderlich, wenn Relution
ebenfalls hinter dem Proxy liegt
```

Fehlersuche

Kommt es zu Problemen mit dem SMG-Dienst – etwa bei der Verbindung zu Exchange oder beim Start des Containers –, hilft ein erhöhtes Loglevel bei der Analyse. Eine Anleitung dazu ist unter Loglevel einstellen → zu finden.

Am einfachsten lässt sich das Loglevel direkt im SMG-Container über dessen `application.yaml` aktivieren, indem folgender Abschnitt am Ende ergänzt wird:

```
smg/application.yaml
```

```
logging:
  level:
    io.relution: DEBUG
```

Changelog

Aktuell unter `latest` verfügbare Version: 26.0.6 (Stand 23.09.2026)

Version	Kategorie	Änderung
26.0.6	Fixes	Eingehende HTTP-Header werden jetzt korrekt ohne Beachtung der Groß-/Kleinschreibung behandelt, wodurch potenziell doppelte Header in der weitergeleiteten Anfrage vermieden werden
26.0.5	Konfiguration	Die Standard `forward-headers-strategy` ist jetzt `native`
		Die Standard `max-http-post-size` ist jetzt `1GB`
	Zertifikate	Mehr nützliche Logs zu eigenen CA Zertifikaten im Trust Store
		Mehr nützliche Logs wenn eine Verbindung wegen eines nicht vertrauenswürdigen Zertifikats abgelehnt wird
	Logs	Ein vorzeitiger Verbindungsabbruch wird jetzt protokoliert
		Statuscode des Exchange-Servers wird geloggt, wenn eine Nachricht abgelehnt wird
		HTTP-Fehler sind auch bei der Verwendung von HTTP/2 im Log sichtbar
		Erfolgreiche Verbindungen werden auf `INFO` protokolliert
	Fixes	Vorzeitig beendete Verbindungen werden jetzt sauber aufgeräumt
26.0.4	Release-Prozess	Anpassung des internen Release-Prozesses – keine funktionalen Änderungen
26.0.3	Feature	Unterstützung für selbstsignierte Zertifikate und Proxy-Einstellungen
26.0.2	Fixes	Fehlerhafte Behandlung von 404-Antworten behoben
26.0.1	Metriken	Health-Endpunkt freigegeben
26.0.0	Release-Prozess	Code aus Relution ausgelagert

Objektspeicher für Relution

Standardmäßig speichert Relution bestimmte Ressourcen - wie z.B. native Apps - in seiner Datenbank. Dies kann dazu führen, dass die Tabelle `resource` sehr groß wird, insbesondere wenn viele native Apps verwaltet werden.

Um die Performance zu optimieren, unterstützt Relution die Speicherung dieser Ressourcen in externen S3-kompatiblen Objektspeicher-Buckets.

> MinIO-Benutzer: MinIO hat die Entwicklung im Oktober 2025 eingestellt und erhält keine Updates mehr. Wir empfehlen die Migration zu SeaweedFS → mithilfe unserer Anleitung: Objektspeicher-Migration →

Wann Objektspeicher verwenden

Die Verwendung von externem Objektspeicher ist zwar optional, wird aber besonders in diesen Fällen empfohlen:

- Installation und Verwaltung von nativen Apps auf Windows-Geräten
- Bei einer größeren Anzahl nativer Apps oder nativen Apps größer als 50 MB
- Für Server mit mehr als 5.000 Geräten

Für Version 26.4.0

Verfügbare Optionen

Der bekannteste Objektspeicher ist AWS S3, aber es gibt viele S3-kompatible Lösungen - sowohl cloud-gehostet als auch selbst-gehostet.

Selbst-gehostet / On-Premise

Selbst-gehostete Lösungen ermöglichen es, Cloud-Kosten zu vermeiden und die volle Kontrolle über die eigenen Daten zu behalten.

Anbieter	Beschreibung
SeaweedFS →	Empfohlen. Einfach einzurichten, mit Relution getestet. Unsere Einrichtungsanleitung →
Garage →	Ressourcensparend, für Self-Hosting konzipiert.
Ceph →	Enterprise-tauglich, hochskalierbar.
RustFS →	Rust-basierte Alternative.
MinIO →	Nicht empfohlen. Entwicklung eingestellt. Unsere Migrationsanleitung →

Wir haben SeaweedFS gründlich mit Relution getestet. Andere Backends können funktionieren, wurden aber nicht getestet.

Cloud-Anbieter

on 26.4.0

Anbieter	Hinweise
AWS S3 →	Die ursprüngliche S3-Implementierung, mit Relution getestet.
Hetzner Object Storage →	Deutscher Anbieter, kosteneffizient, mit Relution getestet.

Für verwaltetes Relution-Hosting inkl. Objektspeicher unser Sales-Team kontaktieren → – mehr Infos: Relution Cloud →

Nächste Schritte

Die nächsten Schritte richten sich nach der eigenen Situation:

Situation	Nächste Schritte
Neue Einrichtung mit SeaweedFS (empfohlen)	1. SeaweedFS einrichten → 2. Objektspeicher verbinden →
Neue Einrichtung mit einem Cloud-Anbieter	1. Bei Cloudanbieter einrichten 2. Objektspeicher verbinden →
Migration von MinIO oder anderem Backend	– Migrationsanleitung →

Für Version 26.4.0

SeaweedFS einrichten

SeaweedFS → ist ein Apache-lizenziertes Open-Source Objektspeicher-Backend mit einer S3-kompatiblen API. Es bietet gute Performance, Skalierbarkeit und einen einfachen Einrichtungsprozess. Es kann via Kubernetes, Docker oder direkt auf Linux, FreeBSD, macOS oder Windows eingesetzt werden.

Diese Anleitung erklärt, wie man SeaweedFS neben Relution mit Docker Compose unter Linux bereitstellt.

Obwohl wir es gründlich getestet haben, ist SeaweedFS Software von Drittanbietern und wir können keine Sicherheits- oder Zuverlässigkeitsgarantien dafür geben. Für verwaltetes Hosting bitte unser Sales-Team kontaktieren →. Mehr Infos: Relution Cloud →

Diese Anleitung verwendet SeaweedFS im `mini`-Modus, der alle Komponenten mit Standardeinstellungen bündelt, die für Single-Node-Deployments mittlerer Größe geeignet sind. Für mehr Infos: SeaweedFS Wiki →.

Voraussetzungen

- Eine funktionierende Relution-Installation mit Docker Compose
- Zugriff zum Bearbeiten der `compose.yml`-Datei

Für Version 26.4.0

Vorbereitung der compose.yml

Ein 24-stelliges alphanumerisches Passwort mit einem Passwort-Manager oder aus der Linux-Kommandozeile generieren:

```
pwgen -snc 24 1
```

In der Relution `compose.yml` (bei älteren Installationen: `docker-compose.yml`) unter `services:` den folgenden Service hinzufügen:

```
services:
  seaweedfs:
    image: chrislusf/seaweedfs:4.05 # Neueste Version hier prüfen:
https://github.com/seaweedfs/seaweedfs/releases
    restart: unless-stopped
    ports:
      - 23646:23646
      - 8333:8333
    command: ["mini", "-dir=/data", "-admin.dataDir=/data/admin", "-
admin.password=%IHR-GENERIERTES-PASSWORT%"]
    networks:           # Optional: für Netzwerktrennung das `object-storage` Netzwerk
      - object-storage  # hier und im `networks` Block des `relution` Service ergänzen
    volumes:
      - seaweedfs-data:/data
```

Im Abschnitt `volumes:` das Volume `seaweedfs-data` ergänzen:

```
volumes:
  postgresql: {}
  seaweedfs-data: {}
```

Für Version

Wichtig: Die SeaweedFS-Volumes in die eigene Backup-Routine aufnehmen. Ohne diese Daten kann der Betrieb des Servers und die Verwaltung der Geräte nicht sichergestellt werden.

SeaweedFS starten

Das Image laden und den Service starten:

```
docker compose pull
docker compose up -d seaweedfs
```

SeaweedFS ist innerhalb weniger Sekunden bereit.

Benutzer und Bucket erstellen

SeaweedFS bietet eine Web-UI für die Administration.

1. Im Browser zu `http://localhost:23646/` navigieren
2. Mit dem zuvor generierten Passwort anmelden
3. In der Seitenleiste zu `Object Store` → `Users` gehen
4. Auf Create User (oben rechts) klicken, `relution` als Benutzernamen eingeben und bestätigen
5. Den angezeigten Access Key und Secret Key notieren (diese lassen sich später über das 🔑-Symbol unter *Actions* abrufen)
6. In der Seitenleiste zu `Object Store` → `Buckets` gehen
7. Auf Create Bucket klicken, `relution` als Namen eingeben, `relution` als Bucket-Besitzer auswählen und bestätigen

Konfigurationswerte notieren

Diese Werte werden benötigt, um Relution zu konfigurieren:

Einstellung	Wert
Endpoint	`http://seaweedfs:8333`
Access Key	*(aus Schritt 5)*
Secret Key	*(aus Schritt 5)*
Bucket-Name	`relution`

Nächste Schritte

Relution nun für die Verwendung des neuen Objektspeichers konfigurieren:

Objektspeicher verbinden →

Objektspeicher verbinden

Nachdem ein S3-kompatibles Objektspeicher-Backend bereitsteht - egal ob selbst-gehostet oder cloud-basiert - muss Relution für dessen Verwendung konfiguriert werden.

Voraussetzungen

Die folgenden Informationen vom Objektspeicher-Anbieter werden benötigt:

Einstellung	Beschreibung
Endpoint	Die S3-API-URL
Access Key	Authentifizierungs-Key-ID
Secret Key	Authentifizierungs-Secret
Bucket-Name	Der Name des Speicher-Buckets

Für Version

Die nachfolgenden Konfigurationsbeispiele verwenden Beispielwerte, die zur SeaweedFS-Anleitung → passen. Bei Verwendung eines anderen Backends oder Anbieters diese entsprechend anpassen.

Konfiguration

Eine der beiden folgenden Optionen wählen. Beide erreichen dasselbe Ergebnis.

Option A: Verwendung von application.yml

Folgendes zur eigenen `application.yml` hinzufügen:

```yaml
relution:
  storage:
    resourceStorageType: S3
    s3:
      customEndpoint: http://seaweedfs:8333
      accessKey: %IHR-ACCESS-KEY%
      secretKey: %IHR-SECRET-KEY%
      bucketName: relution
```

Option B: Verwendung von Umgebungsvariablen

Diese Umgebungsvariablen zum `relution` Service in der eigenen `compose.yml` hinzufügen:

```yaml
services:
  relution:
    environment:
      RELUTION_STORAGE_RESOURCESTORAGETYPE="S3"
      RELUTION_STORAGE_S3_CUSTOMENDPOINT="http://seaweedfs:8333"
      RELUTION_STORAGE_S3_ACCESSKEY="%IHR-ACCESS-KEY%"
      RELUTION_STORAGE_S3_SECRETKEY="%IHR-SECRET-KEY%"
      RELUTION_STORAGE_S3_BUCKETNAME="relution"
```

Soll der Objektspeicher mit einem kundenseitigen Schlüssel verschlüsselt werden, muss das vor dem ersten Start geschehen:
Serverseitige Verschlüsselung (SSE-C) →

Services starten

1. Die neuesten Images laden:

```
docker compose pull
```

2. Die Container starten oder neu starten:

```
docker compose up -d
```

3. Relution beginnt automatisch mit der Migration von Inhalten aus der `resource`-Datenbanktabelle in den Objektspeicher-Bucket.

Fortschritt überwachen

Für Version 26.4.0

Den Migrationsfortschritt in den Logs beobachten:

```
docker logs -f relution
```

Zusätzlich lässt sich überprüfen, ob Dateien erstellt werden, indem das Objektspeicher-Backend geprüft wird (z. B. über die SeaweedFS-Web-UI oder die Konsole des Cloud-Anbieters).

Wichtige Hinweise

Nicht umkehrbarer Prozess: Ab Relution 26.0.0 kann die Migration zu Objektspeicher nicht rückgängig gemacht werden.

Backup: Sicherstellen, dass der Objektspeicher-Bucket in die Backup-Routine eingebunden ist. Ohne diese Daten kann der Serverbetrieb und die Geräteverwaltung nicht gewährleistet werden.

Serverseitige Verschlüsselung (SSE-C)

Relution kann die Objekte, die es in einem S3-kompatiblen Bucket speichert, mit Server-Side Encryption und einem kundenseitig bereitgestellten Schlüssel (SSE-C) verschlüsseln. Bei SSE-C sendet Relution den Schlüssel mit jeder Anfrage mit, und das Speicher-Backend verwendet ihn, um Objekte beim Schreiben zu verschlüsseln und beim Lesen zu entschlüsseln. Das Backend speichert den Schlüssel niemals selbst - die sichere Aufbewahrung liegt ausschließlich in der eigenen Verantwortung.

Vor dem Aktivieren lesen: SSE-C wird beim Start sofort wirksam, und Relution verschlüsselt bereits im Bucket vorhandene Objekte nicht. Nur auf einer frischen Instanz mit leerem Bucket aktivieren, oder zuvor alle bestehenden Objekte verschlüsseln. Geht der Schlüssel verloren, sind alle verschlüsselten Daten unwiederbringlich verloren. Details dazu unter Wichtige Hinweise weiter unten.

SSE-C vs. KMS-Verschlüsselung: SSE-C ist nicht dasselbe wie clientseitige Verschlüsselung über AWS KMS (eingeführt in Relution 26.3.3 →). Bei KMS wird ein vom Kunden verwalteter Schlüssel (CMK) von AWS KMS gehalten und verwaltet. Bei SSE-C wird der Schlüssel von Relution bei jeder Anfrage an S3 weitergeleitet und muss eigenständig gespeichert werden. Diese beiden Mechanismen schließen sich gegenseitig aus - aktivierbar ist SSE-C oder KMS oder keines von beiden, aber niemals beide gleichzeitig.

Voraussetzungen

Für Version 26.4.0

- Eine funktionierende S3-kompatible Objektspeicher-Einrichtung - siehe Objektspeicher verbinden →.
- Ein Objektspeicher-Backend, das SSE-C unterstützt. Wir haben die Unterstützung mit SeaweedFS und Hetzner Object Storage getestet. Andere S3-kompatible Backends können funktionieren, wurden aber nicht getestet.
- Ein 256-Bit-Schlüssel (siehe unten).

Schlüssel generieren

SSE-C benötigt einen 256-Bit-Schlüssel (32 Byte), der als Base64-codierte Zeichenkette bereitgestellt wird. Ein Schlüssel lässt sich mit `openssl` generieren:

```
openssl rand -base64 32
```

Den resultierenden Wert sicher aufbewahren. Geht dieser Schlüssel verloren, können alle verschlüsselten Objekte im S3-Bucket nicht mehr entschlüsselt werden und sind unwiederbringlich verloren.

Konfiguration

SSE-C wird aktiviert, sobald ein Schlüssel konfiguriert ist. Der Schlüssel kann entweder direkt über die Konfiguration `relution.storage.s3.serverSideEncryption.key` angegeben (Option A und B) oder als Datei über `relution.storage.s3.serverSideEncryption.keyFile` bereitgestellt werden (Option C). Sind beide gesetzt, hat die Schlüsseldatei Vorrang.

Option A: Verwendung von application.yml

Den `serverSideEncryption`-Block zur `application.yml` hinzufügen:

```yaml
relution:
  storage:
    resourceStorageType: S3
    s3:
      customEndpoint: http://seaweedfs:8333
      accessKey: %IHR-ACCESS-KEY%
      secretKey: %IHR-SECRET-KEY%
      bucketName: relution
      serverSideEncryption:
        key: %IHR-BASE64-SCHLÜSSEL%
```

Für Version

Option B: Verwendung von Umgebungsvariablen

Die folgende Umgebungsvariable zum `relution` Service in der `compose.yml` hinzufügen:

```yaml
services:
  relution:
    environment:
      - RELUTION_STORAGE_S3_SERVERSIDEENCRYPTION_KEY=%IHR-BASE64-SCHLÜSSEL%
```

Option C: Schlüssel als Datei

Neu in 26.5

Alternativ zur direkten Angabe kann der Schlüssel aus einer Datei gelesen werden. Das ist vor allem dann sinnvoll, wenn der Schlüssel als Docker- oder Kubernetes-Secret in den Container eingehängt wird. Der Pfad zur Schlüsseldatei wird über `relution.storage.s3.serverSideEncryption.keyFile` konfiguriert:

```yaml
relution:
  storage:
    s3:
      serverSideEncryption:
        keyFile: /pfad/zu/ssec.key
```

Oder über die entsprechende Umgebungsvariable:

```yaml
services:
  relution:
    environment:
      - RELUTION_STORAGE_S3_SERVERSIDEENCRYPTION_KEYFILE=/pfad/zu/ssec.key
```

Die Datei muss denselben Base64-codierten 256-Bit-Schlüssel enthalten wie bei der direkten Angabe (z. B. erzeugt mit `openssl rand -base64 32`). Ein abschließender Zeilenumbruch ist unkritisch, da der Wert automatisch bereinigt wird; binär oder hexadezimal codierte Schlüssel werden abgelehnt.

Beim Start protokolliert Relution das Einlesen mit `Reading SSE-C key from file <Pfad>`. Fehlt die Datei oder enthält sie keinen 32-Byte-Schlüssel, bricht der Start mit einer entsprechenden Fehlermeldung ab.

Für Version 26.4.0

Wichtige Hinweise

Keine Migration bestehender Dateien: SSE-C wird sofort wirksam, sobald Relution mit konfiguriertem Schlüssel startet. Relution verschlüsselt keine Objekte, die bereits im Bucket vorhanden sind. SSE-C nur auf einer frischen Instanz mit leerem Bucket verwenden, oder alle bestehenden S3-Objekte verschlüsseln, bevor Relution mit dem Schlüssel gestartet wird. Andernfalls bleiben zuvor gespeicherte Objekte unverschlüsselt und können unzugänglich werden.

Schlüsselverlust bedeutet Datenverlust: Das Speicher-Backend speichert den Schlüssel nicht - die sichere Aufbewahrung liegt ausschließlich in der eigenen Verantwortung. Geht der Schlüssel verloren, werden alle verschlüsselten Objekte im Bucket unwiederbringlich verloren, und Relution kann keine Apps oder Ressourcen mehr aus dem Objektspeicher ausliefern. Den Schlüssel an einem sicheren Ort aufbewahren.

Schlüsselrotation erfordert Neuverschlüsselung: Die Rotation des Schlüssels liegt in der eigenen Verantwortung. Relution verschlüsselt Objekte bei einem Schlüsselwechsel nicht neu. Zum Rotieren des Schlüssels müssen alle bestehenden Objekte im Bucket mit dem neuen Schlüssel neu verschlüsselt werden (z.B. durch Kopieren mit dem neuen Schlüssel), bevor Relution mit der aktualisierten Konfiguration gestartet wird. Wird Relution mit einem neuen Schlüssel gestartet, während Objekte noch mit dem alten verschlüsselt sind, werden diese Objekte unzugänglich.

Gegenseitiger Ausschluss mit KMS: Serverseitige (SSE-C) und clientseitige (KMS) Verschlüsselung können nicht gleichzeitig aktiv sein. Höchstens eine von beiden konfigurieren.

Für Version 26.4.0

Migrationsanleitung

Diese Anleitung erklärt, wie sich Relution-Daten von einem Objektspeicher-Backend zu einem anderen migrieren lassen. Häufige Szenarien sind:

- Migration von MinIO zu SeaweedFS (MinIO wird nicht mehr gewartet)
- Umzug von Cloudanbieter zu selbst-gehostet (oder umgekehrt)
- Wechsel zwischen Cloud-Anbietern

Die folgenden Beispiele zeigen eine Migration von MinIO zu SeaweedFS, aber die Schritte können für jede S3-kompatible Quelle und jedes Ziel angepasst werden.

Der Migrationsprozess besteht aus vier Schritten:

1. Neues Speicher-Backend einrichten
2. Daten vom alten zum neuen Speicher kopieren
3. Relution-Konfiguration aktualisieren
4. Altes Backend entfernen

Voraussetzungen

- Zugriff auf beide Speicher-Backends gleichzeitig
- Das `rclone` Kommandozeilen-Tool (Installationsanleitung →)
- Zugangsdaten für beide Speicher-Backends

Für Version 26.4.0

Neues Backend einrichten

Bei einer Migration zu SeaweedFS zuerst der SeaweedFS-Einrichtungsanleitung → folgen, aber Relution noch nicht starten.

Sicherstellen, dass sowohl altes als auch neues Speicher-Backend laufen:

```
docker compose up -d minio seaweedfs
```

rclone konfigurieren

Das `rclone` Tool bietet eine schnelle und zuverlässige Möglichkeit, Daten zwischen S3-kompatiblen Backends zu kopieren.

rclone installieren

Den Anweisungen auf rclone.org/install → für das jeweilige Betriebssystem folgen.

Remote-Konfigurationen erstellen

Den Konfigurationsassistenten starten:

```
rclone config
```

Die Quelle konfigurieren (MinIO):

1. `n` für neuen Remote tippen
2. Name: `source`
3. Storage-Typ: `s3` wählen
4. Provider: `Minio` wählen (oder `Other` für generisches S3)
5. Den eigenen Access Key und Secret Key eingeben
6. Endpoint: `http://localhost:9000`
7. Die Standardwerte für die verbleibenden Optionen übernehmen
8. Mit `y` bestätigen

Das Ziel konfigurieren (SeaweedFS):

1. `n` für neuen Remote tippen
2. Name: `dest`
3. Storage-Typ: `s3` wählen
4. Provider: `Other` wählen
5. Den neuen Access Key und Secret Key eingeben
6. Endpoint: `http://localhost:8333`
7. Die Standardwerte für die verbleibenden Optionen übernehmen
8. Mit `y` bestätigen

`q` tippen, um die Konfiguration zu beenden.

Für Version 26.4.0

Port-Zugriff überprüfen

Sicherstellen, dass die S3-API-Ports auf dem eigenen Host freigegeben sind. Die `compose.yml` prüfen:

```
minio:
  ports:
    - "9000:9000" # S3 API - muss erreichbar sein
    - "9001:9001" # Web-Konsole
# ...
seaweedfs:
  ports:
    - "8333:8333" # S3 API - muss erreichbar sein
    - "23646:23646" # Web-Konsole
```

Daten kopieren

1. Überprüfen, dass Relution gestoppt ist, um Datenänderungen während der Migration zu verhindern:

```
docker compose ps  # Sollte Speicher-Backends anzeigen, aber NICHT relution
```

2. Den Transfer starten:

```
rclone copy source:relution dest:relution --progress
```

3. Auf den Abschluss warten. Die Übertragungszeit hängt von der Datenmenge im Bucket ab.
4. Den Transfer überprüfen:

```
rclone check source:relution dest:relution
```

Erwartete Ausgabe: `0 differences found`

Relution-Konfiguration aktualisieren

Die Relution-Konfiguration aktualisieren, um auf das neue Backend zu zeigen. Dabei muss Folgendes geändert werden:

Einstellung	Alter Wert	Neuer Wert
Endpoint	`http://minio:9000`	`http://seaweedfs:8333`
Access Key	Alter Key	Neuer Key
Secret Key	Alter Secret	Neuer Secret

Eine detaillierte Beschreibung der Einrichtung/Änderung: Objektspeicher verbinden →

Überprüfen und Aufräumen

1. Relution starten:

```
docker compose up -d relution
```

2. Die Funktionalität überprüfen: Bei Relution anmelden und bestätigen, dass Apps und Ressourcen korrekt geladen werden.

3. Das alte Backend entfernen (nur nach gründlicher Überprüfung):

```
docker compose down minio  # Alten Service stoppen
```

4. Die Konfiguration bereinigen: Den alten Service aus der eigenen `compose.yml` entfernen.

5. Alte Daten löschen: Das alte Speicher-Volume oder -Verzeichnis entfernen (z. B. `./volumes/minio/data`).

6. rclone bereinigen: Optional lässt sich die rclone-Konfiguration entfernen:

```
rclone config delete source
rclone config delete dest
```

Connection refused / Timeout

Sicherstellen, dass die S3-API-Ports freigegeben und nicht durch eine Firewall oder Netzwerktrennung blockiert sind. Die Verbindung testen:

```
curl http://localhost:8333  # Sollte einen S3-Fehler zurückgeben
```

Access denied / 401 / 403

Überprüfen, dass die Zugangsdaten korrekt sind und der Benutzer Zugriff auf den Bucket hat.

Fehlende Dateien nach der Migration

Die Überprüfung erneut ausführen:

```
rclone check source:relution dest:relution
```

Wenn Unterschiede gefunden werden, `rclone copy` erneut ausführen; es werden nur fehlende Dateien übertragen.

Veraltet: MinIO

Wichtig: MinIO hat die Weiterentwicklung ohne vorherige Ankündigung im Oktober 2025 eingestellt. Wir raten deshalb davon ab, MinIO weiterhin zu verwenden.

Neue Infos für Objektspeicher gibt es hier:
Objektspeicher →

Für die Migration von MinIO haben wir eine Anleitung erstellt: Objektspeicher-Migration →

Veraltete MinIO-Installationsanleitung

Checkliste

Nach Abschluss der Installation folgt hier eine Liste kleiner Aufgaben, mit denen sich sicherstellen lässt, dass die Installation wie erwartet funktioniert.

Anmeldung

Aus Sicherheitsgründen ist die Anmeldung nur via HTTPS möglich. Beim Login-Versuch via HTTP erscheint folgende Fehlermeldung:

```
Zugang nicht gestattet
```

System Administrator

Mit Hilfe des Systemadministrators können weitere Organisationen erstellt werden.

Die Anmeldung bei Relution als Systemadministrator erfolgt mit den Anmeldedaten, die in der `application.yml` oder in den Umgebungsvariablen definiert sind.

Für Version 26.4.0

application.yml

```yaml
relution:
  system:
    admin:
      password: ""
      email: ""
```

Umgebungsvariablen

```
SYSTEM_ADMIN_PASSWORD=""
SYSTEM_ADMIN_EMAIL=""
```

Aus Sicherheitsgründen ist es erforderlich, das Passwort nach der ersten Anmeldung zu ändern! Zudem wird das Sysadmin Password nur beim Initialen Anlegen (i.d.R. erster Serverstart) ausgewertet und gesetzt. Es lässt sich

danach über die Konfiguration nicht ändern.

Organisationsadministrator

Die Anmeldung bei Relution als Organisationsadministrator ist möglich. Bei Verwendung von LDAP → sicherstellen, dass eine Anmeldung mit mindestens einem LDAP-Benutzerkonto möglich ist.

Test
Die Anmeldung mit einem lokalen Konto ist möglich
Die Anmeldung mit einem LDAP-Konto ist möglich

Aus Sicherheitsgründen empfehlen wir dringend, das Passwort nach dem ersten Anmeldung zu ändern.

Zertifikate

Für Version 26.4.0

Sicherstellen, dass eine Verbindung zu Relution über den externen Hostnamen möglich ist. Mobile Geräte können strenger sein, wenn es um die Überprüfung von SSL-Zertifikaten geht. Selbst wenn der Desktop-Browser eine gültige HTTPS-Verbindung anzeigt, können die Geräte die Verbindung ablehnen, wenn einige Dinge nicht richtig konfiguriert sind. Wir empfehlen dringend die Verwendung von SSL Labs →, um zu überprüfen, ob alles richtig eingestellt ist.

Häufige Fehler

- Unvollständige Zertifikatskette (fehlende Zwischenzertifikate). Chrome, Firefox usw. können dies ignorieren, aber mobile Geräte können die Verbindung ablehnen.
- Der Revers Proxy nutzt Server Name Indication (SNI). Dies wird von einigen älteren Android-Versionen nicht unterstützt. Als Abhilfe sicherstellen, dass das Zertifikat des MDM-Servers das erste ist, das zurückgegeben wird.

Mobile Geräte lehnen das Zertifikat ab

Mögliche Ursache

- Die Zertifikatskette kann unvollständig sein. Eine unvollständige Kette wird von den meisten Desktop-Browsern ignoriert, kann aber auf mobilen Geräten zu Fehlern führen.

Lösung

- SSL Labs → verwenden, um zu überprüfen, ob das SSL- Zertifikat korrekt eingerichtet ist. Es dauert etwa 5 Minuten, bis der Test abgeschlossen ist. Alle gemeldeten Probleme beheben.

Mobile Geräte erhalten ein anderes Zertifikat

Mögliche Ursache

- Der Server verwendet möglicherweise die Server Name Indication (SNI), die nicht von allen mobilen Geräten unterstützt wird.

Lösung

- Den Webserver so konfigurieren, dass das erste Zertifikat, das zurückgegeben wird, dasjenige ist, das von den mobilen Geräten benötigt wird. Die Geräte sind nicht in der Lage, ein bestimmtes Zertifikat anzufordern, und verwenden immer das erste, das vom Server gesendet wird.

Datenbankbackups

Sicherstellen, dass eine `funktionierende` Datenbanksicherung vorhanden ist. Dies ist wichtig für den Fall, dass die Hardware ausfällt oder eine Aktualisierung schief geht.

Test
Die Datenbank von Relution wird in automatische Backups einbezogen
Die Datenbank lässt sich wiederherstellen (auf einem anderen Rechner)

iOS

Wir empfehlen immer die Verwendung der Relution App Family für iOS aus dem öffentlichen App Store. Diese werden automatisch in den Relution App Store importiert.

Android

Zur Verwendung der nativen Version dieser Anwendungen direkt in Relution stehen diese hier zur Verfügung: Bis Relution Server 5.10:

- Android →

Ab Relution Server 5.11:

- Android Companion →
- Android Agent →

Support

Für Support-Zwecke kann es sinnvoll sein, den Fernzugriff auf den Relution-Server zu erlauben. Empfehlenswert ist die Aktivierung oder Installation von Fernzugriffssoftware wie Remote Desktop, SSH oder TeamViewer. Für die bestmögliche Sicherheit empfiehlt sich die Verwendung von SSH mit schlüsselbasierter Authentifizierung.

Empfehlenswert ist zudem die Verwendung eines separaten Benutzerkontos für das Supportpersonal (z. B. für Audit-Zwecke). Der Support benötigt in der Regel Lese- und Schreibzugriff auf das Installationsverzeichnis von Relution und die Fähigkeit, den Relution-Dienst neu zu starten.

Der Relution Support ist in der Regel kostenpflichtig.

Für Version 26.4.0

Mail Versand

Ab Relution Server Version 5.22 kann über die grafische Oberfläche die globale SMTP Serveranbindung konfiguriert werden. Diese Anbindung ist notwendig, wenn Relution aktiv Mails versenden soll. Dies können beispielsweise Mails für einen Passwort-Reset, eine Einschreibung oder Benachrichtigung sein. Die Anbindung eines SMTP Servers ist optional. Bis Version 5.21 musste die Anbindung des SMTP Servers über die `application.yml` auf dem Server konfiguriert werden.

Konfiguration

Für System-Administratoren steht in der `Global`-Organisation unter `Einstellungen` → `Konfiguration des E-Mail-Servers` die Konfiguration des SMTP-Servers zur Verfügung. Sie umfasst folgende Felder:

- Host und Port
- Sicherheit der Verbindung: Keine, STARTTLS, STARTTLS (REQUIRETLS) oder SSL/TLS. Bei STARTTLS wechselt Relution auf eine verschlüsselte Verbindung, sofern der Server dies unterstützt; bei STARTTLS (REQUIRETLS) schlägt der Versand fehl, wenn der Server kein STARTTLS anbietet.
- Extended Hello (EHLO) verwenden
- Lokaler Hostname für HELO/EHLO: Bleibt das Feld leer, wird der externe Hostname des Servers verwendet.
- Benutzername und Passwort: Bleibt das Passwortfeld beim Bearbeiten leer, wird das bestehende Passwort beibehalten.
- Absenderadresse: Pflichtfeld; diese Adresse wird als Absender ausgehender E-Mails verwendet.

Im Bereich E-Mail-Konfiguration testen wird über Senden eine Test-E-Mail an die hinterlegte E-Mail-Adresse des System-Administrators verschickt.

Für Version 26.4.0

Vorrang zwischen Oberfläche und application.yml

Die in der Oberfläche gespeicherte Konfiguration hat Vorrang. Die Werte aus der `application.yml` bzw. aus den Umgebungsvariablen werden nur verwendet, solange in der Oberfläche keine Konfiguration gespeichert ist. Eine bestehende Konfiguration wird in der Kategorie Konfiguration des E-Mail-Servers im Bereich Konfiguration löschen über Löschen entfernt; danach greift Relution auf die `application.yml` zurück.

Änderungen an der `application.yml` werden erst nach einem Neustart des Relution-Servers wirksam.

application.yml

```yaml
relution:
  mail:
    username:
    password:
    host: localhost
    port: 25
  smtp:
    starttls: false
    ssl: false
    ehlo: true
```

Die oben gezeigten Einstellungen sind die Standardwerte, wenn sie nicht konfiguriert sind. SMTP-Konnektivität wird als Teil der Server-Zustandsprüfungen getestet, die im Systemportal angezeigt werden.

Der frühere Schlüssel `ttls` anstelle von `starttls` wird weiterhin ausgewertet. Sind `ssl` und `starttls` beide `true`, verwendet Relution SSL/TLS.

> Relution liest die Mail-Konfiguration ausschließlich unter `relution.mail` und `relution.smtp`. Einträge unter `spring.mail` werden ignoriert. Steht die Konfiguration dort, versucht Relution, Mails über `localhost` auf Port `25` zu versenden.

Für Version 26.4.0

Alternativ lassen sich die Werte über Umgebungsvariablen setzen, z. B. in einer Docker-Installation:

Umgebungsvariable	Schlüssel in der application.yml
`SMTP_HOST`	`relution.mail.host`
`SMTP_PORT`	`relution.mail.port`
`SMTP_USERNAME`	`relution.mail.username`
`SMTP_PASSWORD`	`relution.mail.password`
`SMTP_TTLS`	`relution.smtp.starttls`
`SMTP_SSL`	`relution.smtp.ssl`
`SMTP_EHLO`	`relution.smtp.ehlo`

Ein Wert, der in der `application.yml` explizit gesetzt ist, hat Vorrang vor der Umgebungsvariable.

Zusätzliche Optionen für die Mail-Session

Über `relution.mail.properties` lassen sich weitere Optionen direkt an die Mail-Bibliothek (Jakarta Mail) übergeben. Die Einträge werden unverändert übernommen und überschreiben die von Relution gesetzten Werte. Sie wirken nur, solange die Konfiguration aus der `application.yml` stammt, also keine Konfiguration in der Oberfläche gespeichert ist.

```yaml
relution:
  mail:
    host: smtp.example.com
    port: 587
    username: "relay@example.com"
    password: "xxx"
    properties:
      "[mail.smtp.from]": "mdm@example.com"
      "[mail.smtp.starttls.required]": "true"
      "[mail.smtp.ssl.trust]": "smtp.example.com"
  smtp:
    starttls: true
    ssl: false
    ehlo: true
```

Für Version 26.4

Die Schlüssel enthalten Punkte und stehen deshalb in eckigen Klammern und Anführungszeichen. Häufig benötigte Optionen:

Option	Wirkung
`mail.smtp.from`	Absenderadresse. Ohne Angabe bildet Relution eine Adresse aus der externen Server-URL (`no-reply+relution@<Domain>`).
`mail.smtp.localhost`	Hostname, der im `EHLO`-Befehl gemeldet wird. Ohne Angabe wird der Hostname der externen Server-URL verwendet.
`mail.smtp.starttls.required`	Bricht den Versand ab, wenn der Server kein STARTTLS anbietet.
`mail.smtp.ssl.trust`	Hosts, deren Zertifikat ohne Prüfung vertraut wird. Hilft bei Mailservern mit unvollständiger Zertifikatskette.

`mail.smtp.ssl.trust` sollte den konkreten Hostnamen des Mailservers enthalten. Der Wert `*` vertraut jedem Zertifikat jedes Servers. Die bessere Lösung bleibt, das Zertifikat der ausstellenden Zertifizierungsstelle in den Truststore aufzunehmen.

Schlägt der Versand fehl, protokolliert Relution die vollständige SMTP-Kommunikation, sobald das Loglevel für `io.relution.setting.system.email.SystemEmailConfigurationService` auf `DEBUG` steht. Loglevel anpassen →

Amazon Simple Email Service (SES) SMTP

Die empfohlenen Einstellungen für die Verbindung mit Amazon SES sind wie folgt:

```yaml
relution:
  mail:
    username: ABCDEFGHIJKLMNOPQ123
    password: "abcdefghijklmnopqrstuvwxyz/BASE64+1234567890"
    host: email-smtp.eu-central-1.amazonaws.com
    port: 587
  smtp:
    starttls: true
    ssl: false
    ehlo: true
```

Die SMTP-Parameter `Benutzername` und `Passwort` müssen ein AWS-Zugangsschlüssel und ein geheimer Schlüssel eines IAM-Benutzers mit `AmazonSesSendingAccess`-Berechtigungen sein, der `ses:SendRawEmail`-Rechte gewährt. Sicherstellen, dass die korrekte Region als Teil von `host` mit angegeben ist. Diese Einstellungen können auf der Seite `SMTP-Einstellungen` des SES-Services in der AWS-Konsole nachgeschlagen werden.

Für Version 26.4.0

Microsoft Office365 SMTP

Die empfohlenen Einstellungen um Mails über Office365 senden zu können sind diese:

Die Absenderadresse unter `Einstellungen` → `Konfiguration des E-Mail-Servers` muss mit dem Benutzernamen des Kontos übereinstimmen. Erfolgt die Konfiguration über die `application.yml`, wird die Absenderadresse über `mail.smtp.from` gesetzt (siehe Zusätzliche Optionen für die Mail-Session →). Für das Konto muss SMTP AUTH aktiviert sein.

```yaml
relution:
  mail:
    username: "email@somewhere.de"
    password: "xxx"
    host: smtp.office365.com
    port: 587
  smtp:
    starttls: true
    ssl: false
    ehlo: true
```

Disaster Recovery

Diese Anleitung beschreibt das Backup- und Sicherungskonzept für einen Relution Server, der eine Datenbank (PostgreSQL oder MariaDB) verwendet und optional ein On-Premises betriebenes S3-kompatibles Storage-System (wie z. B. MinIO) einbindet.

Das Ziel ist es, die Datenintegrität sicherzustellen, Ausfallzeiten zu minimieren (RTO) und eine zuverlässige Wiederherstellbarkeit im Notfall zu gewährleisten.

> Die Konfiguration der Backupautomatisierung, das Monitoring sowie die Sicherstellung der Durchführung der Sicherungen obliegt dem Kunden.

Zu sichernde Komponenten

Die Relution-Infrastruktur besteht typischerweise aus folgenden Komponenten, die gesichert werden müssen:

- Applikationsserver: Hostet die Relution Anwendung und Dienste.
- Datenbank (On-Premises): MariaDB oder PostgreSQL.
- S3 Storage (On-Premises): Objektbasiertes Speichersystem (optional) zur Ablage von Dateien, Backups und persistenten Daten.

> Alle Applikationen können auch auf einer einzigen Maschine gemeinsam betrieben werden. Die Verwendung des S3 Storage ist optional, aber im Verwendungsfall ist ohne die Inhalte des S3 Buckets ein Betrieb des Relution Servers nicht möglich.

Für Version 26.4.0

Backup-Ziele

- Minimierung des Datenverlusts (RPO – Recovery Point Objective)
- Schnelle Wiederherstellung der Dienste (RTO – Recovery Time Objective)
- Schutz vor Hardwareausfall, Softwarefehlern und menschlichen Fehlern
- Schutz vor Datenmanipulation sowie Ransomware

1. Datenbank-Backup

Strategie	Details
Häufigkeit	Tägliche vollständige Dumps (z. B. via `mariadb-dump` oder `pg_dump`)
Inkrementell	Stündliche inkrementelle Backups (je nach Notwendigkeit)
Verwaltung	Automatisierte Rotation und Aufbewahrungsregeln
Sicherheit	Verschlüsselung der Backupdateien (AES256 oder GPG) je nach Notwendigkeit
Konsistenz	Während des Backups sollte der Relution-Dienst vorübergehend gestoppt werden, um Inkonsistenzen zu vermeiden!

2. S3-Storage-Backup (Optional)

Für Version 26.4.0

Strategie	Details
Methode	Replikation auf zweites S3-Ziel oder regelmäßiges Syncing (`s3cmd sync`, `rclone sync`)
Umfang	Sicherung kritischer Buckets in definierten Intervallen
Konsistenz	Während des Backups sollte der Relution-Dienst vorübergehend gestoppt werden, um Inkonsistenzen zu vermeiden!

3. Server-Konfigurationsbackup

Es müssen alle relevanten Konfigurationsdateien gesichert werden:

- `/opt/relution` (Verzeichnis des Relution Servers)
- `compose.yml` (oder vergleichbare Startskripte)
- `application.yml` (Relution Konfiguration)
- Ggf. die NginX Konfigurationsdatei
- SSL Zertifikat und Schlüssel

Backup-Speicherorte

Es wird die Einhaltung des 3-2-1-Backup-Prinzips empfohlen:

- 3 Kopien der Daten
- 2 unterschiedliche Systeme/Medien
- 1 Kopie extern/offsite

Zeitplanung

Intervall	Sicherung
Täglich	Voll-Backup der Datenbank
Stündlich	Inkrementelles DB-Backup (je nach Notwendigkeit)
Täglich	S3-Sync kritischer Buckets
Wöchentlich	Vollständiges Server-Konfigurationsbackup

Für Vers

Weitere Aspekte

Bereich	Details
Automatisierung	Cronjobs oder systemd Timer; Logging aller Prozesse; Benachrichtigungen bei Fehlern
Verschlüsselung	Verschlüsselung aller Backups; TLS/HTTPS/SSH für Transport
Integritätsprüfung	Monatliche Test-Wiederherstellung

1. Datenbank-Wiederherstellung

1. Auswahl der korrekten Backupdatei
2. Zielsystem vorbereiten (Datenbankdienst stoppen)
3. Import der Daten durchführen (z. B. via `psql` oder `mysql`)
4. Funktionstest der Relution-Anwendung

2. S3 Storage-Wiederherstellung

1. Auswahl der Objekte/Buckets
2. Wiederherstellung via `rclone`, `s3cmd` oder API
3. Integritätscheck (Prüfen, ob Dateien in Relution vorhanden sind)

3. Gesamtsystem-Wiederherstellung

- Wiederherstellung der Konfigurationen (aus den Server-Konfigurationsbackups)
- Neustart aller Dienste
- Funktionstest der kompletten Anwendung

Für Version 26.4.0

Monitoring & Alarmierung

- Überwachung aller Backupprozesse (z. B. mit Tools wie Grafana + Prometheus)
- Alarmierung bei:
  - Fehlern bei der Sicherung
  - Niedrigem Speicherplatz
  - Integritätsfehlern
  - Fehlern beim Test-Restore

Sicherheit

- Zugriffsbeschränkungen (Least Privilege-Prinzip)
- Sichere Speicherung von Schlüsseln und Zugangsdaten
- Regelmäßige Updates der verwendeten Software

Dokumentation

- Dokumentation aller Prozessänderungen (Konfiguration, Zeitpläne)
- Klare Zuständigkeiten für Backup und Restore
- Aufbewahrung der Logdaten mindestens 90 Tage

Abschluss

Dieses Sicherungskonzept stellt sicher, dass sowohl die Datenbank als auch das On-Premises S3 Storage-System zuverlässig geschützt und im Ernstfall schnell wiederherstellbar sind. Durch Automatisierung und regelmäßige Prüfungen wird die Betriebssicherheit langfristig gewährleistet.

Für Version 26.4.0

Update

Die folgenden Schritte dienen zur Aktualisierung der Relution Installation.

> Vor dem Start sicherstellen, dass ein funktionierendes Backup der Datenbank und ggf. des S3 Storage erstellt wurde! Ein Snapshot des Servers ist in der Regel auch ausreichend.

Docker Installation

Die `docker-compose.yml` Datei bearbeiten und `image: relution/relution:xxx` mit `image: relution/relution:latest` ersetzen

Relution zu aktualisieren ist dann sehr einfach:

```
cd /opt/relution/
docker compose pull
docker compose up --detach
```

Für Versi

Bei neueren Docker Versionen hat sich die Schreibweise auf docker compose ohne Bindestrich geändert.

Sicherstellen, dass `docker_relution` mit dem Namen des Relution Containers `container_name`, der in der `docker-compose.yml` angegeben wurde, ersetzt wird, wenn er vom Standard abweicht.

Dieser Befehl wird die neuste Version des Docker Images herunterladen und installieren. Der Relution Dienst wird für einige Minuten nicht erreichbar sein, solange der Container neu startet.

Mit dem folgenden Kommando können alte Container und Caches gelöscht werden, wodurch teilweise sehr viel Speicherplatz frei wird.

```
docker system prune -a
```

```
WARNING! This will remove:
  - all stopped containers
  - all networks not used by at least one container
  - all images without at least one container associated to them
  - all build cache

Are you sure you want to continue? [y/N]
```

Image-Integrität verifizieren

Vor der Durchführung eines Docker-Updates den Image-Digest überprüfen:

1. Den SHA-256-Digest für das neue Release aus dem Relution-Release-Manifest beziehen.
2. Das neue Image herunterladen und dessen Digest überprüfen:

```
docker pull relution/relution:<new-version>
docker inspect --format='{{index .RepoDigests 0}}' relution/relution:<new-version>
```

3. Den Digest mit dem veröffentlichten Manifest vergleichen. Bei Abweichungen nicht fortfahren.
4. Nach der Überprüfung die Image-Referenz im Deployment-Manifest aktualisieren, um den verifizierten Digest zu pinnen.

Für Version 26.

Bekannte Fehlermeldungen

Update hängt bei GeneratedSelfSignedSignerKeyStore

Problem: Das Update bleibt beim Schritt `GeneratedSelfSignedSignerKeyStore` hängen.

Ursache: Ab Relution 26.x wird aus Compliance-Gründen ein anderer kryptografischer Zufallszahlengenerator verwendet (ein DRBG nach NIST SP 800-90A). Beim Start erzeugt Relution damit ein selbstsigniertes Signaturzertifikat (`GeneratedSelfSignedSignerKeyStore`) mit einem 4096-Bit-RSA-Schlüssel.

Lösung: Update auf einen aktuellen Kernel bzw. ein aktuelles Rocky- oder Alma-Linux, wie in der Docker-Installation (empfohlen) → vorausgesetzt.

Native Installation Linux

1. Das neuste Relution Paket herunterladen: Latest Relution Package →
2. Den Relution Dienst stoppen
3. Die Relution Datenbank sichern
4. Das Installationsverzeichnis sichern

```
mv <INSTALL_DIR> <INSTALL_DIR>.bak
```

5. Das Zip-Paket nach `<INSTALL_DIR>` extrahieren
6. Erneut den Eigentümer des `<INSTALL_DIR>`-Verzeichnis setzen, z.B.:

```
sudo chown -R relution:relution /opt/relution
```

7. `<INSTALL_DIR>.bak/application.yml` nach `<INSTALL_DIR>/application.yml` kopieren
8. Den Relution Dienst starten
9. Warten, bis der Relution Dienst gestartet ist

Die Datenbank wird auf den neusten Stand geupdatet. Das Update der Datenbank kann etwas Zeit in Anspruch nehmen.

Für Version 26

Native Installation Windows

1. Das neuste Relution Paket herunterladen: Latest Relution Package →
2. Den Relution-Dienst über die Diensteverwaltung (`services.msc`) stoppen
3. Das bestehende Installationsverzeichnis nach `relution_bak_` sichern
4. Das Zip-Paket in das alte Installationsverzeichnis `<INSTALL_DIR>` extrahieren
5. Die Konfigurationsdatei aus der Sicherung `relution_bak_/application.yml` nach `<INSTALL_DIR>/application.yml` kopieren
6. Den Relution Dienst starten
7. Warten, bis der Relution Dienst gestartet ist. Im Verzeichnis `<INSTALL_DIR>/log/relution.txt` kann die Log eingesehen werden

   Die Datenbank wird auf den neusten Stand geupdatet. Das Update der Datenbank kann etwas Zeit in Anspruch nehmen.

Bekannte Fehlermeldungen

Erscheint beim Starten des Relution-Dienstes die folgende Meldung, kann dies auf eine zu niedrige Java-Version hinweisen:

ion 26.4.0

```
Der Dienst "Relution" auf "Lokalem Computer" konnte nicht gestartet werden
Der Dienst hat keinen Fehler zurückgegeben
Es kann sich um einen internen Windows-Fehler oder einen internen Dienstfehler handeln
Falls das Problem weiterhin besteht, den Systemadministrator kontaktieren
```

Zur Behebung die aktuelle Java 21 LTS von folgendem Link herunterladen und installieren: Adoptium Java →
Während der Installation die Option `Home PATH setzen` aktivieren, andernfalls muss der Home Path nachträglich manuell in den Windows-Variablen eingetragen werden.
Nach der Installation den Relution-Dienst erneut starten.

Checkliste nach dem Update

- Benötigen Relution Apps auf den mobilen Geräten ebenfalls ein Update?
- Benötigen angepasste CSS Dateien ein Update?
- Sind eingeschriebene Geräte noch erreichbar?
  - Eine `Geräteinformationen aktualisieren` Aktion an ein Gerät senden
- Funktioniert die Einschreibung für die verschiedenen Plattformen noch?

Update von 26.0.3 auf 26.1/26.2 schlägt fehl

Problem: Beim Update von `Relution 26.0.3` auf `Relution 26.1` oder `26.2` schlägt das automatische Datenbank-Update mit der Fehlermeldung `Cannot change column 'action_uuid'` fehl. In den Server-Logs erscheint folgender Fehler:

```
java.sql.SQLException: (conn=1539) Cannot change column 'action_uuid': used in a
foreign key constraint 'fk_mdm_sb_actn_action_uuid'
```

Ursache: Beim Relution-Update versucht Liquibase, einer Tabellenspalte einen `NOT NULL`-Constraint hinzuzufügen, die als Fremdschlüssel definiert ist. Bei den MariaDB-Versionen `10.11.5` – `10.11.7` schlägt das mit MariaDB-Fehler 1832 fehl — ein bekanntes MariaDB-Problem (MDEV-34392 →).

Lösung: Vor dem Relution-Update muss MariaDB aktualisiert werden. Empfohlen wird eine aktuelle LTS-Version (`10.11.18`, `11.4.12`, `11.8.8` oder `12.3.2`). Vor dem MariaDB-Update ist unbedingt ein vollständiges Backup der Datenbank anzulegen.

> Da MariaDB nur noch bis Ende 2027 als Datenbankserver unterstützt wird, empfiehlt sich langfristig die Migration auf PostgreSQL → (Version 14 oder neuer).

Für Version 26.4.0

Hinweis: Update von Relution 5.3x.x auf 26.2.x

Bei einem Update von `Relution 5.3x.x` auf `Relution 26.2.x` muss zwingend zuerst auf `Relution 5.35.4` und anschließend auf die Zwischenversion `Relution 26.0.3` aktualisiert werden.

Docker

Bei Docker-Installationen kann die Version direkt in der `compose.yml` festgelegt werden.

1. Zuerst auf die letzte veröffentlichte 5.x-Version aktualisieren:

```
relution:
  image: relution/relution:5.35.4
```

2. Anschließend auf die letzte veröffentlichte 26.0.x-Version:

```
relution:
  image: relution/relution:26.0.3
```

3. Nach erfolgreichem Update kann wieder auf `latest` gestellt werden, um automatisch die aktuellste Version zu nutzen:

```
relution:
  image: relution/relution:latest
```

Linux und Windows (nativ)

Für Version 26

Für native Installationen unter Linux und Windows gilt der gleiche Ablauf wie bei Docker:

1. Update auf `Relution 5.35.4`
2. Update auf `Relution 26.0.3`
3. Update auf die aktuellste Version (`latest`)

Downloads:

- Relution 5.35.4 →
- Relution 26.0.3 →
- Relution Latest →

APNS Push Zertifikate

Um mit Apple-Geräten über MDM kommunizieren zu können, benötigt Relution ein signiertes APNS-Push-Zertifikat → (Apple Push Notification Service). Dieses Zertifikat ist an eine Apple Account gebunden und muss vor Ablauf erneuert werden.
Läuft ein Zertifikat ab, verlieren alle eingeschriebenen Apple-Geräte ihre MDM-Verbindung und müssen neu eingeschrieben werden.

Ab Relution 26.3.0 sind Neuinstallationen verpflichtet, ein eigenes APNS-Zertifikat über den Self-Service-Assistenten bereitzustellen, der auf dieser Seite beschrieben wird. Bestehende Installationen funktionieren weiterhin mit ihrer aktuellen Konfiguration und können in eigenem Tempo zur neuen Methode wechseln.

Immer das bestehende Zertifikat erneuern, anstatt ein neues zu erstellen. Wird ein Zertifikat mit einem anderen Push-Topic hochgeladen, verwenden eingeschriebene Geräte weiterhin das alte Zertifikat, bis es abläuft — danach müssen sie neu eingeschrieben werden.

Migration vom bisherigen Ablauf

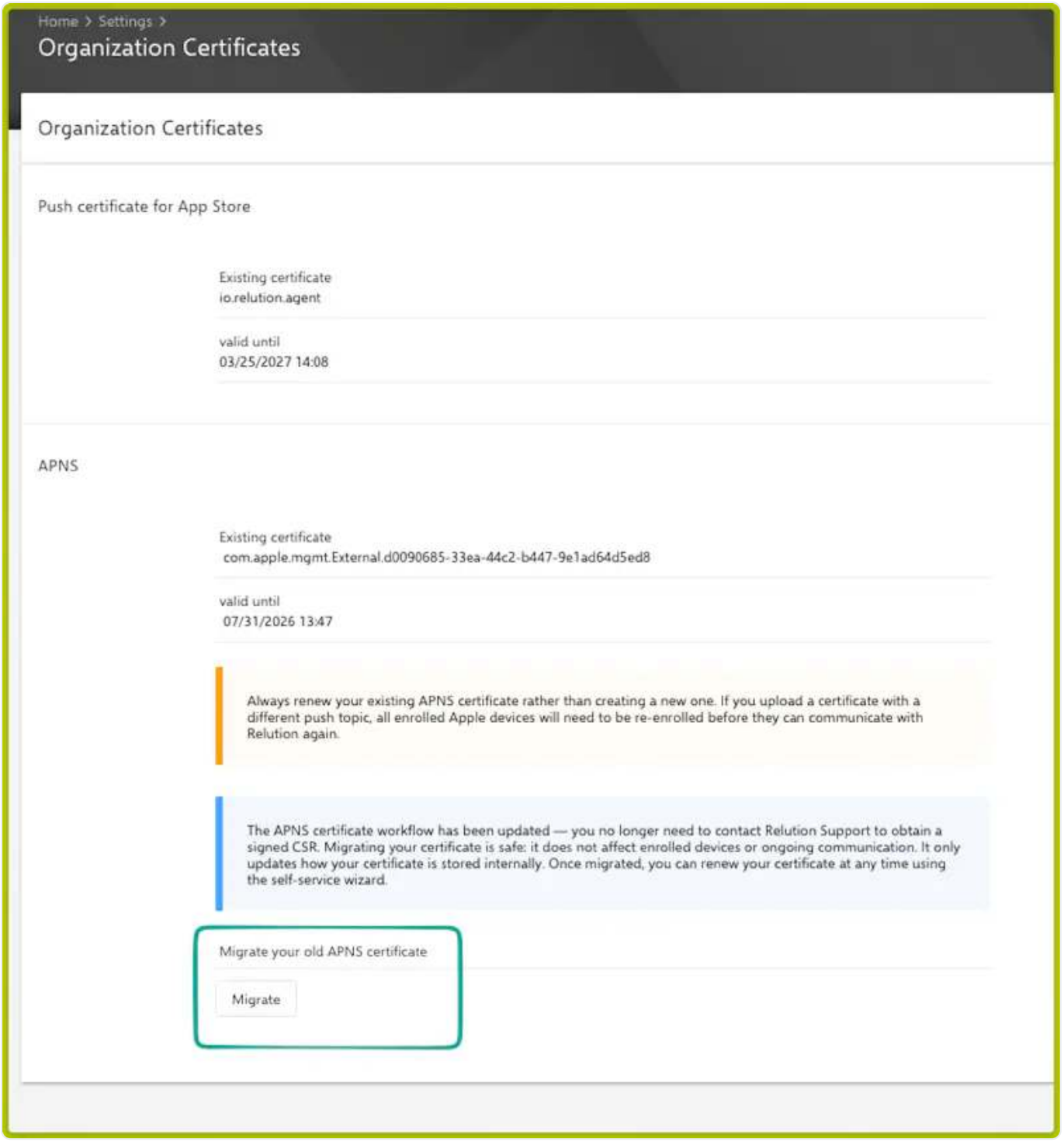
Neu in 26.3

Für Version 26.4.0

Dieser Abschnitt gilt nur, wenn zuvor ein eigenes APNS-Zertifikat durch Einsenden einer CSR an den Relution-Support bereitgestellt wurde. Wird eine neue Installation eingerichtet oder wurde das Relution-Standardzertifikat verwendet, kann dieser Abschnitt übersprungen werden.

Wurde die Relution-Installation vor Version 26.3.0 eingerichtet und wurde bisher ein Zertifikat durch Einsenden einer CSR an den Relution-Support bereitgestellt, muss vor der Nutzung des Self-Service-Assistenten einmalig eine Migration durchgeführt werden.

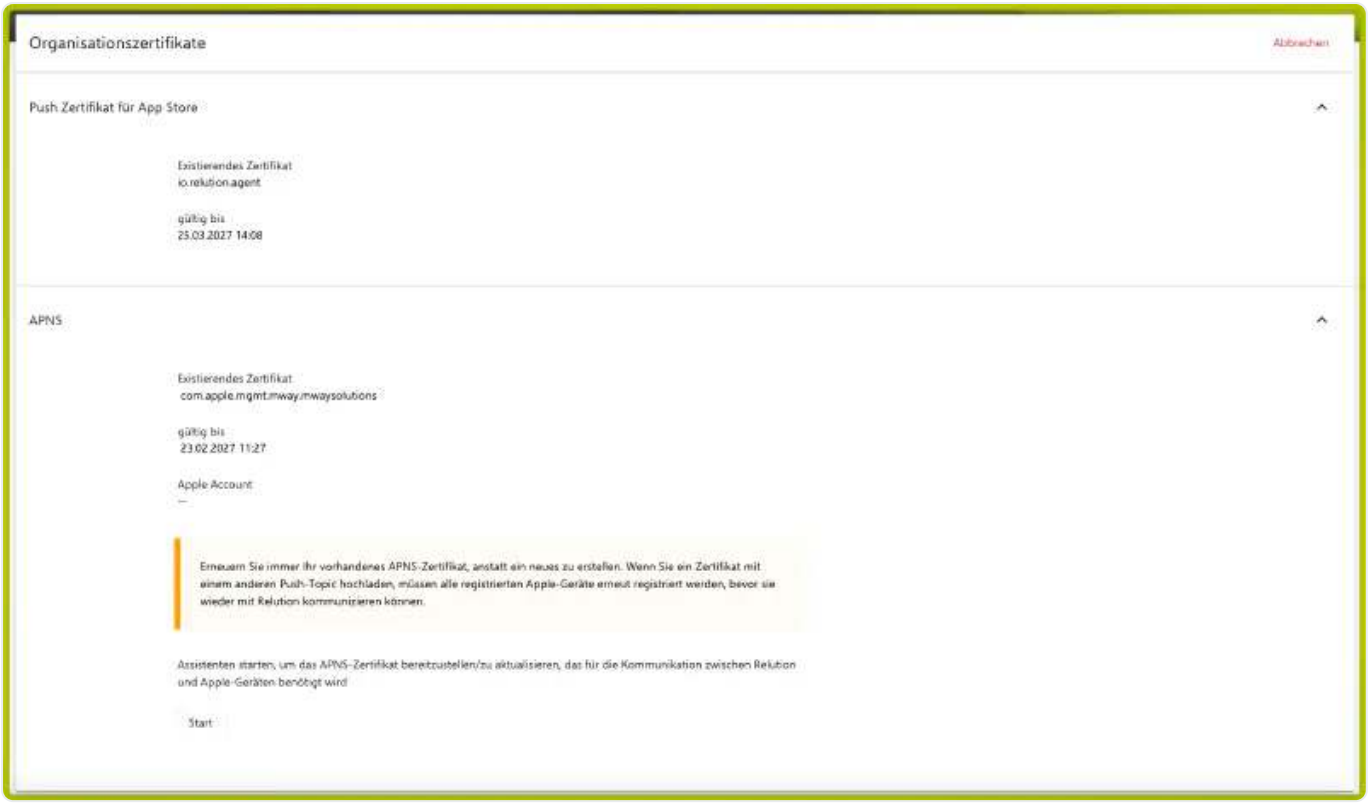
Zu `Einstellungen` → `Organisationszertifikate` navigieren. Ist eine Migration für die eigene Organisation verfügbar, erscheint eine Infobox mit der Schaltfläche Altes APNS-Zertifikat migrieren. Darauf klicken.



Die Migration ist sofort abgeschlossen und sicher: Sie hat keinen Einfluss auf eingeschriebene Geräte oder die laufende MDM-Kommunikation. Es wird lediglich aktualisiert, wie das Zertifikat intern in Relution gespeichert wird. Nach der Migration lässt sich der Self-Service-Assistent für alle künftigen Zertifikatserneuerungen nutzen.

Zertifikat einrichten oder erneuern

Zu `Einstellungen` → `Organisationszertifikate` navigieren und im APNS-Bereich auf Start klicken.

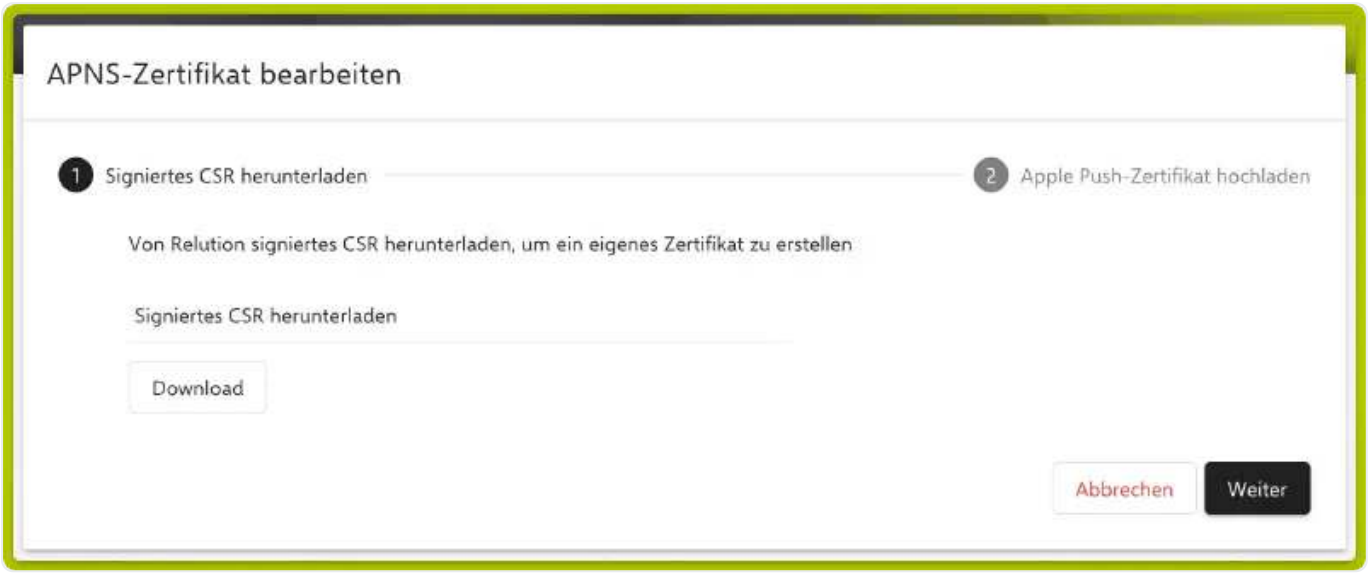


Daraufhin öffnet sich der APNS-Zertifikatsassistent.

Für Version 26.4.0

1. Signierte CSR herunterladen

Relution erstellt und signiert automatisch einen Certificate Signing Request (CSR). Auf Download klicken, um ihn zu speichern. Warten, bis der Download abgeschlossen ist, bevor auf Weiter geklickt wird.

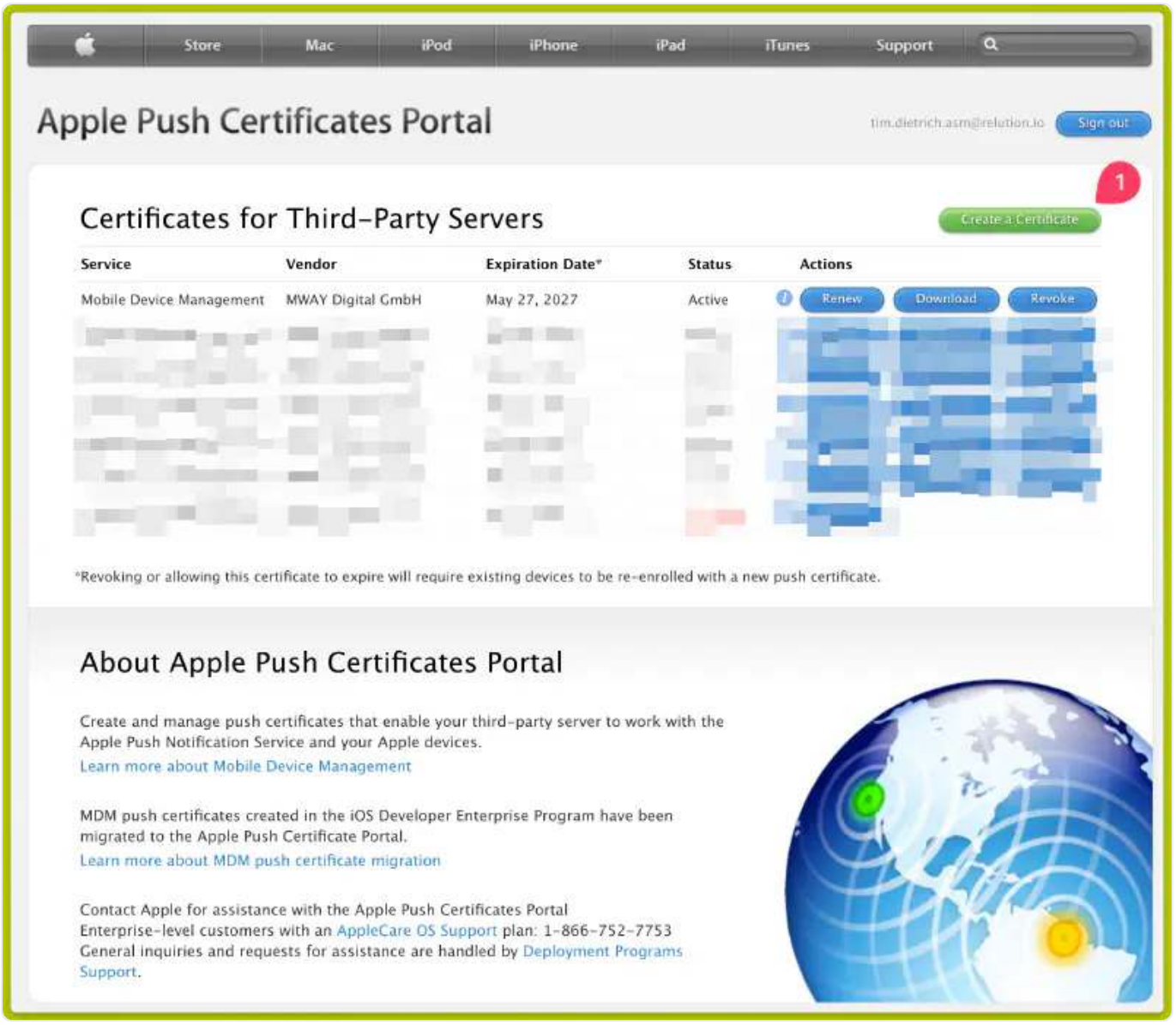


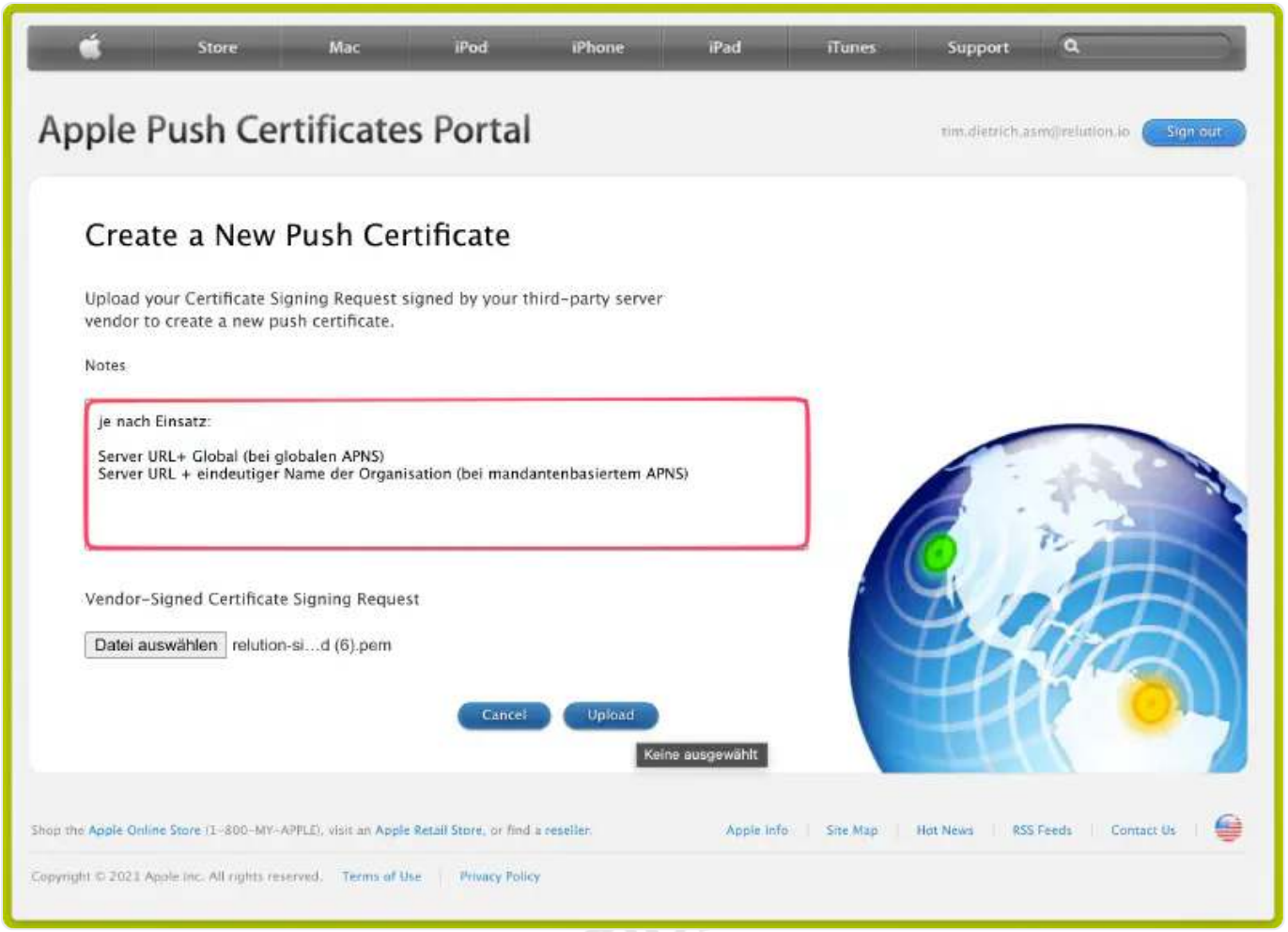
2. Apple Push-Zertifikat hochladen

Das Apple Push Certificates Portal → öffnen und sich mit der eigenen Apple-Account anmelden.

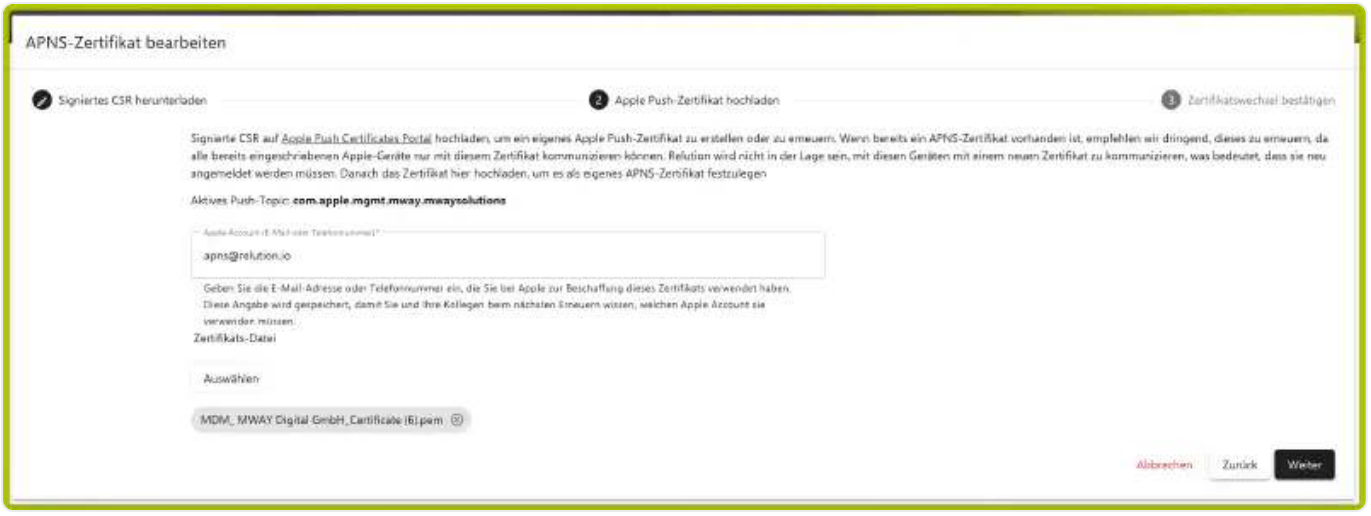
- Bestehendes Zertifikat erneuern: Das eigene Zertifikat in der Liste suchen und auf Renew klicken. Die CSR-Datei aus Schritt 1 hochladen. Dadurch bleibt das Push-Topic erhalten, sodass eingeschriebene Geräte nicht neu eingeschrieben werden müssen.
- Neuinstallation: Auf Create a Certificate klicken und die CSR-Datei hochladen.

Die `.pem`-Zertifikatsdatei vom Apple-Portal herunterladen.




Store
Mac
iPod
iPhone
iPad
iTunes
Support
Apple Push Certificates Portal
tim.dietrich.asm@relution.io
Sign out
Create a New Push Certificate
Upload your Certificate Signing Request signed by your third-party server vendor to create a new push certificate.
Notes
je nach Einsatz:
Server URL+ Global (bei globalen APNS)
Server URL + eindeutiger Name der Organisation (bei mandantenbasiertem APNS)
Vendor-Signed Certificate Signing Request
Datei auswählen
relution-si...d (6).pem
Cancel
Upload
Keine ausgewählt
Shop the Apple Online Store (1-800-MY-APPLE), visit an Apple Retail Store, or find a reseller.
Apple Info
Site Map
Hot News
RSS Feeds
Contact Us
Copyright © 2021 Apple Inc. All rights reserved.
Terms of Use
Privacy Policy

Store
Mac
iPod
iPhone
iPad
iTunes
Support
Apple Push Certificates Portal
tim.dietrich.asm@relution.io
Sign out
Confirmation
You have successfully created a new push certificate with the following information:
Service Mobile Device Management
Vendor MWAY Digital GmbH
Expiration Date Jun 3, 2027
Manage Certificates
Download
Shop the Apple Online Store (1-800-MY-APPLE), visit an Apple Retail Store, or find a reseller.
Apple Info
Site Map
Hot News
RSS Feeds
Contact Us
Copyright © 2021 Apple Inc. All rights reserved.
Terms of Use
Privacy Policy



In das Freitextfeld den Apple Account eintragen, der das Zertifikat generiert hat.

Das Zertifikat in Relution über den Datei-Uploader in diesem Schritt hochladen.

Das aktive Push-Topic wird oberhalb des Datei-Uploaders angezeigt. Sicherstellen, dass das richtige Zertifikat erneuert wird — das Push-Topic des hochgeladenen Zertifikats sollte mit dem angezeigten übereinstimmen.

- Stimmt das Push-Topic überein, auf Speichern klicken — der Assistent ist abgeschlossen.
- Hat sich das Push-Topic geändert, geht der Assistent zu Schritt 3 über.

Für Version 26.4.0

3. Zertifikatwechsel bestätigen (nur bei Push-Topic-Konflikt)

Dieser Schritt erscheint nur, wenn das hochgeladene Zertifikat ein anderes Push-Topic als das aktuelle aufweist. Dies kann passieren, wenn ein neues Zertifikat erstellt statt das bestehende erneuert wurde, oder wenn eine andere Apple Account verwendet wurde.

Wird der Assistent zum ersten Mal in einer Organisation verwendet, die bisher das Relution-Standardzertifikat genutzt hat, ist ein Push-Topic-Konflikt zu erwarten — das neue Zertifikat hat ein anderes Push-Topic. Ein Zertifikat, das auf der globalen Organisation konfiguriert ist, gilt für alle Organisationen; eines auf einer Meta-Organisation für alle ihre Unterorganisationen. Einzelne Organisationen können es mit einem eigenen Zertifikat überschreiben. Vor der Bestätigung prüfen, welche Organisationen diese Einstellung erben und ob in diesem Bereich Apple-Geräte eingeschrieben sind.

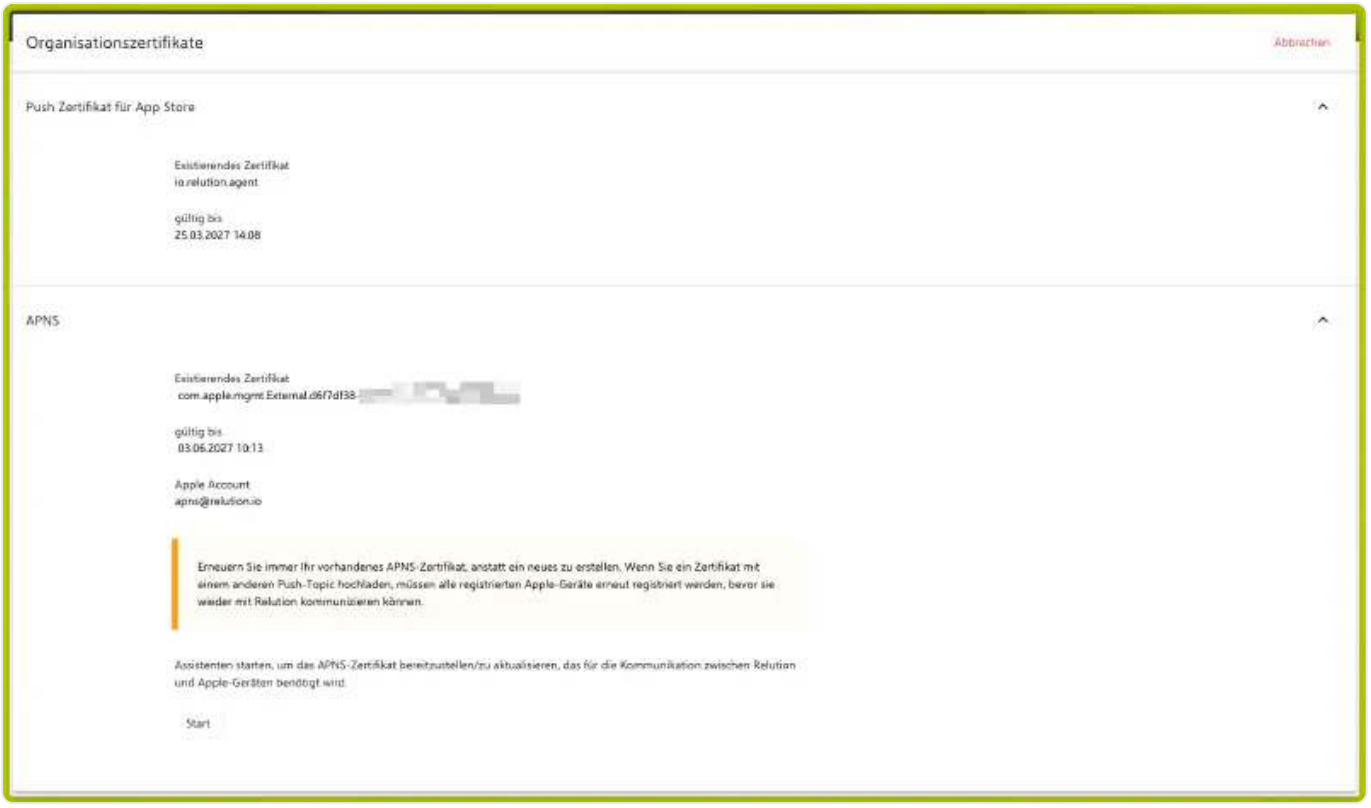
Die Änderung des Push-Topics wirkt sich auf eingeschriebene Apple-Geräte in der betroffenen Organisation aus:

- Beim Wechsel vom Relution-Standardzertifikat zu einem eigenen: Bestehende Geräte nutzen weiterhin das von Relution bereitgestellte Zertifikat — eine sofortige Neueinschreibung ist nicht erforderlich. Relution plant, das gemeinsame Zertifikat künftig einzustellen, wird jedoch ausreichend Migrationszeit sicherstellen.
- Beim Ersetzen des bestehenden eigenen Zertifikats durch ein anderes: Eingeschriebene Geräte verwenden weiterhin das alte Zertifikat, bis es abläuft. Danach verlieren sie die MDM-Verbindung und müssen neu eingeschrieben werden.

Der Assistent zeigt das alte und das neue Push-Topic an. Um die Änderung zu bestätigen:

1. Das Kontrollkästchen Ja, ich möchte das Zertifikat aktualisieren aktivieren, um zu bestätigen.

Auf Speichern klicken, um die Änderung zu übernehmen.



Ablauf und Erneuerung des Zertifikats

Die Seite Organisationszertifikate zeigt das Ablaufdatum des aktiven Zertifikats an. Relution warnt, wenn das Ablaufdatum näher rückt.

Das Zertifikat vor Ablauf erneuern. Wird der Termin verpasst:

- Alle eingeschriebenen Apple-Geräte verlieren sofort ihre MDM-Verbindung.
- Geräte müssen nach dem Hochladen des erneuerten Zertifikats neu eingeschrieben werden.

Hinweise

- Beim Erneuern eines Zertifikats immer dieselbe Apple Account verwenden. Die Verwendung einer anderen Apple Account erstellt ein neues Push-Topic und erfordert eine vollständige Neueinschreibung aller Geräte.
- Immer das bestehende Zertifikat erneuern, anstatt ein neues zu erstellen. Wird ein Zertifikat mit einem anderen Push-Topic hochgeladen, verwenden eingeschriebene Geräte weiterhin das alte Zertifikat, bis es abläuft — danach müssen sie neu eingeschrieben werden.
- Läuft ein Zertifikat ab, verlieren alle eingeschriebenen Apple-Geräte ihre MDM-Verbindung und müssen neu eingeschrieben werden.

Für Version 26.4.0

iOS-Signierungszertifikat

Sollte kein eigenes Signierungszertifikat benötigt werden, liefert Relution ab der Version 5.31.0 ein gültiges Signierungszertifikat mit. Die folgenden Schritte sind also nur notwendig, wenn der On-Premise-Server unter Version 5.31.0 liegt, oder ein eigenes Zertifikat hierfür verwendet werden soll.

Relution liefert in der Basiskonfiguration bei der Einschreibung von Apple Geräten ein Signierungszertifikat aus, dass nicht vertrauenswürdig und abgelaufen ist. Dies stellt funktional kein Problem dar, kann aber durch eine Änderung an der Konfiguration behoben werden. Auf dem Endgerät zu finden unter `Einstellungen` → `Allgemein` → `VPN & Geräteverwaltung` → `MDM Profil` → `Signierungszertifikat`

```
SIGNIERUNGSZERTIFIKAT
scep-WIN2008SCEP-CA
Ausgestellt von: scep-WIN2008SCEP-CA
Abgelaufen: 28. Oktober 2015
```

Konfiguration anpassen

Für Version 26.4.0

Das Zertifikat kann geändert werden. In diesem Fall muss in der `application.yml` folgender Abschnitt hinzugefügt werden:

```yaml
relution:
  signer:
    certificatePath: "PATH TO YOUR CERTIFICATE"
    keyPath: "PATH TO YOUR KEY"
```

Relution erwartet die beiden Dateien immer unter `/opt/relution`. Der Wert `/opt/relution` wird dem Pfad immer vornan gestellt.

In diesem Beispiel muss sowohl das Zertifikat, als auch der dazugehörige Schlüssel unter dem entsprechendem Pfad abgelegt sein.

Dockerumgebung

Wird Relution im Docker betrieben, müssen die Zertifikate noch in den entsprechenden Container gemountet werden:

```yaml
services:
  relution:
    volumes:
      - "./application.yml:/opt/relution/application.yml"
      - "./server.pem:/opt/relution/server.pem"
      - "./server.key:/opt/relution/server.key"
```

Das Volume application.yml muss nur hinzugefügt werden, sofern es noch keine solche Datei gibt.

Für Version 26.4.0

SSL-Zertifikat umwandeln

PFX-Zertifikate werden verwendet, um digitale Identitäten und Verschlüsselung in einem Dateiformat zu speichern. Die Umwandlung ist notwendig, um die Kompatibilität zwischen verschiedenen Systemen sicherzustellen. Durch die Konvertierung in andere Formate wie PEM können die Zertifikate in einer breiteren Palette von Anwendungen verwendet werden.

Konvertierung in separate PEM-Dateien

Privaten Schlüssel aus einer PFX-Datei in eine PEM-Datei extrahieren

```
openssl pkcs12 -in filename.pfx -nocerts -out key.pem
```

Das Passwort aus dem extrahierten privaten Schlüssel entfernen

```
openssl rsa -in key.pem -out server.key
```

Zertifikat exportieren

```
openssl pkcs12 -in filename.pfx -clcerts -nokeys -out server.pem
```

Das Intermediate muss in der Server.pem enthalten sein, dies kann auf folgender Seite einfach geprüft und korrigiert werden WhatsMyChainCert →

SMG

Bei der Verwendung von SMG muss die komplette Zertifikatskette als `server.pem` exportiert werden.

```
openssl pkcs12 -in filename.pfx -nokeys -out server_full_chain.pem
```

SSL-Zertifikat erneuern

Ein abgelaufenes SSL-Zertifikat des Servers hat Auswirkungen auf die Verwaltung von eingeschriebenen Geräten. Es ist daher wichtig, das SSL-Zertifikat regelmäßig zu aktualisieren, um einen reibungslosen Betrieb und die Kontrolle über die Geräte sicherzustellen.

Das Zertifikat muss erneuert werden. Die Vorgehensweise unterscheidet sich je nach Betriebssystem und Installation.

Docker

Bei einer Docker-Installation wie folgt vorgehen:

1. In der `docker-compose.yml` prüfen, wo das Zertifikat bzw. der `Key` abgelegt sind. Normalerweise sind diese Dateien `server.pem` und `server.key` genannt. Sie liegen üblicherweise im gleichen Verzeichnis.

2. In der Datei `docker-compose.yml` nach folgendem Abschnitt suchen:

```
nginx:
  volumes:
    - "./server.pem:/etc/nginx/server.pem"
    - "./server.key:/etc/nginx/server.key"
```

3. In diesem Beispiel liegen die Dateien im gleichen Verzeichnis wie die `docker-compose.yml`

4. Die `server.pem`-Datei mit dem neuen Zertifikat ersetzen. Alternativ lässt sich auch die Datei öffnen und der Inhalt ersetzen.

5. Den Docker Container neu starten.
   Dazu zunächst mit dem Befehl `docker compose down` den Container stoppen und anschließend mit `docker compose up -d` wieder starten.

Native Installation Windows mit nginx

Bei einer Windows-Installation wie folgt vorgehen:

1. Befindet sich die Datei `server.pem` nicht in dem Verzeichnis `%ProgramFiles%\nginx\conf\`, in der `nginx.conf`-Datei prüfen, wo das Zertifikat abgelegt wurde. Die Datei liegt üblicherweise unter `%ProgramFiles%\nginx\conf\nginx.conf`

2. Innerhalb dieser Datei nach diesem Abschnitt suchen:

```
nginx.conf
ssl_certificate      server.pem;
```

3. Die `server.pem`-Datei durch die des neuen Zertifikats ersetzen oder die Datei in einem Editor öffnen (als Administrator ausführen) und den Inhalt durch den des neuen Zertifikats ersetzen.

4. Im Anschluss den Dienst `nginx` neu starten.

Native Installation CentOS Linux mit nginx

Bei einer nativen Linux-Installation wie folgt vorgehen:

1. Prüfen, ob das abgelaufene Zertifikat an der Stelle `/etc/pki/tls/certs/server.pem` vorhanden ist.

2. Ist dies der Fall, eine Kopie erstellen, die Datei öffnen, den Inhalt entfernen und den Inhalt des neuen Zertifikats in die `server.pem`-Datei hineinkopieren.

3. Alternativ lässt sich die bestehende Datei auch umbenennen und das neue Zertifikat unter dem Namen `server.pem` in diesem Pfad ablegen:

```
sudo mv server.pem /etc/pki/tls/certs
sudo chown root:root /etc/pki/tls/certs/server.pem
sudo chmod 644 /etc/pki/tls/certs/server.pem
```

4. Im Anschluss muss der Dienst `nginx` noch neu gestartet werden. Dazu `systemctl stop nginx` gefolgt von `systemctl start nginx` eingeben.

Certbot

Es kann vorkommen, dass Certbot aus verschiedenen Gründen kein neues Zertifikat angefordert hat. Dies lässt sich auch manuell durchführen. Dazu in der Konsole `certbot renew` eingeben, um ein neues Zertifikat anzufordern.

Für Version 26.4.0

CA-Zertifikat in Docker

Für die Anbindung von Diensten mit selbstsigniertem oder unternehmensinternem TLS-Zertifikat muss die zugehörige Root- oder Intermediate-CA im Trust Store des Relution-Containers hinterlegt werden, damit die Verbindung als vertrauenswürdig eingestuft wird. Je nach Relution-Version kommen dafür unterschiedliche Verfahren zum Einsatz.

Zertifikate über die Benutzeroberfläche hinterlegen

Neu in 26.4

Das Docker-Image von Relution basiert ab Version 26.4 auf Ubuntu statt auf AlmaLinux. Dadurch entfällt im Container der Pfad `/etc/pki/ca-trust/source/anchors/`, sodass ein Copy-Skript auf Basis dieses Pfads fehlschlägt. Ab Relution 26.4 erfolgt die Hinterlegung von CA-Zertifikaten daher über die Benutzeroberfläche — ein Vorteil dabei ist zudem, dass sich die Konfiguration so auch im laufenden Betrieb anpassen lässt.

Dafür sind folgende Schritte erforderlich:

- Ein bestehendes Prerun-Script (Umgebungsvariable `RELUTION_PRERUN_SCRIPT` in der `docker-compose.yml`) wird aus der Konfiguration entfernt, anschließend wird der Relution-Container neu gestartet.
- Die Anmeldung erfolgt in der globalen Organisation.
- Unter `Einstellungen` → `Zertifikate` werden die gewünschten CA-Zertifikate hochgeladen (siehe Zertifikatsverwaltung →).
- Unter `Einstellungen` → `TLS-Vertrauenskonfiguration` → `Vertrauenswürdige Zertifikate` werden die hochgeladenen CA-Zertifikate über Zertifikat hinzufügen aus der Zertifikatsbibliothek ausgewählt.

Für Version 26.4.0

Script-basierte Einbindung (vor Relution 26.4)

Anleitung anzeigen

CA-Zertifikat in Java Keystore

Es kann notwendig sein, ein Zertifikat in den Java Keystore zu laden und dieses vertrauenswürdig zu machen. Dies kann nötig sein, wenn beispielsweise ein selbstsigniertes Zertifikat eines Exchange Servers mit dem Relution Secure Mail Gateway genutzt werden soll.

Anleitung

1. Die Windows-Kommandozeile mit administrativer Berechtigung öffnen.
2. In das Verzeichnis `%JAVA_HOME%\lib\security` wechseln.
   Der Pfad kann je nach Java Version und Anbieter abweichen.
3. Diesen Befehl in der CMD ausführen (im Beispiel liegt das Zertifikat unter C:\temp\mdeCert.cer):

```
keytool -import -trustcacerts -alias mdecert -file C:\temp\mdeCert.cer -keystore
cacerts
```

4. Wird nach einem Passwort gefragt, `changeit` eingeben. Dies ist das Standardkennwort des Keystores.
5. Erfolgt die Frage, ob dem Zertifikat vertraut werden soll, `yes` eingeben. Das Zertifikat wird importiert und es sollte eine Meldung mit dem Inhalt: `Zertifikat wurde zum Keystore hinzugefügt` erscheinen.

DB Konvertierung zu UTF8MB4

UTF8MB4 ist eine Erweiterung des UTF-8-Zeichencodierungsformats. Das ursprüngliche UTF-8-Format verwendet eine variable Anzahl von Bytes, um Unicode-Zeichen darzustellen. Es unterstützt jedoch nur die Zeichen des ursprünglichen Unicode-Standards, der maximal 65.536 Zeichen umfasste.

> Wird diese Anleitung als PDF-Datei betrachtet, kann es sein, dass Anführungszeichen durch ihre typografischen, d.h. geschweiften Versionen ersetzt wurden. Dadurch wird die Syntax des Skripts falsch. Sicherstellen, dass die Markdown- oder HTML-Version dieses Dokuments verwendet wird.

Konvertierung der DB

Sicherstellen, dass:

- Die `my.cnf`/`my.ini` mit der in der Relution-Installationsanleitung für das jeweilige Betriebssystem angegebenen übereinstimmt.
- Eine Datenbank existiert.
- Die Datenbank die richtigen Berechtigungen hat.

Zum Update:

1. Den Relution-Dienst stoppen.
2. Diese Query auf der Datenbank ausführen.

Für Version 26.4.0

```
USE information_schema;
SELECT "SET SESSION innodb_strict_mode=OFF, NAMES 'utf8mb4' COLLATE
'utf8mb4_general_ci';" as _sql
UNION
SELECT concat("SET foreign_key_checks = 0;") as _sql
UNION
SELECT concat("ALTER DATABASE `",table_schema,"` CHARACTER SET = utf8mb4 COLLATE =
utf8mb4_general_ci;") as _sql FROM `TABLES` where table_schema like "relution" group by
table_schema
UNION
SELECT concat("ALTER TABLE `",table_schema,"`.`",table_name,"` ENGINE=InnoDB
ROW_FORMAT=COMPRESSED;") as _sql
FROM `TABLES` where table_schema like "relution" group by table_schema, table_name
UNION
SELECT concat("ALTER TABLE `",table_schema,"`.`",table_name,"` CONVERT TO CHARACTER SET
utf8mb4 COLLATE utf8mb4_general_ci;") as _sql
FROM `TABLES` where table_schema like "relution" group by table_schema, table_name
UNION
SELECT concat("ALTER TABLE `",table_schema,"`.`",table_name, "` CHANGE
`",column_name,"` `",column_name,"` ",data_type,"(",character_maximum_length,")
CHARACTER SET utf8mb4 COLLATE utf8mb4_general_ci;") as _sql
FROM `COLUMNS` where table_schema like "relution" and data_type in ('varchar')
UNION
SELECT concat("ALTER TABLE `",table_schema,"`.`",table_name, "` CHANGE
`",column_name,"` `",column_name,"` ",data_type," CHARACTER SET utf8mb4 COLLATE
utf8mb4_general_ci;") as _sql
FROM `COLUMNS` where table_schema like "relution" and data_type in
('text','tinytext','mediumtext','longtext')
UNION
SELECT concat("SET foreign_key_checks = 1;") as _sql;
```

Dadurch wird ein SQL-Skript generiert, das für die Migration der Datenbank verwendet werden kann.

1. Das Ergebnis der Abfrage kopieren und als neue SQL-Abfrage ausführen.
2. Sicherstellen, dass die Tabellen die folgenden geänderten Angaben haben:
    - Row Format = Compressed
    - File Format = Barracuda
    - Table collation = utf8mb4_general_ci.

Illegal mix of collations

Bei Installationen mit MariaDB brechen einzelne Vorgänge mit dem Datenbankfehler `1267` ab. Häufig fällt das zuerst bei der Automatischen Geräteregistrierung (ADE, im Portal: DEP) auf: Die Synchronisierung der Geräte schlägt für alle Organisationen fehl, während der übrige Betrieb normal weiterläuft. Im Relution-Log erscheint bei jeder Synchronisierung eine Meldung wie die folgende:

```
Internal Exception: java.sql.SQLException: Illegal mix of collations
(utf8mb4_general_ci,IMPLICIT) and (utf8mb4_unicode_ci,IMPLICIT) for operation '='
Error Code: 1267
Call: DELETE FROM `mdm_auto_enrllmnt_dflt_plcy` USING `mdm_auto_enrllmnt_dflt_plcy`,
`TL_mdm_auto_enrllmnt` WHERE `mdm_auto_enrllmnt_dflt_plcy`.`auto_enrollment_uuid` =
`TL_mdm_auto_enrllmnt`.`uuid`
```

Die genannten Collations können je nach Installation abweichen, z. B. `utf8mb4_uca1400_ai_ci` statt `utf8mb4_unicode_ci`. Kennzeichnend ist eine Tabelle mit dem Präfix `TL_` in der Abfrage. Wo die Log-Dateien liegen, ist unter Relution Logs → beschrieben.

Für Version 26.4.0

Ursache

Relution erwartet für alle Textspalten die Collation `utf8mb4_general_ci`. Die Tabellen der Datenbank sind entsprechend angelegt, und auch die Datenbankverbindung von Relution arbeitet mit dieser Collation.

Für Massenänderungen, etwa das Löschen mehrerer Geräteregistrierungen während der ADE-Synchronisierung, legt Relution kurzzeitig temporäre Hilfstabellen mit dem Präfix `TL_` an. Für diese Tabellen wird keine Collation vorgegeben, sie übernehmen daher die Standard-Collation der Datenbank. Weicht diese Standard-Collation von `utf8mb4_general_ci` ab, kann MariaDB die Spalten der Hilfstabelle nicht mit den Spalten der eigentlichen Tabellen vergleichen und bricht die Abfrage ab. Die gespeicherten Daten sind davon nicht betroffen.

Eine abweichende Standard-Collation entsteht typischerweise in folgenden Fällen:

- Die Datenbank wurde auf einem MariaDB-Server angelegt, dessen `collation-server` nicht auf `utf8mb4_general_ci` gesetzt ist. Neuere MariaDB-Versionen verwenden ohne explizite Konfiguration eine andere Standard-Collation.
- Die Datenbank wurde per Dump auf einen neuen Server oder in einen neuen Container übertragen. Der Dump stellt die Tabellen mit ihrer ursprünglichen Collation wieder her, die neu angelegte Datenbank selbst erhält jedoch die Vorgabe des neuen Servers.

Lösung

Die Standard-Collation der Datenbank wird an die Collation der Relution-Tabellen angeglichen. Dabei ändert sich ausschließlich die Vorgabe für neu angelegte Tabellen, bestehende Tabellen und Daten bleiben unverändert.

> Vor dem Eingriff in die Datenbank wird ein vollständiges Backup der Datenbank empfohlen.

Erforderliche Schritte:

1. Der Relution-Dienst wird gestoppt.
2. Ein Backup der Datenbank wird erstellt.
3. Das nachfolgende Skript wird als Datei `repair_temp_table_collation_mariadb.sql` gespeichert und auf der Relution-Datenbank ausgeführt.
4. Die Ausgabe des Skripts wird geprüft (siehe unten).
5. Der Relution-Dienst wird gestartet.

Der Neustart ist zwingend erforderlich. Die temporären Hilfstabellen bestehen jeweils für die Dauer einer Datenbankverbindung. Bereits geöffnete Verbindungen verwenden sonst weiterhin die mit der falschen Collation angelegte Hilfstabelle.

Skript

Das Skript ermittelt die Collation der Relution-Tabellen, listet abweichende Spalten auf und setzt die Standard-Collation der Datenbank. Es kann gefahrlos mehrfach ausgeführt werden.

> repair_temp_table_collation_mariadb.sql

Die Platzhalter in spitzen Klammern werden in den folgenden Befehlen durch die Werte aus der `application.yml` bzw. `docker-compose.yml` ersetzt. Der Name der Relution-Datenbank (`<database>`) steht in der `application.yml` am Ende der Datenbank-URL, z. B. `relution` bei `jdbc:mariadb://localhost/relution?useServerPrepStmts=true`.

Für Version 26.4.0

Docker

Die Befehle werden im Verzeichnis `/opt/relution/` ausgeführt, in dem auch das Skript abgelegt ist.

```
docker compose stop relution

docker exec <containername> mariadb-dump -u <username> -p<password> --single-
transaction <database> > relution_backup.sql

docker exec -i <containername> mariadb -t -u <username> -p<password> <database> <
repair_temp_table_collation_mariadb.sql

docker compose start relution
```

Das Passwort wird hier direkt hinter `-p` angegeben, da die Eingabe des Skripts über die Standardeingabe erfolgt und eine interaktive Passwortabfrage dabei nicht möglich ist.

> Um zu vermeiden, dass das Passwort im Klartext in der Shell-Historie gespeichert wird, kann dem Befehl ein Leerzeichen vorangestellt oder die Historie anschließend bereinigt werden.

Nativ

Unter Linux:

```
sudo systemctl stop relution

mariadb-dump -u <username> -p --single-transaction <database> > relution_backup.sql

mariadb -t -u <username> -p <database> < repair_temp_table_collation_mariadb.sql

sudo systemctl start relution
```

Das Skript kann alternativ auch über ein Verwaltungstool wie `HeidiSQL` oder `DBeaver` auf der Relution-Datenbank ausgeführt werden.

Ausgabe prüfen

Die letzte Ausgabe des Skripts zeigt die neue Standard-Collation der Datenbank. Sie entspricht danach der Collation der Relution-Tabellen, in der Regel `utf8mb4_general_ci`.

Wird stattdessen die Meldung `ERROR: mdm_auto_enrllmnt.uuid not found - wrong schema?` ausgegeben, wurde das Skript nicht auf der Relution-Datenbank ausgeführt, meist weil beim Aufruf der Datenbankname fehlt. In diesem Fall wurde nichts geändert.

Für Version 26.4.0

Abschnitt 2 des Skripts listet alle Textspalten auf, deren Collation von der Referenz abweicht. Im Normalfall ist diese Liste leer. Enthält sie Einträge, wurden seit dem Anlegen der Datenbank Tabellen mit der falschen Collation erstellt, etwa durch Datenbank-Updates im Rahmen von Relution-Updates. Diese Tabellen können bei anderen Vorgängen denselben Fehler auslösen. Sie werden mit der Anleitung unter DB Konvertierung zu UTF8MB4 → vollständig auf `utf8mb4_general_ci` umgestellt.

Vorbeugung

Damit neu angelegte Datenbanken direkt die richtige Collation erhalten, wird der MariaDB-Server mit folgenden Einstellungen im Abschnitt `[mysqld]` betrieben:

```
[mysqld]
collation-server=utf8mb4_general_ci
character-set-server=utf8mb4
character-set-collations=utf8mb4=utf8mb4_general_ci
```

Ab MariaDB 11.5 ist die Zeile `character-set-collations` erforderlich. Ohne sie verwendet MariaDB für Verbindungen die Collation `utf8mb4_uca1400_ai_ci`, auch wenn Datenbank und Tabellen auf `utf8mb4_general_ci` stehen. Die Option gibt es ab MariaDB 11.2. Ältere Versionen wie MariaDB 10.11 LTS kennen sie nicht und starten mit dieser Zeile nicht; dort entfällt sie.

Die Prüfung der aktuellen Einstellungen erfolgt in der MariaDB-Konsole. Dabei wird zuerst die Relution-Datenbank ausgewählt:

```
USE <database>;
SHOW VARIABLES LIKE '%collation%';
```

Die Werte für `collation_server` und `collation_database` lauten dabei `utf8mb4_general_ci`. Ohne `USE` ist keine Datenbank ausgewählt (erkennbar am Prompt `MariaDB [(none)]`), und `collation_database` zeigt nur den Standard des Servers statt der Einstellung der Relution-Datenbank. Steht `collation_connection` ab MariaDB 11.5 auf `utf8mb4_uca1400_ai_ci`, fehlt in der Konfiguration die Zeile `character-set-collations`. Die vollständige Konfiguration ist in der Installationsanleitung für Linux → beschrieben.

Für Version 26.4.0

DatabaseChangeLogLock gesperrt

Die Sperre auf der Changelog-Tabelle konnte nicht aufgehoben werden. Der Relution-Dienst startet nicht mehr oder fährt immer wieder neu hoch (Docker). Im Log sind folgende Meldungen zu sehen:

```
ion.boot.LiquibaseConfig: Relution build version is … []
ion.boot.LiquibaseConfig: Database is … (Data source 'dataSource') []
ion.boot.LiquibaseConfig: Detected database type '…', version '…' []
ion.boot.LiquibaseConfig: Registering Liquibase customizations []
iquibase.MariaDBDatabase: Connected to relution@… []
iquibase.MariaDBDatabase: Setting auto commit to false from true []
vice.StandardLockService: Waiting for changelog lock.... []
vice.StandardLockService: Waiting for changelog lock.... []
```

Die letzte Meldung wiederholt sich dabei periodisch, bis der Dienst schließlich mit einem `Timeout` beendet wird und ggf. automatisch neu startet (Docker).

Ursachen

Für Version 26.4.0

Beim Start prüft der Relution-Dienst zunächst, ob Datenbank-Updates ausgeführt werden müssen. Um zu verhindern, dass im Cluster-Betrieb zwei Knoten zur selben Zeit das Datenbankschema verändern, wird dazu immer eine Sperre in der `DATABASECHANGELOGLOCK`-Tabelle gesetzt. Diese wird nach Abschluss der Prüfung und/oder der Updates wieder aufgehoben.

Wird der Relution-Dienst in diesem Zustand hart beendet, so bleibt diese Sperre bestehen. Beim nächsten Startvorgang wartet Relution darauf, dass die Sperre aufgehoben wird, da der Dienst davon ausgeht, dass ein anderer Knoten die Datenbank aktualisiert. Ist das nach ca. 5 Minuten nicht der Fall, beendet sich der Dienst mit einer entsprechenden Fehlermeldung.

Dieser Zustand tritt meist dann auf, wenn Relution während des Ausführens von größeren Datenbankupdates frühzeitig beendet wird, da der Startvorgang ungewohnt lange dauert.

Nativ

Um den Zustand zu beheben, kann entweder der (einzige) Eintrag aus der Tabelle `DATABASECHANGELOGLOCK` entfernt oder der Wert der Spalte `LOCKED` von `1` auf `0` geändert werden. Je nach Datenbank wird anstelle von `1` ggf. auch `True` angezeigt und muss entsprechend auf `False` geändert werden.

Zum Aktualisieren der Datenbank kann das entsprechende Verwaltungstool der Datenbank oder auch eine freie Alternative verwendet werden (`BeeKeeper`, `DBeaver`, `HeidiSQL`, …). Je nach Datenbank ist das Update auch über entsprechende Kommandozeilentools möglich. Im Fall von `DBeaver` zum Beispiel:

```
TRUNCATE TABLE DATABASECHANGELOGLOCK;
```

Die Platzhalter in spitzen Klammern müssen entsprechend mit den Werten aus der `application.yml` bzw. `docker-compose.yml` ersetzt werden.

Docker

Bei einem Docker-Betrieb kann der Befehl zum Entsperren der Tabelle vom Server aus im `/opt/relution/` Verzeichnis wie folgt ausgeführt werden:

Beispiel Lang

```
docker exec -it <containername> \
  mariadb --user=<username> \
        --password=<password> \
        --database=<database> \
        --execute="TRUNCATE TABLE DATABASECHANGELOGLOCK;"
```

Für Version

Beispiel Lang ausgefüllt:

```
docker exec -it docker_mariadb \
  mariadb --user=relution \
        --password=admin123 \
        --database=relution \
        --execute="TRUNCATE TABLE DATABASECHANGELOGLOCK;"
```

Beispiel Kurz

```
docker exec -it docker_mariadb mariadb -u <username> -p<password> <database> -e
"TRUNCATE TABLE DATABASECHANGELOGLOCK;"
```

Beispiel Kurz ausgefüllt

```
docker exec -it docker_mariadb mariadb -u relution -padmin123 relution -e "TRUNCATE
TABLE DATABASECHANGELOGLOCK;"
```

Um zu vermeiden, dass das Passwort in der Bash-Historie im Klartext gespeichert wird, kann die Option `-p` oder `--password` beim Befehl ohne Passworteingabe verwendet werden. Dadurch wird das Datenbankpasswort nach Absenden des Befehls interaktiv abgefragt.

Für Version 26.4.0

Migration MariaDB zu PostgreSQL

Dieser Leitfaden beschreibt den Prozess der Datenbankmigration für eine Relution-Instanz innerhalb einer Docker-Umgebung.

Voraussetzungen

Vor Beginn der Migration sicherstellen, dass folgende Bedingungen erfüllt sind:

- Speicherplatz: Mindestens so viel freier Speicherplatz wie die aktuelle MariaDB-Datenbank groß ist (1:1 Verhältnis).
- S3 Speicher: Ein kompatibler S3-Speicher muss bereits eingerichtet sein.
  Dokumentation zu S3/SeaweedFS →
- Version: Die Relution-Instanz sollte auf die Version 26.0.0 aktualisiert werden, mindestens jedoch auf Version 5.31.0 aktualisiert sein.

Datensicherung (Optional)

Falls keine Snapshots der virtuellen Maschine oder externe Backups vorhanden sind, einen manuellen Export und eine Dateisicherung durchführen.

Für Version 26.4.0

1. Export der MariaDB in eine SQL-Datei

```
docker exec docker_mariadb mariadb-dump -u relution -p --max_allowed_packet=5G
relution > relution.sql
```

2. Backup der Konfigurationsdateien

```
cd /opt/relution/ && zip -r backup.zip ./*
```

Relution aktualisieren

Sicherstellen, dass die Installation auf dem neuesten Stand ist:

```
cd /opt/relution/ && docker compose pull && docker compose up -d
```

Dienste stoppen

Den Relution-Container stoppen, um Datenkonsistenz während der Vorbereitung zu gewährleisten:

```
docker compose down relution
```

Docker-Konfiguration anpassen

Die eigene `docker-compose.yml` ergänzen. Die Services für `pgloader` und die neue `database` (PostgreSQL) hinzufügen und den `relution`-Block anpassen.

Für Version 26.4.0

Neue Services hinzufügen

```
services:
  pgloader:
    image: ghcr.io/dimitri/pgloader:latest
    networks:
      - relution-network
    volumes:
      - "./pgloader.load:/pgloader.load"
    tty: true

  database:
    image: postgres:18
    restart: unless-stopped
    container_name: database
    environment:
      TZ: "Europe/Berlin"
      POSTGRES_DB: "relution"
      POSTGRES_USER: "relution"
      POSTGRES_PASSWORD: "$PASSWORD"
    expose:
      - "5432"
    volumes:
      - "postgresql:/var/lib/postgresql"
    networks:
      - relution-network
```

Bestehenden Relution-Block anpassen

Die Abhängigkeiten ändern und das Migrations-Argument hinzufügen:

```
  relution:
    image: relution/relution:latest
    restart: on-failure # Geändert von always auf on-failure
    container_name: docker_relution
    networks:
      relution-network:
        aliases:
          - relution-docker
    depends_on:
      - database # Geändert von mariadb
    environment: # ggf. alte Listen-Schreibweise (z. B. "- TZ=Europe/Berlin") ersetzen,
nicht mit der Mapping-Schreibweise mischen
      TZ: "Europe/Berlin"
      RELUTION_ARGUMENTS: "--database-migration-only" # Neu hinzugefügt

volumes:
  mariadb:
  postgresql: # Neu hinzugefügt
```

---

pgloader Konfiguration

Für Version 26.4.0

1. Die Datei pgloader.load → in das Verzeichnis `/opt/relution/` herunterladen.
2. Die Konfiguration an die eigene Umgebung anpassen.

```
    FROM mysql://relution:dbpassword@mariadb-docker:3306/relution
    INTO postgresql://relution:dbpassword@database:5432/relution
```

Datenbank-Schema initialisieren

Zuerst die `application.yml` anpassen, damit Relution weiß, dass nun PostgreSQL genutzt wird:

```
relution:
  database:
    type: postgresql
    url: jdbc:postgresql://database/relution?currentSchema=public
    username: relution
    password: $PASSWORD
```

Nun PostgreSQL und Relution starten. Relution wird aufgrund des Flags `--database-migration-only` nur das Schema in PostgreSQL erstellen und sich dann beenden.

```
docker compose up -d database && docker compose up relution
```

Der Prozess ist abgeschlossen, wenn der Container mit Code 0 beendet wurde: `docker_relution exited with code 0`

```
docker_relution  | 2026-01-09 14:38:12.878  INFO 9 [        main] liquibase.changelog     : View mdm_parent_app_installed_app_view created []
docker_relution  | 2026-01-09 14:38:12.881  INFO 9 [        main] liquibase.changelog     : ChangeSet db/view/mdm_parent_app_installed_app_view.xml::mdm_parent_app_installe
d_app_view::REL-6120 ran successfully in 22ms []
docker_relution  | 2026-01-09 14:38:12.896  INFO 9 [        main] liquibase.ui            : Running Changeset: db/view/mdm_plcy_view.xml::mdm_plcy_view::REL-6120 []
docker_relution  | 2026-01-09 14:38:12.919  INFO 9 [        main] liquibase.changelog     : View mdm_plcy_view created []
docker_relution  | 2026-01-09 14:38:12.932  INFO 9 [        main] liquibase.changelog     : ChangeSet db/view/mdm_plcy_view.xml::mdm_plcy_view::REL-6120 ran successfully in
 33ms []
docker_relution  | 2026-01-09 14:38:12.942  INFO 9 [        main] liquibase.ui            : Running Changeset: db/view/security_group_members_view.xml::security_group_membe
rs_view::REL-6120 []
docker_relution  | 2026-01-09 14:38:12.955  INFO 9 [        main] liquibase.changelog     : View security_group_members_view created []
docker_relution  | 2026-01-09 14:38:12.964  INFO 9 [        main] liquibase.changelog     : ChangeSet db/view/security_group_members_view.xml::security_group_members_view::
REL-6120 ran successfully in 21ms []
docker_relution  | 2026-01-09 14:38:12.973  INFO 9 [        main] liquibase.ui            : Running Changeset: db/view/security_user_course_stud_usr_view.xml::security_user
_course_stud_usr_view::REL-6120 []
docker_relution  | 2026-01-09 14:38:12.988  INFO 9 [        main] liquibase.changelog     : View security_user_course_stud_usr_view created []
docker_relution  | 2026-01-09 14:38:12.990  INFO 9 [        main] liquibase.changelog     : ChangeSet db/view/security_user_course_stud_usr_view.xml::security_user_course_s
tud_usr_view::REL-6120 ran successfully in 16ms []
docker_relution  | 2026-01-09 14:38:13.014  INFO 9 [        main] liquibase.ui            : Running Changeset: db/view/security_user_course_teach_usr_view.xml::security_use
r_course_teach_usr_view::REL-6120 []
docker_relution  | 2026-01-09 14:38:13.028  INFO 9 [        main] liquibase.changelog     : View security_user_course_teach_usr_view created []
docker_relution  | 2026-01-09 14:38:13.042  INFO 9 [        main] liquibase.changelog     : ChangeSet db/view/security_user_course_teach_usr_view.xml::security_user_course_
teach_usr_view::REL-6120 ran successfully in 27ms []
docker_relution  | 2026-01-09 14:38:13.051  INFO 9 [        main] liquibase.ui            : Running Changeset: db/view/security_user_dynamic_perm_role_view.xml::security_us
er_dynamic_perm_role_view::REL-6120 []
docker_relution  | 2026-01-09 14:38:13.063  INFO 9 [        main] liquibase.changelog     : View security_user_dynamic_perm_role_view created []
docker_relution  | 2026-01-09 14:38:13.066  INFO 9 [        main] liquibase.changelog     : ChangeSet db/view/security_user_dynamic_perm_role_view.xml::security_user_dynami
c_perm_role_view::REL-6120 ran successfully in 14ms []
docker_relution  | 2026-01-09 14:38:13.072  INFO 9 [        main] liquibase.ui            : Running Changeset: db/view/security_user_group_view.xml::security_user_group_vie
w::REL-6120 []
docker_relution  | 2026-01-09 14:38:13.086  INFO 9 [        main] liquibase.changelog     : View security_user_group_view created []
docker_relution  | 2026-01-09 14:38:13.094  INFO 9 [        main] liquibase.changelog     : ChangeSet db/view/security_user_group_view.xml::security_user_group_view::REL-61
20 ran successfully in 21ms []
docker_relution  | 2026-01-09 14:38:13.104  INFO 9 [        main] liquibase.ui            : Running Changeset: db/view/security_user_view.xml::security_user_view::REL-6120
[]
docker_relution  | 2026-01-09 14:38:13.116  INFO 9 [        main] liquibase.changelog     : View security_user_view created []
docker_relution  | 2026-01-09 14:38:13.131  INFO 9 [        main] liquibase.changelog     : ChangeSet db/view/security_user_view.xml::security_user_view::REL-6120 ran succe
ssfully in 26ms []
docker_relution  | 2026-01-09 14:38:13.165  INFO 9 [        main] liquibase.util          : UPDATE SUMMARY []
docker_relution  | 2026-01-09 14:38:13.166  INFO 9 [        main] liquibase.util          : Run:                       3561 []
docker_relution  | 2026-01-09 14:38:13.166  INFO 9 [        main] liquibase.util          : Previously run:               8 []
docker_relution  | 2026-01-09 14:38:13.166  INFO 9 [        main] liquibase.util          : Filtered out:                34 []
docker_relution  | 2026-01-09 14:38:13.166  INFO 9 [        main] liquibase.util          : ------------------------------- []
docker_relution  | 2026-01-09 14:38:13.166  INFO 9 [        main] liquibase.util          : Total change sets:         3598 []
docker_relution  | 2026-01-09 14:38:13.166  INFO 9 [        main] liquibase.util          : FILTERED CHANGE SETS SUMMARY []
docker_relution  | 2026-01-09 14:38:13.166  INFO 9 [        main] liquibase.util          : DBMS mismatch:               34 []
docker_relution  | 2026-01-09 14:38:13.175  INFO 9 [        main] liquibase.util          : Update summary generated []
docker_relution  | 2026-01-09 14:38:13.211  INFO 9 [        main] liquibase.command       : Update command completed successfully. []
docker_relution  | 2026-01-09 14:38:13.211  INFO 9 [        main] liquibase.ui            : Liquibase: Update has been successful. Rows affected: 1 []
docker_relution  | 2026-01-09 14:38:13.224  INFO 9 [        main] liquibase.lockservice   : Successfully released change log lock []
docker_relution  | 2026-01-09 14:38:13.227  INFO 9 [        main] liquibase.command       : Command execution complete []
docker_relution  | 2026-01-09 14:38:15.142  INFO 9 [        main] io.relution.boot.Main   : Started Main in 226.807 seconds (process running for 230.488) []
docker_relution  | 2026-01-09 14:38:15.157  INFO 9 [        main] io.relution.boot.Main   : Startup took 00:03:47.782 []
docker_relution exited with code 0 (restarting)
```

Datenmigration durchführen

Den pgloader-Container starten und die Migration der Daten von MariaDB zu PostgreSQL durchführen:

```
docker compose up -d pgloader && docker compose exec pgloader bash
```

Innerhalb des Containers den Migrationsbefehl ausführen:

```
pgloader pgloader.load
```

```
                 public.schul_connex_configuration        0        0                  6.046s
                  public.schul_connex_orga_mapping        0        0                  6.060s
            public.schul_connex_sync_result_error         0        0                  6.075s
             public.security_asm_location_mapping         0        0                  6.086s
                  public.security_asm_sync_result         0        0                  6.069s
             public.security_email_configuration          0        0                  6.084s
                                public.security_ldap      0        0                  6.086s
                   public.security_ldap_edu_sync          0        0                  6.105s
                 public.security_ldap_group_sync          0        0                  6.105s
public.security_ldap_organization_mapping_settings        0        0                  6.114s
            public.security_ldap_server_properties        0        0                  6.111s
                 public.security_ldap_server_url          0        0                  6.123s
                public.security_ldap_sync_result          0        0                  6.130s
            public.security_ldap_teacher_mapping          0        0                  6.124s
                  public.security_ldap_user_sync          0        0                  6.144s
                              public.security_oidc        0        0                  6.162s
             public.security_organization_domain          0        0                  6.144s
                 public.security_orga_properties          0        0                  6.161s
                              public.security_user        0        1     0.2 kB       6.166s
                       public.security_user_term          0        1     0.2 kB       6.181s
                       public.srv_ntf_usr_hidden          0        0                  6.179s
                 public.stg_app_expr_ntfn_ml_msg          0        0                  6.177s
                 public.stg_app_hstry_ntfn_ml_msg         0        0                  6.213s
               public.stg_app_str_add_upldr_tmplt         0        0                  6.200s
            public.stg_app_str_whtlstd_app_dwnld          0        0                  6.200s
                   public.stg_dep_ntfn_ml_ttl             0        0                  6.219s
                         public.stg_dvc_lnd_tms           0        0                  6.210s
                 public.stg_enrllmnt_ntfn_ml_ttl          0        0                  6.242s
                public.stg_ex_prxy_andrd_blcklst          0        0                  6.225s
                public.stg_ex_prxy_macos_blcklst          0        0                  6.239s
                              public.stg_linux_mdm        0        0                  6.244s
                   public.stg_ntfn_ml_rply_to             0        0                  6.256s
                      public.stg_ntfn_psh_msg             0        0                  6.260s
                         public.stg_spprt_faq             0        0                  6.279s
                      public.stg_spprt_faq_qstn           0        0                  6.297s
                         public.stg_spprt_phn             0        0                  6.312s
         public.stg_system_email_configuration            0        0                  6.296s
                   public.stg_vpp_ntfn_ml_msg             0        0                  6.325s
                          public.system_state             0        1     0.2 kB       6.317s
                           public.time_series             0        0                  6.328s
                        public.vpp_assignment             0        0                  6.329s
                           public.vpp_publctn             0        0                  6.339s
                     public.weblink_lite_image            0        0                  6.342s
-------------------------------------------------------------------------------------------
                       COPY Threads Completion            0        4                  9.999s
                                Reset Sequences           0        0                  0.020s
                      Create Foreign Keys                 0      532                  0.215s
                         Install Comments                 0        0                  0.000s
-------------------------------------------------------------------------------------------
                        Total import time                 ✓      551   424.3 MB      10.234s
root@e78469ec45d4:/#
```

Bereinigung und Abschluss

Nach erfolgreicher Migration müssen die temporären Konfigurationen und der alte MariaDB-Container entfernt werden.

1. In der `docker-compose.yml` entfernen:
   - Den gesamten Block `mariadb:` unter `services`.
   - Den Block `pgloader:` unter `services`.
   - Das Volume `mariadb:` unter `volumes`.
2. Im `relution` Block anpassen:
   - `restart: unless-stopped` (wieder zurückstellen auf `always`).
   - Entfernen der Zeile: `- RELUTION_ARGUMENTS=--database-migration-only`.
3. Aufräumen:

```
rm pgloader.load
```

Dienste neu starten: Alles herunterfahren, um verwaiste Container zu löschen, und das System neu starten:

```
docker compose down --remove-orphans && docker compose up -d
```

Die Migration ist damit abgeschlossen und Relution läuft nun nativ auf PostgreSQL.

Für Version 26.4.0

MSSQL zu MariaDB migrieren

Mit Relution 5.25 wird der Support für Microsoft SQL Server endgültig eingestellt. Nachfolgend haben wir eine Anleitung (gültig ab Relution Version 5.24.2 / 5.25.0) wie mittels HeidiSQL GUI eine Migration durchgeführt werden kann. Bei benötigter Unterstützung bitte an das Relution Helpdesk Team wenden.

Für Version 26.4.0

Migration

1. Relution herunterfahren
   1.1 Neue Datenbank anlegen und my.cnf konfigurieren cnf Vorlage →
   1.2 Mit HeidiSQL neue Datenbank anlegen

2. Alte und neue Datenbank in HeidiSQL verbinden

3. In der neuen Datenbank Schema anlegen

4. in der application.yml folgende Werte aktualisieren
   4.1 `database type` auf `mariadb` ändern
   4.2 JDBC connection string anpassen

```
- jdbc:mariadb://<db_server>:3306/<db_name>?useServerPrepStmts=true
```

   4.3 Datenbank Benutzername und Passwort aktualisieren

5. Relution gegen die neue Datenbank starten mit foreground.bat + Parameter

```
/relution/windows-bin/foreground.bat --database-migration-only
```

6. Relution beenden

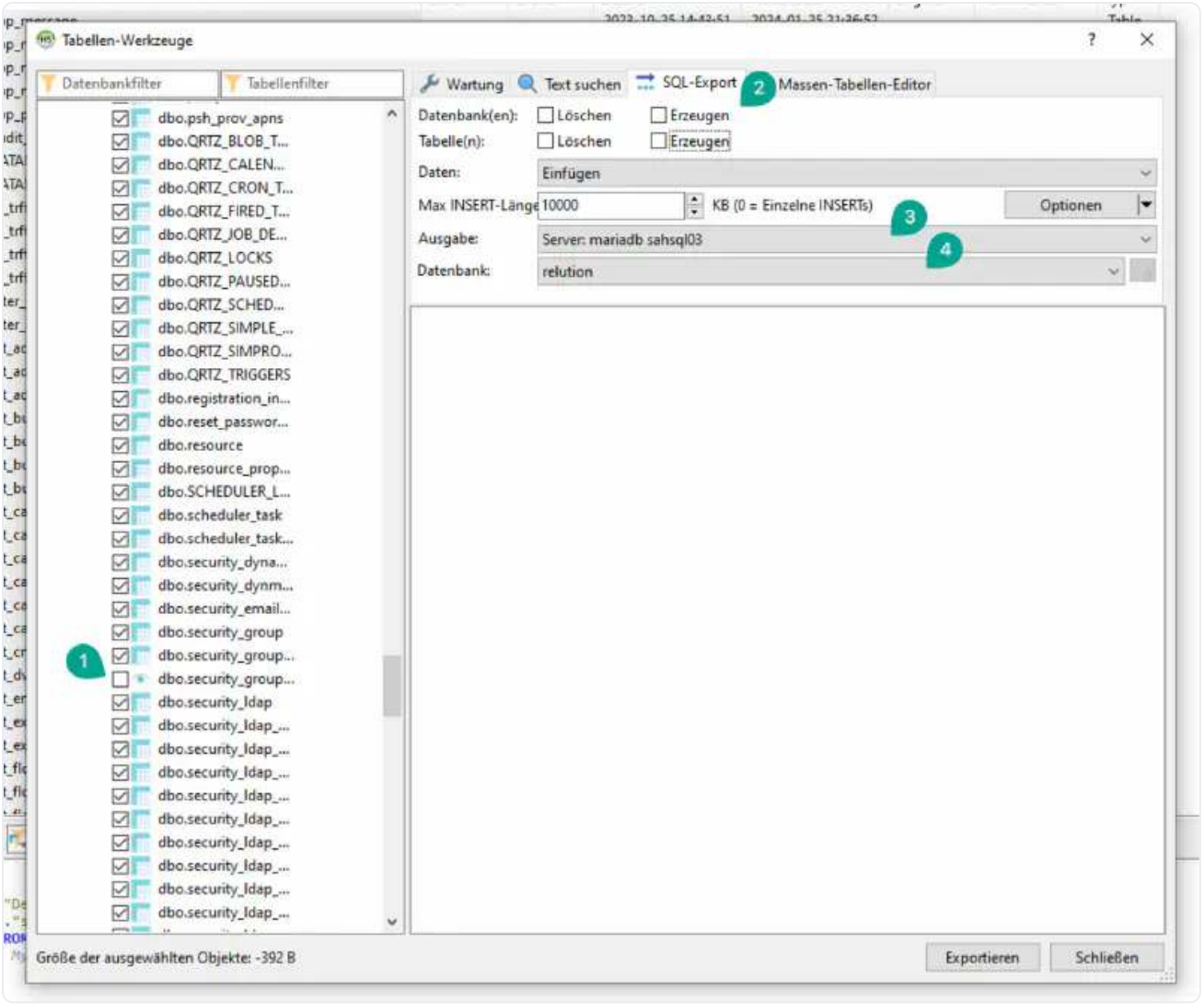
7. Rechtsklick auf die alte Datenbank

8. Datenbank Export

9. Databasechangelog + DatabaseChangeLockLock Table + alle Views abwählen + JGROUPSPing

10. Max INSERT Länge auf 10k

11. Alles abwählen bei Datenbanken und Tabellen



12. Ausgabe: Neue Datenbank Server

13. Datenbank: Neue Datenbank

14. Migration Starten

Nach der Migration

1. Relution Starten
2. Relution Log anschauen ob der Start korrekt funktioniert
3. In Relution einloggen und prüfen ob Ressourcen geladen werden können
4. Device Inventory aufmachen (prüfen ob die Datenbank views aufgehen)

Migration von Windows zu Docker

Diese Anleitung führt Schritt für Schritt durch die Migration der bestehenden Relution-Installation auf einem Windows Server hin zu einer modernen Docker-basierten Installation auf einem Linux-Server.

Jeden Abschnitt vollständig durchlesen, bevor ein Befehl ausgeführt wird.

Was passiert bei dieser Migration?

Die bisherige Relution-Installation läuft auf einem Windows Server mit einer MariaDB-Datenbank. Das neue Setup läuft auf einem Linux-Server in sogenannten „Containern" (Docker). Der Unterschied, der diese Migration notwendig macht: Windows unterscheidet bei Dateinamen und Tabellennamen nicht zwischen Groß- und Kleinschreibung. Linux hingegen schon. Deshalb müssen bestimmte Tabellennamen in der Datenbank nach dem Umzug auf Großbuchstaben umgestellt werden – dafür gibt es am Ende ein fertiges Script.

Die Migration läuft in diesen Phasen ab:

1. Datensicherung (Dump) der Datenbank auf dem Windows Server erstellen
2. Den neuen Linux-Server mit Docker vorbereiten
3. Die Datensicherung in die neue Datenbank einspielen
4. Tabellennamen auf Großbuchstaben umbenennen
5. Relution starten und prüfen

Für Version 26.4.0

Voraussetzungen vor dem Start

Sicherstellen, dass folgendes vorhanden ist:

- Zugriff auf den Windows Server (direkt vor Ort oder per Remote Desktop / RDP)
- Den Namen der Relution-Datenbank – falls unbekannt, beim Administrator nachfragen oder in der bisherigen Relution-Konfigurationsdatei nachschauen. Häufig lautet der Name schlicht `relution`.
- Das Passwort des MariaDB-Datenbankbenutzers (meist `root` oder ein dedizierter Relution-Benutzer)
- Einen Linux-Server (Ubuntu 22.04 oder 24.04 empfohlen) auf dem Docker und Docker Compose bereits installiert sind
- Zugriff auf den Linux-Server per SSH (ein Terminal-Programm wie PuTTY unter Windows oder das eingebaute Terminal unter macOS/Linux)
- Ein Dateiübertragungsprogramm wie WinSCP → (kostenlos), um Dateien vom Windows Server auf den Linux-Server zu kopieren

Phase 1 – Datensicherung auf dem Windows Server erstellen

In diesem Schritt entsteht eine vollständige Sicherungskopie der Relution-Datenbank als SQL-Datei. Diese Datei enthält alle Daten und wird später in die neue Umgebung eingespielt.

1.1 Eingabeaufforderung als Administrator öffnen

1. Auf dem Windows Server die Tastenkombination Windows-Taste + R drücken
2. `cmd` eingeben und Strg + Umschalt + Enter drücken (nicht nur Enter) – dadurch öffnet sich die Eingabeaufforderung mit Administratorrechten
3. Die Sicherheitsabfrage mit Ja bestätigen

1.2 Zielordner für die Sicherung anlegen

Folgenden Befehl eingeben und Enter drücken:

```
mkdir C:\backup
```

Dieser Befehl legt den Ordner `C:\backup` an, in dem wir die Sicherungsdatei ablegen. Falls der Ordner schon existiert, erscheint eine harmlose Meldung – einfach weitermachen.

Für Version 2

1.3 Datenbankpfad herausfinden

`mysqldump` ist das Programm, das die Sicherung erstellt. Es liegt im Installationsverzeichnis von MariaDB. Prüfen, welcher Pfad zutrifft:

```
dir "C:\Program Files\MariaDB"
```

Es erscheint z. B. ein Ordner namens `MariaDB 10.6` oder `MariaDB 10.11`. Die genaue Versionsnummer notieren – sie wird im nächsten Schritt benötigt.

1.4 Datenbank-Dump erstellen

Im folgenden Befehl `10.11` durch die tatsächliche MariaDB-Versionsnummer und `relution` durch den Namen der Datenbank ersetzen, falls dieser abweicht:

```
"C:\Program Files\MariaDB\MariaDB 10.11\bin\mysqldump.exe" -u root -p --single-transaction --routines --triggers --default-character-set=utf8mb4 relution > C:\backup\relution_dump.sql
```

Nach dem Drücken von Enter wird das Datenbankpasswort abgefragt. Es eingeben (die Eingabe ist unsichtbar – das ist normal) und Enter drücken.

Erscheint kein Fehler und ist wieder der normale Eingabeprompt sichtbar, war der Export erfolgreich.

Kurze Erklärung der verwendeten Optionen:

Option	Bedeutung
`-u root`	Anmeldung als Datenbankbenutzer `root`
`-p`	Passwort wird interaktiv abgefragt
`--single-transaction`	Sicherung ohne Datenbanksperre (laufender Betrieb bleibt möglich)
`--routines`	Gespeicherte Prozeduren werden mit gesichert
`--triggers`	Trigger werden mit gesichert
`--default-character-set=utf8mb4`	Zeichensatz für Sonderzeichen und Emojis

1.5 Sicherung prüfen

Prüfen, ob die Datei korrekt erstellt wurde:

```
dir C:\backup\relution_dump.sql
```

Die Datei sollte mit einer Größe angezeigt werden (typischerweise mehrere MB). Ist die Datei 0 Byte groß, ist etwas schiefgelaufen – dann den Befehl aus 1.4 erneut ausführen und auf Fehlermeldungen achten.

1.6 Sicherungsdatei auf den Linux-Server übertragen

WinSCP öffnen, mit dem Linux-Server verbinden (IP-Adresse, Benutzername und Passwort eingeben) und die Datei kopieren:

- Quelle (Windows): `C:\backup\relution_dump.sql`
- Ziel (Linux): `/opt/relution/relution_dump.sql`

Falls der Ordner `/opt/relution/` auf dem Linux-Server noch nicht existiert, diesen zuerst anlegen (siehe Phase 2, Schritt 2.1).

Phase 2 – Linux-Server vorbereiten

Alle folgenden Befehle werden auf dem Linux-Server in einem SSH-Terminal ausgeführt.

2.1 Arbeitsverzeichnis anlegen

```
mkdir -p /opt/relution
cd /opt/relution
```

Der Befehl `mkdir -p` legt den Ordner und alle übergeordneten Ordner an, falls sie noch nicht existieren. Mit `cd` wechseln wir in diesen Ordner.

Für Version 26.4.0

2.2 Docker Compose Datei erstellen

Docker Compose ist eine Methode, um mehrere zusammengehörige Programme (hier: Datenbank + Relution) gemeinsam zu starten und zu verwalten. Die Konfiguration wird in einer Datei namens `docker-compose.yml` gespeichert.

Datei erstellen:

```
nano /opt/relution/docker-compose.yml
```

Der Befehl `nano` öffnet einen einfachen Texteditor direkt im Terminal. Den folgenden Inhalt vollständig hineinkopieren:

> Vollständiges Konfigurationsbeispiel anzeigen

Die drei Platzhalter durch sichere Passwörter eigener Wahl ersetzen:

- `HIER_ROOT_PASSWORT_EINSETZEN` → z. B. `Tr0mmelFeuer!92`
- `HIER_RELUTION_PASSWORT_EINSETZEN` → z. B. `Rel@ution#2024` (beide Stellen müssen identisch sein!)

Die Datei speichern und schließen: Strg + O (speichern), dann Enter, dann Strg + X (beenden).

2.3 Nur die Datenbank starten

Jetzt starten wir zunächst nur den Datenbankcontainer – Relution selbst noch nicht. Das ist wichtig, damit Relution beim ersten Start nicht auf eine leere Datenbank trifft und anfängt, eigene (falsche) Tabellen anzulegen.

```
cd /opt/relution
docker compose up -d mariadb
```

Die Option `-d` steht für „detached" – der Container läuft im Hintergrund und blockiert das Terminal nicht.

2.4 Warten bis die Datenbank bereit ist

```
docker logs -f relution-db
```

Dieser Befehl zeigt die Logs (Protokollmeldungen) des Datenbankcontainers in Echtzeit an. Warten, bis folgende Meldung erscheint:

Version 26.4.0

```
[Note] mariadbd: ready for connections.
```

Sobald diese Meldung sichtbar ist, Strg + C drücken, um die Anzeige zu beenden. Die Datenbank läuft weiter im Hintergrund.

Phase 3 – Datensicherung einspielen

Falls die Dump-Datei noch nicht auf den Server übertragen wurde, dies jetzt nachholen (siehe Phase 1, Schritt 1.6).

3.1 Dump in die Datenbank importieren

```
docker exec -i relution-db mariadb \
  -u root -pHIER_ROOT_PASSWORT_EINSETZEN \
  relution < /opt/relution/relution_dump.sql
```

Zwischen `-p` und dem Passwort steht kein Leerzeichen. `HIER_ROOT_PASSWORT_EINSETZEN` durch das in der `docker-compose.yml` vergebene Root-Passwort ersetzen.

Kurze Erklärung was hier passiert: `docker exec -i relution-db` bedeutet, dass wir einen Befehl innerhalb des laufenden Datenbankcontainers ausführen. `mariadb ... < datei.sql` spielt die SQL-Datei in die Datenbank ein.

Der Import kann je nach Datenmenge einige Minuten dauern. Erscheint kein Fehler und ist wieder der normale Prompt sichtbar, war der Import erfolgreich.

3.2 Import prüfen

```
docker exec -it relution-db mariadb \
  -u root -pHIER_ROOT_PASSWORT_EINSETZEN \
  relution -e "SHOW TABLES;" | head -30
```

Dieser Befehl listet die ersten 30 Tabellen der Datenbank auf. Es sollten bekannte Tabellennamen zu sehen sein (z. B. `databasechangelog`, `qrtz_triggers` usw.). Wenn die Liste leer ist oder eine Fehlermeldung erscheint, Phase 3 wiederholen.

Phase 4 – Tabellennamen auf Großbuchstaben umbenennen

Für Version 26.4.0

Wie eingangs erklärt: Linux unterscheidet Groß- und Kleinschreibung, Windows nicht. Relution erwartet unter Linux Tabellennamen in Großbuchstaben. Dieser Schritt benennt alle betroffenen Tabellen um.

Da man eine Tabelle nicht direkt von `beispiel` in `BEISPIEL` umbenennen kann (Linux sieht das als denselben Namen), läuft das Umbenennen in zwei Runden: erst zu temporären Namen (mit `_tmp`), dann zu den finalen Großbuchstaben-Namen.

4.1 Script-Datei anlegen

```
nano /opt/relution/rename_tables.sql
```

Folgenden Inhalt vollständig in den Editor kopieren:

> Vollständiges Konfigurationsbeispiel anzeigen

Speichern und beenden: Strg + O, Enter, Strg + X.

4.2 Script ausführen

```
docker exec -i relution-db mariadb \
  -u root -pHIER_ROOT_PASSWORT_EINSETZEN \
  relution < /opt/relution/rename_tables.sql
```

Erscheint keine Fehlermeldung, war das Umbenennen erfolgreich.

4.3 Ergebnis prüfen

```
docker exec -it relution-db mariadb \
  -u root -pHIER_ROOT_PASSWORT_EINSETZEN \
  relution -e "SHOW TABLES;"
```

In der Ausgabe sind jetzt Tabellennamen in Großbuchstaben zu sehen, z. B.:

sion 26.4.0

```
DATABASECHANGELOG
DATABASECHANGELOGLOCK
JGROUPSPING
QRTZ_BLOB_TRIGGERS
...
```

Phase 5 – Relution starten

Jetzt, da die Datenbank korrekt befüllt und vorbereitet ist, starten wir den vollständigen Stack inklusive Relution:

```
cd /opt/relution
docker compose up -d
```

5.1 Start beobachten

```
docker logs -f relution-app
```

Die Ausgabe verfolgen. Relution führt beim ersten Start verschiedene Datenbankprüfungen durch – das kann 1–3 Minuten dauern. Der Start war erfolgreich, wenn eine Meldung wie folgt zu sehen ist:

```
Started Relution in XX seconds
```

Die Log-Ansicht mit Strg + C beenden.

5.2 Relution im Browser aufrufen

Einen Browser öffnen und Relution aufrufen:

```
http://IP-ADRESSE-DES-SERVERS:8080
```

`IP-ADRESSE-DES-SERVERS` durch die tatsächliche IP-Adresse des Linux-Servers ersetzen.

Häufige Probleme und Lösungen

`Table doesn't exist` beim Ausführen des Rename-Scripts Das bedeutet, der Dump-Import war nicht vollständig. Mit `SHOW TABLES;` prüfen, welche Tabellen fehlen, und Phase 3 wiederholen.

Relution startet nicht / bleibt in einer Schleife In die Logs schauen: `docker logs relution-app`. Häufigste Ursachen sind ein falsches Datenbankpasswort in der `docker-compose.yml` oder Tabellen, die noch nicht korrekt umbenannt wurden.

Die Dump-Datei ist 0 Byte groß Der Export-Befehl hat nicht funktioniert. Den Pfad zu `mysqldump.exe` und das Datenbankpasswort überprüfen.

Port 8080 ist bereits belegt Ein anderes Programm nutzt Port 8080. In der `docker-compose.yml` die Zeile `"8080:8080"` auf z. B. `"8181:8080"` ändern und Relution dann unter Port 8181 aufrufen.

WinSCP verbindet sich nicht Sicherstellen, dass auf dem Linux-Server der SSH-Dienst läuft (`sudo systemctl status ssh`) und dass die Firewall Port 22 freigibt.

Zusammenfassung der wichtigsten Dateipfade

Datei	Pfad auf dem Linux-Server
Docker Compose Konfiguration	`/opt/relution/docker-compose.yml`
Datenbank-Dump	`/opt/relution/relution_dump.sql`
Rename-Script	`/opt/relution/rename_tables.sql`

Nächste Schritte nach erfolgreicher Migration

Sobald Relution läuft und sich erfolgreich einloggen lässt:

- Prüfen, ob alle Geräte, Benutzer und Einstellungen korrekt übernommen wurden
- Ein SSL-Zertifikat einrichten (HTTPS), falls noch nicht vorhanden – Anleitung: SSL-Zertifikat einrichten →
- Sicherstellen, dass regelmäßige Backups der Docker-Volumes eingerichtet sind
- Den alten Windows Server erst abschalten, wenn die neue Umgebung mehrere Tage stabil läuft

Für Version 26.4.0

Dienst startet nicht

Unter Linux lässt sich der Relution Dienst nicht starten und über `systemctl status relution` werden diese Fehler ausgegeben:

```
Apr 12 12:02:52 Relution systemd[1]: Started Relution Server.
Apr 12 12:02:52 Relution systemd[1]: relution.service: Main process exited,
code=exited, status=203/EXEC
Apr 12 12:02:52 Relution systemd[1]: relution.service: Failed with result 'exit-code'.
Apr 12 12:02:52 Relution systemd[1]: relution.service: Service RestartSec=100ms
expired, scheduling restart.
Apr 12 12:02:52 Relution systemd[1]: relution.service: Scheduled restart job, restart
counter is at 1.
Apr 12 12:02:52 Relution systemd[1]: Stopped Relution Server
```

Relution lässt sich zudem über die `relution-foreground.sh` ganz normal starten und funktioniert wie gewohnt. Das Problem ist möglicherweise darauf zurückzuführen, dass die `Bash` nicht die Standardshell des Betriebssystems ist.

Für Version 26.4.0

Relution-Service-Datei anpassen

Hierzu kann in der `Relution Services`-Datei eine kleine Anpassung vorgenommen werden und der Dienst sollte im Anschluss wieder starten.

In der Zeile `ExecStart` der Datei `/etc/systemd/system/relution.service` muss `/bin/bash` hinzugefügt werden.
Im Anschluss lässt sich erneut versuchen, den Dienst zu starten.

```
ExecStart=/bin/bash /opt/relution/bin/relution-foreground.sh
```

Relution Logs

Docker schreibt standardmäßig keine Logs. Alles, was sich in den Protokollen lesen lässt, ist im `Systemlog` des Containers enthalten. Dies ist für die meisten Änderungen ausreichend. Es wird empfohlen, den Fehler zu provozieren, um ihn sichtbar zu machen, bevor man die Schritte durchführt.

Container-ID finden

1. Ein Terminal starten und sich ggf. einloggen
2. Herausfinden, welchen Namen und welche ID der Docker hat. Container ID und Name anzeigen

```
sudo docker ps
```

Das Terminal sollte nun die folgende Ausgabe anzeigen

ion 26.4.0

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS	NAMES
5858aa05c24c	relution/relution:latest	“/relution-docker. sh…	6 days	Up 9 seconds (health: starting)	8080/tcp 0.0.0.0:4000->4000/tcp. 8099/tcp	docker_relution

Die Informationen werden sich von denen im Beispiel unterscheiden. Zum Starten des Protokolls können der Name oder die ID des Containers verwendet werden. Im Beispiel wurde der Name verwendet

Log mit Containername starten

```
docker logs -f docker_relution
```

Die Option `-f` sorgt dafür, dass das Log immer fortlaufend angezeigt wird. Daher wird schnell viel Text im Terminal angezeigt. Das Log lässt sich mit `CTRL + C` anhalten, danach kann nach oben gescrollt werden.

Log in Datei speichern

Um die Protokolle in einer Datei im aktuellen Pfad zu speichern, diesen Befehl verwenden

```
docker logs -f docker_relution > my_logfile.txt
```

Es ist auch möglich, einen alternativen Pfad zu verwenden

```
docker logs -f docker_relution > /opt/relution/my_logfile.txt
```

Zum Übertragen der Datei auf den eigenen PC `Filezilla`, `WinSCP` oder einen anderen `SCP-Client` verwenden

Logrotation

Für Version 26.4.0

Docker-Logs sind grundsätzlich flüchtig. Manchmal kann es sinnvoll sein, diese über einen längeren Zeitraum aufzubewahren. Nachfolgend ein Beispiel auf Basis einer Rocky Linux 9 + Docker Installation.

Logrotation für Docker-Host Logs konfigurieren

Docker speichert seine Standard-Logs unter `/var/lib/docker/containers/<container-id>/<container-id>-json.log`. Damit diese Logs handhabbar bleiben, kann die integrierte Log-Rotation von Docker über die Datei `/etc/docker/daemon.json` aktiviert werden:

```
{
  "log-driver": "json-file",
  "log-opts": {
    "max-size": "10m",
    "max-file": "30"
  }
}
```

Danach den Docker-Dienst neu starten:

```
sudo systemctl restart docker
```

Logs täglich rotieren, zippen und ins Relution-Verzeichnis verschieben

Für die tägliche Archivierung kann `logrotate` verwendet werden. Hierfür muss es nachträglich auf dem Linux System installiert werden via:

```
sudo dnf install logrotate
```

Dafür muss zuerst ein Logs-Ordner erstellt werden:

```
sudo mkdir /opt/relution/logs
```

Anschließend muss eine Konfigurationsdatei unter `/etc/logrotate.d/docker` mit folgendem Inhalt erstellt werden:

Die beiden WILDCARD-Wörter in der ersten Zeile durch `*` ersetzen.

Für Version 26.4.0

```
/var/lib/docker/containers/WILDCARD/WILDCARD.log {
daily
missingok
rotate 30
compress
delaycompress
notifempty
copytruncate
create 640 root root
postrotate
    TIMESTAMP=$(date +%Y-%m-%d-%H%M%S)
    for file in $(find /var/lib/docker/containers/ -type f -name "*.log.*.gz"); do
        DIR="/opt/relution/logs"
        FILENAME="relution-${TIMESTAMP}.log.gz"
        mv "$file" "${DIR}/${FILENAME}"
    done
endscript
}
```

Mittels folgendem Test-Befehl kann eine Log sofort erstellt werden:

```
sudo logrotate --force /etc/logrotate.d/docker
```

Anschließend sollte im `/opt/relution/logs`-Ordner eine Log-Datei gespeichert sein:

```
ls -lah /opt/relution/logs
```

Linux

Wurde Relution im Standardverzeichnis `/opt/relution` installiert, finden sich die Logs in `/opt/relution/log` Die aktuellste Logdatei heißt relution.log, während archivierte Logdateien `relution.log.<Datum>.gz` genannt werden. Wenn Relution an einem anderen Ort installiert wurde, wird das Log-Verzeichnis relativ zu seinem Installationsverzeichnis gefunden

---

Windows

Für Version 26.4.0

Wenn Relution im Standardverzeichnis `C:\Programme\Relution` installiert wurde, finden sich die Logs in `C:\Programme\Relution\log`. Die aktuellste Protokolldatei heißt `relution.log`, während archivierte Protokolldateien `relution.log.<Datum>.gz` heißen. Wenn Relution an einem anderen Ort installiert wurde, wird das Log-Verzeichnis relativ zu seinem Installationsverzeichnis gefunden.

Loglevel für erweiterte Fehleranalyse anpassen

Reichen die Standard-Logs für die Analyse eines Problems nicht aus, kann das Log-Level gezielt auf `DEBUG` angehoben werden (z. B. im laufenden Betrieb ohne Neustart über die Web API oder das System-Portal). Eine ausführliche Anleitung dazu ist unter Loglevel einstellen → beschrieben.

Docker startet nicht auf EL10

Auf den Minimal- und Cloud-Images von RHEL, AlmaLinux und Rocky Linux 10 (EL10) fehlt ein Kernel-Modul-Paket, das Docker für sein Netzwerk-Setup benötigt — in diesem Fall startet Docker nicht, und die Installation von Relution lässt sich nicht fortsetzen. Diese Anleitung beschreibt, wie das fehlende Paket vor dem ersten Docker-Start nachinstalliert wird.

> Nur EL10 (Version 10) ist betroffen. Auf EL9 ist dieser Schritt nicht erforderlich — dort ist das Paket bereits vorinstalliert.

Problem

Auf den Minimal- und Cloud-Images von RHEL, AlmaLinux und Rocky Linux 10 fehlt das Paket `kernel-modules-extra`. Ohne dieses Paket kann iptables das Kernel-Modul `xt_addrtype` nicht laden, das Docker für sein Bridge- und NAT-Setup benötigt. Der Docker-Dienst startet dann nicht und bricht mit folgender Meldung ab:

```
failed to add jump rules to ipv4 NAT table: ... xt_addrtype
```

Full Version

In der Ausgabe von `systemctl status docker` erscheint häufig nur der Folgefehler `Start request repeated too quickly` — die eigentliche Ursache steht in `journalctl -xeu docker.service`.

Lösung

Die folgenden Schritte werden vor dem ersten Start von Docker ausgeführt:

```
# 1. Modul-Paket passend zum LAUFENDEN Kernel installieren
sudo dnf install -y "kernel-modules-extra-$(uname -r)"

# 2. Module laden
sudo modprobe xt_addrtype br_netfilter ip_tables

# 3. Persistent hinterlegen – werden bei jedem Boot automatisch geladen
echo -e "xt_addrtype\nbr_netfilter\nip_tables" | sudo tee /etc/modules-
load.d/docker.conf

# 4. Docker starten
sudo systemctl reset-failed docker.service
sudo systemctl enable --now docker
```

Warum diese zwei Punkte wichtig sind

- Versioniert installieren (`kernel-modules-extra-$(uname -r)`): stellt sicher, dass die Module zum *aktuell laufenden* Kernel passen. Ein einfaches `dnf install kernel-modules-extra` liefert die Module gegebenenfalls nur für einen neueren, noch nicht gebooteten Kernel — dann schlägt `modprobe` mit `Module xt_addrtype not found` fehl, bis das System neu gestartet wird. Meldet `dnf` umgekehrt kein passendes Paket zum aktuell laufenden Kernel (z. B. nach einem vorherigen `dnf update` ohne Neustart), ist stattdessen ein Neustart auf den zuletzt installierten Kernel nötig, bevor der Befehl erneut ausgeführt wird.
- **`/etc/modules-load.d/docker.conf`**: sorgt über `systemd-modules-load.service` dafür, dass die Module bei jedem Neustart automatisch geladen werden. Ohne diese Datei wäre der Fix nach dem nächsten Reboot wieder verloren.

Für Version 26.4.0

Prüfen, ob es funktioniert hat

```
sudo modprobe xt_addrtype && echo "OK – Modul ladbar"
sudo systemctl is-active docker
sudo docker run --rm hello-world
```

Erscheint bei `modprobe` keine Fehlermeldung, meldet der Dienst `active` und gibt der Testcontainer `Hello from Docker!` aus, ist der Schritt abgeschlossen.

Loglevel einstellen

In manchen Fällen ist die Ursache eines Problems im Standard Loglevel nicht zu erkennen; hier kann das Loglevel entsprechend eingestellt und der Informationen-Output erhöht werden.

Das Loglevel kann über die `application.yml`, die Web API oder das System-Portal gesetzt werden. Der Weg über die Web API wirkt sofort, benötigt keinen Neustart und keine zusätzliche Freischaltung und ist daher der empfohlene Weg im laufenden Betrieb. Für das System-Portal ist seit Relution 26.4 eine einmalige Freischaltung des zugehörigen Actuator-Endpoints erforderlich.

> Das Log-Level DEBUG sollte dabei nur zu Analysezwecken verwendet werden, da deutlich mehr Informationen ins Log geschrieben werden und dieses entsprechend stärker anwächst. Nach Abschluss der Analyse ist das Log-Level wieder auf INFO zurückzusetzen.

Speicherort der Log-Dateien

Wo sich die Protokolldateien für Docker, Linux und Windows befinden, ist unter Relution Logs → beschrieben.

Aktivierung des System-Portals

Für Version 26.4.0

Diesen Abschnitt in der `application.yml` im Relution-Verzeichnis hinzufügen:

```
relution:
  spring-boot-admin:
    enabled: true
```

> Unbedingt auf die Einrückung der einzelnen Zeilen achten (zwei Leerzeichen je Ebene). Es empfiehlt sich, das System-Portal nach Beenden der Arbeiten wieder zu deaktivieren.

Freischaltung der Actuator-Endpoints

Seit Relution 26.4 stellt Relution aus Sicherheitsgründen standardmäßig nur den Health-Endpoint bereit. Im System-Portal ist deshalb zunächst ausschließlich der Bereich `Details` sichtbar. Der Bereich `Logger` erscheint erst, nachdem der zugehörige Endpoint in der `application.yml` des Relution-Servers freigeschaltet wurde:

```yaml
management:
  endpoints:
    web:
      exposure:
        include:
          - health
          - loggers
```

Die Liste ersetzt die Standardkonfiguration vollständig. `health` muss darin enthalten bleiben, da andernfalls der Health-Endpoint entfällt und damit auch die Statusanzeige des System-Portals sowie die Health-Prüfungen von Loadbalancern und Cluster-Knoten.

Nach der Anpassung ist ein Neustart des Relution-Servers erforderlich, damit die Änderung wirksam wird.

Weitere Bereiche des System-Portals lassen sich nach demselben Muster einzeln ergänzen:

Bereich im System-Portal	Endpoint
Logger	`loggers`
Environment	`env`
Metrics	`metrics`
Threads	`threaddump`
Caches	`caches`
Scheduled Tasks	`scheduledtasks`
Mappings	`mappings`
Configuration Properties	`configprops`
Logfile	`logfile`
Quartz	`quartz`

Die Actuator-Endpoints werden auf dem Management-Port 8099 ohne Authentifizierung bereitgestellt. Dieser Port darf nicht aus nicht vertrauenswürdigen Netzwerken erreichbar sein. Die Endpoints env, configprops und heapdump geben darüber hinaus Konfigurationswerte und Speicherinhalte inklusive Zugangsdaten preis. Freischaltungen sind daher nach Abschluss der Analyse wieder zu entfernen.

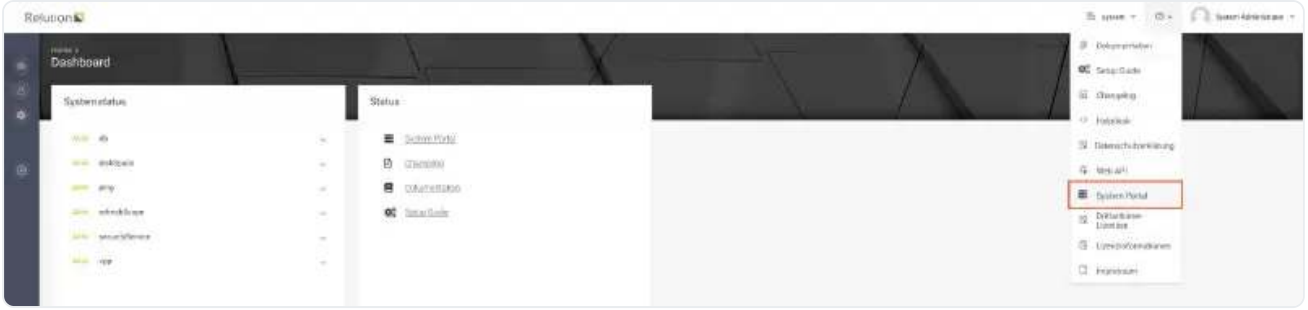
Aktivierung des DEBUG Logs im System-Portal

Voraussetzung sind ein aktiviertes System-Portal sowie ein freigeschalteter `loggers`-Endpoint, siehe die beiden vorangehenden Abschnitte.

Für Version 26.4.0

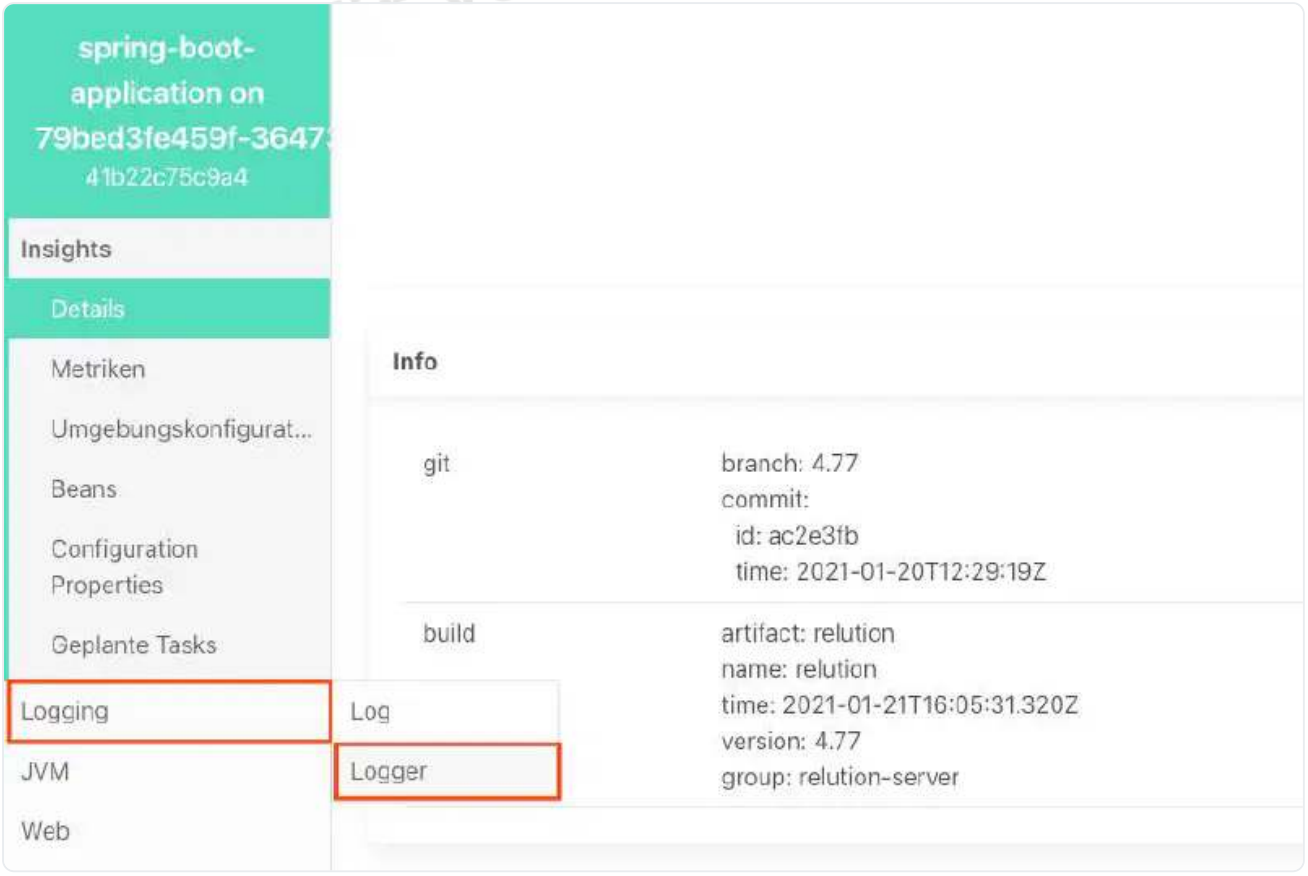
1. In Relution als System-Administrator anmelden. Der Standard-Benutzername ist `admin`.

2. Im System-Menü auf System-Portal gehen.



3. Anschließend lässt sich die zugehörige Instanz aufrufen. Dazu auf den Kasten klicken und nicht direkt auf den grünen Link.

4. In den Bereich `Logger` wechseln.



5. Die Suche nutzen, um die entsprechenden `Logger` auf `DEBUG` zu stellen. `ROOT` aktiviert sämtliche `Logger` und ist daher nur in Ausnahmefällen zu nutzen, da schnell viel Inhalt generiert wird. Im Beispiel ist die `AppleMDMResource` aktiviert worden.

Die Einstellung ist direkt aktiv, ohne dass Dienste neu gestartet werden müssen. Beim Neustart des Relution-Dienstes oder des Docker-Containers wird das Log wieder zurück auf `INFO` gestellt.

DEBUG-Log auch über einen Neustart hinaus aktiv lassen

Da das `DEBUG`-Log nach einem Neustart der Instanz wieder auf `INFO` zurück gestellt wird, ist es auf dem oben beschrieben Weg nicht möglich, initiale Fehler beim Startvorgang, z.B. im Kontext einer LDAP-Anbindung, zu loggen. Hierfür gibt es die Möglichkeit, das Log in der `application.yml` zu definieren. Diese wird direkt beim Start geladen und aktiviert somit das `DEBUG`-Log.

Nachfolgenden Inhalt direkt in die erste Zeile an Position 1 einfügen.

ROOT auf DEBUG setzen

Für Version 26.4.0

> Bei einem Logging auf `ROOT`-Ebene kann unter Umständen schnell viel Inhalt generiert werden. Diese Funktionalität sollte nur in absoluten Ausnahmefällen für kurze Analysetätigkeiten genutzt werden. Bereits bei kleineren Installationen kann es hier zu erheblichen Performance-Einbußen kommen.

Es wird empfohlen, einen oder mehrere Logs individuell und zielgerichtet zu aktivieren. Dazu einfach die einzelnen `Logger` untereinander in die Datei einfügen:

```
logging.level.io.relution: DEBUG
```

Mehrere individuelle Logs

```
logging.level.io.relution.security.ldap: DEBUG
logging.level.io.relution.apple.mdm.AppleMdmResource: DEBUG
```

Im Beispiel wären jetzt die LDAP-Funktionalität und die `AppleMdmResource` im `DEBUG`-Log aktiviert. Die Bezeichnungen der `Logger` sind im System-Portal einsehbar, sofern der `loggers`-Endpoint freigeschaltet ist; andernfalls entsprechen sie dem Paket- beziehungsweise Klassennamen aus dem Log.

Setup Loglevel mit einem Logging User über die Web API

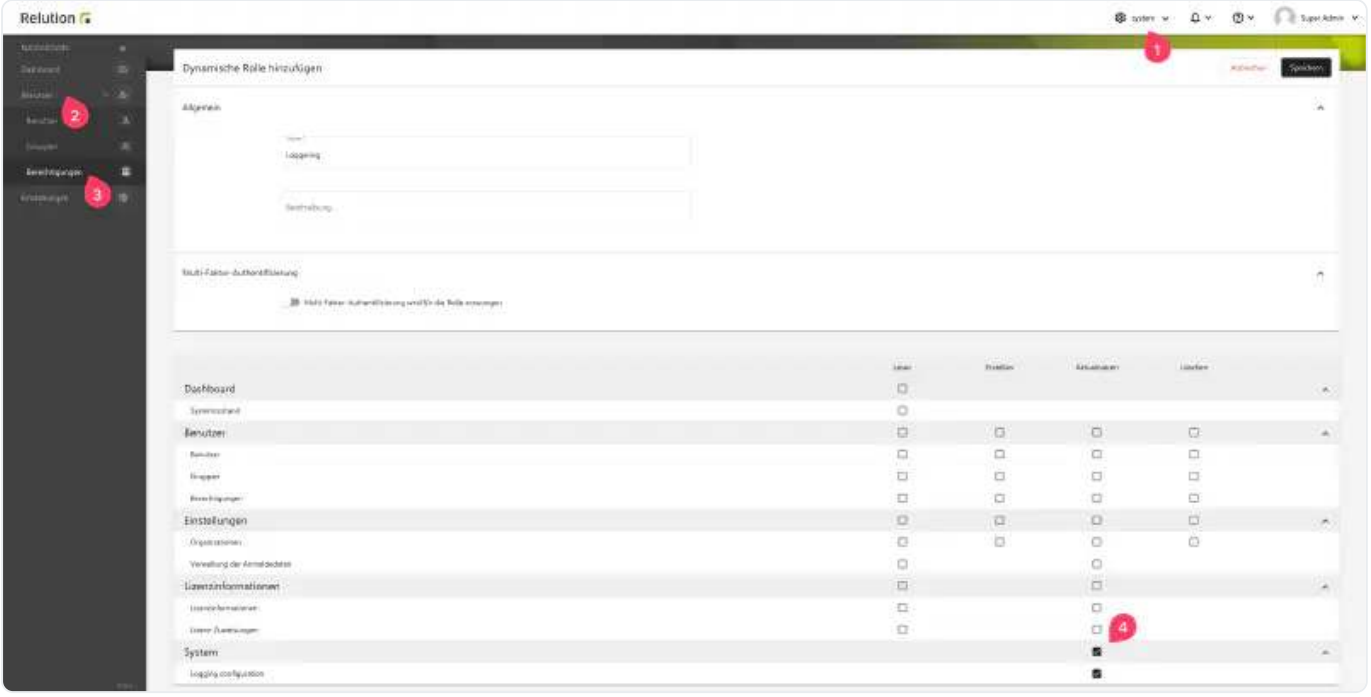
Ab Relution 5.18 besteht die Möglichkeit, auf der System-Organisation einen speziellen Logging-User zu erstellen, der das Loglevel über die Web API komfortabel ändern kann. Dies erspart das manuelle Bearbeiten der YAML-Konfigurationsdatei sowie einen Neustart des Servers.

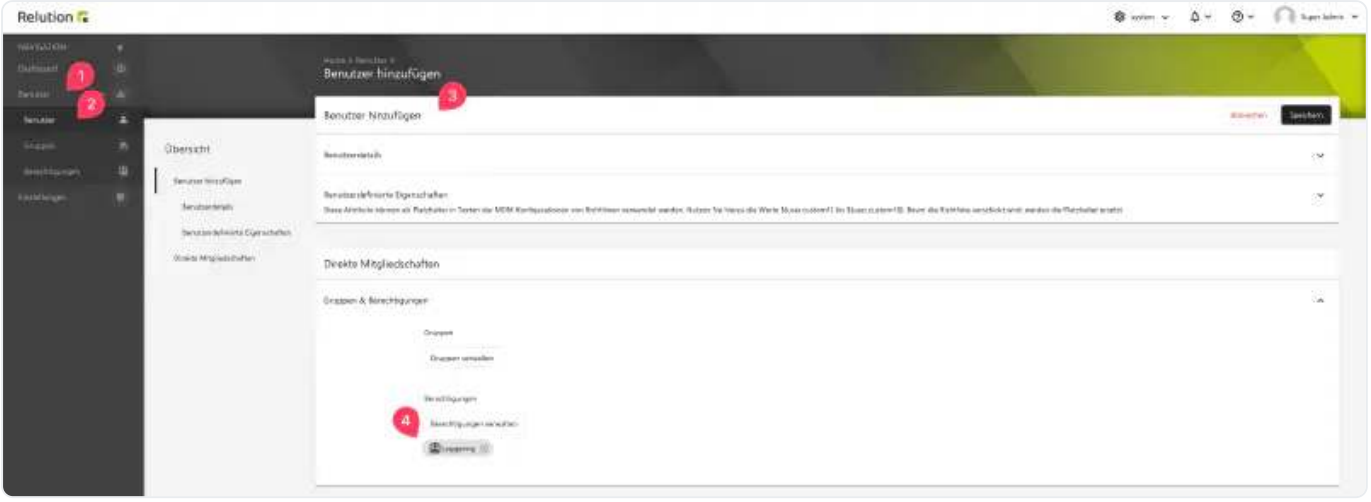
Dieser Weg setzt weder ein aktiviertes System-Portal noch eine Freischaltung von Actuator-Endpoints voraus und ist deshalb der empfohlene Weg, um Log-Level im laufenden Betrieb zu ändern. Wie im System-Portal gilt auch hier: Nach einem Neustart der Instanz sind die gesetzten Log-Level wieder auf ihren Ausgangswert zurückgesetzt.

Für Version 26.4.0

1. Berechtigung und Benutzer erstellen

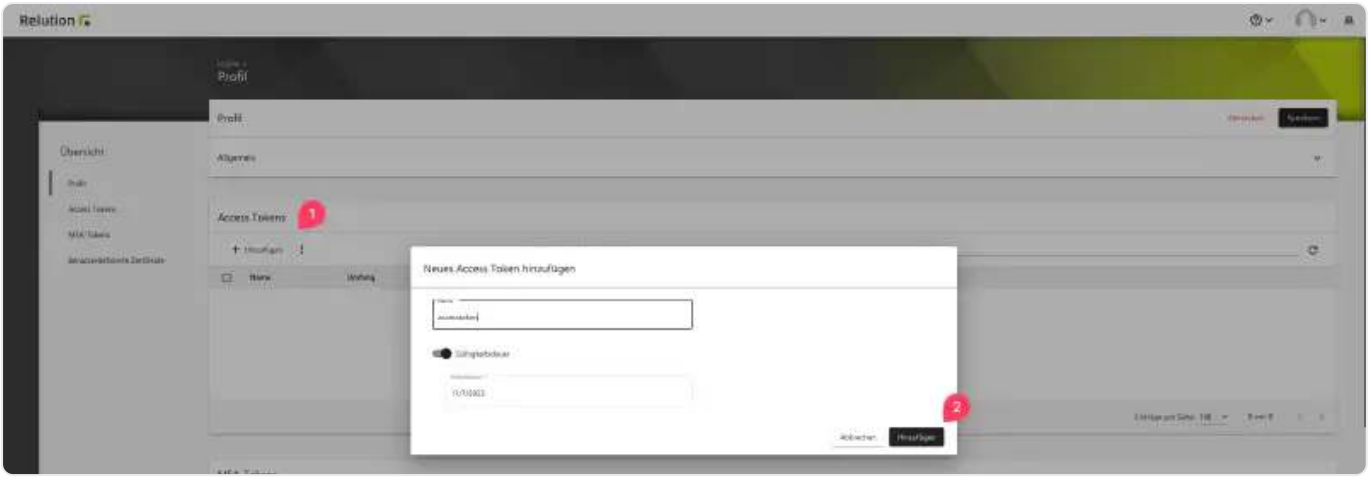
Um den Logging-User zu erstellen, muss zunächst auf der System-Organisation eine neue Berechtigung erstellt werden, bei der die Option “System > Logging configuration” aktiviert und gespeichert wird. Anschließend kann ein neuer Benutzer ausschließlich für den Logging-Access erstellt werden, dem die zuvor erstellte Berechtigung zugewiesen wird. Hinweis: Der System Administrator verfügt per default über diese Berechtigung.

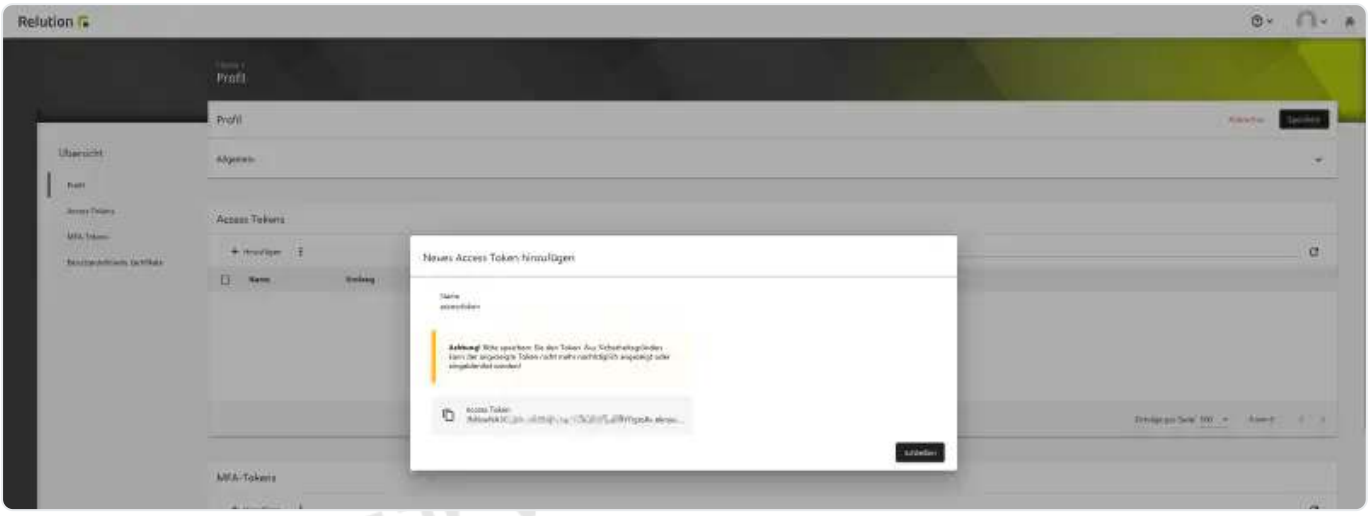




2. Access Token erstellen

Für diesen neuen Benutzer kann ein Access Token erstellt werden, um die Handhabung zu erleichtern. Hierzu muss sich der Benutzer zunächst anmelden und über das Benutzerprofil den Token erstellen. Der Access Token wird nur einmalig angezeigt, ein weiterer Token kann bei Bedarf erstellt werden.

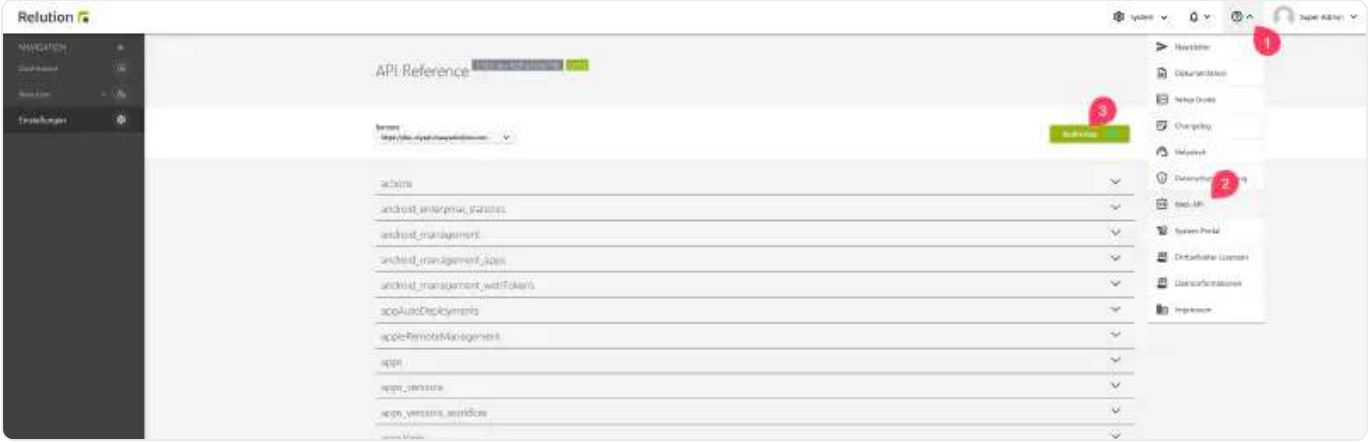


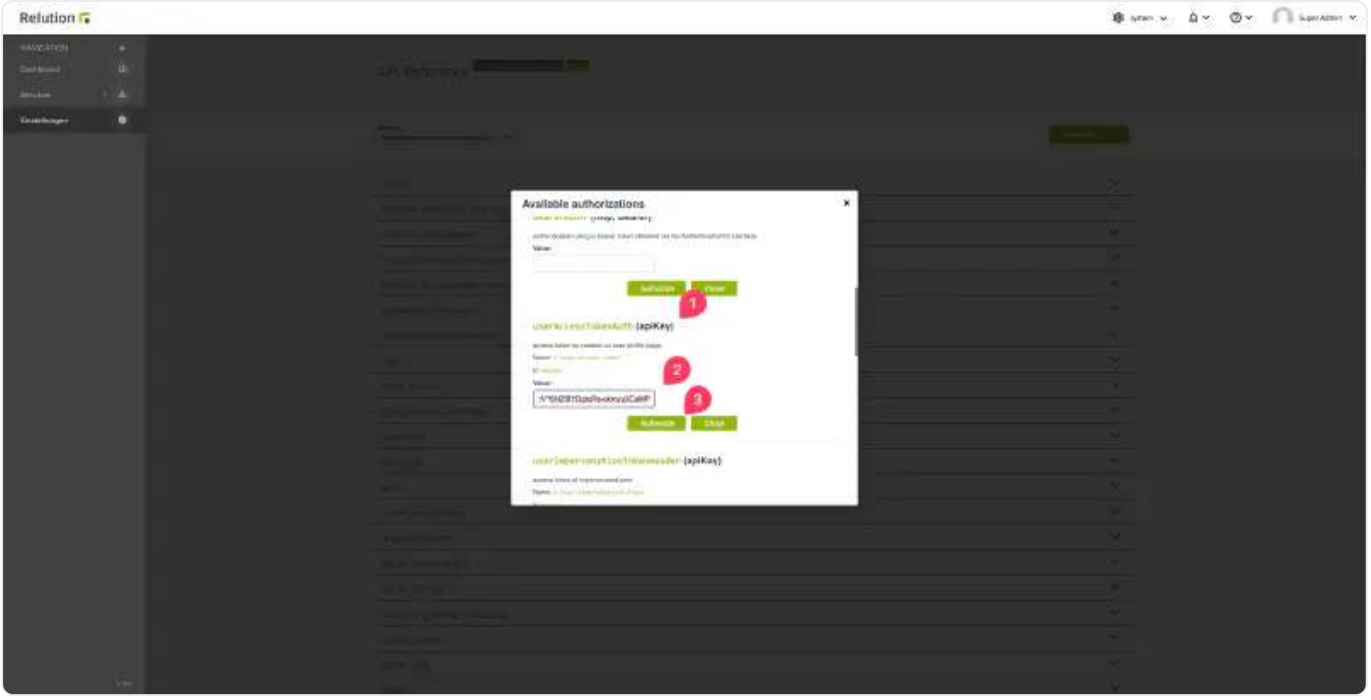


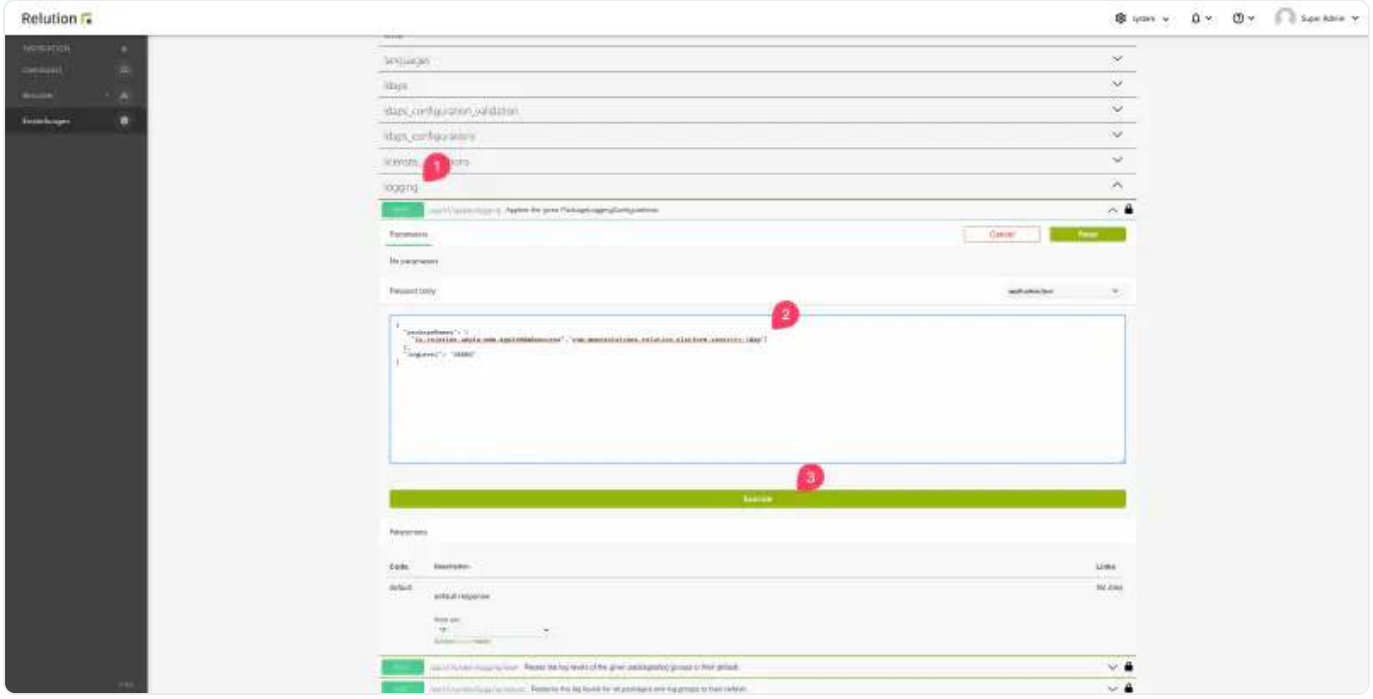
3. Steuerung des Loglevels über die Web API

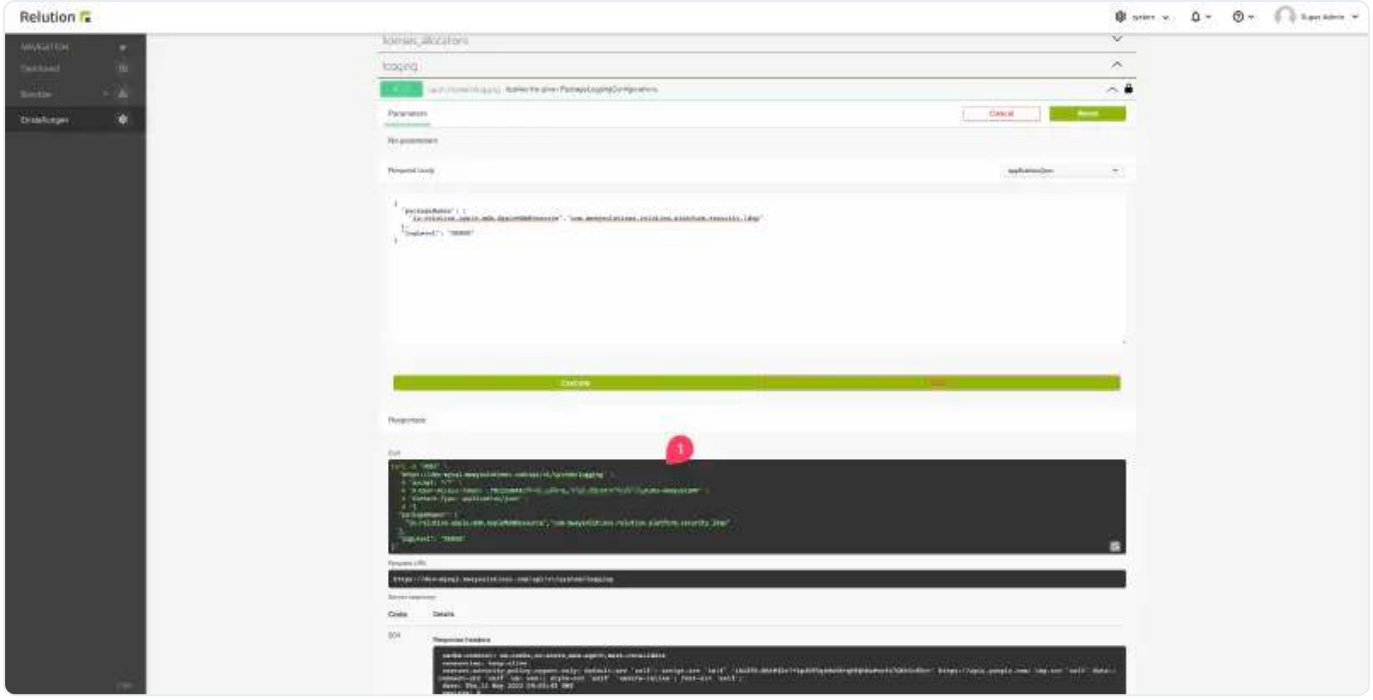
Um das Loglevel über die Web API zu steuern, kann der Logging-User in der System-Organisation über das ⚙️ Symbol > Web API > Authorize aufgerufen werden. Hier kann der Access Token des Logging-Users verwendet werden, um den Zugriff zu erleichtern und die Authentifizierung beim Curl automatisch hinzuzufügen. Im Punkt `userAccessTokenAuth` muss der Token eingefügt und autorisiert werden. Hinweis: Alternativ kann man sich mit System System Orga Admin anmelden und die Eingabe des Tokens überspringen.

Beim Punkt `logging` können die benötigten Logging-Punkte sowie das Loglevel definiert und ausgeführt werden. Eine erfolgreiche Ausführung wird mit dem Code 204 bestätigt, und der ausgeführte Curl-Befehl wird angezeigt.

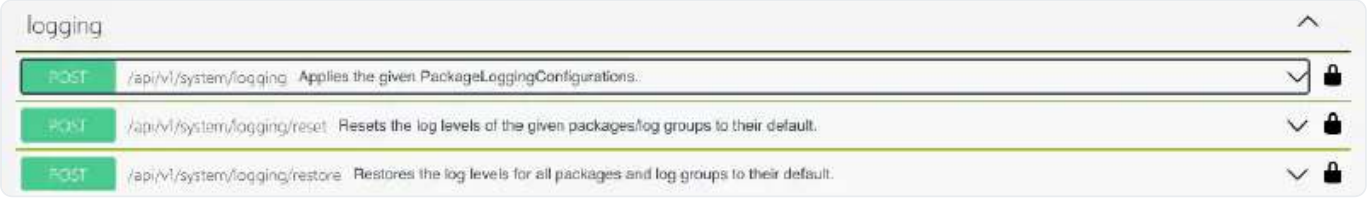

Relution
API Reference
actions
android_enterprise_statistics
android_management
android_management_apps
android_management_webTokens
appleAutoDeployments
appleRemoteManagement
apps
apps_versions
apps_versions_workflows
1
2
3


Relution
Available authorizations
(apiKey)
(apiKey)
1
2
3





Zusätzlich besteht die Möglichkeit, das Logging auf die Standard-Einstellungen zurückzusetzen, indem ein Reset oder Restore der Logging-Punkte ausgelöst wird.



4. Steuerung des Loglevels über den Curl Befehl

Es besteht auch die Möglichkeit, das Loglevel über den Curl-Befehl zu steuern, indem der über die Web API generierte Curl als Alias oder Skript für die zukünftige Verwendung gespeichert wird.

```
~ >>> curl -X 'POST' \
          'https://dev-mysql.mwaysolutions.com/api/v1/system/logging' \
          -H 'accept: application/json' \
          -H 'X-User-Access-Token: .fMilz[illegible]DgtoRs-ekmyu3CaMP' \
          -H 'Content-Type: application/json' \
          -d '{
        "packageNames": [
          "io.relution.apple.mdm.AppleMdmResource","com.mwaysolutions.relution.platform.security.ldap"
        ],
        "logLevel": "DEBUG"
      }'
```

5. Verwendung für Support-Mitarbeiter oder andere Mitarbeiter

Um einem Benutzer, beispielsweise einem Relution-Support-Mitarbeiter, Zugriff zu gewähren, genügt es, entweder den Token weiterzugeben oder die E-Mail-Adresse des Logging-Benutzers, die mit einer gültigen Relution-Instanz verknüpft ist, dem Relution-Support-Team mitzuteilen.

Für Version 26.4.0

Problem bei Update auf 26.1

Nach einem Update auf Relution 26.1 startet der Docker-Container nicht mehr. Im Container-Log erscheint wiederholt folgender Fehler:

```
Exception in thread "main" java.lang.reflect.InvocationTargetException
Caused by: java.io.IOException: Permission denied
    at java.base/java.io.File.createTempFile(File.java:2184)
    at io.relution.boot.Main.checkTempDirectory(Main.java:291)
    at io.relution.boot.Main.main(Main.java:216)
```

Ursache

Mit Version 26.1 wurde die ID des Benutzers im Container aufgrund von aktualisierten Sicherheits-Best-Practices geändert. Das bestehende Temp-Verzeichnis (`/tmp`) im Docker-Volume gehört dadurch einem falschen Benutzer, weshalb der Relution-Dienst beim Start keinen Schreibzugriff hat und abbricht. Dies lässt sich leider nicht automatisch beim Update beheben.

Beim Start prüft der Dienst den Zugriff auf das Temp-Verzeichnis:

- Ist es nicht vorhanden, wird es neu angelegt (mit korrekten Berechtigungen).
- Ist es vorhanden, versucht er es zu leeren – was mit falschen Berechtigungen fehlschlägt.

Für Version 26.4.0

Lösung

Mit dem folgenden Befehl wird der Relution-Container inklusive des Volumes neu erzeugt.

```
docker compose up -d --force-recreate --renew-anon-volumes --no-deps relution
```

`relution` ggf. durch den tatsächlichen Service-Namen des eigenen Containers ersetzen.

Nach dem Neustart legt Relution das `relution.tmp`-Verzeichnis mit den korrekten Berechtigungen selbstständig neu an. Der Fehler `Permission denied` tritt nicht mehr auf und der Dienst startet normal.

Weitere Hinweise

- Dieser Fehler tritt ausschließlich bei Updates von einer älteren Version auf 26.1 auf, da das Verzeichnis mit den alten Berechtigungen bereits existiert.
- Bei Neuinstallationen ab Version 26.1 ist das Problem nicht vorhanden.
- Sollte der Fehler nach diesen Schritten weiterhin auftreten, prüfen, ob weitere Volume-Mounts eigene `tmp`-Verzeichnisse enthalten.

Für Version 26.4.0

Serverstart bei S3 mit selbstsigniertem Zertifikat

Nach einem Update von einer Version vor 26.2 direkt auf Relution 26.4 oder neuer startet der Server nicht mehr, wenn der angebundene S3-Objektspeicher über TLS mit einem selbstsignierten oder unternehmensinternen Zertifikat erreichbar ist. Im Log erscheint folgender Fehler:

```
2026-08-18 10:06:09.875 ERROR 12 [ main] s.boot.SpringApplication: Application run
failed []
AccessDeniedException: software.amazon.awssdk.core.exception.SdkClientException: Unable
to execute HTTP request: (certificate_unknown) PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid
certification path to requested target (SDK Attempt Count: 3)
```

Ursache

Beim Start liest Relution das Signaturzertifikat für JWT aus dem konfigurierten Objektspeicher. Ist das Zertifikat der ausstellenden CA nicht als vertrauenswürdig hinterlegt, schlägt die TLS-Verbindung zum S3-Endpunkt fehl und der Startvorgang bricht ab.

Für Version 26.4.0

Dabei wirken die folgenden Punkte zusammen:

- Bei konfiguriertem Objektspeicher werden Ressourcen dorthin ausgelagert. Davon betroffen sind auch Zertifikate und damit das Signaturzertifikat für JWT.
- Mit Relution 26.2 werden Zertifikate als sicherheitsrelevant eingestuft und dauerhaft in der Datenbank gehalten. Bereits ausgelagerte Zertifikate werden dabei automatisch aus dem Objektspeicher zurück in die Datenbank migriert.
- Mit Relution 26.4 werden CA-Zertifikate nicht mehr im Betriebssystem des Containers, sondern in der Datenbank hinterlegt und über die Benutzeroberfläche verwaltet (siehe CA-Zertifikat in Docker →). Damit setzt das Hinterlegen des Zertifikats einen laufenden Server voraus, während der Server umgekehrt erst startet, wenn dem Zertifikat bereits vertraut wird.

Erfolgt das Update in Zwischenschritten über 26.2 oder 26.3, liegt das Signaturzertifikat nach der Rückmigration wieder in der Datenbank, sodass der Start unter 26.4 keinen Zugriff auf den Objektspeicher mehr benötigt. Ausschließlich bei einem direkten Update von einer Version vor 26.2 auf 26.4 oder neuer unterbleibt diese Rückmigration, während zugleich das CA-Zertifikat nicht mehr über das Betriebssystem hinterlegt werden kann.

Lösung

Damit der Server startet, wird das betroffene Signaturzertifikat aus der Datenbank entfernt. Beim nächsten Start erzeugt Relution ein neues Signaturzertifikat und legt dieses in der Datenbank ab, sodass für den Startvorgang kein Zugriff auf den Objektspeicher erforderlich ist.

Vor dem Eingriff in die Datenbank wird ein vollständiges Backup der Datenbank empfohlen.

Erforderliche Schritte:

1. Der Relution-Dienst wird gestoppt.
2. Der Datensatz des Signaturzertifikats wird mit der nachfolgenden Anweisung aus der Datenbank entfernt.
3. Der Relution-Dienst wird gestartet.

Für PostgreSQL wird der Spaltenname `usage` in doppelte Anführungszeichen gesetzt. In MariaDB ist `usage` ein reserviertes Schlüsselwort und wird dort in Backticks gesetzt.

PostgreSQL:

```
DELETE FROM mdm_crtfct WHERE "usage" = 'JWT_SIGNER_CERTIFICATE';
```

MariaDB:

```
DELETE FROM mdm_crtfct WHERE `usage` = 'JWT_SIGNER_CERTIFICATE';
```

Auswirkungen

Für Version 26.4.0

Mit dem folgenden Start wird ein neues Signaturzertifikat für JWT erzeugt. Die bestehenden Anmelde-Cookies sind damit ungültig, sodass eine erneute Anmeldung aller Benutzer erforderlich ist.

Nach dem Serverstart

Nach dem erfolgreichen Start wird das Zertifikat der internen CA nachgetragen, damit die Verbindung zum Objektspeicher wieder als vertrauenswürdig eingestuft wird:

- Die Anmeldung erfolgt in der globalen Organisation.
- Unter `Einstellungen` → `Zertifikate` wird das Zertifikat der internen CA hochgeladen (siehe Zertifikatsverwaltung →).
- Unter `Einstellungen` → `TLS-Vertrauenskonfiguration` → `Vertrauenswürdige Zertifikate` wird das hochgeladene Zertifikat über Zertifikat hinzufügen aus der Zertifikatsbibliothek ausgewählt.

> Unterbleibt dieser Schritt, startet der Server zwar, alle Zugriffe auf den Objektspeicher schlagen jedoch weiterhin fehl. In der Folge lassen sich bereits hochgeladene native Apps nicht mehr herunterladen und App-Icons werden nicht angezeigt.

Die Übernahme erfolgt im laufenden Betrieb, ein weiterer Neustart des Servers ist dafür nicht erforderlich. Anschließend werden auch die übrigen sicherheitsrelevanten Zertifikate — etwa das Signaturzertifikat für externe Dienste und das SCEP-CA-Zertifikat — aus dem Objektspeicher in die Datenbank übernommen.

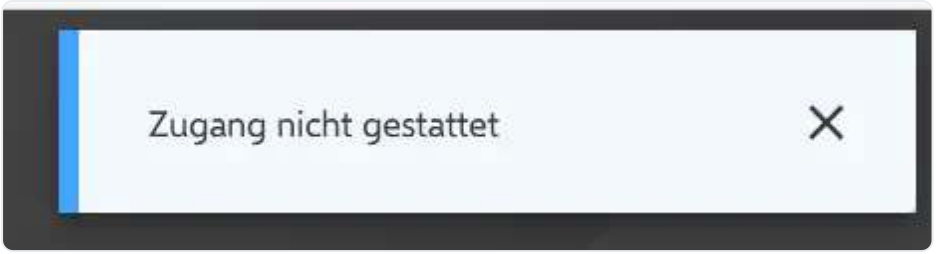
Weitere Hinweise

- Wird der Objektspeicher ohne TLS oder mit einem öffentlich vertrauenswürdigen Zertifikat angebunden, tritt das Problem nicht auf.
- Die Rückmigration der Zertifikate in die Datenbank erfolgt über einen Hintergrundjob, der standardmäßig einmal täglich ausgeführt wird. Bei einem Update in Zwischenschritten ist daher sicherzustellen, dass die Migration unter 26.2 oder 26.3 abgeschlossen ist, bevor auf 26.4 aktualisiert wird.
- Die Konfiguration des Objektspeichers ist unter Objektspeicher verbinden → beschrieben.

Für Version 26.4.0

Login: Zugang nicht gestattet

Mit Relution 26.4.0 wurde der interne Anwendungsserver von Undertow auf Tomcat umgestellt. Läuft der Reverse-Proxy (z.B. nginx oder Traefik) auf einem anderen Server als Relution selbst, kann es dadurch beim Login zu folgendem Fehler kommen:



Im Server-Log von Relution erscheint dazu ein entsprechender `ERROR`-Eintrag mit dem Hinweis `TLS required`.

Ursache

Damit eine Anmeldung möglich ist, muss die Verbindung zwischen Reverse-Proxy und Relution zwei Bedingungen gleichzeitig erfüllen:

1. Der Reverse-Proxy muss von einer als intern eingestuften IP-Adresse mit Relution kommunizieren. Als intern gelten dabei standardmäßig nur die privaten IPv4-Bereiche `10.x.x.x`, `172.16.x.x` – `172.31.x.x` und `192.168.x.x` sowie `localhost`.
2. Der Header `X-Forwarded-Proto` muss vom Reverse-Proxy mit dem Wert `https` gesendet werden.

Für Version 26.4.0

Nur wenn beide Bedingungen erfüllt sind, stuft Tomcat die eingehende Verbindung als TLS-gesichert ein. Läuft der Reverse-Proxy auf einem separaten Server mit eigener (externer) IP-Adresse, ist bereits die erste Bedingung nicht erfüllt. Fehlt zusätzlich oder stattdessen der `X-Forwarded-Proto`-Header, wird die Verbindung ebenfalls nicht als sicher erkannt. In beiden Fällen bricht Relution den Login mit `TLS required` im Server-Log ab, im Browser erscheint dazu die Meldung `Zugang nicht gestattet`.

Fehler bestätigen (optional)

Um die Ursache zu bestätigen, kann das DEBUG-Logging der zuständigen Tomcat-Komponente aktiviert werden. Dazu folgenden Eintrag auf oberster Ebene in die `application.yml` einfügen:

```yaml
logging:
  level:
    org.apache.catalina.valves.RemoteIpValve: DEBUG
```

Anschließend einen erneuten Login-Versuch durchführen. Erscheint im Log danach ein Eintrag wie folgt, ist die IP des Reverse-Proxys die Ursache: Die Anfrage wird nicht als vertrauenswürdig eingestuft.

```
DEBUG ... ina.valves.RemoteIpValve: Skip RemoteIpValve for request
/api/device/v1/currentDevice/actions/next with originalRemoteAddr '<externe-IP-des-
Proxys>' []
```

Erscheint dieser Eintrag nicht, die Fehlermeldung aber weiterhin auftritt, liegt es stattdessen am fehlenden bzw. falschen `X-Forwarded-Proto`-Header, siehe Lösung →.

> Alternativ zum Eintrag in der `application.yml` (welcher einen Neustart erfordert) kann das Log-Level für `org.apache.catalina.valves.RemoteIpValve` auch im laufenden Betrieb ohne Neustart über die Web API oder das System-Portal auf `DEBUG` gesetzt werden. Nach Abschluss der Analyse ist das Log-Level wieder auf `INFO` zurückzusetzen, siehe Loglevel einstellen →.

Lösung

Für Version 26.4.0

Je nachdem, welche der beiden Bedingungen aus dem Abschnitt Ursache nicht erfüllt ist, ist eine der beiden folgenden Anpassungen nötig — bei Bedarf auch beide.

IP des Reverse-Proxys als vertrauenswürdig hinterlegen

Damit Relution die Anfragen des Reverse-Proxys akzeptiert, muss dessen IP-Adresse explizit als vertrauenswürdiger interner Proxy bekannt gemacht werden. Dazu folgenden Eintrag auf oberster Ebene in die `application.yml` eintragen:

```yaml
server:
  tomcat:
    remoteip:
      internal-proxies: '<Proxy-IP>|127\.\d{1,3}\.\d{1,3}\.\d{1,3}|0:0:0:0:0:0:0:1|::1'
```

`<Proxy-IP>` muss dabei durch die tatsächliche, mit Punkten maskierte IP-Adresse des Reverse-Proxys ersetzt werden, z. B. `194\.95\.62\.71`. Bei mehreren Proxy-Servern lassen sich weitere IPs, jeweils getrennt durch `|`, ergänzen.

Die `application.yml` enthält in der Regel bereits weitere Einträge, etwa für den Systemadministrator, die externe URL oder die Datenbankverbindung. Der neue Eintrag `server` steht dabei als eigener, oberster Schlüssel neben dem bestehenden `relution`-Block, nicht als dessen Unterpunkt — auch wenn unterhalb von `relution` ebenfalls ein Abschnitt namens `server` existiert (dort z. B. mit `externalURL`). Das folgende Beispiel zeigt eine vollständige Datei mit beiden Blöcken:

```yaml
server:
  tomcat:
    remoteip:
      internal-proxies: '<Proxy-IP>|127\.\d{1,3}\.\d{1,3}\.\d{1,3}|0:0:0:0:0:0:0:1|::1'

relution:
  system:
    admin:
      password: %SYSTEM_ADMIN_PASSWORD%
      email: %SYSTEM_ADMIN_EMAIL%
  server:
    externalURL: %EXT_HOSTNAME_URL%
  database:
    type: mariadb
    # Adjust hostname in the url if the database runs outside docker compose
    url: jdbc:mariadb://mariadb/relution?useServerPrepStmts=true
    username: relution
    password: %MYSQL_PASSWORD%
```

Alternativ kann dem Relution-Server auch eine lokale/private IPv4-Adresse zugewiesen werden, über die die Kommunikation mit dem Reverse-Proxy intern erfolgt. In diesem Fall ist keine zusätzliche Konfiguration notwendig, da private IPv4-Bereiche standardmäßig als intern akzeptiert werden.

Für Version 26.4.0

X-Forwarded-Proto Header setzen

Zusätzlich muss der Reverse-Proxy den Header `X-Forwarded-Proto` mit dem Wert `https` an Relution weiterleiten. Im `location /`-Block der nginx-Konfiguration muss dazu folgende Zeile gesetzt sein:

```
proxy_set_header X-Forwarded-Proto $scheme;
```

Diese Zeile ist im Standard-Template `relution-nginx.conf` bereits enthalten. Bei einer eigenen bzw. angepassten Reverse-Proxy-Konfiguration, oder wenn sich ein weiterer Proxy davor befindet, ist zu prüfen, ob der Header korrekt gesetzt und nicht durch einen vorgelagerten Proxy überschrieben wird.

Nach dem Anpassen der `application.yml` bzw. der Reverse-Proxy-Konfiguration muss der Relution-Dienst bzw. Container (und ggf. der Reverse-Proxy) neu gestartet werden, damit die Änderung wirksam wird.

Weitere Hinweise

- Dieses Problem betrifft in erster Linie Installationen, bei denen der Reverse-Proxy nicht auf demselben Host wie Relution läuft.
- Betroffen sind Relution-Installationen ab Version 26.4.0.
- Die Meldung `Zugang nicht gestattet` ist eine allgemeine Fehlermeldung, die im Portal für verschiedenste, vom Server abgelehnte Anfragen angezeigt wird. Die in diesem Artikel beschriebene Lösung ist nur dann zutreffend, wenn im Server-Log zusätzlich der `ERROR`-Eintrag `TLS required` erscheint.
- Siehe auch: Docker Installation - Optional: nginx →

Für Version 26.4.0

Fehlersuche und Hilfe

Ist der Zugriff auf das Systemadministratorkonto von Relution verloren gegangen und lässt sich das Passwort nicht über die konfigurierte E-Mail-Adresse zurücksetzen, ist es auch möglich, das Passwort über die Datenbank zurückzusetzen. Dieses Verfahren erfordert Schreibzugriff auf den Datenbankserver und die Datenbank von Relution auf dem Datenbankserver.

Das Passwort sollte zunächst über den Passwort vergessen?-Link zurückgesetzt werden, bevor der Weg über die Datenbank versucht wird. Diese Möglichkeit sollte nur als letzter Rettungsanker dienen.

Um das Passwort zurückzusetzen, muss zunächst über die Kommandozeile oder ein Verwaltungstool eine Verbindung mit der Datenbank hergestellt werden. Anschließend das SQL-Skript ausführen, das für den jeweiligen Datenbankserver geeignet ist.

MariaDB/MySQL

```
UPDATE security_user usr
    JOIN security_organization org on org.uuid = usr.organization_uuid
    SET password = SHA1(CONCAT('password123', '{', usr.uuid, '}'))
    WHERE usr.name = 'admin'
    AND org.name = 'system';
```

Für Vers

`password123` mit dem neuen gewünschten Passwort ersetzen.

Microsoft SQL Server

```
UPDATE security_user SET password = LOWER(CONVERT(VARCHAR(40), HASHBYTES('SHA1',
CONCAT('password123', '{', usr.uuid, '}')), 2))
    FROM security_organization org
    JOIN security_user usr on usr.organization_uuid = org.uuid
    WHERE usr.name = 'admin'
    AND org.name = 'system';
```

`password123` mit dem neuen gewünschten Passwort ersetzen.

Server startet nicht

Die Logdateien im Verzeichnis `log`, das sich innerhalb des Installationsverzeichnisses von Relution befindet, prüfen. Lässt sich das Problem nicht selbst identifizieren, ein Support-Ticket öffnen und die Logs zur Verfügung stellen.

Log Dateien

Wo sich die Log-Dateien für Docker, Linux und Windows finden, ist unter Relution Logs → beschrieben.

Performance-Analyse mit Glowroot

Neu in 26.5

> Diese Anleitung gilt ab Relution 26.5.

Bei Performance-Problemen kann der Relution Support um eine Analyse mit Glowroot → bitten. Glowroot zeichnet auf, welche Anfragen wie lange dauern, und zeigt das Ergebnis in einer eigenen Weboberfläche an.

Im Docker-Betrieb ist Glowroot nicht Teil des Images, es wird beim Start automatisch heruntergeladen, sobald `RELUTION_ENABLE_GLOWROOT` gesetzt ist:

Für Version 26.4.0

```
  relution:
    image: relution/relution:latest
    environment:
      - RELUTION_ENABLE_GLOWROOT=true
      -
RELUTION_GLOWROOT_ADMIN_JSON_BASE64=ewogICJ3ZWIiOiB7CiAgICAiYmluZEFkZHJlc3MiOiAiMC4wLjA
uMCIKICB9Cn0=
    ports:
      - '4000:4000'
```

Die zweite Variable enthält lediglich die Base64-kodierte Glowroot-Konfiguration `{"web": {"bindAddress": "0.0.0.0"}}`. Ohne sie ist die Oberfläche nur innerhalb des Containers erreichbar. Nach einem Neustart des Containers steht sie unter Port 4000 zur Verfügung.

Die Aufzeichnungen liegen im Container und gehen verloren, sobald dieser neu angelegt wird. Für die Dauer einer Analyse ist das in der Regel ausreichend. Sollen sie erhalten bleiben, `RELUTION_GLOWROOT_DIR` auf ein für die UID `20001` beschreibbares Verzeichnis setzen.

> Glowroot nur so lange aktivieren, wie die Analyse dauert. Die Oberfläche auf Port 4000 ist nicht durch ein Passwort geschützt und gibt Datenbankabfragen, Antwortzeiten und Stacktraces preis. Sie darf keinesfalls aus dem Internet

erreichbar sein.

Zum Deaktivieren `RELUTION_ENABLE_GLOWROOT` wieder entfernen und den Container neu starten.

Sicherheitshinweise

- Die neuesten Betriebssystem- und Software-Updates und Sicherheits-Patches installieren.
- Sichere Kennwörter für Administratorkonten verwenden.
- Lange Passwörter für die Kommunikation von Dienst zu Dienst verwenden. Passwörter müssen nicht von Menschen benutzt oder gemerkt werden.
- Sicherstellen, dass das Benutzerkonto, das für den Zugriff auf das eigene LDAP verwendet wird, über Nur-Lese-Zugriff verfügt.
- Keine Konten mit schwachen Passwörtern wie `password` oder `test` erstellen.
- Passwörter nicht in Dateien speichern, die weltweit lesbar sind.

Für Version 26.4.0

Lokaler Exchange ohne SMG

Die Konfiguration eines lokalen Exchange-Servers ohne SMG kann leicht fehlschlagen. Aus diesem Grund haben wir häufig auftretende Ursachen identifiziert und entsprechende Lösungen erfasst. Um die grundlegende Konnektivität zu überprüfen, sind vier Schritte durchzuführen.

Logfile analyse

Hier wird die Log vom Reverseproxy (zB nGinx) für die weitere Analyse benötigt

- bei Linux liegt die Log in folgendem Verzeichniss `/var/log/nginx/relution_access.log`
- für Windows zB im jeweiligen nGinx Installationspfad `/nGinx/logs/relution_access.log`

Werden auf dem Endgerät die Mails abgerufen, sollte in der Log ein Hinweis zu folgender URL enthalten sein `/Microsoft-Server-ActiveSync`

Wird der Eintrag /Microsoft-Server-ActiveSync hinterlassen, funktioniert die Verbindung.

Für Version 26.4.0

Fehlerbehebung

Wenn in der Log nichts eingetragen wird, muss die URL im Browser eingegeben werden ob dieser generell erreichbar ist. `https://myexchange.com/Microsoft-Server-ActiveSync` Bei aufrufen muss ein Eintrag im nGinx Log hinterlassen werden, ist dieser nicht zu finden muss die Infrastruktur geprüft werden. Ist der Eintrag zu finden, sind vermutlich die Einstellung der Exchange Konfiguration in der Relution Richtlinie nicht korrekt gesetzt oder ungültig.

Prüfen der Verbindung

Mit einem Curl Befehl kann die Verbindung von Relution zum Exchange Server geprüft werden:

```
curl https://outlook.XXX.de/Microsoft-Server-ActiveSync --user Ihre-Exchange-
Domäne\\Exchangeuser@Domain.de:ExchangePWvomUser --verbose --http1.1 -i
```

```
Es könnte eine Ausgabe mit einem Zertifikatsfehler wie dargestellt kommen:
Trying 172.16.105.109:443...
Connected to outlook.XXX.de (172.000.000.000) port 443 (#0)
schannel: disabled automatic use of client certificate
ALPN: offers http/1.1
schannel: SEC_E_UNTRUSTED_ROOT (0x80090325) - *Die Zertifikatkette wurde von einer
nicht vertrauenswürdigen Zertifizierungsstelle ausgestellt.*
Closing connection 0
curl: (60) schannel: SEC_E_UNTRUSTED_ROOT (0x80090325) - *Die Zertifikatkette wurde von
einer nicht vertrauenswürdigen Zertifizierungsstelle ausgestellt.*
More details here: https://curl.se/docs/sslcerts.html
```

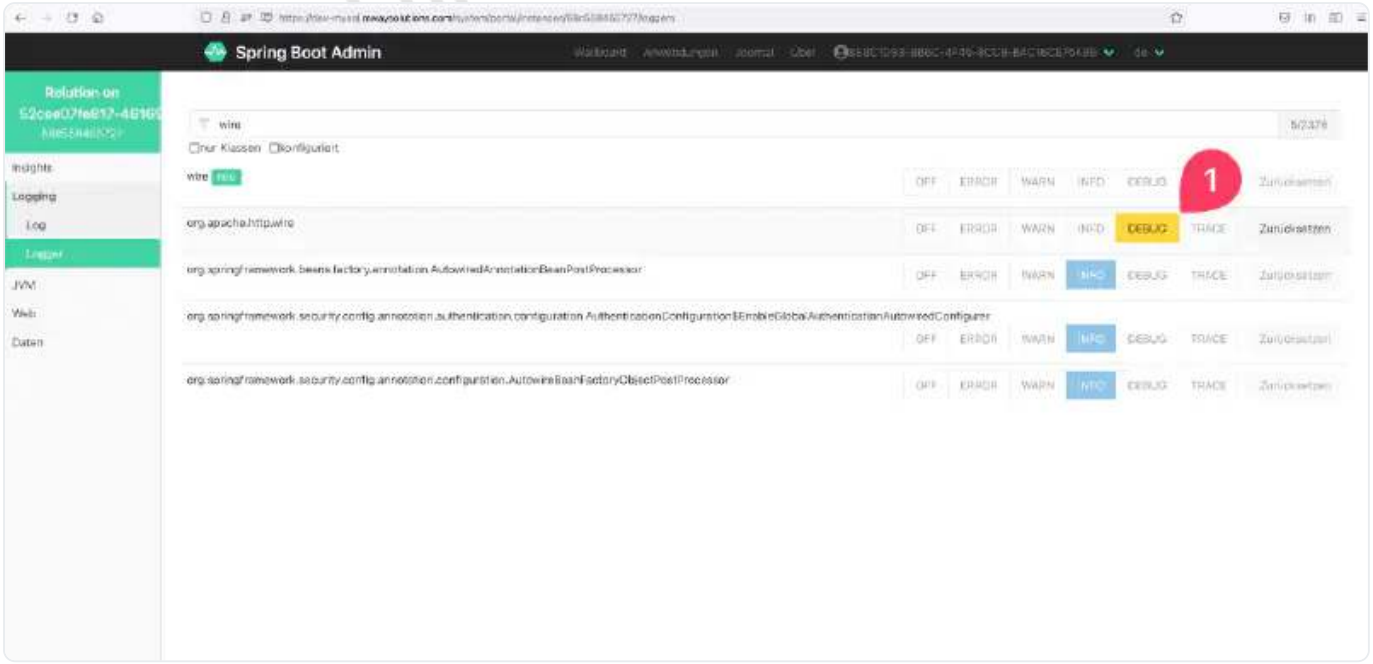
Wird die Fehlermeldung wie oben angezeigt, ist das Zertifikat der CA nicht im Betriebssystem des Servers hinterlegt, je nach Betriebssystem muss das Zertifikat daher entsprechend installiert werden.

Beispiel für Relution in Docker →

HTTPS Kommunikation auslesen

Für Version 26.4.0

Wird das Log-Level des Loggers `org.apache.http.wire` auf `DEBUG` gesetzt, lässt sich die HTTPS-Kommunikation zwischen Relution und dem Exchange in der Logdatei nachvollziehen. Die möglichen Wege zum Setzen des Log-Levels — Web API, `application.yml` oder System-Portal — sind unter Loglevel einstellen → beschrieben. Der im folgenden Screenshot gezeigte Weg über das System-Portal setzt seit Relution 26.4 eine Freischaltung des zugehörigen Actuator-Endpoints → voraus.

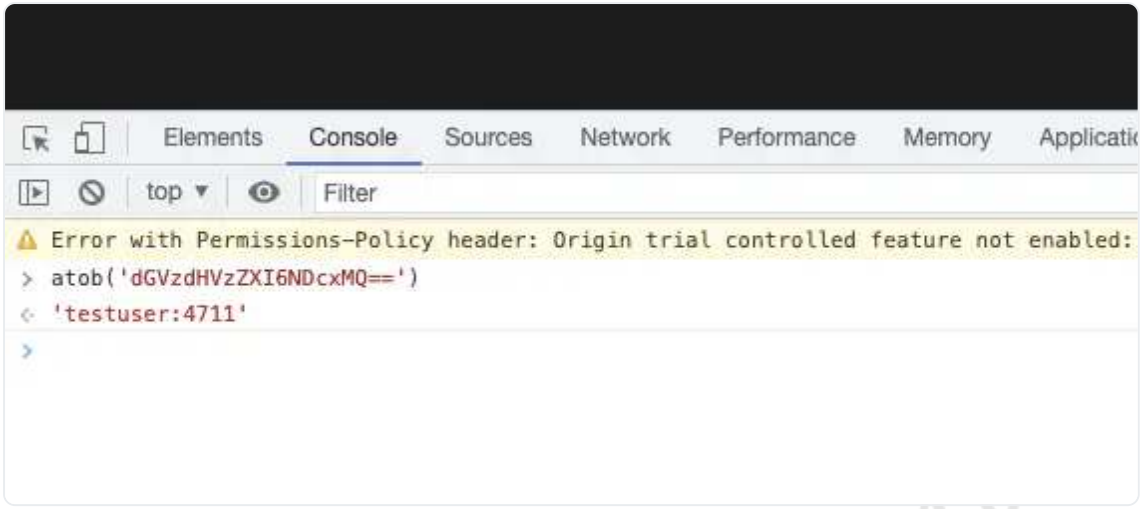


Eine Kommunikation muss vom Gerät angestoßen werden um die Log mit Hinweisen zur Ursache zu füllen.
Das Loglevel muss nach der Analyse wieder auf `INFO` gestellt werden.

Log auswerten

Anschließend kann durch das erhöhte Loglevel nach auffälligen Hinweisen gesucht werden. Sind beispielsweise die User und Usercredentials nicht korrekt, scheitert der Login und eine `401 Unauthorized`-Meldung wird eingetragen, die in basic Auth so aussehen kann: `dGVzdHVzZXI6NDcxMQ==`

Diese lassen sich im Browser in der Console decodieren, um so das übermittelte Passwort sowie den User zu vergleichen `atob('dGVzdHVzZXI6NDcxMQ==')`



SMG ist nicht mit Outlook365 funktional, Microsoft hat hierzu Basic Auth deaktiviert und verwendet OAuth2

Deprication of Basic Auth →

Für Version 26.4.0

Ankündigungen und Hinweise

Hinweise: Software in End-Of-Life (EOL)

Aus Sicherheitsgründen unterstützt Relution generell keine Software, die bereits ihr End-Of-Life (EOL) erreicht hat, da dort keine Sicherheitspatches mehr zur Verfügung gestellt werden.

Ankündigungen und Abkündigungen

- Update auf 26.4.0+: Mit Relution 26.4.0 wurde der interne Anwendungsserver von Undertow auf Tomcat umgestellt. Läuft der Reverse-Proxy auf einem anderen Server als Relution selbst, kann der Login danach mit der Meldung `Zugang nicht gestattet` (`TLS required` im Server-Log) fehlschlagen. In diesem Fall ist eine Anpassung der Konfiguration entsprechend der dort beschriebenen Schritte erforderlich: Login: Zugang nicht gestattet →.
- Neues Basis-Image: Ubuntu statt AlmaLinux: Ab Version 26.4.0 basiert das Relution-Container-Image auf Ubuntu statt bisher AlmaLinux.
- Secure Mail Gateway: Ab Relution 26.4.0 ist der Einsatz des Secure Mail Gateway Features nur noch mit dem eigenständigen SMG-Dienst möglich – ohne diesen Dienst steht das Feature nicht mehr zur Verfügung. In 26.3 kann der neue Modus bereits optional über einen Feature-Toggle aktiviert werden. Weitere Informationen und Migrationsanleitung: Secure Mail Gateway →.
- Update auf 26.1+: Vor einem Upgrade auf Version 26.1 oder höher muss eine 26.0.x Version installiert und mindestens einmal gestartet worden sein. Ist bereits eine 26.0.x Version im Einsatz, ist kein Update auf 26.0.3 im Speziellen erforderlich. Hintergrund: Relution 26.1 unterstützt Datenbank-Upgrades nur ausgehend von Version 26.0, daher ist eine 26.0.x Version als Zwischenschritt erforderlich. Beim Update auf 26.1 kann es zudem dazu kommen, dass der Docker-Container aufgrund eines Berechtigungsproblems im Temp-Verzeichnis nicht mehr startet. Die Lösung dazu unter Problem bei Update auf 26.1 →.
- Object Storage: Bei Verwendung von MinIO als lokalem S3-kompatiblen Speicher empfiehlt sich die Migration zu SeaweedFS, da MinIO die Entwicklung eingestellt hat. Eine Anleitung hierfür unter Object Storage Migration →.
- Gerätegruppen: Wie bereits angekündigt werden mit Relution 26.0 noch nicht migrierte Organisationen automatisch auf Gerätegruppen umgestellt, der Support für die Legacy-Funktionalität entfällt. Zudem entfallen endgültig die Regelwerke, die durch Gerätegruppen-Aktionen ersetzt wurden.
- Java: Ab 5.35 erfordert Relution *Java 21*. Mit 26.0 ist ein Start von Relution mit älteren Java-Versionen nicht mehr möglich.
- MariaDB: Relution 5.30 erfordert *MariaDB 10.11 oder höher*. Der *Support für MariaDB wird insgesamt nur noch bis Ende 2027 verfügbar sein.*
- PostgreSQL: Relution 5.29 erfordert *PostgreSQL 14 oder höher*. Es wird empfohlen, direkt *PostgreSQL 18* einzusetzen.

Neue Handbuchartikel

Neue Funktionen der letzten drei Versionen im Überblick, mit Links zu den jeweiligen Handbuch-Artikeln.

Für Version 26.4.0

Version 26.5

On Premises Installation

- Fehlersuche und Hilfe → Performance-Analyse mit Glowroot
- Serverseitige Verschlüsselung (SSE-C) → Option C: Schlüssel als Datei
- Relution Shield (Add-on) → Anlegen eines technischen Users und API-Access-Tokens{#create-technical-user}

Allgemein

- Dashboard
- Teacher → Weblinks und Surfeinschränkungen
- Erweiterte Platzhalter → Benutzerzertifikate
- Konfigurationsprofil für ADE → Mindest-Betriebssystemversion
- Gerätegruppen → Bildungsgruppen

Apple macOS

- Wiederherstellungssperre → Wiederherstellungssperre verifizieren
- Relution Decon (Inhaltsfilter)

Bildung

- Bildungsgruppen

Android Enterprise

- Organisation verknüpfen → Registrierung reparieren

Einstellungen

- Zertifikatspool
- TLS-Vertrauenskonfiguration → Certificate Pinning (Apple-Enrollment)
- Meta-Organisationen
- OIDC mit Entra → Redirect-URI für die Geräte-Einschreibung
- Relution als Identity Provider
- OIDC mit Workspace → Redirect-URI für die Geräte-Einschreibung

Für Version 26.4.0

Version 26.4

On Premises Installation

- CA-Zertifikat in Docker → Zertifikate über die Benutzeroberfläche hinterlegen
- Login: Zugang nicht gestattet
- Secure Mail Gateway → Pflichtkomponente ab 26.4.0

Allgemein

- Self-Service Portal → Standort auf einer Karte anzeigen
- Konfigurationsprofil für ADE → Benutzerauthentifizierung bei der Einschreibung

Apple iOS

- Softwareupdates → Verwaltete Softwareupdates

Apple macOS

- Wiederherstellungssperre → Wiederherstellungssperre setzen
- Softwareupdates → Verwaltete Softwareupdates

Android Enterprise

- Android Gerät orten → Standort im Self-Service Portal anzeigen

Windows

- Companion konfigurieren

Einstellungen

- Global-Organisation → Organisationswechsler
- TLS-Vertrauenskonfiguration
- OIDC mit Entra → Umleitungs-URI hinzufügen
- OIDC mit Workspace → Scoped Redirect-URIs
- Secure Mail Gateway → Konfiguration des Secure Mail Gateway

---

Version 26.3

On Premises Installation

- APNS Push Zertifikate → Migration vom bisherigen Ablauf
- Serverseitige Verschlüsselung (SSE-C)
- Secure Mail Gateway → Feature-Toggle für On-Premise-Installationen (26.3)

Erste Schritte

- Apple Geräte verwalten → Zertifikate

Apple iOS

- Intelligence-Einstellungen
- Externe Intelligenz-Einstellungen
- Tastatur-Einstellungen
- Siri-Einstellungen

Für Version 26.4.0

Apple macOS

- Intelligence-Einstellungen
- Externe Intelligenz-Einstellungen
- Tastatur-Einstellungen
- Siri-Einstellungen
- Migrationsassistent → Einstellungsdeklaration

Apple visionOS

- Intelligence-Einstellungen

Einstellungen

- Organisationszertifikate

Technisches Changelog

Die Seite beschreibt das technische Changelog, das für erfahrene Anwenderinnen und Benutzer gedacht und nur auf Englisch verfügbar ist. Die ausführlichen, deutschen Release Notes gibt es hier →.

Allgemein empfohlene Version

Die hier gelisteten Versionen werden erst mit Verzögerung auch unter `latest` allgemein bereitgestellt, da diese zuvor mehrere zusätzliche Quality Gates durchlaufen.

Aktuell unter `latest` verfügbare Version: 26.5.4 (Stand 20.10.2026)

Vor dem Update auf Relution 26.1

Eine 26.0.x Version (zum Beispiel die aktuellste Version 26.0.3 →) muss installiert und mindestens einmal gestartet worden sein, bevor ein Upgrade auf Version 26.1 oder höher durchgeführt werden kann. Ist bereits eine 26.0.x Version im Einsatz, ist kein Update auf 26.0.3 im Speziellen erforderlich.

Hintergrund: Relution 26.1 unterstützt Datenbank-Upgrades nur ausgehend von Version 26.0. Ein direktes Upgrade auf 26.1 oder höher ohne vorherige Installation und einmaligen Start einer 26.0.x Version wird daher nicht unterstützt.

Zusätzlich kann es beim Update auf Version 26.1 dazu kommen, dass der Docker-Container aufgrund eines Berechtigungsproblems im Temp-Verzeichnis nicht mehr startet. Die Lösung dazu unter Problem bei Update auf 26.1 →.

Für Version 26.4.0

Ankündigungen und Hinweise

Siehe Abschnitt Ankündigungen und Hinweise →.

Version 26.5.4

2026-10-20

Fixes

- Auth Bypass, see security advisories [RVD-2026-6]

Version 26.5.3

2026-10-16

Fixes

- Permission Issue, see security advisories [RVD-2026-2]
- Code Execution, see security advisories [RVD-2026-3]
- Database Access Vulnerability, see security advisories [RVD-2026-4]

Version 26.5.2

2026-10-01

Fixes

- Brute-Force Vulnerability, see security advisories [REL-13800] [RVD-2026-5]
- Adjust template resolver configuration [REL-13910]
- Prevent upload of files without organization scope [REL-13913]

Für Version 26.4.0

Version 26.5.1

2026-09-24

New

- Remove invalid RSA key size from Apple SCEP configuration [REL-13552]
- Restrict RSA key sizes to 3072 and 4096 [REL-13551]

Updates

- Allow restricting outbound TSFI TLS connections to a whitelist [REL-13073]
- Optimize performance when using different types of access tokens [REL-13558]

Version 26.5.0

2026-09-15

New

- Add a sticky header to the login history table [REL-13425]
- Add a Verify Recovery Lock action for macOS devices [REL-12537]
- Add Autofill Option to Android Enterprise Restrictions to control the behaviour for the build in function. [REL-12213]
- Add enhanced retry and backoff handling for object storage operations [REL-11912]
- Add option to enforce the minimum OS version during DEP enrollment [REL-12746]
- Add placeholders for user certificates [REL-13109]
- Add separate authorities for the different access token types [REL-11610]
- Add support for certificate pinning during enrollment for apple devices [REL-12744]
- Add support to upload multiple user certificates for a subtype [REL-12989]
- Add the missing legacy widgets to the new default dashboard [REL-5902]
- Add the push method to the Android device details [REL-12980]
- Adjust matching of authorized devices to API scopes [REL-13006]
- Allow creating sub organizations below an existing meta organization in the wizard [REL-11985]
- Allow disconnecting from Android Enterprise while preserving devices instead of wiping them [REL-9082]
- App licenses bound to a device are automatically released when the device is deleted from the inventory. [REL-11834]
- Apply the Relution UI design to the dashboard [REL-12855]
- Ask for confirmation before deleting a dashboard widget [REL-13432]
- Assign every endpoint to an API scope [REL-13088]
- Certificate is installed when decon policy is applied on a Windows device [REL-9421]
- Enable enrollment of Newline whiteboards [REL-13317]
- Enable enrolment of VS whiteboards [REL-13318]
- Fix the button order in the dashboard dialogs [REL-13448]
- Fix the standby and sleep timer on Promethean boards [REL-13022]
- Harden action message population against incompletely loaded entities [REL-12066]
- Improve device history localization by storing translation keys and translating entries when read [REL-12067]
- Improve VPP user handling when accounts are moved between organizations [REL-64]
- Keep installed apps when migrating a device from another MDM [REL-12442]
- Make API access token scope aware [REL-13019]
- Make JWT and login endpoints API scope aware [REL-13005]
- Move the Android Enterprise Companion endpoints to a dedicated API scope [REL-11954]
- Move the self service endpoints to the selfService API scope [REL-6905]
- Obfuscate WNS credentials [REL-12820]
- Only allow access to endpoints of enabled API scopes [REL-5555]
- Preserve the audit fields of nested entities on update [REL-12593]
- Relution can now act as its own OpenID Connect / OAuth2 Identity Provider — register client applications directly in Relution and let users sign in with their existing Relution account across all of them [REL-13113]
- Repair the Android Enterprise connection by repeating the signup process [REL-9078]
- Rework dashboard to allow creating custom widgets [REL-8093]
- Rework the user profile view [REL-13180]
- Scope dashboard widget filter definitions per entity and authorization [REL-5905]
- Serve the decon endpoints under a dedicated API scope [REL-11957]
- Set default to power save mode 1 when eco mode is off on ViewSonic Boards [REL-13117]
- Show a dedicated page when the requested login method is not available [REL-13171]
- Show the meta badge in all relevant places [REL-11983]
- Support SSE-C encryption for the S3 resource storage [REL-11913]
- Unify and translate the sub-action failure messages of Apple and Windows [REL-12069]
- Use consistent naming for the meta organization in the organization list and details [REL-13464]

Updates

Für Version 26.4.0

- Add a numerical error code to eSIM action errors [REL-12567]
- Add dedicated enrollment API scope [REL-13004]
- Add Education device groups to provide complex MDM operations during a lesson [REL-12031]
- Add MCP tools for policies and settings [REL-11938]
- Add support of certificate pools as PKI source [REL-13444]
- Add support of Meta Organizations [REL-13372]
- Allow navigating from a widget to the filtered entity list [REL-5906]
- Allow restricting outbound TSFI TLS connections to a whitelist [REL-13073]
- Choose the organization type (standalone, meta or sub) when creating an organization [REL-11949]
- Compact the default dashboard layouts and reduce the columns of the keystores widget [REL-12805]
- Dialogs for CA certificate selection now only show CA certificates [REL-12863]
- Entra ID sign in with OIDC is possible when oid is set as the username attribute [REL-13015]
- Fix generated images not being uploaded to S3 [REL-13159]
- Fix inconsistent policy status on devices [REL-9629]
- Fix the organization scoping of device base info queries [REL-11952]
- Fix the parent app link status not being rolled back when sending the email fails [REL-12597]
- Fix the password configuration not updating correctly and clarify its wording [REL-13286]
- Fix the spacing of the count element in the device group actions tab [REL-13477]
- Fix Windows Exchange configuration changes having no effect; the Exchange user name can no longer be edited [REL-2005]
- Generate certificates in a dedicated thread pool and create KME capabilities as fallback [REL-11909]
- Hide the scope tab bar when registration on live is active [REL-13389]
- Isolate the SchulConneX education sync per organization and raise the request timeout [REL-12715]
- Log aborted client connections as warning instead of error [REL-13095]
- Migrate the compliance history UUID columns from varchar to uuid [REL-12988]
- Normalize the base64 output of user certificate placeholders and expose the PKCS#12 password [REL-13456]
- Optimize automatic refresh of device action list [REL-12233]
- Polish the empty, loading and no-permission states of dashboard widgets [REL-12017]
- Poll the Apple Event Status through a dedicated client and skip expired tokens [REL-11832]
- Provide option to import weblinks via CSV in the teacher console [REL-12025]
- Reduce the maximum HTTP header size to 64 KB [REL-13094]
- Renew Apple push certificates, valid until July 2027. The previous ones will expire in January 2027 [REL-12488]
- Require a dedicated authority for device group actions [REL-11643]
- Serve management and content downloads to device tokens through dedicated device-scoped endpoints [REL-13374]
- Show devices of all organizations in the policy details of the global organization [REL-1932]
- Show the expiration date of parent app links only for the states Open and Invited [REL-12586]
- Support configuring external URL per API scope [REL-13087]
- Support editing icons of winget apps [REL-8118]
- Support Relution Decon on macOS devices [REL-13055]
- Support the current Android API levels and icon sizes when parsing APKs [REL-13046]
- Support using a key file for SSE-C encrypted object storage [REL-12853]
- Use the external URL for SMTP EHLO/HELO and group the email configuration into sections [REL-13070]
- Validate the package name format in detection rule forms [REL-12575]

Fixes

Für Version 26.4.0

- Add a Microsoft account policy to block creation and login of Microsoft accounts on Windows [REL-5840]
- Add important security improvement addressing authorization issue affecting authenticated users [REL-13078]
- Add important security improvement addressing authorization issue affecting authenticated users [REL-13085]
- Add important security improvement addressing authorization issue affecting authenticated users [REL-13092]
- Add the missing platforms to the policy prioritization dialog [REL-13269]
- Adjust the ActivPanel PIN configuration [REL-13319]
- Adjust the column size of dashboard widgets to the available space [REL-13513]
- Allow clearing the default StrongSwan VPN profile in StrongSwan restrictions [REL-7232]
- Allow previewing a widget before entering its name [REL-13378]
- Allow selecting native apps for the remove app action [REL-12978]
- Attach server CA certificates with the type AUTHORITY instead of inline PEM fields [REL-12830]
- Base VPP asset and assignment clean-up on the assignments received from Apple [REL-11371]
- Center the widget states in the widget body [REL-13105]
- Clean up compliance violations for platforms that only communicate via the companion app [REL-12974]
- Clear stale dynamic device group memberships on re-enrollment [REL-12612]
- Close the remote session dialog and report the error on unhandled error codes [REL-11203]
- Correct the German translation of the parent app link status Open [REL-13483]
- Disallow uninstalling apps that are managed by a Android Enterprise policy [REL-11373]
- Do not deliver media actions while a device is awaiting its configuration [REL-13072]
- Do not log aborted client requests as errors [REL-13039]
- Do not offer user certificates in the certificate selection of policies [REL-13271]
- Do not request the user list while a device is awaiting its configuration [REL-12777]
- Fall back to the defaults when a removed section of the KSP configuration is reset [REL-13299]
- Fix a MariaDB deadlock when updating VPP asset counts [REL-11018]
- Fix a race condition where the work queue reported itself idle during completion [REL-13048]
- Fix a redirect loop that prevented a second login in the WebView [REL-13345]
- Fix an out of memory error when uploading an Android APK [REL-13481]
- Fix automatic disassociation of VPP users, when a user change event has been triggered [REL-12984]
- Fix creation of compliance history entries in various cases [REL-12843]
- Fix duplicate key violation when storing VPP notification entries [REL-5679]
- Fix heartbeat requiring extra management endpoint configuration or otherwise blocking server start [REL-13309]
- Fix icon alignment on several places [REL-12214]
- Fix iOS wallpaper configurations not respecting the configuration priority [REL-6223]
- Fix misleading percentage rounding in dashboard widget legends [REL-13459]
- Fix the always empty installed apps list of the remove app action [REL-13446]
- Fix the bug reporter when removing the metric filter of a widget [REL-13172]
- Fix the CSV import class assignment when multiple users share the same class [REL-12837]
- Fix the dashboard failing when impersonating another administrator [REL-13183]
- Fix the displayed user name and tenant in the portal header [REL-12288]
- Fix the initial focus in the user and profile view [REL-13098]
- Fix the layout of the policy priority dialog [REL-13439]
- Fix the layout of the printed enrollment QR code [REL-11726]
- Fix the overflowing organization type column [REL-13454]
- Fix the policy filter of the dashboard widgets [REL-13369]
- Fix the sizing behaviour of the dashboard widget legend [REL-13445]
- Fix the tooltip hints of the Android Enterprise managed app install types [REL-11457]
- Fix the unresolved placeholder in the policy version tooltip [REL-13467]
- Fix the user and group domain search by marking browsable security providers [REL-12378]
- Fix uninstallation of Windows Classic native apps [REL-13438]
- Fix visibility of SMG service url field [REL-12993]
- Fix VPP user invitations not registering the user [REL-8449]
- Handle non-JSON VPP error responses without logging a stacktrace [REL-11406]
- Harden the OneRoster token renewal during long running synchronizations [REL-12473]
- Hide system apps in the installed apps list of the remove app action [REL-13038]

Für Version 26.4.0

- Hide system groups in organizations management settings from the selection, so that the prefilling during organization creation can't fail anymore because of invalid prefilled groups [REL-13472]
- Hide the empty toolbar on read-only dashboards [REL-13426]
- Honour the trusted TLS CA certificates for all outbound connections [REL-13380]
- Improve the layout and wording of the create widget dialog [REL-13457]
- Improve the UX of the dashboard widget modals [REL-13104]
- Link DEP certificates and private keys to their owner [REL-13040]
- Load the metric filter into the form when editing a widget [REL-12741]
- Make the audit columns of security roles non-nullable and insert-only [REL-12400]
- Make the columns of table widgets resizable and horizontally scrollable [REL-12770]
- Make the companion signing key certificate fingerprints configurable and skip stale APK deployments [REL-12379]
- Make the KSP and system certificate widgets resizable [REL-13114]
- Make VPP assignment synchronization idempotent to avoid duplicate assignments [REL-11231]
- Map all Apple platforms to the Apple external app store [REL-13024]
- Map Windows Pro for Workstations to the PRO OS edition [REL-13053]
- Offer the Update MDM profile action for Apple user enrolled devices [REL-13238]
- Prevent changes to provider-managed groups for provider-managed users [REL-13033]
- Prevent uploading a native app while it is in archive state [REL-1201]
- Refuse stale education configuration writes [REL-13081]
- Remove outdated policy related compliance violations [REL-12970]
- Remove the stray dot behind the selector in the associate license dialog [REL-13458]
- Remove the unused ChromeOS specific scope and the obsolete server CA PEM fields [REL-12055]
- Removed unsupported EAP Phase 2 authentication types from the Android Enterprise Wi-Fi configuration [REL-12776]
- Report more specific error messages when user certificates are missing on Apple and Windows devices [REL-11739]
- Report the UUID of the existing user in CSV import skip messages [REL-13042]
- Require a confirmation before deleting a user certificate [REL-12737]
- Reset the enrollment cycle on re-enrollment and Return to Service [REL-12992]
- Respect the JVM proxy settings and apply a connect timeout during the OIDC token exchange [REL-13391]
- Respect the policy version state filter in dashboard widgets [REL-13227]
- Revoke the JWT token when logging out from any client [REL-13365]
- Show a validation message for the host in the Windows Exchange configuration [REL-13452]
- Show the app name of removable apps [REL-13025]
- Show the correct info page when a user denies the consent during the IdP login [REL-12806]
- Show the export progress and fix crashes when exporting large device lists [REL-12002]
- Show the no-permission state in custom dashboard widgets [REL-13103]
- Skip device group locking when the memberships are unchanged [REL-13057]
- Skip externally managed courses during the CSV import [REL-12931]
- Stop logging an error for every revoked certificate during the certificate migration [REL-13388]
- Stop the nightly resource migration from rewriting unchanged files [REL-13268]
- Validate the SSE-C encryption configuration to prevent misconfiguration [REL-13449]

Für Version 26.4.0

Version 26.4.6

2026-09-07

Fixes

- Ensure that apps from a global VPP token are also preserved when the "Preserve all existing apps" option is active in the DEP profile [REL-13320]

Version 26.4.5

2026-08-19

Fixes

- Fix persisting the push token of Android Classic devices [REL-13243]

Version 26.4.4

2026-08-18

Updates

- Augment “preserve all apps” functionality for Apple device migration [REL-13167]

Fixes

- Prevent loss of ON-Demand App Installation for Apps iOS 26 device migration [REL-12442]
- Improve caching of Image Render Service [REL-13159]

Für Version 26.4.0

Version 26.4.3

2026-08-12

New

- Add support to upload multiple user certificates for a subtype [REL-12989]
- Add new “Managed software updates” configuration for apple devices [REL-12745]
- Add support for ECDSA keys to certificate templates and Apple IKEv2 VPN configuration [REL-11898]

Updates

- Dialogs for CA certificate selection shows only CA certificates [REL-12863]

Fixes

- Fix an issue where a lifetime licensed device cannot be re-enrolled after migration to another organization [REL-13026]
- Fix an issue where a lifetime licensed device cannot be enrolled when the device license metric of the organization is exceeded [REL-12471]

Version 26.4.2

2026-08-11

Fixes

- Add important security improvement addressing authorization issue affecting authenticated users [REL-13078] [REL-13085] [REL-13086] [REL-13092] [RVD-2026-1]

Version 26.4.1

2026-07-30

Fixes

- Fix automatic disassociation of VPP users, when a user change event has been triggered [REL-12984]
- Fix visibility of SMG service url field [REL-12993]
- Fix creation of compliance history entries in various cases [REL-12843]

Version 26.4.0

Für Version 26.4.0

2026-07-16

With Relution 26.4.0, the internal application server was switched from Undertow to Tomcat. If the reverse proxy runs on a different server than Relution itself, logging in may subsequently fail with the message `Access is forbidden` (`TLS required` in the server log). In this case, the configuration must be adjusted according to the steps described in Login: Access is forbidden →

New

- Improve self-service portal device locate flow so authorised users can access location feedback [REL-11014]
- Add shutdown action support for Newline smartboards [REL-10615]
- Add time zone information to Apple device details [REL-12447]
- Add enhanced retry and backoff handling for object storage operations [REL-11912]
- Improve foundation of object storage and general resource storage handling with better resilience and observability [REL-11910]
- Improve object storage client connection handling and timeout configuration [REL-11911]
- Improve device history localization by storing translation keys and translating entries when read [REL-12067]
- Add support for DEP enrollment using username and enrollment code authentication [REL-11841]
- Add support for managing additional CA certificates in global settings for outbound SSL/TLS connections [REL-11453]
- Add server version to audit log start and stop entries [REL-12423]
- Improve organization switcher to pin specific items [REL-11748]
- Introduce scoped OIDC redirect URIs for reverse-proxy path gating. Legacy URI stays valid but is deprecated, register the new URIs at your Identity Provider, check Relution Hub for more information [REL-10832]
- Add support for automatically updating the assigned device user when a user logs into a managed Windows device, with organization-level and device-level controls [REL-8313]
- Extend agent-scope API support by mirroring relevant server endpoints and migrating Relution Assets to use only endpoints from its dedicated API scope [REL-10523]
- Add search bar to Apple and Android app compliance lists to make apps easier to find [REL-12023]

Updates

- Exclude obsolete Relution client certificates from key store checks and cleaned up leftover database entries [REL-11535]
- Update Spring Boot to Version 4 [REL-10462]
- Disable audit logs for get actions management endpoint by default [REL-12475]
- Support pinning the TLS certificate for Apple Software Update lookup service (GDMF) requests [REL-11344]
- Adjust handling of VPP apps being reported with zero licenses [REL-10792]
- Improve reliability of macOS VPP app update detection and installation [REL-11659]
- Improve SSO failure log messages with more useful context for troubleshooting [REL-12286]
- Improve handling of expired Apple VPP tokens by validating token expiry before associate/disassociate actions and reducing unnecessary error logging [REL-463]
- Add support for the macOS security action “Set Recovery Lock” on supervised and managed devices [REL-11630]
- Improve database performance for VPP assignment and app lookup operations by adding missing indices [REL-1744]
- Add a warning log when Apple TokenUpdate messages are received without a push token [REL-12068]
- Change embedded web server from Undertow to Tomcat [REL-11894]
- Add “Unspecified” option for Android Enterprise configurations [REL-11881]
- Add collapsible placeholders in configuration editors to improve usability for large forms [REL-11933]
- Do not show empty description and changelog sections for native app versions [REL-12175]
- Improve readability of compliance violation details by making non-compliant reasons easier to view in Poral [REL-7443]
- Improve DEP account wizard by fixing duplicate loading indicators and disabling “Cancel” during account setup [REL-12110]
- Improve native iOS app details view so the URL Schemes section is shown correctly and aligned consistently [REL-12126]
- Change AE settings user interface into a tab-based layout [REL-10589]

Fixes

Für Version 26.4.0

- Fix missing file size information for native apps in required apps lists [REL-12141]
- Fix Shared iPads not automatically receiving Educational Configuration after reset and re-enrollment [REL-12510]
- Fix validation and error messaging for Windows Firewall configurations [REL-11482]
- Fix searching for large numbers of device serial numbers at once [REL-11855]
- Fix Windows Firewall policy deployment for firewall rules that reference apps [REL-12430]
- Fix support of per-app VPN connection in iOS email configuration [REL-12429]
- Fix an issue on multi node setups that lead to ObjectAlreadyExistsExceptions (DashboardNotificationPullJob) [REL-12428]
- Avoid applying changes to users and classes when a OneRoster or ASM sync fetch is incomplete [REL-12412]
- Fix an issue with certain instances that are reporting empty metrics due to a cache initialization issue [REL-12358]
- Fix an issue where providing an own APNS Certificate via global did not get propagated properly to other organizations [REL-12370]
- Fix an issue where android enterprise sim card details did not get updated properly [REL-12315]
- Display Decon block page also on Android Enterprise devices [REL-12202]
- Fix creation of audit log entry for specific events from a device [REL-12217]
- Fix PKG app detection rule dialog showing the wrong rule form when no rule type was selected [REL-12453]
- Fix iOS Web Clip URL validation to allow custom app protocol handlers and placeholders [REL-12432]
- Fix download link for native app downloads via Portal on iOS/iPadOS devices [REL-12323]

Version 26.3.3

2026-07-01

Updates

- Exclude obsolete Relution client certificates from key store checks and clean up leftover database entries [REL-11535]

Für Version 26.4.0

Fixes

- Fix an issue with lifetime licenses to provide license claims during license handshake in case the status of the corresponding device has changed [REL-12538]
- Fix an issue that prevented certain organizations from performing a license handshake in case certificates of different key sizes where present on the same instance [REL-12481]

Version 26.3.2

2026-06-22

Updates

- Adjust default log level for incoming requests from SMG standalone service [REL-12476]
- Disable creation of audit log entries for `GET` action management endpoint in default configuration [REL-12475]

Fixes

- Avoid applying changes to users and classes when a OneRoster or ASM sync fetch is incomplete [REL-12412]
- Fix cluster broadcast problems when saving courses during Schulconnex sync [REL-12408]
- Fix large Schulconnex districts failing to sync due to the response exceeding the in-memory buffer limit [REL-12408]
- Prevent Schulconnex users from being disabled or deleted when a person-info request fails [REL-12408]
- Improve logging of failed user saves during Schulconnex sync to include the underlying cause [REL-12408]
- Fix an issue with certain instances reporting empty metrics due to a cache initialization issue [REL-12358]
- Fix re-enrolled Apple devices retaining the push certificate from their previous enrollment instead of picking up the organization's currently configured push certificate [REL-12436]

Version 26.3.1

2026-06-11

Fixes

- Fix an issue where providing an own APNS Certificate via global did not get propagated properly to other orgas [REL-12370]
- Fix problems with license handshake in cluster setup [REL-12200]
- Fix an issue where Android Enterprise SIM card details did not get updated properly [REL-12315]

Version 26.3.0

2026-06-08

Für Version 26.4.0

New

- Update Relution Teacher to use only endpoints from its dedicated API scope [REL-10526]
- Require an APNS Certificate for Apple device enrollment on new instances [REL-11825]
- Update Parent App to use only endpoints from its dedicated API scope [REL-10527]
- Update Windows Companion to use only endpoints from its dedicated API scope [REL-10519]
- Allow selecting user certificate type and target channel in Apple certificate configuration [REL-8846]
- Add support for EAP-PWD as an EAP outer method for Android Enterprise Wifi-Configurations [REL-11478]
- Add support for device enrollment with managed Google account user authentication [REL-8955]
- Encrypt sensitive fields in detail records stored in the database [REL-10738]
- Add support for private DNS configuration on Android Enterprise devices [REL-11393]
- Add option to define the install behaviour of Android Enterprise Apps [REL-10013]
- Require the custom APNS setup workflow for new organization instances [REL-11477]
- Move the SCEP enrollment endpoint to the device API scope [REL-10837]
- Add macOS 26.4 migration assistant declaration and status report [REL-11513]
- Add TLS 1.2 and TLS 1.3 support via the embedded web server [REL-10471]
- Add WPA3 Support for Windows Wifi config [REL-10697]
- Add a local/global filter for device groups [REL-11869]
- Allow adding devices to policies published only as test versions [REL-11186]

Updates

- Improve SchulConnex sync so users without an email address can still be synchronized using their person ID as login name [REL-11897]
- Show teacher group and student group counts in LDAP test organization mapping [REL-11862]
- Add support for Decon on Android Enterprise [REL-9062]
- Improve policy publishing and deletion by updating affected devices through the device group change workflow [REL-11086]
- Create public apps in Production state by default [REL-8119]
- Add missing Unspecified options to affected configurations for Android Enterprise [REL-11624]
- Streamline API responses for user and group information (downwards compatible) [REL-6628]
- Improve policy version history by showing configuration names where possible [REL-11584]
- Fix enrollment filters in dynamic device groups to work as expected [REL-11681]
- Improve Teacher App organization handling for multi-tenant users by only showing organizations with teacher permissions [REL-7179]
- Route the Device Catalog Service through the Service Gateway [REL-11299]
- Exclude obsolete Relution client certificates from key store checks and clean up leftover database entries [REL-11535]
- Improve the copy-to-organization dialog by removing a redundant loading overlay and correctly disabling navigation buttons during loading [REL-11829]
- Fix validation of certificate templates in Portal if expiration in days is less than automatic renewal [REL-7724]
- Fix empty context menu for revoked device certificates [REL-11728]
- Fix iOS system app search so apps can also be found by bundle ID [REL-11678]

Fixes

- Fix URL encoding in Windows Kiosk configurations so URLs are applied correctly [REL-12070]
- Fix an issue where the Schulconnex provider name was not correctly resolved in the audit log [REL-12140]
- Improve resource migration handling to prevent permanently failing S3 uploads from blocking other migrations [REL-11818]
- Fix incorrect sorting by organization in the groups modal [REL-11639]
- Fix iOS error 4001 when ending a Single App Mode lesson whose app is not on the policy whitelist [REL-11810]
- Fix incorrect VPP assignment detection between Apple User Enrollment and device-based assignments [REL-11823]
- Reduce required permissions for viewing conditional access information in device details [REL-10161]
- Add creation date for CSV-imported users [REL-10760]
- Fix missing display of invalid 2FA attempts after successful password entry [REL-7224]
- Fix message sending during lesson failures caused by long titles [REL-11587]
- Fix auto-renewal failures for SCEP-issued device certificates when using the Invalidate renewal behavior [REL-11725]
- Improve reliability of pending action detection in dynamic lesson information processing [REL-11742]
- Improve audit log reliability for delete operations to avoid missing resource information [REL-10408]
- Fix managed configuration boolean values to properly support null for Heineking configuration [REL-11531]
- Fix Windows Autopilot enrollment when the device already exists in Relution [REL-11410]
- Fix search of special characters in winget store leads to no results [REL-11607]
- Fix incorrect display setting values being applied on CVTE Heineking Media C10 devices [REL-11330]
- Fix possible repeated installation of managed media when marked ‘Managed but uninstalled’ on Apple devices [REL-11558]
- Fix VPP token display in meta organizations so global tokens are shown with the correct organization label [REL-9244]
- Fix an issue where outdated Relution News did not get removed properly [REL-11437]
- Fix Apple VPN IKEv2 configuration not sending certificateType and enableFallback to the REST API on save [REL-11896]
- Improve the action overview to make the triggering device group context clearer [REL-7592]
- Fix the roaming dashboard filter so devices with unknown country values are handled correctly [REL-7920]
- Fix an issue where the context menu in VPP sync history appeared empty for finished, failed, or canceled tasks [REL-4932]
- Improve validation by correctly highlighting invalid fields [REL-9623]
- Improve MDM user scope description in Entra ID wizard [REL-11424]
- Fix missing Android Enterprise compliance violation details [REL-11462]
- Fix incorrect validation highlighting for the optional DNS servers (IP addresses) field in Apple Encrypted DNS settings [REL-11694]
- Fix the available storage bar to show available storage instead of used storage [REL-11661]
- Fix creation of Windows detection rules when Safari 26.4 is used as browser [REL-11601]

Für Version 26.4.0

Version 26.2.2

2026-05-18

Fixes

- Fix AuditLog translation issues [REL-11797]
- Fix creating wrong AuditLog issues [REL-11831]
- Fix problem with wrong WinGet identifiers [REL-11799]

Version 26.2.1

2026-05-05

Updates

- Disable multiple device related audit log entries and audit log read attempt entries in the default server setup [REL-11780]

Fixes

- Fix thread pool doesn’t close DB connections, even when the DB already closed it [REL-11779]
- Fix exception in cluster setup when the server tries to write an audit log entry [REL-11782]

Für Version 26.4.0

Version 26.2.0

2026-04-24

New

- Add new restrictions and declarations for Apple OS 26.4, add new fields to Extensible SSO configuration [REL-11407]
- Allow to upload more than 15 teachers per class via ASM - SFTP upload. [REL-11609]
- Add an audit log entry, when older audit log entries are removed by a cleanup job [REL-10580]
- Add OneRoster API connector [REL-11281]
- Fix translation of compliance violations titles in Relution Agent [REL-8988]
- Add audit log entries when the device OS version changes [REL-10577]
- Added printer restriction for Android Enterprise. [REL-10032]
- Added work account upgrade configuration for Android Enterprise. [REL-8957]
- Add option to control the behaviour of AssistContent for Android Enterprise. [REL-10031]
- Add option to control private space for Android Enterprise. [REL-10029]
- Changed the RSA key-length to 4096 bit. [REL-10478]
- Added preferential network service configuration for Android Enterprise. [REL-8730]
- Add audit log entries when applied policies on a device changes [REL-10576]
- Control data roaming option for iOS. [REL-10799]
- Add audit log entries when a user tries to read the audit log [REL-10579]
- Add a table displaying available updates for Windows devices [REL-9199]
- Add policy to define default applications for Android Enterprise. [REL-10023]
- Support native apk installation for Android Enterprise. [REL-11006]
- Add device enrolment, re-enrolment and deletion in audit log. [REL-10771]
- Add CSV export of audit log table. [REL-10647]
- Moved teacher api scope to /api/teacher/. [REL-6908]
- Add result column in audit log to show the operation result [REL-11011]
- Add option to control the connection state of android enterprise devices like: Wifi, UWB, 2G & airplane-mode. [REL-4184]
- Changelog handled via GitLab YML [REL-10608]
- Add option to highlight difference between policy versions. [REL-9157]
- Add content protection and MTE setting for Android Enterprise to control the scanning of deceptive apps. [REL-10015]
- Add support for custom app installation [REL-11004]
- Add the option to test all versions of a policy to check the different settings that were made in the previous versions. [REL-9143]
- Add start and shut down entries for the server to audit log. [REL-10573]
- Move “device” endpoints to “device” api scope [REL-6909]
- Add filter options to audit log [REL-11046]
- Add audit log entries when device certificates are updated [REL-10575]

Für Version 26.4.0

Updates

- Add description to custom properties of LDAP groups [REL-11472]
- Fix connection timeout in SMG on Provision/Settings ActiveSync-Requests of devices with an unknown EAS identifier [REL-11559]
- Fix stall in SMG communication that can occur in some cases when a client sends a large email (i.e. with attachment) [REL-11559]
- Allow to configure the external URL via Relution settings. [REL-11619]
- Add placeholder support to the Android Enterprise account upgrade configuration [REL-11544]
- Allow to define the credential provider on Android Enterprise devices. [REL-10011]
- Improved scalability of background sync and polling tasks by switching to Java 21 virtual threads [REL-11443]
- Add not yet supported options to Apple cellular configuration [REL-11277]
- Improved performance of group membership and role lookups on PostgreSQL 14+ [REL-11230]
- Added advanced security overrides option for Android Enterprise devices. [REL-7601]
- Optimize handling of device group web hook actions [REL-10568]
- Add permission to change the device user. [REL-10842]
- Update glowroot version [REL-9797]
- Update sales contact information in the license information view [REL-11368]
- Show LDAP sync start time in portal [REL-11257]

Fixes

- Add audit log entries when the device policy changes [REL-11586]
- Fix search of special characters in winget store leads to no results [REL-11607]
- Fix VPP filter returns wrong results in apps list [REL-11588]
- Fix possible repeated installation of managed media when marked ‘Managed but uninstalled’ on Apple devices [REL-11558]
- Fix race condition which could result in assigning the wrong policy version on a device [REL-11434]
- Fix problem with upload of different files, e.g. fonts, csv, … [REL-6618]
- Fix calculation of license counts for TeamViewer Addon [REL-11191]
- Fix update mechanism of Android Classic companion [REL-11229]
- Prevent adding system groups to admin group during organization creation [REL-7106]
- Fix SQL exception when multiple device groups are updated at once [REL-10882]
- Update macOS screensaver configuration for macOS 26+ devices [REL-11133]
- Fix lookup of the default language when creating a Weblink and english is removed [REL-11029]
- Fix cloning of iOS system update configuration skips the target OS version field [REL-11038]
- Fix geofence filter options are not displayed in filter menu [REL-11638]
- Add missing translations for filtering menus, when a value gets selected [REL-11635]
- Reload device counts in a device groups, when the number of devices changes in the list [REL-11582]
- Skip installation of Android Enterprise public apps, when not all required information is given [REL-11418]
- Fix managed app editor doesn’t display data of nested bundle [REL-11455]
- Fix creation of windows detection rules when Safari 26.4 is used as browser [REL-11601]
- Add missing translations in the Android Enterprise Advanced Security Overrides configuration [REL-11603]
- Fix height of filter menu, when less than 5 entries are available [REL-11581]
- Fix CSS issue in Safari 26.4 which results in hidden column content [REL-11486]
- Fix saving of selected credential provider under Android Enterprise managed app configuration [REL-11488]
- Fix scroll behaviour in execute action confirmation step for powershell scripts [REL-9861]
- Add keyguard option to restriction for Android Enterprise devices. [REL-9627]
- Hide wifi passwords in sub organizations [REL-11421]
- Display posture details in device details of an Android Enterprise device [REL-10538]
- Fix problem with saving modified device groups. [REL-10983]
- Fix nullpointer exception when an Android Enterprise App should be updated via action [REL-11103]

Für Version 26.4.0

Version 26.1.2

2026-04-21

Updates

- Add description to custom properties of LDAP groups [REL-11472]

Fixes

- Fix duplicate PayloadUUID in iOS MDM profiles causing policy update failures on stricter iOS versions [REL-11645]
- Fix connection timeout in SMG on Provision/Settings ActiveSync-Requests of devices with an unknown EAS identifier [REL-11559]
- Fix stall in SMG communication that can occur in some cases when a client sends a large email (i.e. with attachment) [REL-11559]
- Fix rendering issue in Android enterprise managed app editor [REL-11455]

Version 26.1.1

2026-03-30

Fixes

- Fix database migration issues. [REL-11402]
- Fix managed app editor doesn't display data of nested bundle. [REL-11455]

Version 26.1.0

2026-03-16

New

- Add the option to test all versions of a policy to check the different settings that where made in the previous versions. [REL-9143]
- New baseline for database created. Before updating to versions higher than 26.0.0, the version 26.0.3 needs to be installed first. [REL-6842]
- Improve the DPA view to get a better guidance. [REL-10802]
- Allow to assign or remove device groups to multiple auto enrollments. [REL-9346]
- Show the number of devices with a specific version in the policy sidebar. [REL-9155]
- Add option in certificate templates to decide whether to revoke or keep certificates issued per device on automatic renewal [REL-10439]
- Added re-usage of TeamViewer-Settings in different organisation. [REL-10249]
- Enable support of policy type (publisched & testing) for device groups. [REL-10893]
- Add support for devices of CTOUCH. [REL-10430]
- Added option to upgrade Google Play accounts to managed Google domain enterprise accounts for Android Enterprise. [REL-8958]
- Added the Enterprise Display Name of an Android Enterprise [REL-9020]
- Adapt rating settings as optional in restriction configurations for iOS. [REL-10350]
- Changelog handled via GitLab YML [REL-10608]
- Added SoftwareUpdateSettings for iOS to configure software updates. [REL-10554]
- Added option to configure audio accessory settings for iOS. [REL-8970]
- Update System Update configurations for Apple. [REL-10570]
- Allow to assign or remove device groups to multiple devices via inventory. [REL-10188]
- Add support of starting the teacher app directly in specific organisation. [REL-10547]
- Move "device" endpoints to "device" api scope [REL-6909]
- Group management API endpoints under a common path [REL-6910]
- Added configuration for math/calculator settings on Apple devices. [REL-8971]
- Make Windows app action timeouts optional and adjust min and max values [REL-6289]

Updates

Für Version 26.4.0

- Add option to test policy versions before releasing them to all devices [REL-10972]
- Extend the available metric for Pub/Sub communication of Android Enterprise. [REL-5810]
- Deduplicate automatically triggered deploy app actions on shared iPads [REL-10466]
- LDAP group import preview now shows the correct foreign key instead of always displaying a group's DN [REL-10618]
- LDAP cycle detection now correctly identifies cycles only when a group contains itself, avoiding incorrect warnings in the logs for different membership paths to the same group. [REL-10618]
- Device placeholders in user messages configuration of Android Enterprise is now supported. [REL-10793]
- Add support for filtering in the device inventory for Windows device ID. [REL-10774]
- Provide dedicated endpoint to switch the user of a device [REL-10644]
- Optimize database access during Apple MDM communication [REL-10045]
- Allow importing tvOS only apps via VPP [REL-10315]
- Improve performance impact of nested dynamic device group filters with user group recursion [REL-10205]
- Fix empty states in lists which are not embedded in the layout [REL-10928]
- Update favicons of Relution Portal [REL-3486]
- No longer display the provided error informations from the URL to the user, to prevent URL manipulation by a 3rd party. [REL-10536]
- Update admin portal to Angular 20 [REL-9108]
- Improve UI of managed app configuration editor [REL-9050]

Fixes

- Fix calculation of license counts for TeamViewer Addon [REL-11191]
- Fix update mechanism of Android Classic companion [REL-11229]
- Update license counts, when a device is moved from one organization to another [REL-11069]
- Add setting for unmanaged classes screen observation prompting in iOS / iPadOS restrictions [REL-10800]
- Allow to delete an organisation with a TeamViewer configuration. [REL-11008]
- Fix missing web links on Relution shared devices via auto-deployment. [REL-10874]
- Fix update option of foreign VPP managed media. Only media of own (orga) VPP tokens can be updated. [REL-10975]
- Fix problem of reenrolled device for same user with failed education configuration update. [REL-10996]
- Cleanup leftover ruleset database table [REL-10962]
- Importing groups of users rejects groups without a foreign key once again [REL-10877]
- LDAP test buttons no longer lead to "no sync running" errors in the logs [REL-10877]
- Fix add local account action on windows devices, when only non admin users are added [REL-10831]
- Automatically trigger deploy app actions on windows devices, for missing apps, during refresh device info action [REL-9951]
- Fix wifi configuration not being deployed during DEP re-enrollment when wifi whitelisting is enforced [REL-10530]
- Fix asynchronous communication with 3rd party systems potentially failing until server restart when having IPv6 disabled [REL-10563]
- Fix wrong count in "Purchased Apps" view for assigned licenses. [REL-8750]
- Allow saving of iOS certificate configuration only, when the policy version is draft [REL-11214]
- Allow editing the Airplay configuration only, when the policy version is in draft state [REL-11215]
- Allow editing of an iOS managed app configuration only, when the policy version is in draft state [REL-11222]
- Improve performance of filter menu in lists [REL-11124]
- Fix Android Enterprise user facing message configuration UI [REL-11205]
- Allow custom user fields in the ios mail configuration. [REL-10809]
- Allow lending period that starts and ends on the same day. [REL-10772]

Für Version 26.4.0

Version 26.0.3

2026-02-11

Fixes

- Fix Secure Mail Gateway returning HTTP 403 instead of 401 when unauthenticated leading to reduced number of password prompts [REL-10973]

Version 26.0.2

2026-02-05

New

- Add support for disabling Safari history retention in Apple Web Content Filter configurations [REL-10181]

Fixes

- Fix Windows Push token update failing for unexpected device response causing communication errors in special cases [REL-10778]
- Prevent license handshake request creation failing due to license claim retrieval for lifetime licenses [REL-10866]
- Fix Local Windows Account action failure when creating non-admin accounts only [REL-10831]
- Fix saving Web Content Filter configurations with plugin filter type [REL-10883]

Für Version 26.4.0

Version 26.0.1

2026-01-15

Updates

- Provide dedicated endpoint to switch the user of a device [REL-10644]

Fixes

- Fix possible error in login flow [REL-10542]
- Make Time-based policies work as expected for Android Classic [REL-10285]
- Fix asynchronous communication with 3rd party systems potentially failing until server restart when having IPv6 disabled [REL-10563]

Version 26.0.0

2025-12-17

New

- Add support for Apple visionOS devices [REL-9735]
- Add support for Apple watchOS devices [REL-9736]
- Automatically migrate all organizations to device groups after server startup [REL-6972]
- Adjust handling and updating of Android Classic Companion [REL-10386]
- Group management API endpoints under a common path [REL-6910]
- Group device API endpoints under a common path [REL-6909]
- Make Windows app action timeouts optional and adjust min and max values [REL-6289]
- Users can now sign data processing agreements in Relution itself [REL-9519]
- Improve WinGet search in public app store concerning pagination and icons and enable to find results by searching for IDs [REL-6633]
- Include device requests in audit log [REL-8621]
- Add Decon configuration for Android Enterprise [REL-9058]
- Add setting to skip MDM profile restoration from backup in DEP profile [REL-8977]
- Add support for time-based app restriction via Relution Parent [REL-2901]
- Support restoring the draft version of a policy to any historical version of the policy [REL-9150]
- Add support for DAP signing and status reporting [REL-9215]
- Add TeamViewer connection reporting to device history [REL-8415]
- Optimize display and sorting of Windows editions [REL-9889]
- Show desktop client join link for TeamViewer “Bring your own license” remote support [REL-9087]
- Automatically install VC Redistributable when required for WinGet [REL-6084]
- Support all certificate options (single select, user, and certificate templates) in Windows Certificate configuration [REL-4436]
- Add several new fields to the Promethean Android Classic integration. The Relution Promethean Companion must be updated to 26.0.0 or above [REL-9427]
- Optimize display of policy version history [REL-9153]
- Add Support for TeamViewer Remote Control for iOS [REL-10250]
- Remove rule-set feature [REL-2614]

Updates

Für Version 26.4.0

- Improve performance impact of nested dynamic device group filters with user group recursion [REL-10205]
- Adjust gzip handling in license handshake [REL-10404]
- Drop redirects for legacy API paths which were replaced with Relution 5 [REL-10399]
- Ensure device group migration also covers edge case where the global has been migrated but not all tenant organizations [REL-10375]
- Apply Windows Wifi configuration regardless of known network adapter existence [REL-7134]
- Ensure Windows Store app can be added when icon is unavailable [REL-10203]
- Optimize memory footprint of wallpaper handling on Apple devices [REL-10198] [REL-10204]
- Adjust compliance violations for MSCA devices [REL-10134]
- Optimize Windows CSP Status handling to show more detailed status and error messages [REL-5339]
- Make it possible to add Windows Store apps whose icon provides no content-type [REL-10190]
- Further improve throughput of Secure Mail Gateway for large emails [REL-9989]
- Optimize memory usage of Secure Mail Gateway when client connection is slow [REL-9989]
- Fix potential stalls in Secure Mail Gateway when handling extremely large payloads [REL-9989]
- Optimize performance when accessing static Portal resources [REL-10133]
- Add the Relution File Shares configuration for Android Enterprise [REL-10056]
- Avoid misleading warn log message when creating iOS certificate configurations [REL-10062]
- Add definition of not filterable fields to filter API [REL-9281]
- Optimize database access during Apple MDM communication [REL-10045]
- Properly shut down APNS event loop when Relution is shut down [REL-10051]
- Add header to extend status reporting for WNS pushes [REL-10016]
- Updating a user through REST API no longer fails when organizationUuid is not specified [REL-10010]
- Avoid excessive error logging in Apple password hashing if password is empty [REL-10000]
- Rejected Secure Mail Gateway connections no longer result in bogus sign-in attempts [REL-9984]
- Add support for gzip compression for License Handshake 2.0 to Relution [REL-9739]
- Fix german audit log translations [REL-10441]
- Add latest security patches for Angular [REL-10288]
- Add Remote Desktop action to Device Group actions [REL-7617]
- Properly enforce required values in set password action for macOS [REL-10002]
- Optimize server health widget layout on global organization dashboard [REL-10172]
- Hide “Update via CSV” option in the device inventory of the global organization, because the updater can only update devices of the organization itself [REL-10474]
- Add new 26.2 skip keys to DEP profiles [REL-10469]

Für Version 26.4.0

Fixes

- Remove unintended data from logging [REL-10445]
- Last connection date for Android Enterprise once again matches last update of device details [REL-10211]
- Remove hidden default rating settings in iOS / iPadOS restrictions [REL-10385]
- Avoid showing communication errors for freshly created Android Enterprise connections [REL-10344]
- Adjust audit log data context display for several entries [REL-10389]
- Certificates using templates and auto-renewal are now properly renewed on Android Enterprise [REL-10372]
- Fix MSCA enrollment of windows devices [REL-10321]
- Continue script actions on macOS after companion installation [REL-10353]
- Fix shared device lessons keeping stale local app references after app scope changed to global later preventing deletion of organisations [REL-10284]
- Fix Android Enterprise subscription pulling possibly not recovering after a network outage [REL-10195]
- Fix WiFi selection in “Return To Service” device group action [REL-10227]
- Continue pending script installation actions after installation of macOS companion required for their execution [REL-7905]
- Fix deletion of organization after devices have been moved away from it [REL-5484]
- Fix update of web links on lesson devices after they have been changed in the lesson or lesson template [REL-9962]
- Fix failing update wallpaper actions [REL-9937]
- Fix automatically applying managed app configuration for Relution Teacher on Android Enterprise [REL-9907]
- Add missing audit log translations [REL-10411]
- Fix removing a previously set max OS version in Apple system update configuration [REL-10400]
- Fix empty state of user auto deployments list [REL-10367]
- Fix portal login view for apps no longer working after a failed login attempt without reopening it [REL-10334]
- Fix unexpected error message when initially saving Android Enterprise settings [REL-10317]
- Fix display issues with BitLocker information in device details [REL-7906]
- Fix display issues in app auto deployment user selection [REL-10359]
- Fix small issues in app release workflow views [REL-10342]
- Fix audit log translations [REL-10354]
- Add setting for unmanaged classes screen observation prompting in iOS / iPadOS restrictions [REL-10325]
- Fix display issues in app information page [REL-6279]
- Fix display issues in Android application control configuration [REL-6384]
- Fix portal issues in app release workflow [REL-8497]
- Fix display issue in enrollment page [REL-7803]
- Disable VPP user registration button after submitting [REL-7746]
- Improve display of error message when trying to save invalid device lendings [REL-8960]
- Fix saving off time configuration when not subscribing to a state calendar [REL-10229]
- Fix enabled state of save button in macOS content caching configuration [REL-10224]
- Fix display issues in extensible single sign on configuration [REL-10223]
- Improve display of third party libraries [REL-9972]
- Fix sorting icon in profile tables [REL-9298]
- Fix sorting icon in users and groups selector [REL-9969]
- Fix display issues in empty nested tables [REL-10212]
- Avoid duplicated entries in inventory after sorting by phone number [REL-9881]
- Do not show device properties in self service portal where information is not available [REL-10136]
- Restrict max values for Shared iPad settings in Portal [REL-9446]
- Fix links in policy list [REL-9946]
- Do not allow to save empty iOS notification policies in Portal [REL-9445]
- Fix editing of Entra ID connection when not changing the client secret [REL-10053]
- Fix issue when updating meta data of public apps [REL-10087]
- Fix Windows actions clogging push queue with indefinite running requests in rare cases [REL-10461]

Für Version 26.4.0

Version 5.35.4

2025-11-25

Fixes

- Fix opening web version of Relution Teacher in Portal [REL-10210]

Version 5.35.3

2025-11-20

Fixes

- Fix accepting expired device identity certificates [REL-10065]
- Fix display license information for global licensed servers using license allocations [REL-10199]
- Fix issues with permission role authorities which no longer exist [REL-10191]
- Support Windows Store apps with icons of unknown content type [REL-10190]

Version 5.35.2

2025-11-14

Fixes

- Avoid issues with unexpectedly missing organization meta data during license handshake [REL-10163]

Für Version 26.4.0

Version 5.35.1

2025-11-10

Fixes

- Prevent triggering initial certificate signing requests even though an existing certificate is already present [REL-10058]
- Perform initial license handshake 2.0 in background automatically to avoid temporary license signature failure [REL-10052]
- Fix exclusion of the Exchange host header port [REL-10050]
- Fix custom host header setting in Secure Mail Gateway [REL-10050]

Version 5.35.0

2025-11-04

After successfully updating to Relution 5.35, downgrading is no longer possible.

New

- Support restoring the draft version of a policy to any historical version of the policy [REL-9150]
- Add policy version history showing details and changed configurations of each version [REL-9140]
- Group management API endpoints under a common path [REL-6910]
- Add progress, error report and preview to course CSV import [REL-9313]
- Add progress, error report and preview to Decon request CSV import [REL-9348]
- Improve autoenrollment CSV import by adding a preview, progress and error overview [REL-9314]
- Optimize handling of latest connection dates for various platforms [REL-7282]
- Add support to apply a Relution Decon configuration on Windows devices [REL-9135]
- Optimize display of empty states of policy lists [REL-9137]
- Support Shutdown action on Promethean EDLA devices [REL-9071]

Updates

- Migrate to license handshake 2.0 using the service gateway and optimize the license view in Portal [REL-6540]
- Avoid triggering remove app actions if such an action is already pending for the app to be removed [REL-9609]
- Add version 25H2 to known Windows versions [REL-9796]
- Support placeholders in home screen's wallpaper [REL-9674]
- Remove "Priority" from iOS Wi-Fi configuration as it is not supported by iOS [REL-9725]
- Allow to cancel actions of Android Enterprise devices if they are not yet delivered and confirmed. This includes e.g. reboot actions or the wipe triggered upon device deletion. [REL-9460]
- Avoid possible memory issues during VPP sync [REL-9417]
- Use forms in CSV import views [REL-9428]
- Extend license information page for license handshake 2.0 [REL-8012]

Für Version 26.4.0

Fixes

- Fix update of web links on lesson devices after they have been changed in the lesson or lesson template [REL-9962]
- Fix failing update wallpaper actions [REL-9937]
- Fix excessive log output on specific DEP failures [REL-9957]
- Fix OpenID Connect login in Android Enterprise Companion [REL-9913]
- Fix Keep APN password after policy update. [REL-9882]
- Fix automatically applying managed app configuration for Relution Teacher on Android Enterprise [REL-9907]
- Fix deletion of image in Android Wallpaper configuration [REL-9892]
- Remove no longer associated DEP auto-enrollments, when a full DEP sync is triggered [REL-8749]
- Fix small issue in Windows certificate renewal [REL-9593]
- Cache generated wallpapers in configured resource storage for extend durations [REL-9607]
- Avoid issues when loading very old push jobs for non-enrolled devices [REL-9528]
- Avoid excessive memory consumption if groups with a very large number of members are present [REL-9477]
- Fix sorting by "Shared iPad" in "installed on devices" list in app details [REL-9968]
- Fix creating "delete local user" device group actions [REL-9781]
- Fix displaying the phone number column in the `Devices with this app` tab of an app [REL-9536]

Version 5.34.3

2025-11-04

Updates

- Move “email from” setting into global email settings and remove it from individual organizations [REL-9854]

Version 5.34.2

2025-10-31

Updates

- Significantly improve performance when loading lessons with a high number of students [REL-9801]
- Improve performance for off-time policy handling [REL-9820]
- Optimize performance when handling incoming status reports from Apple devices [REL-9806]

Fixes

- Ensure wallpaper preview image is still available when editing a wallpaper configuration [REL-9892]
- Avoid repeated closure of SMG connections when a client connection disappears mid-transfer under high server load [REL-9530]
- Fix failing device information updates for Apple devices [REL-9988]

Für Version 26.4.0

Version 5.34.1

2025-10-20

Updates

- Improve performance when calculating lesson status [REL-9786]
- Optimize incoming Secure Mail Gateway connections to avoid premature and repeated closures under high server load [REL-9530]
- Add indices to speed up access to lesson and student information [REL-9799]
- Avoid unnecessary updates of a devices installed apps if nothing changed [REL-9789]
- Avoid unnecessary repeated loading of disabled policies for each device [REL-9807]
- Avoid redundant database requests by caching meta-organization information [REL-9787]

Fixes

- Fix Relution Companion permissions causing devices to be reported as non-compliant [REL-9784]
- Ensure that a specific foreign key which could have been created manually in the past gets dropped during table modification [REL-9668]
- Add fallback to default name of the app, if no localised name for the app or version is available [REL-9762]
- Fix OffTime date shift due to client/server timezone mismatch [REL-9804]
- Fix Android Enterprise login page not being closed when completed [REL-9782]

Version 5.34.0

2025-09-23

New

- Add option to migrate devices to another MDM server [REL-9176]
- Improve device CSV import by adding a preview, progress and error overview [REL-9315]
- Add new restrictions available with iOS/iPadOS/macOS 26 [REL-8974]
- Add new Safari settings configuration for iOS/iPadOS/macOS 26 devices [REL-8969]
- Add action to define the default app on a iOS/iPadOS 26 device [REL-8975]
- Add new battery health status to the device details available with iOS/iPadOS/macOS 26 [REL-9316]
- Report distribution of Relution client apps on enrolled devices to the Relution license server [REL-7839]
- Add preview, progress and detailed results to user CSV import. This results in breaking changes in the API, please check the hub for migration details [REL-7547] [REL-7546]
- Support 'Return to Service' for tvOS [REL-5551]
- Add global course management [REL-9603]
- Dynamically adjust edu profile during lessons in other tenant [REL-8792]
- Add WiFi roaming setting to Android Enterprise device connectivity configuration [REL-8725]
- Add new system apps of iOS / iPadOS 26 [REL-9592]
- Allow to cancel actions of Android Enterprise devices if they are not yet delivered and confirmed. This includes e.g. reboot actions or the wipe triggered upon device deletion. [REL-9460]
- Add support for Newline EDLA interactive whiteboards [REL-9334]
- Add Relution news to notification center [REL-9168]

Für Version 26.4.0

Updates

- Renew Apple push certificates, valid until August 2026. The previous ones will expire in February 2026 [REL-9277]
- Optimize handling of wallpaper rendering to avoid blocking web server requests [REL-8840]
- Set auto update mode to high priority for OEMConfig apps [REL-9524]
- When deleting Android Enterprise corporate devices with personal profile (COPE), only the work profile is removed, preserving personal data [REL-9172]
- Use wipe action to remove Android Enterprise devices instead of AMAPI delete [REL-9077]
- Add prometheus metric for health indicators [REL-7999]
- Update dependencies [REL-9309]
- Prevent the uninstallation of the Knox service plugin to ensure that the Play Store continues to install, update or uninstall apps [REL-9053]
- Ignore outdated KSP premium license key information during calculation of compliance violations [REL-9054]
- Remove image data from set wallpaper action to avoid DB bloat when using static lesson wallpapers [REL-9224]
- Add new proxy configuration fields to the strong swan profile configuration [REL-9301]
- Update several dependencies to address possible vulnerabilities [REL-9311]
- Adjust certificate handling on Windows devices [REL-8892]
- Keep pending update status until Apple devices report a new update status [REL-8953]
- Remove unnecessary extra certificate payload used during enrollment of Apple devices [REL-9236]
- Reduce log volume for no longer available Apple app IDs with many associations [REL-7261]
- Optimize throughput and responsiveness of Secure Mail Gateway [REL-8842]
- Add HTTP/2.0 support to Secure Mail Gateway for additional performance and reduced latency [REL-9182] [REL-8842]
- Improve UI of managed app configuration editor [REL-9050]
- Add total file size to managed media configuration view [REL-9375]
- Update CSV export and import labels [REL-6902]
- Add CSV export functionality to auto enrollment profile list [REL-9578]

Fixes

- Fix organization context in mail service event handling [REL-7818]
- Fix possible issue for certificate renewal when a specific order of configurations is present and the device responds with “not now” [REL-9597]
- Avoid excessive logging when authentication fails during during SchulConnex sync [REL-9560]
- Fix small issue in Windows certificate renewal [REL-9593]
- Avoid issues when loading very old push jobs for non-enrolled devices [REL-9528]
- Support users performing a password reset even when an invitation for them is still pending [REL-9420]
- Fix handling of possible exception during DEP sync [REL-9561]
- Resolve issue preventing some VPP publications not being imported into Relution [REL-9558]
- Fix deletion of DEP profiles during deletion of DEP accounts [REL-9564]
- Prevent value of device model of HKM devices from changing dynamically when it was provided by multiple sources [REL-9569]
- Fix small issues when parsing favicons for web links [REL-9464]
- Avoid excessive memory consumption if groups with a very large number of members are present [REL-9477]
- Improve detection of available app updates on the device [REL-9307]
- Fix an issue that prevents users to successfully link their device with Conditional Access [REL-9412]
- Update global scripts after they have been changed in Relution and are applied via script configuration on Windows devices [REL-9383]
- Fix name of App Store in system app list [REL-9391]
- Fix blocking of Android apps via Android Enterprise [REL-9239]
- Fix VPP sync failure occuring when a very large number of assignments has been removed [REL-8284]
- Fix trying to upload the same file twice [REL-9604]
- Add translation for device logging action [REL-9444]

Für Version 26.4.0

Version 5.33.1

2025-09-03

Updates

- Batch some VPP license association requests to reduce total number of requests [REL-9286]
- Update to latest Windows Store API [REL-9270]
- Move legacy `api/v1/store/` endpoints to `api/v1/global/` [REL-9305]

Fixes

- Fixed an issue that prevented users from linking their devices with Conditional Access [REL-9412]
- Do not show Windows Store apps which are not installable through Relution in store search result [REL-9396]
- Update global scripts after they have been changed in Relution and are applied via script configuration on Windows devices [REL-9383]
- Drop unused store endpoints [REL-9305]
- Fix permission error during user creation, when the current user has no permission to access the password policy settings of the organization [REL-9371]
- Split VPP license disassociation into smaller batches to avoid running into VPP API limits [REL-9037]

Version 5.33.0

2025-08-18

New

- Add known restrictions for iOS/iPadOS 26 and macOS 26 [REL-9005]
- Dynamically adjust education profiles during lessons in other tenant [REL-8792]
- Avoid Windows devices being immediately non-compliant after enrollment due to companion installation not being performed yet [REL-8888]
- Allow disabling individual policies in device details policy view for the device only [REL-7887]
- Allow to keep the system apps on the device for Android Enterprise enrollments [REL-8781]
- Improve the license view by adding unique name and enable sorting [REL-7867]
- Fix applying values on ViewSonic devices [REL-8923]
- Support configuring Bluetooth sharing for Android Enterprise devices [REL-8715]
- Display planned OS updates for Apple devices in device inventory [REL-7865]
- Display VPP information of all organizations in global organization [REL-8131]
- Display DEP information of all organizations in global organization [REL-7860]
- Added APN Configuration for Android Enterprise [REL-8661]
- For Windows devices display the DNSComputerName as the device name [REL-7863]
- Add Device Name configuration to Windows devices [REL-7863]
- Add option to deactivate the Jailbreak detection via iOS restrictions [REL-8789]
- Optimize handling and renewal of device certificates for Windows devices [REL-2724]
- Allow to duplicate device groups and their associated items [REL-7861]
- Add update modes to the iOS Exchange configuration, allowing it to update only when the policy is updated. This prevents updates when a configured placeholder value changes the configuration content [REL-8495]
- In dynamic device groups support filtering devices by device groups they are contained or not contained in [REL-7984]

Für Version 26.4.0

Updates

- Keep pending updates until apple devices report a new update status [REL-8953]
- Add support to define a wallpaper configuration on Android Enterprise devices [REL-9233]
- Secure Mail Gateway now fully utilizes Java NIO for better throughput and responsiveness [REL-8842]
- Secure Mail Gateway now optionally supports HTTP/2.0 for additional performance and reduced latency [REL-8842]
- Add notification for Relution News to the portal [REL-9168]
- Increase the maximum length for the un-/install parameters of Windows apps to 4000 [REL-5209]
- Fix LDAP group sync fails due to ambiguous foreignKey across multiple providers [REL-8861]
- Keep Android Enterprise Pub/Sub statistics in sync on all cluster nodes [REL-8421]
- Allow to trigger the MDM certificate renewal in the Windows device details for an expired MDM certificate [REL-8886]
- Follow redirects when retrieving icons for web links [REL-8833]
- Prevent unreachable Exchange servers from negatively impacting clients of other servers under high load [REL-8693]
- Update Geolocation DB for IPv4 address mapping [REL-8813]
- Add option to use Relution as PKI proxy for SCEP authorities [REL-6958]
- Ensure license models Public, NGO, and MAM display actual instead of Free license limitations [REL-9012]
- Add option to select the extension type in the Relution File Shares configuration [REL-8667]

Fixes

- Fix compliance violation behaviour for Windows devices between policy version changes [REL-8428]
- Fix blocking of Android apps via Android Enterprise [REL-9239]
- Fix handling of connection failures when receiving VPP notifications for new apps [REL-9173]
- Update of CORS header to enable Zero Touch in Android Enterprise settings [REL-9158]
- Fix lending system, so that duplicate active lendings are no longer possible [REL-8943]
- On enrollment of an Android legacy device Relution no longer sents an unsupported device name action [REL-7732]
- Fix Wi-Fi SSID as required for Android Enterprise connectivity configuration [REL-8857]
- Fix autopilot enrollments [REL-8885]
- Resolve action details permanently storing device credential data intended for single-usage only [REL-5529]
- Add sorting by name and description in category list [REL-9291]
- Update app detail screen on multi tenant switch [REL-9287]
- Fix minimum permissions needed to show the dashboard [REL-9255]
- Fix resetting of filters in lists [REL-9246]
- Fix navigation sometimes switching you back to previous tenant when navigating between views in different organizations [REL-9242]
- Add translation to all setup modes in macOS global ethernet settings configuration [REL-6605]
- Fix wrong last connection date for Android Enterprise devices [REL-7907]
- Update view for Windows “Add Accounts” action [REL-7622]
- Fix checking activation state of Android Enterprise at several places in web portal [REL-8856]
- Ensure that only the latest Relution File Shares configuration can be edited [REL-7412]
- Fix layout of MFA setup dialog [REL-8733]
- Fix opening links in new tabs when navigating in a tenant organisation at various places [REL-9216]
- Fix radio button alignment in MFA token modal [REL-2116]

Version 5.32.2

Für Version 26.4.0

2025-08-12

Fixes

- Fix database migration issue for MariaDB — Resolved a migration failure on some instances containing DEP host certificates, likely related to internal InnoDB index prefix length handling [REL-9002]
- Ensure license models ‘Public’, ‘NGO’, and ‘MAM’ display correct license limitations by default [REL-9012]

Version 5.32.1

2025-07-17

Fixes

- Fix Android Enterprise connection warning notifications in cluster setups [REL-8852]
- Fix handling of configuration templates in LDAP still defined via YML configuration file [REL-8919]
- Fix creation of new ASM SFTP sync settings in Portal [REL-8925]
- Fix autopilot enrollments [REL-8885]

Version 5.32.0

2025-07-03

New

- Support configuring Decon via lessons [REL-8334]
- Support configuring web content filter for weblinks in lessons [REL-7899]
- Add enable and disable BitLocker actions [REL-7946] [REL-6793]
- Support hiding the reset-password link globally or per organization. This is useful when user accounts are provided by an external system such as an OIDC or LDAP/AD server [REL-7864]
- Support for enabling relying party initiated logout in OpenID Connect [REL-7957]
- Support back-channel logout in OpenID Connect configurations [REL-7951]
- Extend ASM sync settings with the option to disable creating new users and to update managed Apple Accounts of users of other providers [REL-8351]
- Support up to 15 teachers in classes in ASM sync, which is the maximum Apple currently supports [REL-8410]
- Add placeholders for readable device model name and device category [REL-7869]
- Make app selection in managed app configuration for Apple devices more convenient by using app selector [REL-8127]
- Support placeholders in web link URLs [REL-7868]
- Support placeholders in add shortcut action [REL-8767]
- Add option to select the extension type in the Relution File Shares configuration [REL-8667]
- Add support for EDLA devices of the hardware manufacturer CVTE [REL-8669]
- Support relinquishing ownership of supported Android Enterprise devices via the enterprise wipe action [REL-8411]
- Extend information shown for SIM slots of compatiable Apple devices [REL-8426]
- Add user's device list to user and profile view [REL-7858]
- Add support for Dahua interactive whiteboards [REL-8670]

Für Version 26.4.0

Updates

- Optimize database model of device and sub action table [REL-7908]
- Avoid unnecessary multiple loading of app data in app details [REL-8014]
- Optimize query parameter handling in Portal [REL-8017]
- Add Prometheus metrics for scheduled jobs and Google Cloud Pub/Sub [REL-7055] [REL-7843]
- Add logging to scheduled tasks to simplify evaluating cluster instance activity [REL-8342]
- Display supported placeholders in wallpaper configurations [REL-8666]
- Streamline database column names [REL-8187]
- Using multiple URLs for LDAP no longer results in an invalid URL being used for the authentication test while no base-DN has been specified [REL-7454]
- Optimize device group preview query [REL-8429]
- Adjust pub/sub configuration properties [REL-8551]
- Optimize processing of Google Pub/Sub messages [REL-8542]
- Add a few previously missing configurable permissions to Portal dynamic permission role view [REL-7435]
- Optimize handling of Google pub/sub subscriptions [REL-8185]
- Display specific OEMConfig feedback channel entries also in the device details view [REL-7891]
- Optimize Android Enterprise communication [REL-8494]
- Add unique keys for a few tables previously allowing duplicate entries [REL-8188]
- Optimize Android Enterprise subscription polling in clustered installations [REL-8186]
- Adjust display of required fields in macOS Content Caching configuration [REL-8672]
- Allow time based policies to be deactivated at the next day [REL-8729]
- Alarm action in device groups now correctly shows that duration is only supported on Android [REL-8655]
- Adjust required field validation in Android Enterprise managed app configuration [REL-8570]
- Optimize license info view [REL-8376]
- Improve async context handling in SMG when configured servers are not available [REL-8693]

Fixes

Für Version 26.4.0

- Fix position of content menu in iOS AirPrint configuration [REL-8639]
- Fix handling of empty sections in macOS Content Caching configuration [REL-8776]
- Include query params in device group web hook actions [REL-8772]
- Fix issue with display of lost mode status for Apple devices in rare cases [REL-8757]
- Fix ‘Allow clients from the following address range only’ option in macOS Content Caching configuration [REL-8236]
- Fix auto-updating of public Google Play apps [REL-8625]
- Adjust display of app store search error messages [REL-8608]
- Fix on leave device group notification actions being sent to devices which were not part of the group before [REL-7635]
- Fix connection reuse improving reliability of firing webhooks [REL-7638]
- Filter out not yet known action types when companions query their next action [REL-8591]
- Fix Android Classic migration if Relution Agent is uploaded as a global app [REL-8466]
- Add compliance violation types for interactive whiteboard EShare and hotspot configurations [REL-3171]
- Optimize Decon license query [REL-7523]
- Prevent users from changing their profile when they are synced via external providers [REL-8377]
- Fix opening of links in a new tab via CMD+click shortcut [REL-8804]
- Fix validation in macOS Content Caching configuration [REL-8773]
- Fix persisting the column order under settings > languages [REL-8308]
- Prevent changing Android Enterprise managed app configuration if there is no active enterprise binding [REL-8595]
- Streamline audit log filter translation for user name [REL-8456]
- Fix UI issues when switching action types in device group action details [REL-8616]
- Improved message of webhook connectivity test [REL-7636]
- Abort loading of iFrame, when the user left the view [REL-8384]
- Fix validation issues in license allocation during new organisation creation wizard [REL-8388]
- Fix retrieval icons for web links [REL-8828]
- Fix opening device links in global list in new tabs [REL-8829]

Version 5.31.2

2025-06-12

Fixes

- Fix hindered auto-update of public PlayStore apps [REL-8625]
- Fix policy deployment for guest users on shared iPads [REL-8631]

Version 5.31.1

2025-06-06

Fixes

- Fix possible race condition with initial license handshake [REL-8614]
- Fix on leave device group notification actions being sent to devices which were not part of the group before [REL-7635]
- Adjust display of app store search error messages [REL-8608]
- Fix adding apps for different platforms with the same identifier [REL-8574]
- Adjust handling of education configuration for shared iPads to immediately show all classes on logout if configured [REL-8559]
- Fix next button in powershell script device group action [REL-8592]

Für Version 26.4.0

Version 5.31.0

2025-05-27

New

- Add VPP and DEP email notifications [REL-7982]
- Make student passcode policy for ASM SFTP upload configurable [REL-8412]
- Support synchronizing teacher and student groups as course members in LDAP sync [REL-7639]
- Support up to 15 teachers in classes in ASM sync, which is the maximum Apple currently supports [REL-8410]
- Add support for syncing users, groups and courses via Schulconnex → [REL-6995] [REL-7715]
- Support front-channel logout in OpenID connect configurations [REL-7994]
- Optimize storing of users [REL-126]
- Add option to show agreements during enrollment of an Android Enterprise device, which the user has to accept [REL-8287]
- Add support for i3-Technologies whiteboards [REL-4052]
- Add automatic client updates for the vendors SMART, Clevertouch and i3-Technologies [REL-8285]
- Optimize processing of installed apps [REL-6969]
- Add post installations scripts for native Windows apps [REL-6787] [REL-8241]
- Automatically migrate to Relution App family for iOS/iPadOS devices instead of the no longer maintained legacy Relution client, which will be removed from Apple App Store soon [REL-6837]
- Show all log in events also in audit log [REL-7594]
- Support linking to the corresponding view when tapping notifications delivered to Relution Agent [REL-6897]
- Allow configuring which field from ASM will be used as Relution user name in ASM sync [REL-6903]
- Allow to define maximum OS version in OS update configuration for Apple devices [REL-7648]
- Add application restrictions to Parental Controls configuration for macOS [REL-6836]
- Optimize performance when creating sub actions [REL-6976]
- Optimize selection and storage of preferred user language in profile, user details, CSV imports and syncs [REL-7229]
- Automatically configure account-driven user enrollment default for DEP accounts for devices with iOS/iPadOS 18.2, macOS 15.2, or greater [REL-6523]
- Add basic macOS parental controls configuration [REL-7228]
- Allow searching managed Google Play in the Android Enterprise settings [REL-7625]
- Prevent saving legacy wallpaper configurations which still have images larger than the configured allowed maximum [REL-6880]
- Separate device location from standard device details [REL-6952]
- Automatically generate signing certificate if not configured explicitly [REL-7004]

Für Version 26.4.0

Updates

- Remove unused “Interface” setting from iOS WiFi configuration [REL-8490]
- Show automated enrollments via Autopilot in audit log [REL-8238]
- Extend clean up of duplicate open actions [REL-6822]
- Execute Windows Deploy app actions with sub actions [REL-5364]
- Optimize Android Enterprise communication [REL-8494] [REL-7462]
- Optimize Android Enterprise subscription polling in clustered installations [REL-8186]
- Extend lesson template with Decon options [REL-7902]
- Improve reliability of access to Relution Google Play, WinGet, Google Places and SMS services [REL-8037]
- Avoid redundant error log for push messages [REL-8150]
- Show package name in open app action details [REL-7895]
- Make device logs include `DEBUG` level logs by default [REL-8142]
- Allow extensible matches and nested structures in LDAP filters [REL-7234]
- Fix criteria for showing hint that Entra ID has been configured in global organization in settings [REL-8160]
- Do not send query action after device reboot for Apple devices [REL-7945]
- Adjust handling of already deleted scripts in script history [REL-2466]
- Add single app mode configuration for tvOS [REL-7702]
- Use default template and language handling for reset password notification mails [REL-7881]
- Replace all HTML email templates with an updated, much more appealing, template [REL-6951]
- Decrease default push queue delays and reduce number of multiple pushes to the same device in a very short amount of time [REL-444]
- Use user preferred language to send notifications via email or push [REL-7230]
- Make dynamic device group filter “security patch level does not contain…” accept Android Enterprise devices only [REL-7809]
- Optimize database model of action table [REL-2640]
- Update iOS SCEP configuration with additional configuration options [REL-7452]
- Optimize page handling during LDAP synchronization [REL-7446]
- Ensure buttons in modals are shown without scrolling in Portal [REL-7122]
- Optimize display of OpenID Connect URLs in settings [REL-8390]
- Show address in device location [REL-8328]
- Allow clearing of fields in the managed app configuration of a managed app in a Android Enterprise policy [REL-7782]
- Remove option to select a custom client for organizations which do not use this feature already [REL-8034]
- Avoid showing notification messages in Portal when location of a device is not available [REL-7890]
- Update icons of several macOS configurations [REL-7626]
- Fix validation of certificate templates in Portal if expiration in days is less than automatic renewal [REL-7724]
- Configure agreements for Apple enrolments [REL-7706]
- Restore teacher device provisioning and always make sure Relution Teacher is available if the device has an app allow list [REL-8374]

Für Version 26.4.0

Fixes

- Allow toggling optional parts of macOS energy saver configuration [REL-7548]
- Fix automated disassociation of VPP licenses on app removal for global apps [REL-8460]
- Fix error message when trying to request an app that already exists as a global app [REL-8489]
- Fix possible issue when handling “Not Now” responses for remove profile requests [REL-8446]
- Fix issues with some international number formats when sending enrollment SMS [REL-8383]
- Prevent users from changing their profile when they are synced via external providers [REL-8377]
- Fix possible values for deadline updates in Windows Update Configuration [REL-8262]
- Optimize Decon license query [REL-7523]
- Fix handling possible performance issue when handling device authorization [REL-8307]
- Fix issue when moving an Apple device enrolled via a multi enrollment [REL-7936]
- Fix location handling for Android Enterprise companion [REL-7840]
- Optimize display and validation of device availability check settings [REL-7516]
- Fix selection of device groups in enrollments [REL-7623]
- Fix S3 health indicator when using AWS S3 [REL-7415]
- Fix issue preventing the windows app store search from functioning properly when receiving empty results [REL-7605]
- Fix installing WinGet apps manually via Portal [REL-8447]
- Fix language of manual link in user CSV import modal [REL-8452]
- Fix caching issue of the web portal during a Relution Update by performing a reload of the browser [REL-8365]
- Allow selecting public scripts in local script configurations [REL-8309]
- Fix handling of invalid filter query URLs in Portal [REL-8161]
- Adjust validation of Android Enterprise internal name for managed apps [REL-8204]
- Fix floating of auto complete selection dialogs in device group filter selection [REL-7741]
- Fix deselecting items in single selection lists via the radio button in Portal [REL-7549]
- Fix refresh of policy version selection in Portal [REL-7987]
- Fix issue that the count of the affected devices in the device group preview and the shown devices in the preview can diverge [REL-7896]
- Hide managed app store option if Andoid Enterprise setup is not completed [REL-7692]
- Show full details of compliance violations as tooltip [REL-6553]
- Fix ICCID column behaviour in new device details view [REL-7837]

Für Version 26.4.0

Version 5.30.1

2025-04-24

Updates

- Make SSO user matching case-insensitivealso on PostgreSQL [REL-8162]
- Add additional iOS and macOS restrictions [REL-8052]
- Prevent possible memory issues when dealing with large email attachments in SMG [REL-5647]

Fixes

- Fix send file action for Android Enterprise [REL-8182]
- Fix handling of re-enrolled Apple devices concerning re-enabling of lost mode [REL-8176]
- Allow selecting externally synced courses in Shared iPad configuration [REL-8174]
- Adjust validation of web clip URLs [REL-7798]
- Adjust validation of Android Enterprise internal name for managed apps [REL-8204]

Version 5.30.0

2025-03-26

New

- Add macOS login window configuration [REL-6765]
- Display compliance violation if device user does not grant permissions to locate geofences or iBeacons [REL-6912]
- Automatically migrate to Relution App family for iOS/iPadOS devices instead of the no longer maintained legacy Relution client, which will be removed from Apple App Store soon [REL-6837]
- Allow setting passwords for ASM-synced users [REL-6029]
- Add support for customizing the user mapping in ASM import [REL-6702]
- Determine available OS updates for Apple devices via the Apple software catalog [REL-6992]
- Extend device details delivered by Android Enterprise Companion [REL-6878]
- Extend Apple education configuration to use user profile images [REL-6810]
- Allow configuring if installed required apps should be removed when they are removed from the app compliance for Apple devices [REL-7000]
- Show associated courses on Shared iPad login screen [REL-6872]
- Add setting to enable displaying active geofences and iBeacons in Relution Agent [REL-6913]
- Add detection rules to `.pkg` files to detect if a pkg was installed correctly or not [REL-6900]
- Add support for `.pkg` apps in app compliance configuration if detection rules are configured [REL-6901]
- Add unlock action for i3 technology interactive boards [REL-7399]
- Allow configuring if the associated user in Relution should be cleared on logout on shared iPad [REL-6800]
- Add macOS login items configuration [REL-6764]
- Add macOS kernel extensions configuration [REL-6869]
- Add macOS system extensions configuration [REL-6760]
- Add macOS Time Machine configuration [REL-6796]
- Add macOS Firewall configuration [REL-6761]
- Allow setting multiple profile images via archive upload in user list [REL-6809]
- Optimize processing of device certificates for Apple devices [REL-6954]
- Add filter for shared iPad property in dynamic device group [REL-6820]
- Move device location to its own entity with its own permissions [REL-6887]
- Improve location push notification handling and show them in the device action list [REL-7305]
- Add third option for “Allow Location” setting in Windows Restriction configuration [REL-7284]
- Add battery level filter for dynamic device groups (Note: the value is updated on regular device details refresh, no live updates are performed) [REL-6818]
- Support custom CSP execution via policy configuration [REL-6982]
- Add macOS dock configuration [REL-6774]
- Remove hidden property from actions [REL-6002]
- Show channel information for actions in action list of a device [REL-2965]
- Add additional settings to Android Enterprise enrollments [REL-6775]
- Display choice fields as dropdown in the managed app configuration for Android Enterprise [REL-7320]
- Update device header box automatically on device changes [REL-6947]
- Add separate permission for re-applying policies [REL-6881]
- Add basic macOS parental controls configuration [REL-7228]
- Show creation and modification information for organizations [REL-7340]

Updates

Für Version 26.4.0

- Migrate Portal to Angular 19.1 [REL-6778] [REL-6794]
- Configure message retention and retry policy of Android Enterprise subscriptions [REL-7844]
- Avoid excessive read timeout when retrieving icons for public apps [REL-7451]
- Add heartbeat endpoint and health indicator [REL-7705]
- Allow configuring temporary overrides for MDM URL for DEP macOS devices via API [REL-7315]
- Renew Apple push certificates, valid until February 2026. The previous ones will expire in August 2025 [REL-7449]
- Improve logging in exchange proxy [REL-6338]
- Configure scheduled OTA updates for Clevertouch [REL-7721]
- Configure agreements for Apple enrolments [REL-7706]
- Add more filter options to the Decon configuration [REL-7437]
- Show Advantouch, Prowise and ViewSonic interactive Board integrations without server adjustments [REL-7555]
- Use UUID v7 for new entities [REL-7718]
- Add option to specify user control of settings in Android Enterprise App policy. This can be set to disallow to disable force quitting an app or clearing its data [REL-7542]
- Adjust handling of user registrations on live.relution.io [REL-7383]
- Improve origin information shown in login history [REL-6924]
- Switch to Java 21 in Relution Docker containers [REL-7464]
- Add configurable Sentry integration [REL-7381]
- Show only latest ‘Refresh device info via Companion’ action [REL-7411]
- Prevent required Android Enterprise Companion being blocked via managed apps configuration [REL-7130]
- Add additional skippable setup items for Apple devices [REL-7366]
- Periodically refresh known Apple device model names via https://repo.relution.io [REL-7268]
- Add support for additional signature algorithms for built-in certificate authorities [REL-7367]
- Ensure S3 Health Indicator is available when S3 ist not configured [REL-7345]
- Allow customizing host header in Exchange Proxy [REL-5276]
- Extend list of available device placeholders and add placeholder support to the iOS google account configuration [REL-6331]
- Remove modified by and created by from fields considered by full text search in user list view [REL-7276]
- Allow leading `#` in the Android Classic Kiosk configuration internal name input [REL-7853]
- Allow adding package names directly to installed apps device group dynamic filter [REL-6819]
- Add hint to user access tokens in Portal [REL-7344]

Für Version 26.4.0

Fixes

- Fix applying of edu configuration if the same teacher user is removed and then added again to the same device [REL-7835]
- Fix possibly missing update of tenant switch after creating new orgas when running Relution as a cluster [REL-7733]
- Add a toggle to bypass internal name mismatches when a new DMG app version gets uploaded [REL-7750]
- Fix S3 health indicator when using AWS S3 [REL-7415]
- Fix race condition when saving compliance violations [REL-7707]
- Fixed an internal server error when adding an unreleased app to the managed app configuration of an Android Enterprise policy. [REL-7694]
- Fix DEP enrollment without user authentication which now also requires a login since 5.29.2 [REL-7631]
- Adjust validation for install priority values in Android Enterprise configuration [REL-6998]
- When importing users from CSV with creation of classes enabled, the import of classes stopped on first encounter of a class without students or teachers. The fix applied merely records the issue to the log, continuing creation of further classes. [REL-7524]
- Adjust behaviour of several filter types in dynamic device groups with platform specific filter criteria like security patch level [REL-7376]
- Fix policy not being imediately removed from all devices when being deleted [REL-7365]
- Adjust error handling when public app store service is not available [REL-5832]
- Fix ICCID column behaviour in new device details view [REL-7837]
- Fix wording in macOS dock configuration [REL-7781]
- Adjust error hint for unique name of organizations [REL-7731]
- Fix an issue where refreshing the app details page lead to an “App does not exist” error when multiple tenants are available. [REL-7796]
- Fix supervision filter in device inventory [REL-7783]
- Add missing translations for action channel filter in action list [REL-7739]
- Show “manage app assignments” in installed app list only for Android Enterprise devices [REL-7693]
- Improve description of macOS firewall confiuration [REL-7674]
- Fix displaying the Relution login page on iOS 15 devices during DEP enrollment and Relution Shared Device [REL-7614]
- Fix validators in Android Enterprise managed app configuration [REL-7633]
- Fix bug reporter popping up in manual macOS user enrollment creation [REL-7630]
- Tweak display of device details after design update [REL-7540]
- Fix on leave device group notification actions being sent to devices which were not part of the group before [REL-7635]

Für Version 26.4.0

Version 5.29.5

2025-03-13

New

- Add heartbeat endpoint and health indicator [REL-7705]

Fixes

- Fix displaying the Relution login page on iOS 15 devices during DEP enrollment and Relution Shared Device [REL-7614]
- Fix DEP enrollment without user authentication which now also requires a login since 5.29.2 [REL-7631]

Version 5.29.3

2025-02-28

Fixes

- Fix Android Enterprise communication for older Relution versions [REL-7607]

Version 5.29.2

2025-02-19

New

- Add support for additional signature algorithms for built-in certificate authorities [REL-7367]
- Allow configuring temporary overrides for MDM URL for DEP macOS devices via API [REL-7315]

Fixes

- Fix web authentication method for SSO in clients [REL-7455]
- Fix linking of parent app to child devices [REL-7461]

Version 5.29.1

2025-01-28

Für Version 26.4.0

Fixes

- Fix lesson templates overview page not loading correctly [REL-7364]

Version 5.29.0

2025-01-24

New

- Add support for making apps globally available in global organization, so all organizations can use them. Existing apps can be migrated manually [REL-5742]
- Make apps added by global VPP tokens global automatically and adjust check if an app is VPP licensed to consider both global and local apps and licenses [REL-5776]
- Prevent having the same app both global and local in organizations. *Custom native client apps must not be made global* [REL-5533]
- Improve executing actions for Windows devices, including refreshing device details after the execution of other device action [REL-5063]
- Update device details view with an optimized design and structure [REL-2947]
- Support auto advance setup in DEP profiles [REL-6783]
- Add macOS accessibility configuration [REL-6797]
- Add macOS Finder configuration [REL-6772]
- Automatically refresh the current users authorization after creating or changing users, groups, permission roles or organizations [REL-6061]
- Optimize handling of completed Windows app deploy actions [REL-6083]
- Extend options for key usage and length in certificate templates [REL-6661]
- Optimize preview for installation and uninstallation parameters for `.exe` Windows apps, and support using environment variables in them [REL-6000]
- Handle refused SSE connections more gracefully [REL-6317]
- Add Samsung KSP widget [REL-6355]
- Add support for additional platform SSO configuration settings introduced with macOS Sequoia [REL-5249]
- Show information about apps being hidden or locked in installed app list of iOS/iPadOS devices [REL-5374]
- Allow managing app assignments created on install or uninstall actions via a dedicated list in Android Enterprise device details [REL-5193]
- Show security patch level for Android Enterprise devices [REL-6301]
- Update unique name validation for organizations to make them URL compatible [REL-6747]
- Prepare notifying Decon server on device configuration changes [REL-7100]
- Add profile images for users which can be managed in the user details and profile [REL-6808]
- Update shared iPad assigned user when receiving updated user information during device details refresh [REL-6873]
- Extend restrictions with new Apple AI settings [REL-6453]

Für Version 26.4.0

Updates

- Skip security information request to devices on “Not Now” response from Apple devices [REL-7279]
- Use default language of the global organization as default language when creating new organizations [REL-7118]
- Add health indicator for external storage [REL-7072]
- Add health check for SCEP CA resource content availability and improve log messages on failure of signature validation [REL-6645]
- Adjust maximum length of user email to 320 characters [REL-6510]
- Temporarily use message action to announce location based assignment changes to devices via push [REL-5680]
- Add database constraints for students and teachers in classes [REL-6302]
- Raise minimum supported version for PostgreSQL to 14 [REL-6592]
- Add a randomized delay scaled by the current work load of outstanding notifications when sending action notifications via SSE to interactive whiteboards not supporting Firebase push messaging natively [REL-6329]
- Reduce likelihood of dead locks when cleaning up old device actions [REL-6526]
- Add organization UUID to links in app request email notifications [REL-6240]
- Improve performance of loading current user information, speeding up actions like login, switching tenants and reload of web portal [REL-6513]
- Deploy CA x509 when PKCS12 configured as identity certificate [REL-6376]
- Adjust default system group creation [REL-5396]
- Show teacher web app link also in tenant organizations, since teacher web now supports them [REL-6586]
- Restructure Decon configuration view [REL-7097]
- Add hint to macOS script actions to avoid `shutdown` commands [REL-6658]
- Adjust display of flags for adding required apps to allow list in app compliance for iOS [REL-6798]
- Add support of pasting a list of values into string array fields [REL-6949]
- Remove custom scrollbar behaviour [REL-6948]
- Add missing platforms in auto deployment list [REL-6970]
- Avoid including deleted policies in policy count of device group tabs [REL-6817]
- Show hint about profile based user enrollment on macOS 15 [REL-6640]
- Add support for multi-select in ownership filter in enrollment list [REL-5980]
- Adjust badges and defaults for Promethean configuration [REL-6375]
- Show certificate usage in certificate list in settings [REL-5987]
- Optimize wallpaper rendering [REL-6636]
- Add minimal support for `REQUIRED_FOR_SETUP` for Android Enterprise companion [REL-6585]
- Disable no longer needed migrations running on startup to speed up the process [REL-6512]
- Improve logging in exchange proxy [REL-6338]
- Adjust license exceeded messages [REL-6666]

Für Version 26.4.0

Fixes

- Fix possible issue in Apple device policy updates which could lead to delays between sub actions of the policy update in some cases [REL-7082]
- Fix reset of lesson schedule settings when disabling global settings override [REL-7278]
- Avoid triggering multiple install actions for macOS companion [REL-7237]
- Avoid double insert of installed managed media leading to error log entries [REL-6265]
- Adapt history entries for Android Enterprise lost mode [REL-6707]
- Fix issuing certificates for VPN when the user certificate option is selected. AnyConnect VPNs may have to be saved and republished since they did not support user certificates before.[REL-7002]
- Adjust uniqueness check for organization unique names on PostgreSQL [REL-6719]
- Fix applying multiple Wi-Fi configurations that refer to the same CA certificate can now be applied on a single Android Enterprise device [REL-6706]
- Ensure user enrolled devices get associated with the correct platform when an AppleID was used for authentication. [REL-6654]
- Fix detection and usage of ImageMagick tool [REL-6635]
- Do not remove Relution Files if Files configuration is removed but the app is part of the required apps [REL-3148]
- Less frequent on-device education configuration updates when syncing LDAPs [REL-5665]
- Fix issue leading to some macOS user enrollments not being deleted when requested [REL-4960]
- Do not show deleted policies in device inventory policy quick filter options [REL-6609]
- Avoid macOS devices from being non-compliant temporarily due to missing macOS companion [REL-4919]
- Avoid triggering change device name actions for interactive boards not supporting it [REL-6427]
- Add windows store image URLs and unsafe-hashes to content security policy [REL-6529]
- Fix missing public app icons when operating cross tenant organization [REL-6529]
- Fix caching issue with lesson entities [REL-6459]
- Ensure active lending is reset when device is being returned, even if the lending state is unexpected [REL-6295]
- Fix race condition for Android Enterprise policy updates when publishing multiple policy versions in a short period of time [REL-6046]
- Fix infite re-renderings of bar charts [REL-4778]
- Fix enabled state of save button after uploading a `.ps` file in Windows scripts [REL-7174]
- Make device group name required when adding a new device group in add policy to device dialog [REL-7108]
- Fix password reset message shown in audit log [REL-6675]
- Fix Portal for device groups whose top level only contains filter groups [REL-6631]
- Fix version filter in policy details “devices with this policy” view [REL-6789]
- Fix preview behaviour when switching from static to dynamic device group [REL-6671]
- No longer show misleading “Device logs deleted” message when deletion is cancelled [REL-6751]
- Avoid cut animations for radio buttons in Portal [REL-5632]
- Ensure DMG install actions cannot be triggered if macOS companion is disabled [REL-6482]
- Optimize polling in action list view in device details [REL-5826]
- Fix button layout in app version view on small screen sizes [REL-4132]
- Disable editing in superseded versions of preferred activity configuration which cannot be saved/changed [REL-5271]
- Allow “Update MDM Profile” action also for non-supervised devices in Portal [REL-6580]
- Prevent adding invalid package names in Android Enterprise manage apps configuration [REL-4762]
- Do not send unsupported Wi-Fi configuration options to Android Enterprise devices with older Android version [REL-7171]

Für Version 26.4.0

Version 5.28.3

2024-12-23

Updates

- Skip retry of change wallpaper actions already in delivered state for iOS devices, to work around issues with devices applying them [REL-6989]
- Optimize wallpaper processing and error handling, especially when using external storage [REL-6989]
- Optimize and re-enable DECON license metricss [REL-6874]

Fixes

- Fix single sign on login in Relution Agent 5.17.0 and above with Relution 5.26.0 and above [REL-7085]

Version 5.28.2

2024-12-10

Updates

- Add setup actions for Android Enterprise to open Companion during enrollment [REL-6585]

Fixes

- Multiple Wi-Fi configurations that refer to the same CA certificate can now be applied on a single Android Enterprise device [REL-6706]
- Disable metrics for DECON [REL-6874]

Für Version 26.4.0

Version 5.28.1

2024-12-06

Updates

- Adjust enrollment of fully managed Android Enterprise devices due to breaking changes in Android Management API in January 2025 [REL-6607]

Fixes

- Ensure user enrolled devices get associated with the correct platform when an AppleID was used for authentication [REL-6654]
- Improve cleanup changeset performance for large instances when migrating the database [REL-6736]

Version 5.28.0

2024-11-25

New

- Fix automated deployment of renewed certificates based on templates if the configuration does not use placeholders [REL-6385]
- Add Relution Decon as optional add-on Feature [REL-5844]
- Allow configuring to require password for removing profiles on macOS [REL-5464]
- Add support for Online Certificate Status Protocol (OCSP) for certificates issued by “built-in” certificate authorities [REL-5296]
- Add Certificate Revocation List (CRL) for certificates issued by “built-in” certificate authorities [REL-4238]
- Support revoking certificates issued by “built-in” certificate authorities [REL-5297]
- Add macOS disk management configuration [REL-5256]
- Add Windows Companion policy configuration [REL-6003]
- Add support for Android Enterprise managed app feedback channel [REL-6055]
- Allow configuring per-app hideability and lockability in iOS app compliance [REL-5376]
- Show information about apps being hidden or locked in installed app list of iOS/iPadOS devices [REL-5374]
- Support updating from Windows 10 to Windows 11 via Windows update configuration [REL-6023]
- Report client migration state to license server [REL-5502]
- Add server support for lesson favorites in Relution Teacher [REL-5274]
- Add Samsung KNOX service plugin configuration for Android Enterprise [REL-6054]
- Add support for AWS customer managed key (CMK) via AWS key management service (KMS) when using S3 compatible external resource storage [REL-5449]
- Show default notification text in notification settings [REL-5817]
- Extend CSV upload for auto enrollments to change both the DEP profile and the organisation to enroll to (global organisation only) [REL-6098]
- Allow importing permissions, group memberships and classes (if user is a teacher or student) in CSV import of user data [REL-6067]
- Add new columns with permissions, group memberships and classes to user list (if the user is a teacher or student) [REL-6097]
- Add support for new Android Classic enrollment types for interactive boards to Relution Device Catalog [REL-5108]
- Support PKCS12 certificates in Windows WiFi configuration [REL-4365]
- Add support for managing Safari extensions on iOS/iPadOS and macOS [REL-5255]
- Add energy saver configuration for macOS [REL-5542]
- Support adding apps to Android Enterprise home screen layout via providing their package name only [REL-3643]
- Enhance app details view for app users with extra permissions by showing additional tabs [REL-5896]

Für Version 26.4.0

Updates

- Add workaround for iOS/iPadOS not showing AirDrop UI by automatically adding the OS-internal identifier for it to the allowed apps if AirDrop is allowed in restrictions and an allow list is configured [REL-6222]
- Improve performance of loading current user information, speeding up actions like login, switching tenants and reload of web portal [REL-6513]
- Reduce log level for Android Enterprise status reports [REL-6493]
- Extend restrictions with new Apple AI settings [REL-6453]
- Add workaround for iOS/iPadOS showing the same web link multiple times until device or spring board is restarted [REL-5797]
- Drop `DISABLE_RESOURCE_HASH` feature flag [REL-6406]
- Add support for devices providing multiple Bitlocker recovery keys [REL-3993]
- Adjust periodic push for devices with open actions to rotate the devices it pushes to [REL-3907]
- Show type of native apps for macOS (`.dmg` or `.pkg`) at additional places [REL-6236]
- Adjust handling of script file updates [REL-6277]
- Make withdraw of Android Classic devices on missing device administrator compliance violation configurable [REL-4241]
- Remove deprecated `/enumerables/pairs` endpoints [REL-5331]
- Add missing unique constraints to a few database tables [REL-4420]
- Adjust default external app store refresh interval and batch size [REL-6245]
- Add support for sending files to Android Enterprise devices [REL-6099]
- Optimise creation of audit log entries [REL-5851]
- Add explicit option to allow login on iOS/iPadOS devices if an allowlist is configured [REL-5873]
- Support mapping of IPv4-Mapped IPv6 addresses → [REL-6087]
- Adjust handling of user logouts [REL-1706]
- Automatically refresh map with device location display in portal [REL-6246]
- Add Samsung KSP widget [REL-6355]

Fixes

Für Version 26.4.0

- Fix server translation encodings [REL-6596]
- Add windows store image URLs and unsafe-hashes to content security policy [REL-6529]
- Fix missing public app icons when operating cross tenant organization [REL-6529]
- Fixed an error which leads to the audit log sometimes not being correctly loaded and shown in the portal [REL-6545]
- Ensure Windows apps installed from microsoft store do not get stuck in action state “delivered” if the device fails to confirm the action [REL-6509]
- Fix race condition for Android Enterprise policy updates when publishing multiple policy versions in a short period of time [REL-6046]
- Fix push messages for Wende 11 devices [REL-6447]
- Fix triggering `.dmg` app installation via Relution Agent on macOS [REL-6517]
- Adjust handling of legacy certificate configurations for Windows [REL-6479]
- Fix Android Enterprise lost mode status update if lost mode has been exited by a user [REL-6303]
- Delete related compliance violations when disabling macOS companion [REL-6504]
- Fix history entries for shared device logout [REL-6292]
- Fix profile removal on device deletion for Apple devices which have been re-enrolled [REL-6452]
- Ensure active lending is reset when device is being returned, even if the lending state is unexpected [REL-6295]
- Fix download of supervision certificates [REL-6413]
- Avoid multiple entries with the same country change in device history [REL-3778]
- Avoid double insert of installed managed media leading to error log entries [REL-6265]
- Prevent duplicate history entries for compliance state, adjust formatting [REL-5837]
- Avoid rare cases of error logs occuring during Android Enterprise policy changes triggered via device groups [REL-2015]
- Remove duplicate index for VPP assignments [REL-3902]
- Fix iOS/iPadOS certificate compliance status [REL-4190]
- Resolve an issue with setting sub actions to the correct state if duplicate compliance violations are encountered [REL-5664]
- Fix sorting device inventory by phone number [REL-6454]
- Fix display of processor architecture in windows device details [REL-6576]
- Fix missing translation in device group filter selection [REL-6536]
- Fix translations in script history filter selection [REL-6473]
- Fix license association during organization creation when no admin is created [REL-6511]
- Fix download of native app versions in review or development in web portal [REL-6468]
- Adjust translations in device group actions to avoid ambiguity for reset password actions [REL-6508]
- Adjust apps shown when editing Android Enterprise Homescreen layout in portal [REL-6481]
- Fix search when selecting devices to be added to a static device group [REL-6503]
- Prevent selecting public static device groups to add devices to in non-global organizations in Portal [REL-6471]
- Fix audit log messages for creating or deleting MFA tokens [REL-6474]
- Hide the location tab in the details of a device, if the is a whiteboard [REL-2702]
- Fix accessing auto enrollment profile details when having read permission only [REL-6332]
- Add missing columns to device list in device groups [REL-6319]
- Fix clicking the empty signature column of a lending triggers a bug report [REL-5523]
- Fix several columns in device inventory CSV export showing “undefined” instead of being empty [REL-4584]
- Enable shutdown of Heinekingmedia boards via Reboot action [REL-6296]
- Update label and tooltip of textfield in Android Enterprise Play Store Management Configuration [REL-6306]
- Add missing translation in app list filtering for the app type Weblink [REL-6311]
- Add missing translations for the security types in the Android Enterprise Wifi configuration [REL-6210]
- Fix pressing enter in the Relution Decon Configuration redirects the browser to the list of configurations [REL-6117]
- Prevent multiple concurrent save actions triggered via edit device group view in portal [REL-6088]
- Allow publishing imported policy versions without having to change them first [REL-4587]
- Improve display of next sync in Entra ID settings [REL-2534]

Für Version 26.4.0

Version 5.27.4

2024-11-19

Updates

- Add workaround for iOS/iPadOS not showing AirDrop UI by automatically adding the OS-internal identifier for it to the allowed apps if AirDrop is allowed in restrictions and an allow list is configured [REL-6222]
- Improve performance of loading current user information, speeding up actions like login, switching tenants and reload of web portal [REL-6513]

Fixes

- Ensure Windows apps installed from microsoft store do not get stuck in action state “delivered” if the device fails to confirm the action [REL-6509]

Version 5.27.3

2024-11-06

Fixes

- Fix automated deployment of renewed certificates based on templates if the configuration does not use placeholders [REL-6385]
- Fix Android Enterprise lost mode status update if lost mode has been exited by a user [REL-6303]

Für Version 26.4.0

Version 5.27.2

2024-10-23

Fixes

- Fix incompatible filter for no longer supported legacy clients [REL-6262]
- Fix issue when uploading new versions of script files when using separate resource storage [REL-6271]
- Fix double domain in user name when using SMG on Windows devices and the `DOMAIN\user` format [REL-6268]
- Fix deserialization of error code and message of Apple MDM errors [REL-6264]
- Fix configuration of default region for external S3 storage [REL-6248]
- Prevent possible deadlock when updating managed application list [REL-6266]

Version 5.27.1

2024-10-14

Updates

- Remove cleanup changeset which can take a long time to run on large instances when migrating the database [BR-14753]

Fixes

- Add missing translations in notification setting titles [REL-6154]

Version 5.27.0

2024-10-08

New

- Deploy macOS companion on enrolled macOS devices to support additional features like script execution and native app installation with `.dmg` files [REL-5835]
- Add Relution Decon configuration and iOS client app support [REL-4797] [REL-6048]
- Add support for Lost Mode for Android Enterprise devices [REL-2144] [REL-3260]
- Add “Enable Remote Desktop” and “Disable Remote Desktop” actions for macOS devices [REL-5547] [REL-5548]
- Show Windows WiFi and ethernet mac addresses in device inventory [REL-5460]
- Show web links configured in lessons on the home screen of students’ Android Enterprise devices [REL-5340]
- Add Google Places information setup to organization creation [REL-5323]
- Allow sending text messages to students in a running lesson [REL-5801]
- Add send file to Android Enterprise devices and several whiteboards [REL-5302]
- Add clear app data action for Android Enterprise devices [REL-4690]
- Add remaining specific enrollment types for white boards [REL-5075] [REL-5526] [REL-4013]
- Add convenience policy association for devices via directly choosing or creating a corresponding static device group [REL-5341]
- Add convenience device association for policies via directly choosing or creating a corresponding static device group [REL-5282]
- Make creating administrator optional when creating new organisations, allow configuring the members of the new organization’s admin group during creation [REL-5372] [REL-5373]
- Support generating the root certificate for built-in certificate authorities [REL-4237]
- Add preview and confirmation when changing dynamic device groups [REL-5286]
- Add navigation to device details from global device list, respective permissions in the device’s organization are required [REL-5202]
- Add support for bootstrap tokens on macOS [REL-5451] [REL-5601]
- Extend available settings Promethean configuration [REL-5294]
- Provide server side events endpoint for companion apps as an alternative action retrieval mechanism when no push service is available [REL-5317]
- Support message action on Android Enterprise and macOS devices [REL-4106]
- Filter device list in device group details when navigating from device or policy [REL-5290]
- Disallow marking System or Relution apps for removal on Android Enterprise [REL-5314]
- Add support for uploading large resources like apps in chunks including resuming, avoiding timeout issues and no longer requiring large body sizes to be configured. During the upload process, resource files such as apps are stored in the database, non-temporary resources are moved to external storage on save. By default files up to 1 GB of size can be uploaded, this can be configured via `relution.storage.max-file-size` [REL-5319]
- Support new iOS restrictions [REL-5386] [REL-6051]
- Support new macOS restrictions [REL-5385] [REL-6051]

Für Version 26.4.0

Updates

- Renew Apple push certificates, valid until August 2025. The previous ones will expire in February 2025 [REL-5614]
- Move supported platforms from version to app [REL-5689]
- Allow triggering MDM profile updates manually [REL-5601]
- Show in audit-log that a log in attempt has been blocked due to IP-based login restriction settings [REL-5266]
- Add Apple Passwords app to known system apps [REL-5888]
- Adjust display of deploy Windows companion actions “failing” due to companion being already installed in the expected version [REL-5708]
- Support placeholders in Apple WebClip configuration [REL-5965]
- Show telephony information in Android Enterprise device details [REL-4607]
- Add ICCID to Android Enterprise device details of devices with Android 13+ [REL-5780]
- Adjust default push queue delays [REL-5886]
- Clean up no longer used app installation counts [REL-5845]
- Use `READ_COMMITTED` transaction isolation level on all supported databases now. On PostgreSQL this was in use by default already. On MariaDB this change effectively disables so called gap-locking that could cause dead-lock issues when the server was under higher loads [REL-5828]
- Extend details and filter options for installed apps of Android Enterprise devices [REL-5509]
- Add option to disable proximity setup when erasing iOS devices [REL-5792]
- Add indices to speed up access to push device information [REL-5779]
- Improve display and handling of expired VPP tokens [REL-4835]
- Unify device deletion workflow in Portal for all Platforms as far as possible [REL-4785]
- Extend Windows Bitlocker configuration [REL-5226]
- Reset expired identity certificate exception when reusing devices on re-enrollment since a new certificate is already issued during the process [REL-4779]
- Show Android Security Patch Level for Android Enterprise devices in inventory [REL-5235]
- Prevent creating enrollments in “Global” organization [REL-5573]
- Adjust Android Management API connection management [REL-5564]
- Optimize startup communication with Windows Companion App, reduce Companion installation actions and fix their result status display when already being installed in the expected version [REL-3573]
- Avoid causing `Duplicate entry` log entries during startup by using database server time [REL-1764]
- Optimize Apple device action handling by directly continuing with the next action in all cases instead of requiring an extra push message [REL-4802]
- Decrease default push queue delays and reduce number of multi-push to the same device [REL-444]
- Allow enabling cellular enrollment in Android Enterprise enrollments [REL-5537]
- Add macOS script action to device group actions [REL-5448]
- Improve logging of errors encountered in LDAP connections [REL-5535]
- Extend known non-compliance reason descriptions for Android Enterprise devices [REL-5532]
- Add extra permission to read the user login history [REL-5237]
- Adjust display names of Apple policies [REL-5424]
- Make handling of bulk (dis-)association of VPP assignments more efficient [REL-1862]
- Adjust Azure AD settings API [REL-4610]
- Extend shown columns when selecting devices to be members of static device group [REL-6073]
- Show hint about profile based user enrollment on iOS 18 [REL-6018]
- Fix filtering in class selection of dynamic device group filter configuration [REL-5871]
- Support navigating back to previous page when encountering a not found error page in Portal [REL-5292]
- Extend filters in enrollment list [REL-2862]
- Move language settings in Portal and make description more accurate [REL-5799]
- Add missing per-item dots menu for managed media list [REL-3718]
- Add Promethean badges for AP9H [REL-5581]
- Do not verify the CA certificate when creating certificates based on intermediates in built-in PKI due to it inherently not being publicly trusted [REL-5520]
- Display the serial number in the device selector when applying scripts on devices [REL-5582]
- Remove all badges from Portal which are below or equal the minimum supported versions [REL-4664]

Für Version 26.4.0

Fixes

- Fix display of available OS versions in device inventory tooltip [REL-5703]
- Fix updating lesson templates with multi tenancy [REL-6009]
- Fix issues in lesson history [REL-6011]
- Resolve an issue with setting sub actions to the correct state if duplicate compliance violations are encountered [REL-5664]
- Avoid issues with re-enrolled macOS devices trying to reuse no longer valid device tokens [REL-5964]
- Improve display of policy changes and re-applies in device history [REL-5847]
- Adjust display of login attempts of deactivated users in login history [REL-5814]
- Resolve issue with updating installed apps of devices which report the same app multiple times [REL-5662]
- Improve dashboard performance by only listing the first 50 organisations [REL-5677]
- Fix issues when trying to delete a public policy [REL-5623]
- Fix database query for lent devices which has an issue since 5.26.0 [REL-5761]
- Fix audit log handling of error cases [REL-5527]
- Adjust device key rotation confirmation to avoid sporadic communication issues of Android Enterprise Companion app when delivery of devices policies gets delayed by communication infrastructure [REL-5620]
- Set latest device details update value for AE devices so dynamic filters can be applied [REL-5096]
- Fix rare case of remove Relution Files action staying in push sent state indefinitely until manually cancelled or deleted by cleanup [REL-5637]
- Extend audit log entries when changing IP based login rules [REL-5267]
- Fix allowed formats of bundle identifiers in package detection rules [REL-5280]
- Ignore and skip invalid DEP tokens during sync [REL-332]
- Fix deleting VPP tokens if they contain managed media deployed on devices [REL-5098]
- Adjust datatype used for various binary data fields on MariaDB to allow storing larger values [REL-5485]
- Avoid multiple identical location change entries in device history [REL-5510]
- Fix display error page of non-accessible resources in Portal [REL-5996]
- Fix filtering VPP users by VPP account [REL-5981]
- Fix issue in Portal when switching organization while being on the filtered user list [REL-4899]
- Disable link for deleted users in audit log [REL-5634]
- Fix creation of web links in Portal requiring to enter the URL twice [REL-5863]
- Fix CSV upload in device inventory when using semicolon as separator [REL-5808]
- Fix display of managed media selection wizard if no VPP tokens are configured and other layout issues [REL-5091]
- Fix selection of enabled service user override settings in iOS Exchange configuration [REL-5773]
- Fix layout of managed media configuration [REL-5681]

Für Version 26.4.0

Version 5.26.4

2024-09-13

Fixes

- Resolve issue with updating installed apps of devices which report the same app multiple times [REL-5662]
- Fix display of selected scheduled days of week in scheduled policies [REL-5798]
- Fix selection of separator of CSV upload in device inventory [REL-5808]
- Resolve a possible issue during database migration if lesson or lesson templates contain unexpected data [REL-5848]

Version 5.26.3

2024-09-02

Fixes

- Fix database query for lent devices which has an issue since 5.26.0 [REL-5761]

Version 5.26.2

2024-08-30

Updates

- Decrease default push queue delays and reduce number of multi-push to the same device [REL-444]

Fixes

- Fix sporadic connection issues of Relution apps on Android Enterprise devices when delivery of devices policies gets delayed by communication infrastructure [REL-5620]
- Improve dashboard performance by only listing the first 50 organisations [REL-5677]

Für Version 26.4.0

Version 5.26.1

2024-08-15

Fixes

- Resolve an issue with erroneously reusing downloaded files for previous versions of client apps if several versions have been released in a short period of time [REL-5627]
- Fix licensing of Relution Shield feature [REL-5462]

Version 5.26.0

2024-08-05

New

- Add Support for installing apps via Windows Package Manager (WinGet) → [REL-5233]
- Add `POST` query endpoints at several additional places allowing to include the query params in body instead of query [REL-1401]
- Start adding specific enrollment types for white boards to allow managing multiple types of boards and other Android Classic devices on the same server and even in the same organisation. More board types will be added with the following releases [REL-5075] [REL-4019]
- Support synchronising users and groups with Apple School Manager, including preview and synchronisation history [REL-4382] [REL-4990] [REL-4384] [REL-4343]
- Add Audit Log for every organization [REL-5030]
- Install Relution macOS companion app on device-enrolled macOS devices to support managing `.dmg` apps and running scripts [REL-5004]
- Add support for generic SCEP certificate authorities to be used to create certificates via certificate templates [REL-5196]
- Allow associating mail domains to organisations for single sign on in global organisation [REL-2798]
- Clean up resources on external storage earlier and more regularly [REL-4453]
- Allow configuring screen brightness and timeout for Android Enterprise devices via the new display configuration [REL-5064]
- Add new view-based endpoint to retrieve policies much faster and with smaller response size [REL-3879]
- Add lending criteria to dynamic device group filters [REL-4373]
- Support delivering admin contact information to Relution license server [REL-4634]
- Add install priority for Android Enterprise apps [REL-4183]
- Add support for white-/blacklist Wifi SSIDs for Android Enterprise [REL-4577]
- Optimize dashboard content for organisations which do not yet have devices, apps, policies, etc. [REL-4871]
- Detach lesson web link handling from app store web links, to make management for teachers and app managers more consistent [REL-5093]
- Use email from when sending password requests which can be configured via UI. Show a notification if it is missing [REL-4177]
- Show security posture in Android Enterprise device details [REL-4688]

Updates

Für Version 26.4.0

- Show telephony information in Android Enterprise device details [REL-4607]
- Support iPad home screen layouts with 5 x 6 items [REL-5010]
- Optimize display of SSO errors in Relution Portal [REL-4912]
- Support searching for UUIDs via full text search bar in Portal at several places [REL-4834]
- Optimize file resource handling at several places [REL-4606] [REL-2905] [REL-5035]
- Update white board configurations which use OpenSDK with ‘Wake on Lan’, ‘Wake on Active Source’, ‘Rename sources’ and ‘No Signal Power Off’ [REL-5016]
- Adjust handling of sensitive information for a number of policy configurations in API and portal [REL-3884]
- Create new organizations always with enabled device groups, regardless of global organization settings. To keep the current behaviour, the feature flag `DEVICE_GROUPS_USE_GLOBAL_SETTING_FOR_NEW_ORGAS` can be enabled. Starting december 2024, newly released versions will only support device groups [REL-5191]
- Also mark ‘N’ versions of supported Windows editions as supported [REL-5418]
- Add settings and endpoints for Relution Shield [REL-4996]
- Ensure provider names to be unique across all available provider types [REL-1712]
- Optimize persistence of lesson and lesson template entities [REL-5225]
- Resource migration now migrates resources in batches and retries the operation when it fails [REL-1763]
- Configure default notification settings on macOS devices [REL-4906]
- Improve memory footprint and performance when adding large native apps [REL-4366]
- Optimize cache library usage [REL-2443]
- Show app icons at additional places like installed apps of a device in Relution Portal [REL-4211]
- Improve handling in console command service [REL-4609]
- Make the Android Enterprise settings page more compact by hiding optional information by default [REL-4900]
- Handle invalid media types sent by Windows when uploading fonts [REL-5020]
- Streamline enrollment link logic for Android Enterprise [REL-5021]
- Optimize descriptive message of change policy actions by making it more specific [REL-4187]
- Extend support for single sign on login via Relution client apps [REL-4840]
- Reduce excessive size of policy API response, especially for policies with a large number of versions [REL-3882]
- Improve performance when requesting students via Relution Teacher [REL-4879]
- Adjust levels of several log messages to reduce the amount of noise in the logs [REL-3844]
- Show progress during analyzing uploaded native apps in Portal [REL-5028]
- Make configuration of relative date filters in dynamic device groups more intuitive, and improve discoverability of their features [REL-5094]
- Use the correct badge for Android Enterprise MAC address randomization setting [REL-5044]

Für Version 26.4.0

Fixes

- Fix deleting users by clearing audit log references on deletion [REL-5419]
- Extend error details shown for several failures in Apple MDM payload generation [REL-1174]
- Fix display of provider names for OIDC configurations which are misconfigured [REL-2503]
- Fix serialization behaviour of some enrollment events [REL-5127]
- Avoid sending expiration notifications for APNS push certificate of the legacy Relution client [REL-4888]
- Fix context information missing from logs [REL-5002]
- Avoid possible deadlocks when adding a device to a large number of static groups with a single operation [REL-4388]
- Adjust cleaning up of finished push jobs [REL-4175]
- Adjust payload properties of generated configurations for macOS [REL-4862]
- Fix responsive behaviour of device group header box [REL-5261]
- Make device group column and filter labels more consistent [REL-5194]
- Improve error handling and display in app uploader [REL-4519]
- Adjust translation in the device group action deletion dialog [REL-5275]
- Fix saving strongSwan Profile configurations that contain a user certificate template [REL-5032]
- Limit filter values in device inventory and trash to values actually occurring in the set of devices shown in the respective list [REL-4572]
- Fix Android Classic passcode configuration, when selecting complex as type [REL-3509]
- Ignore selected permissions when hitting cancel in the permission selection modal in user and group details [REL-5023]
- Show correct last modified date in compliance violation view [REL-4565]
- Disable “add new version” button for public apps since they are retrieved from external app stores [REL-4194]
- Fix possible issue during enrollment of Degen ADVANTouch interactive boards keeping them in ’enrollment pending’ state [REL-5518]

Version 5.25.3

2024-07-26

Für Version 26.4.0

Updates

- Prepare additional permissions for Relution Shield [REL-4996]

Version 5.25.2

2024-07-18

Updates

- Also match against location name when updating VPP tokens, since Apple seems to have changed the token contents without announcing it [REL-5227]
- Clear device certificates on re-enrollment to force creating a new one [REL-5223]
- Make proxy PAC URL optional for automatic proxy type in iOS/iPadOS/tvOS WiFi and Global HTTP Proxy configurations [REL-5216]
- Support issuing device certificates for Android Enterprise strongSwan profiles with default profiles [REL-5125]

Fixes

- The server no longer sends an expiration notification for the old unused APNS app store certificate [REL-4888]
- Ensure apps blocked by parents can still be used in lessons [REL-5163]
- Fix confirmation after requesting an app via Relution Portal [REL-4731]
- Fix selection of VPN in iOS app-to-VPN association always showing an empty list [REL-4849]
- Fix license feature name checked at Relution Shield settings in Portal [REL-4996]

Version 5.25.1

2024-07-01

New

- Include IP address of the caller in audit log [REL-5040]

Fixes

- Fix an issue with existing lessons no longer being updatable after introducing lesson single app mode [REL-5070]
- Fix wallpaper configurations with very long text [REL-4998]
- Fix context information missing from logs [REL-5002]
- Deliver Relution Teacher for native installations [REL-4987]
- Fix Android Enterprise Kiosk configuration with `stayOnPluggedModes` for managed devices with personal usage allowed [REL-5005]
- Fix application of Android Enterprise StrongSwan VPN profiles with VPN type “IKEv2 EAP-TLS” [REL-5018]
- Fix enabled state of save button of Android Enterprise StrongSwan VPN profile configurations that contain a user certificate template [REL-5032]

Für Version 26.4.0

Version 5.25.0

2024-06-18

New

- Add audit log showing API activity in settings of global organisation [REL-4891]
- Add per-app VPN settings for Windows devices [REL-4669]
- Add per-domain VPN settings for Windows devices [REL-4618]
- Allow calling web hooks via device group actions [REL-3876]
- Allow specifying additional mail addresses to notify in device group actions [REL-4342]
- Add notification configuration for iOS/iPadOS and macOS devices [REL-3864]
- Automatically merge multiple Apple notification configurations and enable notifications for Relution apps by default [REL-4328]
- Add FileVault configuration for macOS devices [REL-4114]
- Add “delete device” to available device group actions [REL-4341]
- Add setup assistant configuration for Apple devices [REL-3871]
- Add single app mode for Relution teacher app [REL-4394] [REL-4397]
- Replace default OAuth2 error page with a custom Relution one, and improve error reporting [REL-4381]
- Drop Support for Microsoft SQL Server [REL-4324]
- Allow updating assigned user on auto enrollments via CSV upload [REL-4788]
- Support all certificate options (single select, user, and certificate templates) in Apple Exchange and Certificate configuration [REL-4409]
- Add device logging configurable via global orga to allow collecting logs for specific devices accessible via API [REL-4692]
- Add support for Relution Agent on macOS [REL-2744] [REL-3930] [REL-4562]

Updates

- Allow to select between delta and full sync when synchronizing Azure AD users & groups [REL-3567]
- Add InstallationFailureReason for Android Enterprise devices in compliance violation. [REL-4103]
- Handle possible issue during database migration on invalid resource references [REL-4909]
- Adjust handling of Android Enterprise messages which do not belong to the current server if enterprises are connected to multiple servers (this kind of setup is not recommended!) [REL-4811]
- Allow re-enrolled devices to still be attached to static device groups when re-used after deletion [REL-4528]
- Add additional skippable steps to DEP profiles [REL-4427]
- Adjust handling of referenced resources at several places [REL-2904]
- Optimize access to streamed resources [REL-3715]
- Remove “promote” feature for app versions [REL-4639]
- Add index to speed up apple push notification processing [REL-4735]
- Ignore certificates without CN or subject when checking for missing certificates on Apple devices [REL-4417]
- Adjust handling of translated messages in server [REL-4422]
- Drop support of WebEAM as security provider [REL-4216]
- Reduce memory usage when using Wallpaper configurations and ImageMagick is not enabled [REL-4563]
- Prevent deletion of CAs with certificate templates [REL-1914]
- Extend placeholder support of global HTTP proxy configuration to additional fields [REL-4499]
- Always add a history entry when devices are deleted or withdrawn [REL-3748]
- Skip sending the child device name of the app to the server [REL-4360]
- Add latest policy sync time and latest status report time to Android Enterprise device details [REL-4689]
- Avoid calling the same endpoint twice when manually adding public apps to Relution via web portal [REL-4334]
- Adjust lesson schedule settings view in Portal [REL-4197]
- Adjust filters in policy list view [REL-4200]
- Group macOS devices by major version in dash board view, since Apple changed the versioning scheme [REL-3937]

Fixes

Für Version 26.4.0

- Fix a rare issue with the merge of store and system organization if an organization with an empty UUID exists [REL-4964]
- Fix SAML extra attribute parsing [REL-4901]
- Fix issue in Windows device action processing [REL-4837]
- Fix running with `--database-migration-only` to only create the Relution schema [REL-4807]
- Adjust error handling of query endpoints [REL-4617]
- Add version filter to the list of devices an app is installed on [REL-4455]
- Adjust behaviour concerning unsupported actions for specific Windows versions [REL-4641]
- Fix CIDR evaluation not producing the expected results for in-between network prefix sizes [REL-4501]
- Adjust validation handling in Portal for Windows Update configuration [REL-1413]
- Fix default values and enabled state of save button in alert action view [REL-4459]
- Adjust visibility conditions for auto enrollment profiles view [REL-4338]
- Adjust page range start indicator in tables in web portal [REL-4330]

Version 5.24.2

2024-06-10

Updates

- Adjust periodic push for Apple devices with specific open actions to be more frequent [REL-4796]
- Adjust visibility of interactive whiteboard configurations in Portal [REL-4859]

Fixes

- Fix running with `--database-migration-only` to only create the Relution schema [REL-4807]
- Fix auto enrollment profile filter selection showing an empty list when configuring dynamic device group filters [REL-4836]

Für Version 26.4.0

Version 5.24.1

2024-05-31

Updates

- Switch back to Java 17 in Relution Docker image temporarily to avoid higher CPU usage than expected with Java 21 [REL-4786]
- Switch to Firebase Cloud Messaging protocol HTTP V1 to replace legacy push API that Google discontinues on June 21, 2024 [REL-4392]
- Remove “promote” feature for app versions [REL-4795]

Fixes

- Fix creating compliance violations for required native macOS apps when not installed on the device [REL-4369]
- Fix native app download session handling in cluster environments [REL-4770]

Version 5.24.0

2024-05-13

New

- Add age mode for dynamic device group filters for date fields, allowing to configure e.g. “enrolled in the last seven days” as a condition [REL-3887]
- Extend device group filtering capabilities to allow to filter for devices which have no or any value set for a respective property [REL-3420]
- Add support to run device group actions in a schedule [REL-3872]
- Add dynamic device group filters for auto enrollment and auto enrollment profiles [REL-3959]
- Allow selecting auto-assigned static groups in (auto-)enrollments [REL-3886]
- Add device group action for reapplying device policies [REL-3877]
- Allow pasting multiple values into device group filters which are split automatically at spaces [REL-3504]
- Add option to choose User Principal Name (UPN) as Subject Alternative Name type (SAN) in certificate templates [REL-4403]
- Make Relution Teacher web available as part of Relution Portal [REL-2792] [REL-2793]
- Allow configuring custom validity periods for built-in CA templates [REL-3372]
- Optimize Windows VPN configuration [REL-4281]
- Support hotspot configuration on additional interactive whiteboards [REL-4272]
- Add Active Directory Configuration for macOS [REL-3878]
- Add Font configuration for Apple devices, including font management in settings [REL-3863]
- Add support for PKCS12 certificates in Windows certificate configuration [REL-3238]
- Add Windows Application Control configuration [REL-3975]
- Allow customising preferred activities for Android Enterprise devices [REL-2880]
- Reuse existing Android Enterprise device entity on enrollment of the same device, even when switching between fully managed enrollment types [REL-3546]
- Add support for Degen ADVANTouch interactive whiteboards [REL-3966]
- Clean up resources on external storage earlier and more regularly [REL-2914]
- Add additional security information like FileVault status to macOS device details [REL-3924]
- Update to Spring Boot 3 which requires Java 17+ (Please upgrade to Java 21) [REL-735]
- Switch to Java 21 in Relution Docker image [REL-4454]

Updates

Für Version 26.4.0

- Extend the filter support of the inventory table [REL-3893]
- Add enrollment type to device inventory view [REL-4228]
- Add support for WiFi mac and description in device inventory [REL-3873]
- Adjust widgets content shown in global orga dashboard widgets [REL-3875]
- Add support for parameterised higher resolution versions for system app icons [REL-3234]
- Allow to select between delta and full sync when synchronizing Azure AD users & groups manually [REL-3567]
- Remove remaining non-authority permissions previously used for system (now global) admins and replace them with additional authorities [REL-1803]
- Handle unexpected IP address header content when not using recommended proxy settings [REL-4378]
- Cache generated wallpapers in configured resource storage [REL-4002]
- Remove support for GridFS, Relution will not start if still configured [REL-4220]
- Add missing filters in device details action list [REL-4317]
- Add Device Connectivity Management configuration for Android Enterprise devices [REL-4046]
- Adjust parameters when accessing Microsoft Store [REL-4180]
- Always use a message action to send push notifications, so it can be viewed in the message view in Relution Agent [REL-3318]
- Always add a history entry when devices are deleted or withdrawn [REL-3748]
- Reduce memory footprint of Apple wallpaper command generation [REL-3932]
- Improve wording of device groups and/or options [REL-4379]
- Do not show legacy auto-assignment information in policy header in Portal after migrating to device groups [REL-4337]
- Make sure to not show empty sections in enrollments in Portal after migrating to device groups [REL-3847]
- Show IP address in Android Enterprise device details [REL-3874]
- Add creation and modification information to users and groups [REL-3869]

Fixes

Für Version 26.4.0

- Fix inventory filter values for global organization. [REL-4329]
- Do not include deleted certificates in dash board widget summary [REL-4352]
- Fix CIDR evaluation not producing the expected results for in-between network prefix sizes [REL-4501]
- Fix client dashboard widget referencing the legacy client apps instead of Relution Agent [REL-2495]
- Fix Samsung Classroom not being deployed for teacher devices [REL-4333]
- Ignore devices in “withdrawn” states for all dashboard widgets except “device status” [REL-2486]
- Add missing translations in Windows Update configuration [REL-4583]
- Fix device group action view in Portal sometimes allowing to save when not all required fields have been filled [REL-4544]
- Remove redundant information in create organisation summary screen [REL-4525]
- Fix manufactorer filter in Portal [REL-4541]
- Fix visibility of settings page for users in some minimal settings permission scenarios [REL-4546]
- Fix bulk enrollment action not being shown with minimal required permissions [REL-4503]
- Fix possible translation issue in device group filter edit view [REL-4497]
- Fix minor visual issues in Managed Configuration editor for Android Enterprise [REL-2519]
- Hide locate device action for deleted devices [REL-4188]
- Avoid clearing device group action notification user if the action is saved without changes [REL-4239]
- Fix accessing the description of Android Enterprise app policy, when the app has no app policy [REL-3934]
- An Android Enterprise Wi-Fi configuration for SIM/AKA can be saved immediately when all required fields are filled [REL-3710]

Version 5.23.1

2024-04-18

Updates

- Add prometheus metric with Relution server version [REL-3908]

Fixes

- Ensure deploying Relution Agent on re-enrolled devices immediately, even before device details have been retrieved [REL-4371]
- Fix device group filter for installed apps showing a non-accurate list on editing in Portal [REL-4340]
- Adjust behaviour when logging in on enrolled devices without an associated user [REL-4327]
- Fix LDAP settings UI not showing saved synchronisation settings correctly [REL-4372]
- Correctly show already selected organizations when re-opening dynamic device group filter selection [REL-4240]
- Avoid clearing device group action notification user if the action is saved without changes [REL-4239]
- Fix notification settings view not being able to open global orga after migration when no store organisation was present before [REL-4276]

Version 5.23.0

2024-03-28

New

Für Version 26.4.0

- Replace system organization with new global organization and merge system and store on existing servers [REL-2985] [REL-3412] [REL-4149]
- Allow defining calendar day and month periods for time-based policies during which they are not applied. Allow subscribing or importing calenders to define these periods [REL-2637] [REL-2803] [REL-2819] [REL-2922] [REL-3155] [REL-3413] [REL-3443]
- Add support for uploading and distributing self-hosted Android apps via Android Enterprise [REL-4084]
- Reuse existing device-enrolled iOS/iPadOS, tvOS or macOS device entity on enrollment of the same device [REL-3415] [REL-3546]
- Allow moving Windows, Android Classic, iOS/iPadOS, tvOS or macOS devices to a different tenant in global organization [REL-1554]
- Add Windows Caching configuration allowing to configure usage of Windows built-in PCCR (Peer Content Caching and Retrieval) to speed up downloads on Windows clients [REL-3224] [REL-3228] [REL-3781]
- Add strongSwan VPN configuration for Android Enterprise devices [REL-3738]
- Add Android Enterprise message configuration [REL-2879]
- Add class membership filter for device groups [REL-2712]
- Add reset password action for Windows devices via Windows companion [REL-2797]
- Add server side support for Relution Parent app [REL-4162] [REL-2902]

Updates

- Renew Apple push certificates, valid until February 2025. The previous ones will expire in August 2024 [REL-3678]
- Show a notification if outgoing email settings are not configured [REL-4069]
- Improve the filter selection in the table view to avoid unnecessary reloads [REL-3888]
- Extend Android Enterprise settings with additional configurations [REL-2878]
- Optimize setup and display of Windows app installation and uninstallation commands, including showing a preview [REL-970]
- Optimize compilation and background processing for dynamic device group filters [REL-3776]
- Adjust periodic push for devices with open actions to rotate the devices it pushes to [REL-3907]
- Adjust email uniqueness check and detection of SSO providers to be case insensitive on all databases [REL-3889]
- Adjust display of organization selector [REL-4141]
- Add additional Windows versions used to display device detail information [REL-3764]
- Adjust private key bag display name for certificate / key pairs generated by Relution [REL-3552]
- Show device deletion date and deleted by in device inventory and device details [REL-3747]
- Add action to log out current user on Shared iPad [REL-3462]
- Adjust download session cache settings [REL-3522]
- Add a few additional iOS and tvOS restrictions [REL-3087]
- Add missing error code mapping to display human readable message on script deletion error in Portal [REL-3955]
- Show policy platform when adding policies to a device group [REL-3785]
- Disable “add new version” button for public apps since they are retrieved from external app stores [REL-4194]

Fixes

- Fix keystore expiration notifications recipient detection to avoid logging the mail content instead [REL-3465]
- Adjust Portal validation for Windows app uninstaller path [REL-4169]
- Avoid creating unnecessary multiple deploy actions for Android Classic Companion in some cases [REL-4159]
- Fix immediate dynamic device group filter evaluation if the same field is used in multiple filter expressions combined in a single logical statement [REL-3906]
- Skip change set creating new index which could cause issues on Microsoft SQL server since support for it will be dropped soon anyway [REL-3996]
- Avoid possibly causing deadlocks when cleaning short-lived actions of individual devices on MariaDB [REL-3675]
- Fix issues in system email settings: No longer require repeat password entry when testing previously saved settings, make SSL and STARTTLS mutually exclusive and require EHLO when STARTTLS is enabled [REL-3802]
- Fix public device groups not being evaluated correctly after restarting the server [REL-3774]
- Optimize group assignment evaluation cache behaviour [REL-495]
- Fix policy export dialog behaviour when password auto-fill is enabled [REL-4189]
- Fix icons being displayed cropped at the bottom in lists in Safari on macOS [REL-3620]
- Fix detection rule for Windows apps display in Portal being not up-to-date after editing them [REL-4168]
- Fix display of battery status if it is not known [REL-4142]
- Fix spacing in export policies dialog [REL-4143]
- Fix validation of empty passwords when changing passwords via the user profile [REL-3939]
- Do not allow saving dynamic device groups without any filters [REL-3799]
- Make sure Android Enterprise Wi-Fi configuration for SIM/AKA can be saved immediately when all required fields are filled [REL-3710]
- Fixed device to app assignment for apps supporting multiple platforms (i.e. macOS devices were not shown in the devices selection list) [REL-3526]
- Fix alignment in iOS purchased apps view [REL-3559]
- Fix sorting managed media by type or size [REL-2779]
- Adjust refresh behaviour of detection rule display in Portal [REL-3163]
- Fix selection behaviour in device policy list [REL-3384]

Für Version 26.4.0

Version 5.22.4

2024-03-15

Updates

- Add new iOS 17.4 restriction to (dis)allow marketplace app installations [REL-3909]
- Set new USB Data Access configuration, which is now required by latest Android Device Policy [REL-4004]

Fixes

- Avoid compliance violation concerning CrossProfilePolicies on managed Android Enterprise devices where this policy cannot be applied [REL-3933]
- Fix auto-enrollment list pagination and total count display in Portal [REL-4075]
- Fix missing add button in managed media configuration [REL-3981]

Version 5.22.3

2024-03-01

Updates

- Only apply managed media list query if the organization has managed media, and auto-skip it on devices responding with “not now” due to the issue iOS/iPadOS has with this query [REL-3704]

Für Version 26.4.0

Version 5.22.2

2024-02-28

Fixes

- Resolve a possible rare issue in MDM push queue leading to threads waiting indefinitely (introduced with 5.22.0) [REL-3846]

Version 5.22.1

2024-02-21

Updates

- Adjust logging configuration for Android push [REL-3777]
- Disable managed media query by default until the next release since it causes issues with some Apple devices responding with “not now” for a prolonged duration and without clear reason [REL-3780]

Fixes

- Fix public device groups not being evaluated correctly after restarting the server [REL-3772]
- Resolve issue with MDM push channels on shared iPad and macOS, and push organization context in some cases (introduced with 5.22.0) [REL-3765]
- Fix issue with device group filters not being configurable via Portal when using German translation [REL-3560]

Version 5.22.0

2024-02-14

New

- Extend device group filter to also evaluate group membership of the assigned device user. When saving device groups or performing a login on a shared device, this will be evaluated immediately, otherwise updates will be performed periodically in background [REL-2711] [REL-2849]
- Add device group actions allowing to schedule actions or notifications via device groups. They will fully replace the now deprecated rule sets in a future release, which are no longer shown in organizations not using them already. Please migrate your rule set configurations to device group actions [REL-859] [REL-2919] [REL-2612] [REL-3101]
- Allow notifying users and groups in device group actions via push or email [REL-2613]
- Add extensible SSO policy configuration for Apple devices [REL-2802] [REL-3667]
- Add support making PowerShell scripts public, so they can be used in all organisations of a Relution server [REL-2801]
- Add self-service portal which allows users to view their devices and trigger actions on them if enabled by assigning the necessary permissions [REL-2816]
- Add interactive board configuration for SMART boards [REL-1233]
- Allow configuring outgoing mail server configuration via system organization settings in web portal [REL-2822] [REL-3134] [REL-3177]
- Show if Apple are denied communication due to expired identity certificates and support selectively allowing them anyway to renew their profile. Also add corresponding columns to device inventory and details and add filters to device groups [REL-3282]
- Allow customising compliance enforcement rules for Android Enterprise devices [REL-2877]

Updates

Für Version 26.4.0

- Skip directly to login with username and password if only SSO providers in the store organisation are configured [REL-3054]
- Allow disabling SSO providers for login on Relution Shared Device [REL-3052]
- Reduce memory footprint and optimise scheduling of push messages, e.g. by avoiding queueing multiple open pushes per device [REL-3249]
- Simplify handling of push credentials for devices and Relution client apps [REL-2559]
- Mark all actions with “Not Now” state if devices respond with it, not only actions with multiple sub actions [REL-3658]
- Show Ping actions in device action list [REL-3662]
- Allow canceling actions in state “Not Now” via device action list [REL-3700]
- Allow disabling managed media list query for Apple devices via configuration property [REL-3694]
- Adjust cached user names also for enrollments and auto-enrollments when user names are updated [REL-3553]
- Clear IOT dummy data which might be present on servers created before 2018 [REL-3577]
- Avoid excessive logging when imagemagick is not available [REL-3524]
- Fix an issue with saving device management settings unintentionally setting device groups to OFF again [REL-3557]
- Add “Domain Suffix Match” to enterprise Wi-Fi configuration on Android Enterprise platform [REL-3547]
- Avoid unnecessarily saving actions to update their status when the status is already set [REL-3435]
- Allow running liquibase database migration only, without actually starting Relution, via the argument `--database-migration-only` (environment variable `RELUTION_ARGUMENTS` can be used) [REL-3333]
- Drop support for MySQL and remove scripts and references for no longer supported database types [REL-3332]
- Follow transitive group memberships when doing ASM SFTP sync [REL#227868] [REL-2591]
- Applying device group policies now takes the current tenant organization into account [REL-3220]
- Add “wrong server time” notification, log entry, and endpoint [REL-3039]
- Adjust auto enrollments list actions if device groups are enabled [REL#2210194] [REL-3566]
- Move weblink options to general section of the weblink configuration [REL#229824] [REL-3487]
- Allow configuring provider type for all iOS and macOS VPN types [REL-3034]
- Extend airprint configuration for iOS with port and forceTLS parameters [REL-3213]
- Handle invalid file types with a helpful error message when importing policies from files [REL-3157]
- Support Windows Wallpaper on Windows Pro devices [REL-2386]
- Avoid excessive logging when external services are not available during scheduled public app metadata update [REL-3286]
- Reduce response size of the query auto enrolment endpoint [REL-2988]
- Add ethernet MAC address of Apple TVs to inventory list and device details [REL-2891]
- Adjust limits for DEP accounts and abbreviate if the values delivered by Apple exceed the limits [REL-1091]
- Allow Android Enterprise devices to fetch their own actions [REL-3293]
- Avoid excessive logging when PubSub responds with 502 Bad Gateway [REL-3288]
- Improve handling of Windows Companion updates and versioning [REL-2961]
- Use the same icons for static and dynamic device groups at different places [REL-2050]
- Avoid having to call the analysis of the uploaded file twice when adding new native apps [REL-3550]
- Adjust display of connection check result for certificate authority configuration [REL-3181]
- Adjust error handling possibilities for Windows Office configuration [REL-3223] [REL-3221]

Fixes

Für Version 26.4.0

- Adjust logging when the shared device scheduled logout encounters a device which no longer is in shared mode [REL-3683]
- Clear user reference in auto enrollments when users are deleted [REL-3578]
- Fix cancel button for actions without a details step [REL-3665]
- Add missing lesson template permission in portal authority view [REL-3151]
- Fix clearing of assigned user on application of a Relution shared device configuration [REL-3086]
- Prevent the reset of a policy version, when the version is the only version which exists in the policy [REL-3363]
- Fix adding URLs to the list of allowed URLs in the Windows kiosk mode configuration [REL-3364]
- Avoid hiding the organization switcher when searching for organization names without a match [REL-3284]
- Improve appearance of Portal header boxes for devices with very long names or serial numbers [REL-2546]
- Avoid excessive logging when certificate authorities are not available to issue new certificates [REL-3672]
- Handle error during device details processing of Windows Home devices [REL-2753]
- Fix layout of DEP profile selection dialog [REL-3673]
- Fix creating file detection rules for Windows apps [REL-3668]
- Handle invalid file uploads in the upload VPP token wizard [REL-2488]
- Avoid having to reload the web page to trigger auto enrollment sync after adding a new DEP account [REL-3649]
- Fix issues with enabled state of the save button in iOS VPN configuration when switching VPN types [REL-3218]

Version 5.21.3

2024-02-28

Updates

Für Version 26.4.0

- Disable managed media query by default since it causes issues with some Apple devices responding with “not now” for a prolonged duration and without clear reason [REL-3780]
- Allow enabling managed media list query for Apple devices via configuration property [REL-3694]
- Show Ping actions in device action list [REL-3662]
- Allow canceling actions in state “Not Now” via device action list [REL-3700]

Version 5.21.2

2024-01-18

Fixes

- Fix handling of glowroot agent if configured
- Fix mapping of versions via store organisation [REL-3488]

Version 5.21.1

2024-01-09

Updates

- Add hint about the not yet available group filter to device group wizard as well [REL-3159]

Fixes

- Avoid unnecessary renewal of JWT token [REL-3366]
- Avoid adding apps of public VPP tokens to the system organisation as well on PostgreSQL databases [REL-3321]
- Fix scheduled renewal of Apple education certificates no longer working due to unique constraints introduced with 5.20.0 [REL-3289]
- Fix scheduled cleanup of old login history entries [REL-3285]
- Avoid hiding the organization switcher when searching for organization names without a match [REL-3284]

Version 5.21.0

2023-12-14

New

- Mark device groups no longer as beta. Add a hint about the not yet available user group filter [REL-3159]
- Create new organisations with enabled device groups if the feature is enabled in the store organisation, or if there is no store organisation [REL-2826]
- Create default dynamic device group which contains all active devices for new organizations [REL-1783]
- Extend setup guide with additional steps for device group setup [REL-1776]
- Use software enforce declaration on Apple devices supporting it instead of sending OS update actions [REL-2169]
- Require explicit mapping of store LDAP users to organisations to avoid unintentionally syncing them into the store orga. Also allow defining an orga mapping for the store organisation itself. This behaviour is enabled by default for new providers, and disabled for existing ones [REL-2556]
- Use external tool if installed for image rendering to improve performance and reduce memory footprint [REL-2572]
- Add Office configuration to Windows policies [REL-1852]
- Show FAQ and support in portal for every user if they are configured [REL-2814]
- Add login history to user profile and user detail view [REL-2796] [REL-3150]
- Support desktop login via browser in Portal for Windows client apps [REL-1686]
- Allow selecting multiple apps to be remove from multiple devices at once [REL-2489]
- Add support for IKEv2 AlwaysOn VPN configuration for iOS devices [REL-2308]
- Allow deploying Office 365 apps to Windows devices via explicit action [REL-1694]
- Add support for cross profile policies to Android Enterprise (restrictions) [REL-2865]
- Merge multiple Windows app compliance configurations when applied on devices [REL-2554]
- Add support for communicating with and configuring Relution Teacher on Windows devices [REL-429]
- Allow creating users with empty password intended for SSO login only [REL-1801]
- Add “wrong server time” notification, log entry, and endpoint [REL-3039]

Updates

Für Version 26.4.0

- Extend Android Enterprise restrictions with additional settings [REL-2810]
- Extend Android Enterprise kiosk configuration with additional settings [REL-2811]
- Support Windows scripts with more than 32k characters [REL-1858]
- Allow configuring sync interval for ChromeOS as part of the settings [REL-2557]
- Improve logging for DEP sync when encountering errors returned by the DEP API [REL-2830]
- Improve handling of action display when activation bypass code is not available [REL-2480]
- Fix cleanup of associated device references for deleted devices when deleting users [REL-3139]
- Use rate limiter for Android Enterprise API requests to avoid running in Google's limits [REL-3038]
- Cleanup non-terminal duplicate actions for several additional action types immediately as well [REL-3045]
- Add missing encryption types to tvOS WiFi configuration [REL-3036]
- Clean up device actions more often and earlier by default [REL-2832]
- Set the minimum supported MariaDB version of Relution to 10.5 [REL-2833]
- Add foreign key from enrollment to organization [REL-2356]
- Handle groups without names in Azure AD sync [REL-2725]
- Enable declarative management for devices with iOS/iPadOS/tvOS 17 or macOS 14 and retrieve status updates including app status [REL-2450]
- Migrate resources to another store type in batches and retry the operation on errors [REL-1763]
- Create database indices for all foreign key columsn to avoid deadlocks and improve performance [REL-2336]
- Extend text filter in device inventory to include given and surname of the assigned device user [REL-3046]
- Allow entering exchange host with path in iOS and macOS exchange configurations [REL-2709]
- Rename factory reset protection option for Android Enterprise to be more clear [REL-2558]
- Allow installing VPP apps directly from assigned licenses view [REL-2549]
- Write policy version number to "policy" and "executedPolicy" columns during device inventory CSV export [REL-2548]
- Windows Office configuration will remove installed Office Suites on removal [REL-2636]
- Update configuration of the axe linter to only check for WCAG 2.1 compliance [REL-2873]
- Update main dependencies of the portal [REL-2602]
- Simplify permission checks in device service to get rid of legacy roles [REL-2496]
- Reuse device name when performing "Return to service" action on devices [REL-3024]
- Make sure "Return to Service" continues trough setup assistant automatically, even when using a DEP profile with macOS user customization [REL-3024]
- Add Apple restriction `allowMailPrivacyProtection` [REL-2589]
- Optimize request classification for device and portal requests [REL-2193]
- Drop unused SSH key entity, DB schema and service methods [REL-2201]
- Use a service account for Google Workspace setup for ChromeOS management and streamline setup [REL-2537]
- Retrieve BitLocker details during Windows Companion device details refresh [REL-1609]
- Set Cookies SameSite flag explicitly [REL-1422]
- Adjust empty state of tables in Portal [REL-2599]
- Trim attribute names entered in LDAP UI [REL-3005]

Fixes

Für Version 26.4.0

- Fix missing delivered dates for sub actions on Apple devices [REL-3160]
- Fix clearing of assigned user on application of a Relution shared device configuration [REL-3086]
- Fix chrome management API incompatibility causing device management software to no longer being deployed on ChromeOS devices [REL-3057]
- Avoid repeated evaluation and logging of a few database migrations [REL-2440]
- Fix sorting of columns with specific mappings on PostgreSQL [REL-605]
- Invalidate the device key on device deletion on all cluster nodes immediately [REL-2497]
- Fix marking actions as failed for devices not having an MDM push token [REL-2115]
- Fix deferred initialisation of LDAP connections via `application.yml` when the organisation does not exist yet [REL-2273]
- Fix disabled state of public dynamic device group filter query category inputs in child organizations [REL-3186]
- Improve appearance of Portal header boxes for devices with very long names or serials [REL-2546]
- Fix device inventory not applying a previously configured filter when navigating back to it [REL-2570]
- Handle no longer existent VPP app details in the portal more gracefully, so that the user is able to still use the UI [REL#228258] [REL-2592]
- Fix handling of serial numbers with multiple trailing null terminators on PostgreSQL which some interactive boards are sending [REL-3096]
- Avoid sometimes once more adding devices to device groups which have been switched from dynamic to static [REL-3042]
- Fix repeated “Device deleted from x and inserted to 0 groups” message in logs [REL-2631]
- Fix deletion of specific Windows device from trash [REL-2872]
- Fix action queue on Windows devices getting stuck if a policy containing a PowerShell script configuration is deployed during enrollment [REL-2582]
- Avoid logging errors during post-sync actions of LDAP users with duplicated email addresses [REL-2391]
- Do not report seemingly missing Azure AD settings for system organisation [REL-2455]
- Fix text overflow in Windows enrollment page [REL-3189]
- Adjust permission checks for device groups in Portal to avoid running into a forbidden response from server [REL-3179]
- Make sure to always show an error toast message in Portal when applying an action fails [REL-2511]
- Fix broken link on user cell in device inventory for devices without an assigned user [REL-3047]
- Remove gray square in enrollment QR code modal [REL-2040]
- Fix search field selection when adding policies [REL-2818]
- Fix possible race condition when stopping lessons not having a weblink assigned [REL-3207]
- Fix possible race condition during enrollment of Apple devices leading to some actions being delayed [REL-3094] [REL-3204]

Für Version 26.4.0

Version 5.20.8

2023-11-21

Updates

- Clean up actions in terminal state only by default, since the cleanup now happens earlier than before [REL-3030]
- Use clean up with default expiration instead of short expiration for action types where only one pending, successful and failed action is kept anyway [REL-3030]

Version 5.20.7

2023-11-15

Updates

- Clean up device actions more often and earlier by default. By default, actions are removed after 90d, 30d for short-lived types. The clean up by default runs every 15 minutes between 18:00 and 7:00, and deletes up to two times 1000 actions [REL-2832] [REL-2895]
- Run the clean up of device actions described above also per device when ever an action is put into a terminal state [REL-2894]
- Keep only the latest pending, successful and failed action of several types per device to reduce size of action history [REL-2603]

Fixes

- Fix HTTP method for (not yet used) `POST` endpoint erroneously being marked as `GET` [REL-2843]

Version 5.20.6

2023-11-08

Updates

- Fix running database migration on MySQL databases caused by a behaviour difference in comparison to MariaDB. *Please note: Relution will drop official support for MySQL databases with version 5.22* [REL-2916]

Für Version 26.4.0

Fixes

- Fix expiration notification for the iOS client app push certificate always referencing the legacy client's certificate [REL-2874]
- Fix performance issues in APK parsing by adjusting the parser library [REL-2953]
- Fix rare cases of enrollment of iOS and Windows possibly failing with the message `Organization is not the one which user belongs to` [REL-2866]
- Fix updating devices via CSV on instances which are using a PostgreSQL database [REL#228644] [REL-2868]

Version 5.20.5

2023-10-31

Fixes

- Properly release LDAP connections to pool when done [REL#228488] [REL-2846]
- Fix deserialisation of selected system apps in lessons and lesson templates [REL#228622] [REL-2845]

Version 5.20.4

2023-10-27

Updates

- Handle groups without names in Azure AD sync [REL-2725]

Fixes

- Ensure users can still be deleted even if referenced in (auto-)enrollments or devices with the changes in 5.20.2 [REL-2809]

Version 5.20.3

2023-10-25

Updates

- Optimize performance and handling of DEP syncs, especially for tokens with a very large number of devices [REL-2778]

Version 5.20.2

2023-10-19

Für Version 26.4.0

Fixes

- Resolve performance issue for security provider filter list occurring on instances with a very large number of organizations [REL-2701] [REL-2726]
- Fix database migration for Android Enterprise device details for old deleted devices [REL-2649]
- Fix translations of Lost Mode status in filters and CSV exports [REL-2648]
- Add missing migrations for nullable device user group [REL-1820]

Version 5.20.1

2023-10-13

Updates

- Optimise wallpaper configuration and generation handling to reduce memory footprint [REL-2618]
- Clear the informative `userName` field of auto enrollments when the user is nulled, and allow enrolling to specific users of a target organisation for store auto enrollments [REL-2606]
- Avoid excessive creation of change policy actions on macOS devices when a specific, rare set of circumstances comes together [REL-2601]

Fixes

- Fix creation of education lessons in Relution Teacher app with no longer existing student users [REL-2588]

Version 5.20.0

2023-10-05

New

- Support deleting cached users from shared iPads [REL-2444]
- Add “Return to Service” action for iOS 17 devices [REL-2038] [REL-2514]
- Use `softwareupdate` information from declarative device management for devices supporting it [REL-2171]
- Allow permanently and irreversibly deleting devices from trash, fix cleanup of devices when deleting organisations [REL-2119]
- Enable enrollment without device user [REL-1818]
- Add dynamic filter for device groups for IP ranges (CIDR) [REL-1734]
- No longer create the “Device User” system group, migrate existing ones to standard groups [REL-1820]
- Optimize memory usage of LDAP connections [REL-1707]
- Adjust organizational unit mapping for ChromeOS devices [REL-1814]
- Allow nulling the assigned user instead of using the device user group for devices without an actual user [REL-1819]
- Add Android Enterprise work profile widget settings [REL-1622]
- Add WiFi MAC randomisation setting for Android Enterprise WiFi configuration [REL-1621]
- Support management of installed media (PDFs and ePubs) on supported Apple devices [REL-2137] [REL-1393]
- Added support to auto-update B2B custom apps on Apple devices [REL-1795]
- Streamline login process for different combinations of SSO configurations [REL-1646]
- Support user certificate and certificate templates in Android Enterprise certificate configuration [REL-1529]
- Add badges for iOS and tvOS 17 to restrictions [REL-2039]
- Add VS interactive whiteboard policy configuration [REL-1408]
- Add action to refresh the applied policies on multiple devices in the device inventory [REL-1733]
- Add `DISABLE_DEVICE_NAME_CHANGE` feature toggle to disable synchronising the device name on the device itself with the name in Relution for devices supporting it [REL-2426]
- Support installing Windows Companion on Windows `arm` platform devices [REL-1335]
- Support deleting cached users from shared iPads [REL-2444]

Updates

Für Version 26.4.0

- Renew Apple push certificates, valid until August 2024. The previous ones will expire in February 2024 [REL-2147]
- Do not wait for LDAP initialisation before marking the application as ready [REL-2429]
- Run cleanup operations nightly based on a cron schedule instead of in an interval after system start [REL-2395]
- Prevent deadlocks when saving users when running Relution in a cluster [REL#225904] [REL-2318]
- Removed all legacy code of CockroachDB support [REL-2325]
- Users can now also upload .json files to support setting up the start menu layout for windows 11 devices [REL-1758]
- Adjust order and handling of security filters [REL-2262]
- Changing the password renders all existing logons invalid, effecting immediate logout on all non-enrolled devices and browsers, so that the new credentials need to be entered [REL-1705]
- Handle large Windows apps meta data [REL-1109]
- Add numerical IP address field to make devices sortable and searchable via this property [REL-1823]
- Serve OpenApi web UI as a standalone webpage in the server [REL-254]
- Optimize performance when handling MDM requests of Apple devices [REL-2191]
- OS changes will now be shown in the device history for iOS, Android Enterprise and Windows devices [REL-2175]
- Add a history entry for a device that was deleted due to DEP re-enrollment [REL-2162]
- Add device history entry on ICCID change for iOS [REL-2146] [REL-2146]
- Set connection state of Android Enterprise devices based on the applied state reported by Google [REL-971]
- Exclude disabled Android Enterprise devices from license count [REL-973] [REL-2462]
- Switching from a map of strings to utilizing resource messages for translations [REL-2128]
- Add general user placeholder support for Android Enterprise WiFi configuration [REL-1651]
- Fix iOS system app icons, removed musicmemos system app [REL-1726]
- Move device unlock token to device security information [REL-1704]
- Added new macOS restrictions [REL-1703]
- Companion for Android Enterprise re-installs missing certificates periodically [REL-1530]
- Add option to request apps from Microsoft store [REL-2261]
- Add more keywords to the settings dashboard search to improve search for OIDC, ASM,SFTP and DEP [REL-2172]
- Re-add the list mode of the settings overview as a optional representation [REL-2225]
- Support inviting users in non-store organizations into public vpp tokens within their orga [REL-362]
- Allow configuring synthetic group for LDAP when periodic sync is off [REL-1509]
- Improve handling and display of Azure AD sync settings in store organisation [REL-2504]
- Adjust updating user passwords with administrative permissions [REL-2425]
- Adjust location where the Windows companion stores its files [REL-2194]
- Allow updating MDM profiles of Apple devices with outdated but still valid server urls [REL-2374]
- Improve performance of updating Windows Companion sub-actions [REL-2153]
- Adjust logging of user import service [REL-2246]
- Allow filtering users and groups by deleted providers [REL-2151]
- Change provider name for global Azure AD sync [REL-1009]
- Use system context when distributing apps from store organisation [REL-2042]
- Prevent assigning non-public permission roles to users or groups of other organisations [REL-1750]
- Add hint to iOS/iPadOS wallpaper configuration about changed behaviour on iPadOS 17 [REL-2491]

Fixes

For version 26.4.0

- Fix cause for “User could not be authenticated: Invalid credentials” if Secure Mail Gateway is active [REL-2447]
- Fix translations for device action types filter and support multi-select [REL-2382]
- Show Relution Agent in System certificates dashboard widget instead of legacy system certificate [REL-2453]
- Fix cloning native Windows app detection rules from store organization to child organizations [REL-1835]
- Update password log message [REL-2291]
- Automatic certificate renewal on Android Enterprise now works as expected [REL-2206]
- Fix enrollment clean up on device deletion [REL-2332]
- Fix editing of allocation limit per organization in license allocation table [REL#227617] [REL-2316]
- Fix excessive memory consumption when determining shared device status [REL-1445]
- Apply time based policies correctly on Android Enterprise devices [REL-2279]
- vpp tokens can’t be added multiple times to the same organization [REL-249]
- Fix Android Enterprise devices losing their last location whenever device info is updated, e.g. by a policy update [REL-1213]
- Prevent recreating synthetic groups with every LDAP sync in some cases [REL#225933] [REL-1843]
- Fix whitelisting of web clips and auto-deployed apps for merged App compliance configurations containing at least one blacklist [REL#226711] [REL#227506] [REL-1861]
- Do not display version and permission mappings tabs for incompatible ‘Web clip’ app type [REL#227716] [REL-2379]
- Fix detection of macOS 14 devices on the enrollment landing page [REL-2319]
- Fix value for device inventory Shared iPad column [REL-2333]
- Fix crash in Android Enterprise work profile passcode configuration, when the selected type is `Complex` [REL-2303]
- Fix crash in Android Enterprise device passcode configuration, when the selected type is `Complex` [REL-2303]
- Ensure that the login as organization administrator ignores deactivated administrators [REL#227377] [REL-2275]
- Fix overflow of texts in selection chips [REL-2117]
- Display iOS WiFi configuration EAP details for published policy versions [REL#227354] [REL-2197]
- Fix disabled state of the available apps for selected items of the iOS Homescreen Layout configuration iPhone layout [REL#227220] [REL-2159]
- Fix refresh data button in device lending list [REL-2012]
- Fix updating Windows native apps when also modifying detection rules [REL-2482]
- Adjust display of Android Enterprise connection status when no communication has been triggered yet [REL-2465]
- Adjust device group counts displayed in portal to exclude deleted devices [REL-2485]
- Automatically update display of MSI detection rules after editing them [REL-2481]
- Fix deferred initialisation of LDAP connections via `application.yml` when the organisation does not exist yet [REL-2273]
- Adjust handling of `DeviceStatusChangedEvent` to avoid misleading log messages [REL-2313]
- Fix migrating the store organisation to device groups when using SQL server [REL-2331]
- Fix handling of importing new VPP books to avoid misleading error log messages [REL-2242]
- Avoid unnecessary loading of user and group roles [REL-2035]
- Improve handling of very long orga names in organisation switcher [REL-1886]
- Ensure to commit the transaction clearing resource content in SQL database after migrating to external storage [REL-2555]

Für Version 26.4.0

Version 5.19.5

2023-09-05

Updates

- Optimized memory usage for the LDAP connector [REL-2032] [REL-2133]

Fixes

- Bound cluster communication to local port 7800 instead of a random port [REL-2317]

Version 5.19.4

2023-08-25

Updates

- Allow login for LDAP users with non-matching user DN [REL-2270]

Version 5.19.3

2023-08-21

New

- Set default location permissions of Agent on managed Android Enterprise devices based on COD location settings and allow to override default Agent settings with a manage apps configuration [REL-1829] [REL#225955] [REL#227344]

Fixes

- Resolve potential performance issue of database migration for 5.19.0 [REL-2202]
- Add missing permissions to Portal dynamic role configuration view and make settings visible for users having only LDAP settings permissions [REL-2195]
- Display iOS WiFi configuration EAP details for published policy versions [REL-2197] [REL#227354]

Für Version 26.4.0

Version 5.19.2

2023-08-14

Fixes

- Adjust imprint floating behaviour on login page [REL-2185]
- Adjust allowed checksums for liquibase changes for instances with PostgreSQL or SQL Server which had 5.19.0 installed before [REL-2154]
- Fix SQL Server failing to acquire device group lock due to `FOR UPDATE` clause allowed only for `DECLARE CURSOR` [REL-2165]

Version 5.19.1

2023-08-10

Fixes

- Fix failing of database migration to duplicate entries in `filter_holder_acl` table which should not exist on productive systems. Migration was updated so that this defect is dealt with appropriately [REL-2154]

Version 5.19.0

2023-08-07

New

- Support Android Enterprise devices in Secure Mail Gateway by identifying them as Android devices and add the placeholder `${device.exchangeDeviceId}` for managed configuration [REL-909]
- Allow blocking users automatically after a configurable set of consecutive failed login attempts [REL-693]
- Add support for IP blocking in system organization [REL-1199]
- Add script configuration for Windows [REL-1329]
- Add action to locate Windows devices [REL-1469]
- Add default permission roles in the system organization. The system groups created automatically for each organization now get these permission sets attached [REL-1480]
- Support setup of OIDC single sign on via Portal, also server wide via store organization [REL-840] [REL-841]
- Display deleted and withdrawn devices in a separate device view [REL-1198]
- Display all devices of the server in the device inventory of the store organization [REL-1375]
- Add dynamic links to navigate from the Dashboard to the data sources [REL-1613]
- Show information about the assigned user in device inventory list [REL-1591]
- Add support for VPN on demand rules to additional VPN types [REL-1421]

Für Version 26.4.0

Updates

- Throw explicit error when trying to access Relution using a login cookie without SSL when not originating from `localhost` and cookie secure flag setting now depends on how the client accesses the Relution server. Correct setup of reverse proxy forward headers is required [REL-1766]
- Remove message prefix in the action message column of the action table in a device [REL-1478]
- Add deep link to windows landing page and use access token for login page [REL-1565]
- Add option to use placeholders in script content [REL-525]
- Display warning when Azure group could not be synced because group with same name already exists [REL-1007]
- Keep only the latest pending, successful and failed education action of each device to limit excessive growth of device action history [REL-1371]
- Simplify VPP app association for single device to improve performance [REL-1611]
- Display the configured privacy policy of the server on the enrollment landing page during an Apple enrollment [REL-1644]
- Prevent triggering additional VPP syncs when encountering error 9646 (too many requests) [REL-1760]
- Simplify parsing in Relution SCEP servlet [REL-790]
- Display supplemental build version in iOS system details [REL-1349] [REL-1771] [REL-1860]
- Remove unknown ownership column from device management settings [REL-1477]
- Apply Angular Material Design Components (MDC) migration [REL-1496]
- Remove modes from location sharing from Android Enterprise policies that are no longer supported by Google [REL-1586]
- Use locally served GAPI scripts instead of loading it from remote [REL-1866]
- Restrict the selection of dynamic permission roles to permissions which are available in the organization of the role [REL-1871]
- Add support for additional WiFi EAP modes for Android Enterprise [REL-356] [REL#224386]
- Support deployment of AE WiFI EAP TLS certificates [REL-1497] [REL#225686] [REL#226256]
- Restrict LDAP UI feature to paid licenses [REL-1789] [REL-1790]
- Perform automated VPP app updates on all Apple platforms [REL-1652]
- Use Apple product name for ‘model’ column content on CSV export [REL-1583] [REL#226423]
- Rename installed app list column name ‘Publisher’ to ‘Managed App’ [REL-1849]
- Filter data received on cluster port before deserialization [REL-2136]

Für Version 26.4.0

Fixes

- Fix LDAP UI incorrectly using the teacher’s search scope for classes and never setting the teacher’s search scope [REL-1841]
- Attempting to sign in with invalid credentials is logged as a warning again [REL-1756]
- An installer (msi/exe) writing a single new line to Standard Error is no longer treated as a failed uninstallation [REL-1224]
- Allow legacy Relution clients to update device details [REL-1459]
- Fix LDAP connection check without a port, because the server incorrectly used 386, instead of 389 as default [REL-1616]
- Do not query for activation lock bypass code on Shared iPads as it is not applicable in this case [REL-1832]
- Certificate Authority or Certificate Template update delete does not delete issued certificates [REL-1884]
- Immediate update of dynamic device groups filtering on device name [REL-900]
- Add drag and drop delay to list column selectors on mobile devices, to allow scrolling and dragging via the same gesture [REL-1403] [REL#226035]
- Fix update of device names via CSV [REL-1526]
- Update underscoreJS to fix CVE-2021-23358 in enrollment landing page [REL-1730]
- Fix handling of Android Enterprise system update configuration start and end time fields [REL-1827] [REL#226800]
- Enable ‘Add’ button in installed apps list for iOS and macOS user enrolled devices [REL-1849]
- Fix display of editing a device name in the device inventory [REL-351]
- Add missing icon label to the add shortcut action [REL-677]
- Remove unsupported filter type ‘BuiltIn’ from macOS Web Content Filter configuration [REL-687] [REL#224941]
- Fix clear selection button when editing assigned user of a device [REL-1619]
- Fix `null` as CN of Apple device identity certificates for devices enrolled with legacy certificates. Also fixes repeated unnecessary MDM profile updates [REL-2125] [REL#227063]
- Android agent is correctly auto-deployed when native iOS agent is present in store [REL-2009]
- Avoid unnecessarily reapplying currently inactive policies when refreshing device information [REL-2122]

Version 5.18.2

2023-06-21

Updates

- Support usage of Relution client apps on enrolled devices with users requiring MFA [REL-1620]

Fixes

- Fix failure of LDAP UI connection checks for non-LDAPS connections without an explicitly specified port. The server incorrectly used 386, instead of 389, as default [REL-1616]
- Remove orphaned entries in role, user and group tables to ensure migration of organization column works as expected, especially on long-running Relution servers [REL-1625] [REL#226517]
- Fix restoring certificates previously marked as deleted in settings [REL-1629]

Version 5.18.1

2023-06-15

Fixes

- Resolve a potential performance issue when accessing the `security_group_members_view` introduced with 5.18.0 [REL-1588]
- Fix automated deployment of Relution Files when having a Files configuration but no required app [REL-1582] [REL#226421]
- Fix filter menu header overlapping first filter [REL-1585]

Für Version 26.4.0

Version 5.18.0

2023-06-09

New

- Mark Java below 17 as deprecated and adjust requirements and installation guide [REL-1257]
- Add option configure LDAP connections via UI [REL-1511]
- Add public dynamic permission role support in the store organization [REL-1373]
- Add option to enable and retrieve the activation lock bypass code on supervised iOS/iPadOS and macOS devices [REL-1140] [REL-1144]
- The impersonation of arbitrary users available to the system administrator using the portal UI can now be disabled by setting `relution.security.impersonation.enabled=false` in `application.yml` configuration [REL-1063]
- Set default location permissions of Companion on managed Android Enterprise devices based on COD location settings [REL-1436] [REL#225955]
- Allow to override default Companion for Android Enterprise settings with a manage apps configuration [REL-1436]
- Display compliance violation details for Android Enterprise restrictions configurations [REL-1037]
- Add option to enforce bluetooth in lessons [REL-1102]
- Add action to enable or disable bluetooth on iOS or macOS devices [REL-1149]
- Configure log levels via Relution API [REL-1195]
- Configure certificate and key via new signer properties and support standard certificate formats [REL-946]

Updates

- Log stack trace on ERROR level by default [REL-1197]
- Drop app-installation repeat logic for un-managed apps to force app-updates. [REL-1328]
- Add option to specify JWT secret key and signature algorithm via configuration properties. When no secret is specified, servers create an ES512 key pair automatically on first start. For existing servers this will happen immediately after update, so that they benefit from improved security. As a consequence users need to authenticate and are asked for credentials. [REL-1411]
- Display the enrollment type and platform in the device header box [REL-1067]
- Display the external ID at the device information page of Windows and Android Enterprise devices [REL-1262]
- Update portal dependencies to Angular 15 [REL-1359]
- Add badges for AP7 only features in the Promethean configuration [REL-690]

Für Version 26.4.0

Fixes

- Execute policy assignments in sequential mode, to avoid deadlocks on SQL server [REL-1274]
- Use `BYTEA` instead of `OID` data type on PostgreSQL for `mdm_dvc_instlld_crt.data` and `sso_login_request_state.request` [REL-511]
- Avoid Apple devices having broken identity certificates after restoring from a time machine backup [REL-1062]
- LDAP correctly accepts alternate names for ldap-base (ldapBase, ldap_base), manual mappings, synthetic groups and group roles [REL-1038]
- Correct database transaction boundaries in periodic cleanup operations and some other cases [REL-1178]
- Fix the iOS VPN configuration payload generation, when it defines a specific provider type [REL-1276] [REL#225610]
- Set MFA status correctly after unimpersonation [REL-1282] [REL#225832]
- Fix stopping of education lesson with deleted course [REL-1348]
- Adjust device inventory database view (mdm_dvc_view) to match correct set of devices on Aurora, MySQL and MS SQL Server [REL-1449]
- Fix OS names in device header box for Android Enterprise devices [REL-1067]
- Fix LDAP group selection for rule set action modal. [REL-1230]
- Fix clearing the selection of LDAP users or groups for rule set action modal. [REL-1230]
- Fix LDAP group selection in the user details form [REL-1242]
- Adjust displayed version in policy applied on devices view [REL-1277]
- Sorting by version column in policy applied on devices view [REL-1277] [REL#225238]
- Fix dialog actions not being visible on desktop screens which are zoomed to 125% [REL-1283] [REL#225832]
- Fix saving of fields when editing an app [REL-1284] [REL#225840]
- Fix access to home organization details for mulit-tenant user in `system` organization [REL-1311]
- Deactivate delete action for externally provided courses [REL-1406]
- Fix the search icon size in Android Enterprise managed app configuration, and add missing translations [REL-375]
- Android Enterprise Home Screen Layout light and dark theme are applied when no wallpaper is defined [REL-1564] [REL#226352]

Für Version 26.4.0

Version 5.17.5

2023-05-26

Fixes

- Show local login option also on the organization login page [REL-1476] [REL#226247]
- Always display the correct SAML2 provider name [REL-1476] [REL#226247]

Version 5.17.4

2023-05-15

Updates

- Allow to override default permissions of the Companion for AE on managed devices with a Manage Apps configuration [REL-1423]

Fixes

- Fix login and token handling, especially for users requiring MFA [REL-1404] [REL-1411] [REL#226085] [REL#226086] [REL#226093]
- Ensure LDAP connections revert to correct bind context after user authentication errors [REL-1414]
- Adjust redirect handling during user registration [REL-1420]

Version 5.17.3

2023-05-05

Fixes

- Fix wrong MongoDB database name if connection string is used [BR-11479]

Version 5.17.2

2023-05-03

Fixes

- Allow users of other organizations, to login via the custom login screen of the store organization, during the DEP login process [REL-1327] [REL#225885]

Für Version 26.4.0

Version 5.17.1

2023-04-26

Fixes

- Use the updated designated VPN identifier from app to VPN mapping when installing managed apps [REL-1297] [REL#225863]

Version 5.17.0

2023-04-18

New

- Allow configuring scheduled activation and deactivation of policies [REL-849]
- Add support for exporting and importing dynamic permission roles via JSON files [REL-952] [REL-953] [REL-1026] [REL-1027]
- Create a Home Screen Layout Configuration for Android Enterprise devices when starting a lesson [REL-684]
- Add setting to disable users after a configurable amount of consecutive failed login attempts [REL-851] [REL-852]
- Show a script history for latest script execution results and errors [REL-958]
- Keep the latest IPv4 address devices connected from and the country the address is associated to, and add a history entry when this country changes [REL-703] [REL-704] [REL-705]
- Add a dashboard widget displaying devices grouped by country based on the latest known IP address and roaming status [REL-701]
- Display ICCID and roaming status in device inventory and device details [REL-698]
- Support user CSV import in system organization [REL-1025]
- Show organization specific login page during DEP login process instead of the generic login page [REL-947]
- Update design of settings overview including adding a keyword-sensitive search [REL-371]

Updates

- Renew Apple push certificates, valid until February 2024. The previous ones will expire in October 2023 [REL-654]
- Allow configuring login management settings of the system organization [REL-890]
- Show that Windows Companion is not supported on Windows Home edition and do not try to install it or trigger actions only available with it [REL-896] [REL-981]
- Add notification if the used Java version is deprecated and will soon be no longer supported [REL-950]
- Add auto update mode to Android Enterprise Policy [REL-375]
- Save large script execution output as a separate resource [REL-402] [REL-866]
- Display the installed certificates in the device information page for macOS and tvOS devices [REL-1069]
- Add setting to disallow guest sessions on a Shared iPad to iOS/iPadOS restrictions [REL-895]
- Add new Android Enterprise configuration to manage Always-On VPN [REL-373]
- Add new Android Enterprise configuration to configure a personal profile on a managed device [REL-386]
- Add auto update mode setting to Android Enterprise App compliance policy [REL-749]
- Add preferential network service settings to Android Enterprise restrictions [REL-383]
- Add stay on plugged modes and maximum time to lock for Android Enterprise kiosk configuration [REL-827] [REL-828]
- Replace deprecated microphone disable, camera disable and auto date and time zone settings in the Android Enterprise Restriction configuration [REL-378] [REL-380]
- Add encryption policy property to Android Enterprise Advanced Security Overrides configuration [REL-381]
- Show details of health status for users with `SYSTEM_HEALTH` permission, also when using an access token [REL-1121]
- Adjust `VPNUUID` value for Apple per app/account VPN configurations to optimize behaviour during policy changes [REL-1147]
- Let the device base info endpoint `/api/v1/devices/baseInfo` now also use the inventory database view which leads to slight changes in the response model [REL-275]
- Allow configuration of setup modes in the WiFi configuration for macOS [REL-1118]
- Improve the performance of the installed app list of devices [REL-590]
- Add general endpoint to enable cancellation of internal actions for users with the respective permission [REL-600]
- Update Spring Boot to 2.7.8 which includes support for Java 17 [REL-74]
- Reduce *WARN* log messages for VPP assignment failures [REL-806] [REL#225066]
- Update enrollment settings since Google no longer enforces a 90 day limit for Android Enterprise enrollments [REL-1116]
- Optimize display of policy status in device compliance details [REL-264]
- Show the current version of the Windows companion in the Settings and make Processor architecture in device details easier to read [REL-555]
- Display the username field in Apple WiFi configurations when only TLS is selected as EAP type [REL-977] [REL#225413]
- Automatically provide organization unique name on organization specific login page to bind login to the given organization [REL-990]
- Show Android classic devices having a given public app installed even though deployment is not supported in this case [REL-1045]
- Make connect timeout and response timeout for LDAP configurable in application.yml [REL-1225]

Für Version 26.4.0

Fixes

- Resiliently handle broken content-type response header of in secure mail gateway [REL-992]
- Ensure that a DEP account with too long meta data can still be created [REL-1091] [REL#225598]
- Remove extra license checks in courses API [REL-920] [REL#225354]
- Fix permission check in CSV device import [REL-843] [REL#225037]
- Fix Query Device Info messages stuck on state “Delivered” for some Windows Devices [REL-869] [REL#225180]
- Allow configuring column dimensions of license allocation table [REL-959] [REL#223574] [REL#225292]
- Fix loading of large app metadata for Windows Store apps [REL-870] [REL#225159]
- Ensure Windows wallpaper text placeholders will be replaced correctly [REL-533]
- Prevent displaying out-dated Azure AD sync results [REL-575]
- Support triggering refresh device information action via Relution Agent on Android Enterprise [REL-798]
- Disable affiliation changes for courses synchronized via LDAP [REL-820]
- Fix the disabled state of the setup guide *Policy configured* step [REL-998]
- Ensure that the state of the device policy reflects the compliance violation state of the device [REL-1175]
- Fixed deletion dialog in device inventory [REL-799]
- Reduce default connect timeout for LDAP to ensure health check doesn’t block indefinitely [REL-1225]

Version 5.16.8

2023-04-03

Fixes

- Remember authentication of SingleSignOn provider [BR-11274]

Für Version 26.4.0

Version 5.16.7

2023-03-20

Updates

- Make pub/sub able to gracefully handle intermittent loss of database connectivity [REL-963]
- Optimized SQL query to retrieve the type of the last delivered action for a device [REL-986]

Fixes

- Resiliently handle broken content-type response header in secure mail gateway [REL-992]

Version 5.16.6

2023-03-08

Fixes

- Work around an issue where the Android Management SDK fails to serialize a device returned by itself when disabling devices [REL-908]

Version 5.16.5

2023-03-06

New

- Generate device certificates based on a given CA or intermediate certificate with key without using an external certificate authority [REL-559]

Fixes

- Attach device to new enrollment on re-activation to ensure lookups work as expected [REL-902]

Version 5.16.4

2023-03-02

Für Version 26.4.0

Updates

- Ensure all Android Enteprise device models enrolled with COPE are not non-compliant due to keyguard restrictions [REL-874]
- Ensure Android Enterprise devices running old Android versions do not get non-compliant due to unsupported app permissions [REL-876]

Version 5.16.3

2023-03-01

Updates

- Acknowledge incoming Android Enterprise enrollment requests when trying to enroll devices with deleted enrollments to prevent Google from sending the message again [REL-867]
- Optimize rare case where Android Enterprise compliance violation detail status updates where not acknowledged to prevent Google from sending the message again [REL-867]

Version 5.16.2

2023-02-27

Updates

- Reintroduce Android Enterprise status handling for expired enrollments or confirmed deleted devices disabled in 5.16.1 without triggering any device deletion [REL-845]

Fixes

- Ensure Android devices with work profile are not subject to enforcement rules they cannot comply with [REL-845]
- Ensure the update OS action is shown in all device action lists [REL-861]

Version 5.16.1

2023-02-24

Fixes

- Do not delete Android Enterprise devices when Google sends enrollment messages for existing but no longer valid enrollments [REL-603]

Für Version 26.4.0

Version 5.16.0

2023-02-20

New

- Support for MFA with TOTP or email on user login in Relution Portal. Can be enabled in settings and required for users having specific roles. Support in the Relution clients will be added with one of their next releases [REL-127] [REL-317] [REL-318] [REL-477] [REL-480] [REL-481] [REL-517] [REL-516] [REL-518] [REL-519] [REL-696]
- Support reboot and shutdown action on macOS devices [REL-186] [REL-188]
- Add 802.1X Global Ethernet configuration for macOS [REL-197]
- Add support for viewing and managing all lessons. With the upcoming release of Relution Teacher, users with the required permissions will be able to see an overview of all lessons, including a history of each lesson, and to modify or finish still running lessons [MDM-25182] [REL-336] [REL-337]
- Allow managing PowerShell scripts in Relution and executing them on Windows devices [REL-405] [REL-410] [REL-412] [REL-413] [REL-414] [REL-428] [REL-578]
- Add refresh cellular plans action for iOS (eSIM) [REL-454]
- Show and allow editing course membership in user edit form [REL-424] [REL-502]
- Add Windows SharedPC configuration [REL-393]
- Added getting started guide [REL-81] [REL-82]
- Support PKCS12 certificates by Windows WiFi and VPN [REL-504]
- Use database view for device base info endpoint to enable sorting for additional columns in device inventory and improve its performance [REL-275] [REL-616]

Updates

- Add Freeform to known iOS System Apps [REL-528]
- Allow declaring required permissions in a more streamlined way [REL-580]
- Remove legacy Windows device reactivation [REL-352]
- Use organization's default language as fallback to search public app store [REL-196]
- Support forgot-password feature in clustered installations by sharing state using the database [REL-220]
- Remove implementation and database entities concerning legacy disabled app signing and publishing feature [REL-364]
- Report additional database, operating system and Relution configuration parameters when requesting license information [REL-390]
- Add support for formatting 22H2 Windows versions for display [REL-452]
- Add Preserve Data Plan option to wipe action for iOS [REL-455]
- Download native client apps, e.g. Windows companion, earlier after system start by default [REL-521]
- Prevent that the user filter for push notifications is persisted since for customers with many users it could grow pretty huge [REL-532]
- Do not set login date for impersonated users [REL-631]
- Enhance Secure Mail Gateway preparing for future Java updates and offering better performance [REL-77]
- Improve cluster performance with JGroups version 5.2.11.Final. Also upgrade stack protocols and switch to asynchronous I/O transport [REL-78]
- Set default values for block delay to 20 days and wipe delay to 30 days for Android Enterprise instead of Google's implicit default of 3 and 10 days [REL-644]
- Support configuring auto-deployments in the details of web link apps [REL-305]

Fixes

Für Version 26.4.0

- Relution properly handles Android Enterprise communication when Enrollment is no longer valid [REL-603]
- Properly handle character sequences applying XML-output escaping when creating property lists for iOS device configurations. This corrects an issue when using ampersand in passwords, for example. [REL-308] [REL#224075]
- Always set the scope of imported policies to non-public [REL-556] [REL#224716]
- Do not remove client app from Relution Shared Device when lesson is finished [REL-713] [REL#224805]
- Use commandline arguments on MSI installment via app compliance [REL-715] [REL#224953]
- Fix execution of automated background actions for iOS System Updates configuration [REL-602] [REL#224694] [REL#224523]
- Add support for *Message* action on iOS user enrolled devices [REl-482] [REL#224514]
- Do not log premature client-side connection aborts, incl. any I/O errors caused by the client disconnecting while the response was partly transfered already. Both cases indicate normal webserver operation [REL-219]
- Ensure LDAP users can log in again after being unlocked and emit additional diagnostic when authentication magic value is missing [REL-221]
- Fix calculation of MD5 checksum for resources stored in Azure Blob Storage [REL-592]
- Fix count of migratable Android devices when using a branded agent [REL-636]
- Fix disable state of “Password for outgoing email server” in iOS Email configuration [REL-486]
- Fix and unify stepper icons [REL-557]

Version 5.15.2

2023-01-31

Fixes

- Fixed the issue that a large number of devices were stored in RAM, resulting in an `OutOfMemoryError: Java heap space` [BR-10270] [BR-10462]

Für Version 26.4.0

Version 5.15.1

2023-01-27

Fixes

- Fix issues with Shared iPad caused by a possible bug in iPadOS on devices running iPadOS 16+ [REL-537] [REL#224195] [REL#224310]
- Fix PostgreSQL reporting the error “Cannot change transaction isolation level in the middle of a transaction” in some cases [REL-473]

Version 5.15.0

2022-12-23

New

- Deploy the Windows Companion on enrolled devices and support tasks like installing apps, executing scripts and more [MDM-23016]
- Allow teachers to logout shared devices participating in their lesson. The feature will be available in Relution Teacher app soon [MDM-24909] [REL-141]

Updates

- Change OS version filter in device inventory to allow selecting multiple versions [MDM-24990]
- Start polling device actions if the device user has changed via device header box [MDM-25485]
- Extend wipe action for macOS devices [REL-128]
- Adjust action state after successful withdraw action on apple devices [REL-128]
- Remove `DISABLE_JWT_AUTHENTICATION` feature toggle and unused session handling logic [MDM-25436]
- Adjust iOS agent migration when specific feature toggles are enabled [REL-191]
- Ensure to always send education updates [REL-200]
- Remove redundant compliance history entries for remote logout of shared devices and adjust the text of the entries. [REL-228]
- Discontinue query parameter `versionNameLocaleFallback` of `api/v1/content/apps/baseInfo` [REL-256]
- Improved the UI feedback of the policy deletion process [MDM-25190]
- Add option to refresh the device history [MDM-25418]
- Ignore work profile passcode configuration on fully managed devices [REL-222] [REL#223727]

Fixes

- Avoid adding the supervision host certificate to remote profiles more than once to ensure robustness when multiple DEP accounts are used [MDM-25497]
- Handle SQL server delivering query results as integer instead of long for action metrics [REL-340]
- Trigger Companion refresh info action on Windows app installation, and skip unnecessary queries [MDM-25337]
- Fix exception when Android classic clients confirm the default app compliance configuration [REL-255]
- Fix clearing of app version mappings in the store organization [MDM-25357] [REL#223978]
- Fix App permission mapping view showing bug reporter when users are removed [MDM-25358] [REL#223978]
- Fix UTF-8 encoding of uploaded .mobileconfig files in the Apple Configurator 2 configuration [REL-247] [REL#224168]
- Fix possible rendering crash of tabs under Safari 16.1 on macOS Ventura [REL-292] [REL-224]

Für Version 26.4.0

Version 5.14.1

2022-12-16

Updates

- Adjust username field to be case insensitive on PostgreSQL during login [REL-269]
- Improve robustness of health check [REL-296]
- Extend logging of progress when migrating details JSON data [REL-297]
- Optimize details JSON column data migration to run once per device and table only [REL-299]

Fixes

- Handle publisher names with more than 255 characters for installed apps on Windows devices [REL-301]
- Exclude expired Android Enterprise enrollments having an account identifier from the one-time migration process [REL-300]
- Fix exception that can occur during health checks when formatter is re-used by multiple threads [REL-306]

Version 5.14.0

2022-12-02

New

- Add macOS update configuration [MDM-24376]
- Add monitoring metrics regarding Relution database operations, device actions, web requests, DEP, VPP, Autopilot and Azure AD [MDM-24583] [MDM-24585] [MDM-24589] [MDM-24590] [MDM-24591] [MDM-24828]
- Add configuration for scheduled logout to Relution Shared Device policy [MDM-24621] [MDM-24619]
- Allow teachers to logout students on shared device in the active lesson when deactivating them or finishing the lesson [MDM-24622]
- Add support for Relution Shared Device login via access token based QR codes [MDM-24739] [MDM-24736]
- Automatically retry to subscribe for VPP notifications in background if the subscription state is failed [MDM-24882]
- Provide case-insensitive search and login using the proprietary ILIKE operator on PostgreSQL databases [MDM-25318]

Updates

- Validate passwords also in Portal during password reset [MDM-24806]
- Reduce the response time for VPP test notifications sent during the subscription process [MDM-24882]
- Add android classic policy for additional interactive whiteboard devices [MDM-25071]
- Ensure showing the app name in action details when the Relution Agent is deployed during enrollment [MDM-24106]
- Add EAP option to inner authentication for iOS and tvOS Wi-Fi configuration [MDM-25199]
- Support sorting additional device inventory columns, e.g. Wi-Fi MAC, lost mode status or Shared iPad [MDM-24732]
- Adjust and clean up log messages according to log level definition [MDM-24899]
- Add again automatic refresh of the status of installing apps after triggering an installation on Apple devices. Feature was disabled with 5.13.1 due to performance issues on some databases [MDM-25078] [MDM-25076] [MDM-24122]
- Add human-readable product names of new Apple devices [MDM-25109]
- Improve error responses for cases where no error code was present [MDM-25110]
- Always ping devices in ping interval regardless of last connection date so that device details are updated at least once per ping interval [MDM-25319]
- Redesign history views [MDM-22891] [MDM-22892]
- Set initial zoom level of maps to a more sensible value when a location is known [MDM-24778]
- Adjust tooltip position of action menu in lists to not block another element with which a user can interact [MDM-25176]
- Change order of uninstall parameters and path for .exe files [MDM-25202]
- Make version code read-only in most cases [MDM-25202]
- Automatically focus the input field for the username or password on the login page [MDM-24952]

Fixes

Für Version 26.4.0

- Fix duplicate key errors when fetching VPP entity details for inconsistend VPP data [MDM-25159]
- Fix automated fetching of metadata for existing public store apps [MDM-25326] [REL#223899]
- Fix possible race condition when enrolling Windows devices and directly assigning a policy caused by not yet available push token [MDM-25449] [REL#223974]
- Allow teachers to access VPP license base info so the legacy iOS teacher console can still be used with default permissions [MDM-25455]
- Ensure at least the Settings app is always whitelisted for devices in an active lesson [MDM-25018] [REL#223426]
- Generate form-data bodies in OpenAPI [MDM-25050]
- Fix the certificate field extractor for long values [MDM-25145]
- Ensure not yet managed apps are updated correctly for iOS devices [MDM-25227] [REL#223434]
- Handle case when Apple device reports installed app without name, fallback to identifier [MDM-25372]
- Fix the automatic reset of the encryption type when the SSID is changed in the Windows Wi-Fi configuration [MDM-24934]
- Fix Windows Wi-Fi configuration layout in case any *Personal* encryption type is selected [MDM-24935]
- Fix tvOS Wi-Fi configuration layout and add option to toggle the password visibility [MDM-25022]
- Adjust icon in menu updates when side navigation opens/collapses [MDM-25048]
- Fix possible null reference error when accessing iOS/macOS device details [MDM-25129]
- Remove duplicate toast message, when the deletion of an enrollment fails [MDM-25175]
- Ensure selecting or removing certificates in the iOS exchange configuration always opens certificate modal [MDM-25234]
- Fix display of some compliance violations in rule-sets [MDM-25303]
- Fix highlighting of the current active main menu entry [MDM-25305]
- Disable save button until the required apps are fully loaded in iOS and macOS app compliance views [MDM-25317] [REL#223909]
- Fix login via “organization\username” format in Portal [MDM-25368]
- Skip invalid accounts during DEP sync [MDM-25498]
- Polices applied to Windows devices during enrollment no longer cause invalid noncompliance state [REL-177]
- Avoid adding the supervisioning host certificate to remote profiles more than once to ensure robustness when multiple DEP accounts are used [MDM-25497]

Für Version 26.4.0

Version 5.13.5

2022-11-09

Fixes

- Deploy the custom galneoscreen Relution agent also for galneoscreen 9 devices during migration instead of the default agent [MDM-25112]

Version 5.13.4

2022-11-03

Fixes

- Fix DEP profile lookup for auto-enrollments in store organization using authorization and default profile device name and distributing to other organizations [MDM-25128] [REL#223539]
- Speed up home screen layout editor for Android Enterprise devices by querying installed apps by platform of specific organization only [MDM-25173]
- Avoid periodically logging failures when repeatedly trying to reach Android devices having outstanding ping actions [MDM-25177]
- Fix visibility of location tab for iOS devices which are in the new lost mode states [MDM-25178] [REL#223665]

Version 5.13.3

2022-10-26

Fixes

- Ensure a value is set for lost mode in auto-enrollments, to avoid entries not to be shown in Portal due to filtering [MDM-25105] [REL#223539]
- Fix downloading supervision certificates with tenant users belonging to a different organization [MDM-25118] [REL#223594]
- Fix display of device details when OS update information is not up-to-date [MDM-25129] [REL#223611]

Version 5.13.2

2022-10-20

Für Version 26.4.0

Fixes

- Fix an issue preventing iOS/iPadOS devices from receiving new policy versions when they have an enabled iOS update configuration as part of the policy [MDM-25083]

Version 5.13.1

2022-10-19

Updates

- Even though the version used by Relution was not affected, update Apache Commons Text to 1.10 due to CVE-2022-42889 [MDM-25077]

Fixes

- Disable automatic refresh of the status of installing apps after triggering an installation on Apple devices due to performance implications on some databases, which has been added with 5.13.0. Will be re-introduced once they are resolved [MDM-25076]

Version 5.13.0

2022-10-14

New

- Enable the new permission system. Custom sets of permissions can now be defined via Relution Portal and assigned to groups and users [MDM-20013]
- Support multiple DEP accounts per organization [MDM-23979]
- Support per-user certificates for S/MIME signing and/or encryption in iOS Email and Exchange configuration [MDM-22832]
- Automatically trigger MDM profile update to update the signer certificate of Apple devices to avoid showing a warning on the device [MDM-22899]
- Automatically enable lost mode after DEP device reset if enabled before [MDM-24118]
- Automatically refresh the status of installing apps after triggering an installation on Apple devices [MDM-24122]
- Generate and configure an MDM supervision identity when enrolling new DEP devices. The identity can be downloaded from Relution and imported into Apple Configurator to allow connecting to devices even if pairing is disabled [MDM-24173]
- Dynamically adjust the Apple education configuration on devices when starting a lesson with an ad hoc class [MDM-24247]
- Add macOS OS Update action and configuration [MDM-24374] [MDM-24376]
- Add macOS System Policy Control configuration [MDM-24513]

Updates

- Renew Apple push certificates, valid until October 12th, 2023. The previous ones will expire on May 1st, 2023 [MDM-22876]
- Validate the state of BitLocker configurations on “Refresh device info” and add compliance violations if necessary. [MDM-24230] [REL#222393]
- Prevent timeout when publishing a ruleset version [MDM-23759]
- Prohibit updating a DEP token with a token from a different MDM server [MDM-23959]
- Handle duplicate VPP notifications [MDM-24406]
- Optimize performance when updating information about installed apps on Windows devices [MDM-24804]
- Extended macOS accounts configuration with mobile account configuration [MDM-24512]
- Omit auto-enrollment synchronization for DEP accounts that are not linked to an Apple Business or School manager account [MDM-24762]
- Migrate storage configuration properties in application.yml to a new human-readable structure. The legacy format and environment variables are still supported [MDM-22557]
- Prevent selecting teachers as students of ad hoc lessons [MDM-24925]
- Update Apple education configuration also on inactive or non-compliant devices since the restriction preventing this is no longer necessary [MDM-24989] [REL#223386]

Fixes

Für Version 26.4.0

- Restore the certificate resource reference of the iOS certificate configuration [MDM-24764]
- Ensure metadata of remaining certificates is updated even when a certificate in store is expired or cannot be processed [MDM-24761]
- Fix authentication problem with Relution-Agent and Teacher-Console app for Android-Enterprise if more than one Manage Apps Configuration is present [MDM-24984] [REL#223280]
- Allow saving users without email imported by LDAP in Portal [MDM-25016] [REL#223280]
- Adjust links to Relution documentation to point to repo.relution.io for native packages [MDM-24763]
- Fix updating the domain or password of a Windows Exchange policy leading to an unintended compliance violation [MDM-24418]
- Disable chips delete if configuration is disabled [MDM-24298]
- Fix modal validation when creating lost mode actions for iOS devices [MDM-24572]
- Fix enabling the personal hotspot on iOS devices when the action is triggered via Portal [MDM-24665] [REL#222900]
- Fix *No policy* filter option in device inventory [MDM-24780] [REL#223087]
- Fix and enhance organization search in store organization [MDM-24819] [REL#223162]
- Fix an issue preventing users with few permissions from installing Play Store apps through the Relution agent on Android Enterprise devices [MDM-24982]

Version 5.12.2

2022-09-14

Updates

- Support compression when setting application.yml via environment variables in cloud scenarios [MDM-24705]

Fixes

- Fix display of license views when using system organization based licensing [MDM-24706]
- Fix database migration failing when encountering unexpected invalid references in database [MDM-24704]

Für Version 26.4.0

Version 5.12.1

2022-09-07

Fixes

- Fix issue preventing import of Windows Store Apps due to breaking changes in the Windows Store API [MDM-24597]
- Fix issue preventing a login via a SSO provider during a DEP enrollment on macOS [MDM-24613]
- Fix database schema migration on PostgreSQL [MDM-24605]
- Fix issue which caused duplicate group creations during a LDAP synchronization [MDM-24617]
- Fix issue when a new LDAP user tries to login, that not all group memberships are resolved [MDM-24639]

Version 5.12.0

2022-08-26

New

- Deploy Relution Agent for Android Enterprise devices [MDM-23697]
- Allow enrolling Autopilot auto enrollments from the store organisation into other organisations [MDM-23356] [MDM-23906]
- Add Android Enterprise home screen layout configuration to configure Relution Home Screen app [MDM-23415]
- Provide active branding to client apps over managed configuration [MDM-23898]
- VPP tokens uploaded to the store-organisation will be publicly available in all other organisations [MDM-23827]
- Show an error in the notification center if Android Enterprise communication has issues [MDM-23838]
- Make it possible for Android and Windows devices to download native apps assigned via policies without the explicit need for general app store access [MDM-23970]
- Use built-in APNS push credentials to handle push notifications for the Relution Agent [MDM-24049]
- Use web views supporting single-sign on accounts for DEP authentication and shared device login [MDM-24240] [MDM-24241]
- Add new field to the Android Enterprise Work profile passcode configuration to define if a separate passcode for the work profile is required [MDM-24324]
- Add new restriction flags for iOS 16 and macOS 13 devices [MDM-24476]

Updates

Für Version 26.4.0

- Automatically try to reassign VPP licenses whenever deployment actions get retried [MDM-24454]
- Add the count of open actions and last connection date to lesson device information [MDM-24209]
- Persist additional meta data when parsing certificates [MDM-22995]
- Optimize education updates and removals for Apple devices [MDM-23478]
- Make DEP accounts in store organization global by default [MDM-23725]
- Allow customizing the external VPP notification URL via `relution.vpp.notificationUrl` [MDM-23974]
- Separate roles from authorities to comply with new permission schema in current authorization response [MDM-24032]
- Set actions to error when no push notification could be sent for Windows devices [MDM-24258]
- Consider action priorities when processing Windows actions [MDM-24258]
- Use Gigabyte instead of Gibibyte based conversion for cache limit in macOS content caching configuration [MDM-24269]
- Always activate users synchronized through LDAP even when deactivated on Relution side; users that should not be able to sign in need to be disabled in LDAP instead [MDM-24467]
- Enable reset password action on android enterprise devices with personal profile [MDM-22661]
- Adjust colors of enrollment page for Windows devices [MDM-23595]
- Require the name field of an app version only for the default language [MDM-23619]
- Add more filter options to the device history [MDM-24348]
- Hide Windows paid apps from search results [MDM-23622]
- Change styles of enrollment landing page dynamically, if needed [MDM-23595] [REL#221602]

Fixes

- Fix creation of organizations when administrator password does not conform to password policy [MDM-23127]
- Apple education configuration updates no longer fail if a user is configured as both teacher and student in different courses [MDM-23790]
- Updating a course as Content Manager updates the education configuration on the devices of the users involved. [MDM-23760]
- Fix the first Relution Agent deploy action failing with `LicenseNotFound` error when enrolling a device with DEP [MDM-23954] [REL#222092] [REL#222025]
- Fix error responses not providing an error code in some rare cases [MDM-24107]
- Ensure license restrictions for servers where the system organization has an education or enterprise license are checked correctly [MDM-24128]
- Ensure next synchronization date no longer incorrectly shows *never* after manual AzureAD device synchronization [MDM-24163]
- Update Windows UpdatePush action to error, if it fails several times, with confurable retry count [MDM-24196] [MDM-24196]
- Fix sample app import for new organizations created via a tenant user [MDM-24473]
- Allow Windows platform to download file for action [MDM-24009]
- Fix deletion of rule actions [MDM-23758] [REL#221630]
- Fix unintended clearing of policies when extending enrollments [MDM-23811]
- Fix unintended duplication of version constraints, when switching between app versions [MDM-24100]
- Fix license information menu entry ignoring permission when the user switches between tenants [MDM-24249] [REL#222392]

Version 5.11.4

2022-07-14

Für Version 26.4.0

Updates

- Allow disabling Clustering support on network or even service layer via configuration for restricted network environments [MDM-24131]

Fixes

- Fix issue preventing apps to be installed with VPP via Relution iOS agent and legacy client [MDM-23960] [REL#222264]
- Avoid a possible issue in cluster channel initialization when also having a lot of LDAP connections [MDM-24145]
- Fix issue in the smart board configuration preventing to configure lock screen on specific boards [MDM-24144]
- Fix handling of pagination for requests currently preventing CSV export in some scenarios [MDM-24149] [REL#222294]

Version 5.11.3

2022-07-05

Updates

- Assign VPP license to devices early when creating a deploy app action [MDM-23960] [REL#222264]
- Retry deploy app actions automatically after a short period of time when they fail with a LicenseNotFound error [MDM-23961] [REL#222033]

Fixes

- Include new authorities in well-known system permissions to improve performance when loading groups [MDM-24016]
- Fix Relution Agent deploy action possibly failing once when enrolling an iOS device [MDM-23954] [REL#222092] [REL#222025]
- Do not perform unnecessary multiple re-installations in rare case when an app appears to be stuck in installation [MDM-24025]
- Add vertical scrolling for confirmation step in *Apply action* modal for multiple devices [MDM-23939]

Version 5.11.2

2022-06-08

Updates

- Display a message that explains that installation of the new Relution Teacher App after iOS client migration must happen manually. This can also be done with an App Compliance configuration [MDM-23849]

Fixes

- Fix SSO login button, when single sign on is active for a specific tenant [MDM-23858]
- Fix default value of client migration on Microsoft SQL Server [MDM-23856]

Für Version 26.4.0

Version 5.11.1

2022-06-03

Updates

- Optimize descriptions and translations for iOS client app migration wizard [MDM-22700]
- Optimize handling of client migration on devices with a Relution shared device configuration [MDM-23791]

Fixes

- Fix display of organization push certificates in Portal after migrating to Relution Agent for iOS [MDM-23700]
- Fix logout on shared devices for users which do not have any permissions [MDM-23798]

Version 5.11.0

2022-05-20

New

- Use the new Relution iOS apps for new organizations as a default and allow existing organizations using the public Relution app to migrate to them via the settings view [MDM-22700] [MDM-22705] [MDM-23118]
- Allow making DEP configuration public in the store organization, so auto-enrollments can be assigned to other organizations [MDM-23332]
- Use Json Web Tokens for session handling [MDM-23578]
- Add user impersonation for system administrators using Json Web Tokens [MDM-20138]
- Save and show the most recent synchronization result of Azure AD device sync, user sync and group sync [MDM-22818]
- Add scheduled automated synchronization of Windows Autopilot devices [MDM-22929]

Updates

- Renew Apple push certificates, valid until May 1st, 2023. The previous ones will expire on November 30th, 2022 [MDM-22876]
- Automatically renew the Apple device SCEP CA and device certificates issued by it before it expires, default starting 180 days before expiration [MDM-22742]
- Extend the Azure AD configuration wizard and allow checking the azure ad configuration on the fly while configuring it [MDM-22819] [MDM-22817]
- Provide information about the most recent logged in Azure AD user on Autopilot devices [MDM-22936]
- Make parsing of PKG files for macOS distribution more permissive to support more PKG formats [MDM-22288]
- Automatically clean-up app history and device compliance history entries, per default after two years [MDM-22711] [MDM-22713]
- Save Apple education configuration per device, no longer per action [MDM-22769]
- Assign default groups to teachers & students imported from LDAP even when no courses can be created [MDM-22802] [REL#22820]
- Even if Relution is not affected, add mitigation for Spring4Shell as suggested by the Spring team as an additional safeguard [MDM-23193]
- Disable app signing by default unless the feature toggle APP_SIGNING is set since it is due to be removed [MDM-23458]
- Use the Azure AD `User Principle Name` field for the Relution user email when importing users [MDM-23552]
- Show the SSID for tvOS Wi-Fi configurations as name in tables [MDM-22814]
- Use unified field names for user and groups and device CSV import and export [MDM-23061] [MDM-23060]
- Show additional information in the VPP user and VPP license assignment views [MDM-23143] [MDM-23187]

Für Version 26.4.0

Fixes

- Synchronization errors no longer trigger post-sync actions, which could incorrectly delete users [MDM-22991][REL#221066]
- Fix manual LDAP sync in cluster environments not running when connected to a secondary node [MDM-23125]
- Fix applying a policy in a tenant organization, when the policy contains a Relution Shared Device configuration [MDM-23249] [REL#221342]
- Fix being stuck on login page because of missing permissions after page redirect [MDM-22783]
- Fix organization icon in the portal header not refreshing after switching the organization [MDM-23530] [REL#221485]
- Fix background transparency of information box in the DEP settings [MDM-23551]
- Fix device custom fields only being displayed when the settings were loaded before [MDM-23130] [MDM-23721] [REL#221759]
- Fix print view in Portal [MDM-23247]

Version 5.10.1

2022-05-13

New

- Use new Microsoft Store endpoints to fetch meta data of Windows public apps [MDM-23642]

Version 5.10

2022-03-31

New

- Use Apple VPP v2 API including real-time notifications for updated data [MDM-22114]
- Execute high priority actions (e.g. enable lost mode, reset passcode, locate device) before regular actions for Apple Devices [MDM-22708]
- Add support for Windows Autopilot enrollment [MDM-21897]
- Add properties to Windows Antivirus configuration to improve scheduling defender scans [MDM-22563]
- Make helpdesk link configurable via `relution.legal.helpdeskUrl` [MDM-22915]
- Make imprint link configurable via `relution.legal.imprintUrl` [MDM-22917]
- Add configurable privacy policy and EULA links which will be used instead of the previous privacy policy setting [MDM-22586] [MDM-23126]
- Support user-defined custom device properties names as column header names in the CSV import for auto-enrollments and devices [MDM-22916]
- Add full S/MIME support for iOS Mail configuration [MDM-22602]
- Add custom JSON code for Android Enterprise to enroll a device via a Zero Touch profile. [MDM-23040] [REL#22979]

Updates

Für Version 26.4.0

- Add MDM-initiated auto-renewal of Apple device identity certificates [MDM-22656]
- Disallow spotlight internet results for students in exams [MDM-22812]
- Prevent starting on Oracle databases with a human-readable error message since Oracle is no longer supported [MDM-22099]
- Extend ping action clean-up [MDM-22268]
- Allow Relution client in iOS App Compliance under required apps and allowed apps [MDM-22390]
- Refine API usage and permissions for listing groups and users [MDM-22808] [MDM-22804]
- Reduce log output when SMG is configured [MDM-22810]
- Optimize SQL queries used when checking for pending app or webclip installations [MDM-22908]
- Remove the extra enabled state for categories [MDM-22986]
- Remove supporting for deploying apps onto devices enrolled in other MDMs [MDM-23013]
- Remove URL shortener setting which is no longer used [MDM-22677]
- Allow updating the Apple MDM profile on devices with a legacy MDM server URL when triggered from the devices [MDM-22895]
- Allow entering multiple search values into search bar [MDM-21477]
- Adjust default values for new Windows Firewall configurations [MDM-22575]
- Include original language name in profile language selector [MDM-22657]
- Reduce network traffic when publishing a policy version [MDM-22734]
- Adjust icon style of the state column in the sub action list [MDM-22752]
- Allow uploading user certificates on profile page [MDM-22813]
- Adjust email validation when updating existing user [MDM-22947]
- Show Windows version name instead of build number in the device header box [MDM-22934]
- Add managed app configuration to Relution Teacher when is deployed to iOS devices [MDM-22704]
- Add new setting to deploy Relution Agent for iOS instead of legacy client [MDM-22706]
- Force HTTPS for configured external URL [MDM-22710]

Fixes

Für Version 26.4.0

- Fix education being removed from a device prematurely when the user only had indirect class memberships left [MDM-23132] [REL#221150]
- Fix issue with installation of required apps in tvOS App Compliance configuration [MDM-22840] [REL#22914]
- Fix deletion of users with user certificates [MDM-22883]
- Fix “Elevation prompt for standard users” option for Windows Local Device Security confguration [MDM-23072] [REL#221192]
- Fix device filter when searching for devices without a policy [MDM-22945] [REL#221055]
- Handle the update case of Windows Exchange configuration [MDM-22177]
- Remove existing compliance violations for Windows configurations that are deleted but not applied on the device [MDM-22568]
- Set name, description and custom properties for a Windows device from enrollment, unless reactivation is enabled [MDM-22573]
- Fix server startup when the system administrator was removed [MDM-22811]
- On Relution Shared Devices, when a user is logged in, enable only the Relution client and Settings if no apps are whitelisted [MDM-22898]
- Abbreviate long name and artist name for VPP publications to avoid errors when these values are excessively long [MDM-22941] [REL#221043]
- Do not add Windows store apps without an internal name [MDM-23173]
- Distinguish between Windows 11 and Windows 10 in the version name [MDM-22850]
- Fix template for Apple User Enrollment configuration shown in settings [MDM-22111]
- Adjust DEP profile status filter to avoid receiving false positive results [MDM-22803]
- Make sure selecting configuration types in the configuration list now always navigates to configuration details [MDM-22827]
- Clearing the position field in the user profile raises an exception [MDM-22992]
- Allow resizing the columns in the VPP synchronization history view [MDM-23010]
- Optimize initial performance and fix pagination counts of app selectors [MDM-22997]
- Access of content manager permission to user and group view [MDM-23105] [REL#221228]

Für Version 26.4.0

Version 5.9.2

2022-03-16

Fixes

- Fix pub/sub not working as expected in cluster environments after registration for Android Enterprise in some cases [MDM-22690] [REL#22750]
- Fixed an issue with handling no longer valid VPP tokens that could lead to VPP synchronisations being blocked [MDM-23000] [REL#221095]
- Fix device filter when searching for devices without a policy [MDM-22945] [REL#221055]
- Abbreviate long name and artist name for VPP publications to avoid errors when these values are excessively long [MDM-22941] [REL#221043]

Version 5.9.1

2022-02-22

New

- Assign public policies of store organisation DEP auto-enrollments to enrolled devices [MDM-22823] [REL#22813]

Updates

- Extend logging of LDAP services [MDM-22824]

Fixes

- Fix display of “location” tab for locatable devices [MDM-22503] [MDM-22776] [REL#22603] [REL#22801]
- Fix basic auth login, e.g. during DEP authentication, when the password starts with the basic auth separator character (colon) [MDM-22824]
- Fix navigation bar entries [MDM-22800]

Version 5.9

2022-02-08

New

Für Version 26.4.0

- Support for user enrollment of macOS devices [MDM-21927]
- Support account-driven user enrollment for Apple devices [MDM-22343] [MDM-22111] [MDM-22529] [MDM-21749]
- Add VPN type “Custom SSL” to iOS/macOS VPN configuration [MDM-22183]
- Synchronize users, groups and their members from Azure AD [MDM-21382]
- Synchronize Windows Autopilot devices [MDM-21896]
- Manage auto enrollments for Windows Autopilot devices [MDM-22508]
- Reactivate Windows devices [MDM-22419]
- Use local short URLs for manual enrollments instead of external URL shortening [MDM-22641]
- Add Spanish, French, Italian and Turkish as supported languages to the enrollment landing page [MDM-22556]
- Allow managing pre-installed apps not available in Play Store in Android Enterprise configurations by entering their package name [MDM-21686] [RS-4549] [RS-7101]
- Prioritize “Lost Mode”, “Reset Passcode”, “Wipe” and “Withdraw” actions for Apple devices. [MDM-22370] [REL#22235] [REL#22517]

Updates

- Recreate Android Enterprise enrollments that still use a user account identifier automatically [MDM-22595]
- Use name of a category's default language as fallback for other languages [MDM-22387]
- Search devices by UDID [MDM-22519]
- Add Android Enterprise managed configuration for Relution Agent [MDM-22250]
- Automatically install Relution Teacher Console alongside SCM on Android Enterprise devices of teachers with a Samsung Classroom Management configuration [MDM-21406]
- Ignore policies specified in a DEP auto-enrollment when the device is enrolled in a different organization (system-wide DEP) [MDM-22166] [RS-7858]
- Allow specifying ownership for auto-enrollments [MDM-22295] [RS-5709]
- Base docker images on AlmaLinux 8 instead of CentOS 8, since CentOS Linux 8 has reached End Of Life (EOL) on December 31st, 2021 [MDM-22385]
- Do not send push notifications to Apple devices when they are detected as being in-active [MDM-22388]
- Ensure MDM profile of devices with disabled signature validation is also renewed [MDM-22534]
- The education certificates will be checked and, if need be, fixed automatically if the last education deployment action failed with a specific certificate error [MDM-22660]
- The enrollment validation date for Android Enterprise can only be chosen up to 89 days in the future since Google does not allow a longer period of time [MDM-22208]
- Add missing Windows edition badges in the Restriction policy configuration [MDM-22276]
- Remove deprecated calendar domains, contact domains and mail domains from Apple VPN configuration [MDM-22381]
- Optimize the filter query in iOS app compliance configuration [MDM-22481] [REL#22337]
- Hide remove app action for windows until device and user scope is fully supported [MDM-22571]
- Persist how a policy was assigned to a device (auto-assignment, enrollment, manual) [MDM-21786]
- Adjust S3 Connector to handle partial downloads correctly which improves the performance [MDM-22554]

Fixes

Für Version 26.4.0

- Prevent additional automated re-install actions for devices when another action is already pending [MDM-22394] [REL#22257]
- Create an app history entry when the version number of a public app changes [MDM-22482] [REL#22376]
- Fix rendering of Android Enterprise managed configuration editor in various cases [MDM-22511]
- Fix activation of URL blocklist setting in Samsung Classroom management app configuration [MDM-22392]
- Fix exporting and importing policies as multi tenant user [MDM-22536] [REL#22346]
- Fix update behaviour of Windows certificate configuration [MDM-22170]
- Fix update behaviour of Windows update configuration [MDM-22179]
- Hide details of persistence exceptions and show generic message instead regardless of user permissions [MDM-22269]
- Add missing checks for Windows versions and editions to Windows restriction configuration [MDM-22310]
- Manually created add/remove shortcut actions for Shared iPads and macOS [MDM-22528] [REL#22404]
- Fix installation of missing apps on iOS devices when being triggered by a PING action [MDM-22560] [REL#22478]
- Do not pre-fill user phone number when editing enrollments [MDM-22322]
- Hide empty entry for device serial number in device header box [MDM-22371]
- Inviting VPP users again after having removed them once already [MDM-22375]
- Prevent showing an empty three dots menu if the user selects an item on the VPP synchronization history page [MDM-22431]
- Truncate x-axis label of charts to avoid flickering [MDM-22533] [REL#22437]
- Fix disappearing of multi tenant switcher after switching tenant with a text search active [MDM-22562] [REL#22483]
- Fix unintended removal of multiple policies when assigning DEP profile in auto enrollment list via the short action [MDM-22601] [REL#22464]
- Allow editing the ownership state of a device with ownership state unknown [MDM-22644]

Version 5.8.1

2022-12-20

Updates

- Even though Relution does not use Log4j for logging, update log4j-api again to the newly released 2.17.0 with respect to CVE-2021-45046 → and CVE-2021-44228 → [MDM-22301]

Version 5.8

2022-12-16

New

- Automatically register managed AppleIDs with VPP when enrolling devices with Apple User Enrollment [MDM-22017]
- Automatically associate VPP licenses to assigned users of Apple User Enrollment devices when apps are installed [MDM-22018]
- Display if Apple devices are currently in “Not now” state [MDM-22252]
- Enable public policies for Android Classic [MDM-21732]
- Show all available network adapters on Windows devices in device details [MDM-21962]
- Add Spanish, French and Italian translations [MDM-22149]
- Support managing associated apps in the details of app categories [MDM-21902] [RS-6802] [RS-6848]
- Show all supported app platforms for newly added or refreshed public apps for Apple platforms [MDM-21721]
- Remove *Beta* badge for iOS User-Enrollment [MDM-22018]

Für Version 26.4.0

Updates

- Even though Relution does not use Log4j for logging, update log4j-api to 2.15.0 and always enable `formatMsgNoLookups` as a default with respect to CVE-2021-44228 →. Also update the Splunk logging dependency so it no longer bundles log4j-core [MDM-22301]
- Show user assigned VPP licenses in details of user enrolled devices [MDM-22193]
- Allow filtering apps and app requests by categories [MDM-21901]
- Add iOS system apps “Magnifier” and “Translate” for selection in app compliance and home screen layout [MDM-22104]
- Extend known Apple product names for new devices [MDM-22155]
- Register VPP users with managed Apple IDs without inviting them via mail [MDM-22156]
- Optimize retrieval of installed and managed apps of Android Enterprise devices [MDM-22207] [RS-7940]
- Enable Per-App-VPN configurations for iOS User Enrollment [MDM-22241]
- Optimize installed app list in device details [MDM-21353]
- Remove the option to create unsupervised devices via DEP enrollment since it is no longer supported in iOS 13+ [MDM-21985]
- Remove no longer available app download count from apps list and app version details and remove most downloaded apps widget from dashboard [MDM-22041]
- Hide already selected apps from multiple app selection lists [MDM-22052]
- Adapt Windows email configuration [MDM-22110]
- Hide private Android Enterprise apps when adding apps from Google Play [MDM-22137]
- Display VPP licenses also for newly added apps in required apps list [MDM-18978]

Fixes

- Fix upload of files in specific multi tenant environments [MDM-22303] [RS-7980] [REL#22050]
- Fix Windows Email configuration [MDM-21849]
- Fix icon retrieval and display for Microsoft Store apps [MDM-21854] [MDM-22004]
- Fix handling of compliance violations for Windows configurations in general and especially for the Windows app compliance [MDM-21960]
- Fix sending notification mails concerning keystore expiration [MDM-22012]
- Prevent adding Microsoft Store apps multiple times by using different country stores [MDM-22057]
- Remove support of Windows 10 Home Edition in Windows update configuration [MDM-22154]
- Do not set the app package name in Windows app compliance policy configuration for public apps from the Windows store [MDM-22047]
- Fix upload button alignment when creating apps [MDM-22077]
- Fix importing policies [MDM-22157]
- Fix saving of certificates in tvOS Wi-Fi config [MDM-22164]
- Allow changing device ownership according to organization settings [MDM-22180]
- Fix translation of iOS restriction *Allow USB connection while locked* [MDM-22253]
- Fix using user's phone number as a default when creating new enrollments [MDM-22254] [RS-7991]
- Add redirect for link format used in app request mail notification [MDM-22277] [RS-7966]

Version 5.7.3

2022-12-08

Für Version 26.4.0

Updates

- Display the most recently used communication channel with a Windows device in device details [MDM-22261]
- Show if Windows deploy app and remove app actions belong to user or device scope [MDM-22261]

Fixes

- Avoid blocking windows actions on device scope due to user scope being blocked [MDM-22206] [RS-7938]

Version 5.7.2

2022-11-30

Updates

- Optimize performance of Android Enterprise status report processing and exclude Android system apps from installed app list [MDM-22214]

Fixes

- Make Android Enterprise status report handling more robust [MDM-22171]

Version 5.7.1

2022-11-26

Fixes

- Clean up duplicate entries from the device lending settings table automatically [MDM-22165]
- Fix importing of policies from exported files [MDM-22157]
- Remove invalid search results from Microsoft Store search instead of throwing an error [MDM-22108]
- Fix an issue with Android Enterprise status reports when the Relution store contains the same app twice (public and native) [MDM-22171]

Version 5.7

2022-11-16

New

- Allow making policies public in the store organisation, so all organisations on the server can use them. Currently Android Enterprise, iOS/iPadOS, tvOS and macOS policies are supported. [MDM-21503]
- Make it possible to install Play Store apps on Android Enterprise with an action by dynamically adjusting a device's policy [MDM-21119]
- Make it possible to hide notifications from the notification center [MDM-21484]
- Add support for cron schedules in LDAP synchronization [MDM-21636]
- Enable configuration of cross profile communication for managed apps on Android Enterprise devices [MDM-21718]
- Make it possible to enforce iOS app uninstallation on MDM profile removal in server properties [MDM-21892] [RS-7290]
- Enabled customized icon arrangement for Android Kiosk mode [MDM-21893]
- Don't allow the user of a user enrolled device to be changed [MDM-21910]
- Add support for starting an ASM SFTP sync manually in the settings page [MDM-21925] [RS-6868]
- Add a Windows local device security options configuration [MDM-21471]
- Add settings for setup assistant account creation for macOS devices to DEP profile support, which allows creating MDM-controlled local administrators [MDM-21490]
- Allow changing the password of MDM-controlled local administrator accounts on macOS via an action [MDM-21496]
- Allow powering off interactive whiteboards via the reboot action [MDM-21923]
- Activate device lending system [MDM-22058]

Updates

Für Version 26.4.0

- Add filter for hiding none existing apps to VPP apps list [MDM-21634]
- Add new iOS 15.1 restriction `allowMailPrivacyProtection` to iOS restrictions configuration [MDM-22002]
- Show sub actions of actions in device details [MDM-21872]
- Make assigning of modified DEP profiles run asynchronously to make updates faster for profiles assigned to a large number of devices [MDM-21510]
- Support multiple access tokens per device [MDM-21541]
- Extend the lesson schedule settings to include configuring days on which lessons are held [MDM-21632]
- Replace deprecated black and white list with deny and allow list for devices with iOS 15 or above [MDM-21670]
- Display more details for Android Enterprise app policy compliance violations [MDM-21728] [RS-7106]
- Optimize performance when saving education courses [MDM-21857]
- Always show the store organization in the tenant organization switcher [MDM-21935]
- Extend tooltip for allow simple password checkbox in Windows passcode configuration [MDM-21955]
- Display policy export report [MDM-19798]
- Improve handling of database exceptions [MDM-21432]
- Remove “Screen resolution”, “Phone” and “IMEI” and “Wi-Fi MAC” information from Windows device details since they are not available for Windows devices [MDM-21729] [MDM-21865] [MDM-21886]
- Extend hint shown in the Windows global proxies configuration [MDM-21832]
- Add label and url of “Add Shortcut” actions to tooltip in device action list [MDM-21870]
- Allow cancelling actions in “push sent” state for Apple devices [MDM-21873]
- Display day of week selection as a toggle button group [MDM-21903]
- Make sure the profile name of Windows VPN configurations is unique inside a single policy [MDM-21926]
- Make sure the SSID of Windows Wi-Fi configurations is unique in a policy [MDM-21926]
- Ensure that in case of multiple Windows Wi-Fi or VPN configurations with the same identifier only the one with the highest priority is applied on the device [MDM-21954] [MDM-21956] [MDM-21984]
- Improve display of battery level values [MDM-21931]
- Improve Windows BitLocker configuration and set additional fields validators [MDM-21939]
- Extend hint for iOS home screen layout configuration [MDM-21951] [RS-7503]
- Allow using the user’s email address as a placeholder in Windows email configuration [MDM-22009]

Für Version 26.4.0

Fixes

- Avoid prematurely verifying the MDM signature certificate as a side effect when retrieving it for the Apple MDM signature verification [MDM-22101]
- Make handling of challenge passwords cluster save even in scenarios without IP tables [MDM-22010]
- Truncate action comment field to ensure that the comment does not exceed the database limits [MDM-21924] [RS-7476]
- Fix VPP synchronization error on servers with more than 2,100 licenses when using Microsoft SQL Server [MDM-22027]
- Prevent deploying multiple Wi-Fi configurations with the same SSID on Apple devices [MDM-21743] [RS-7150]
- Prevent duplicated mails for rules when Relution runs as cluster [MDM-18737] [RS-4744]
- Prevent web-links from being added as required apps in Android app compliance configuration [MDM-20352] [RS-4523]
- Use the lesson schedule time zone when checking if a lesson can be started [MDM-21632]
- Handle delivery confirmed not as finished state for actions [MDM-21817]
- Prevent that Windows Wi-Fi configurations are applied on devices that do not have a Wi-Fi adapter attached [MDM-21834]
- Change app management on Windows 10 devices by using the user scope instead of the device scope [MDM-21841]
- Prevent deploying Windows apps that do not have a package family name [MDM-21847]
- Retrieving public app icons from Microsoft Store [MDM-21854]
- Fix copying of Apple Configurator 2 configuration from store organization to other organizations [MDM-21930]
- Remove password enabled checkbox from Windows passcode configuration [MDM-21955]
- Add missing validations for Windows passcode configuration [MDM-21955]
- Support all locales for Windows app store [MDM-22006]
- Prevent the cross-profile communication setting from being applied on Android Enterprise devices with an incompatible enrollment type [MDM-22016]
- Prevent uploading files that are not images in the app details screenshots and icon sections [MDM-21845]
- Display per app vpn section even if configuration is not editable [MDM-21862] [RS-7352]
- Fix checkbox states not being displayed correctly when removing policy from auto enrollments [MDM-21881] [RS-7389]
- Add enabled option for status bar handling in Android Enterprise Kiosk Mode configuration [MDM-21942]
- Fix a race condition that might lead into browsers default language being selected over the one selected in the user profile [MDM-21961]
- Remove emojis that are not processable for Windows configurations or actions [MDM-21838]

Für Version 26.4.0

Version 5.6.5

2022-11-09

Fixes

- Fix race condition on Shared Device sign in, causing the Relution app to incorrectly detect no user and ask for credentials again [MDM-22039] [RS-7561]

Version 5.6.4

2022-11-05

Updates

- Make the dynamic delay used in the MDM push queue configurable via `relution.push.queue` properties and adjust default values [MDM-22029]

Version 5.6.3

2022-11-03

Updates

- Optimize handling of events in various additional services in cluster environments [MDM-21947]

Version 5.6.2

2022-10-29

Updates

- Optimize handling of events in education service in cluster environments [MDM-21947]

Fixes

- Fix possible error in Apple MDM signature validation when multiple concurrent requests arrive at the same time [MDM-21958] [RS-7521]

Für Version 26.4.0

Version 5.6.1

2022-10-27

Fixes

- Fix broken Android Enterprise Work Profile enrollment which used an erroneous setting for personal usage since 5.6 [MDM-21944]

Version 5.6

2022-10-19

New

- Add enrollment setting to allow creating personal profiles on fully managed Android Enterprise devices [MDM-21800]
- Add Windows local device security policy [MDM-21284]
- Add *allow personal usage* setting for Android Enterprise enrollments [MDM-21716]
- Allow removal of teachers, when they are referenced in a lesson or lesson template [MDM-20712] [RS-5508] [RS-6810] [RS-5421]
- Allow custom separator for CSV files [MDM-21547] [RS-6781]
- Extend MDM signature validation for Apple devices [MDM-21639] [MDM-15205] [MDM-21212]
- Add support for Windows 10 to Secure Mail Gateway [MDM-20142] [MDM-20137] [MDM-21654] [MDM-21676]
- Allow configuring when to send push notifications to devices on compliance state changes [MDM-21542]

Updates

- Show cancel button always in the VPP token dialog [MDM-20732]
- Do not report Android Enterprise devices as non-compliant when a device reports an app as not installed with the reason in-progress [MDM-21607] [RS-6040]
- Recreate APNS client periodically to ensure a stuck client does not block push messages indefinitely [MDM-21612]
- Update APNS client to the latest version which fixes channel clean-up after exceptions [MDM-21612] [RS-6882]
- Update APK file parser to allow parsing of additional Android app configurations [MDM-21679] [RS-7102]
- Display a hint if the old password is not correct during password change request [MDM-21474]
- Optimize UI of Android Enterprise Kiosk Mode configuration [MDM-21646] [RS-7017] [RS-7018] [RS-7019] [RS-7020]
- Update text for Android Enterprise Wi-Fi restrictions to better describe what is being disabled [RS-7192]

Fixes

Für Version 26.4.0

- Fix updating devices via CSV [MDM-21652] [RS-7046]
- Never enforce Relution client single app mode for Apple Shared iPad devices since it is not supported [MDM-21672] [RS-7055]
- Do not block server startup until repo.relution.io could be reached [MDM-21475]
- Prevent that devices which are no longer matching the Secure Mail Gateway restrictions are sending additional requests to synchronize emails, contacts etc. [MDM-21668]
- Rename SMTP parameter TTLS to STARTTLS, but allow incorrect spelling for backwards compatibility [MDM-21674]
- Fixed a rare deadlock in pub/sub that could result in subscriptions no longer being polled [MDM-21717]
- Fix app upload with two different apps if the first upload was aborted [MDM-20916]
- Fix column alignments in several modals [MDM-21454]
- Do not ask for the old password of a user, when the system administrator or the organization administrator tries to override the password [MDM-21474]
- Clear all selected elements on all pages on hitting “clear selection” [MDM-21476]
- Set current start page explicitly to dashboard for the user when he accepts terms and conditions for the first time [MDM-21605]
- Set correct OS version filters in device inventory [MDM-21660]
- Deactivate prohibited actions on public policies in standard organizations [MDM-21693]
- Show a confirmation for successfully triggered deploy app actions [MDM-21706]
- Fix deploying Windows apps via the “Installed Apps” tab in device details [MDM-21706]
- Remove phone number validation in the user details [MDM-21735] [RS-7253]
- Do not affect the search result when clearing search values [MDM-21737]
- Fix saving of LDAP users without email address [MDM-21779] [RS-7164]
- Remove required validator on server proxy PAC URL field in tvOS WiFi [MDM-21858] [RS-7412]

Version 5.5.5

2022-10-11

Fixes

- Prevent a possible race condition for Shared iPads in guest mode leading to their action queue waiting until the next login [MDM-21804]

Version 5.5.4

2022-10-06

Updates

- Disable automatic update of iOS/iPadOS/tvOS managed apps for outdated management flags setting as a default. Can be enabled again by setting `relution.mdm.apple.verifyFlagRemoveAppsOnMdmProfileRemoval` to `true` [MDM-21487]

Für Version 26.4.0

Version 5.5.3

2022-09-30

Updates

- Always use device based Google accounts instead of user accounts when enrolling Android Enterprise devices to avoid the 10 devices per user limit [MDM-21733] [RS-6041]

Fixes

- Fix slow requests on systems with many Apple devices and profiles due to a missing database index [MDM-21739] [RS-7242]

Version 5.5.2

2022-09-24

Fixes

- Fix processing error if full sensor data or position estimate batches are completely outdated [BR-2416]

Version 5.5.1

2022-09-10

Fixes

- Fix an issue with Deploy and Remove App actions on Windows devices which are setting the action state to *Error* although the (de-)installation is still in progress [MDM-21610]

Version 5.5

2022-09-08

New

- Add support for certificate templates and user specific certificates to Android Enterprise Wi-Fi configuration [MDM-21304]
- Add kiosk mode configuration for Android Enterprise fully managed devices [MDM-19518] [MDM-19519]
- Add DNS settings configuration for iOS and macOS [MDM-21489] [RS-6167]
- Add macOS content caching configuration [MDM-21488]
- Add Windows wallpaper configuration [MDM-21273]
- Display known Apple product names in a readable format (e.g. iPhone 12 instead of iPhone13,2) [MDM-21231]
- Add new iOS 15 restrictions to iOS restrictions configuration [MDM-21431]
- Extend iOS and macOS device details with information about active user accounts [MDM-21495]

Für Version 26.4.0

Updates

- Use already existing Android Enterprise device if it matches the device identifier of a newly enrolled device [MDM-21434]
- Do not prevent data migration of managed apps on iOS and tvOS to new devices via device backup by disabling automated uninstallation on MDM profile removal [MDM-21487]
- Count delivered actions as open actions for devices [MDM-21527]
- Allow requested apps in released status in teacher console [MDM-21531] [RS-6744]
- Reduce logged warnings when fetching files on Microsoft SQL Server [MDM-21537]
- Clear device location data when lost mode is disabled [MDM-21561] [RS-6831]
- Extend list of known Windows editions [MDM-21608]
- Add filter for devices without a policy [MDM-21361]
- Show tooltip for Android Enterprise enrollment type if Android Enterprise is not set up [MDM-21478]
- Display homescreen layout editor by default [MDM-21519]
- Allow editing search field badges [MDM-21577]
- Add missing iOS 14.5 restrictions tooltips [MDM-21535]

Fixes

- Allow every user to access their home organization, even when not member of the “User” group [MDM-21153] [MDM-21385] [RS-6518] [RS-6650]
- Fix duplicate and missing history entries for Android Enterprise devices [MDM-21417]
- Fix app compliance configurations on Windows 10 devices which prevented other configuration within the same policy to be applied [MDM-21601]
- Fix deploying and removing certain apps on Windows 10 devices [MDM-21610]
- Fix pagination and sorting in the list “Devices with this app” [MDM-21536] [MDM-21552]
- Fix error when LDAP server does not return a group member attribute (e.g. Novell eDirectory) [RS-6874] [MDM-21571]
- Fix persisting pinning state of navigation bar [MDM-21352] [RS-6253] [RS-6424]
- Fix saving of Android Enterprise managed app configuration after filtering [MDM-21526]

Version 5.4.2

2022-08-26

Fixes

- Generated Wi-Fi payload for apple devices with type enterprise WPA2 and enterprise WPA3 [MDM-21562] [RS-6728]

Version 5.4.1

2022-08-11

Für Version 26.4.0

Updates

- Exclude empty bundles and arrays from managed app configurations for Android Enterprise [MDM-21473] [RS-6682]
- Improve rendering of Android Enterprise Managed App Configurations which do not follow Google’s specification [MDM-21472]

Version 5.4

2022-08-06

New

- Support bulk enrollments with provisioning packages for Windows devices [MDM-21110]
- Restrict allowed lesson time frame to lesson schedule when enabled in organisation settings [MDM-18332]
- Managed app configurations for Android Enterprise are now merged when multiple policies are applied [MDM-20962]
- Add 3 new fields to the iOS restriction configuration for iOS 14.5+ devices [MDM-21298]
- Verify whether iOS device has published policy versions applied when device refresh completes and update if needed [MDM-21302]
- Update device name and user via CSV upload in device inventory [MDM-21326] [RS-3906] [RS-4726] [RS-4870] [RS-6137] [RS-6363]
- Add Windows Antivirus configuration [MDM-20792]
- Add Windows Licensing configuration [MDM-21054] [MDM-21044]
- Add Windows version/edition badges for all actions and configurations [MDM-21182] [MDM-21291]
- Add iTunes ID and bundle identifier columns to purchased apps list [MDM-21296]
- Add filter in user list to filter by direct group memberships [MDM-21297]
- Add “created by” column in enrollment list [MDM-21354] [RS-6431]

Updates

- Reduce log messages on WARN level when fetching file content fails because of stream abortion [MDM-21263] [RS-5859]
- Allow update of MDM profile if device certificate is expired [MDM-21349]
- Extend “devices with this app” list in app details with columns containing general device information [MDM-21396]
- Display device serial number in basic device information [MDM-21362] [RS-6159]
- Adjust error code message to clarify that the action can not be cancelled any more as the device is already performing it [MDM-19686] [RS-4208]
- Merge first column and context menu in all table views [MDM-21305]
- Display the configuration name in the policy list of a device [MDM-21346] [RS-6425]
- Adjust color of app history comments to black instead of light grey [MDM-21370]
- Display restricted Play Store mode hint for Android Enterprise restrictions configuration [MDM-21416]
- Remove duplicate translation files from i18n folder [MDM-21436]
- Always re-apply policies on log in on Apple Shared iPad [MDM-21325] [RS-6375]

Für Version 26.4.0

Fixes

- Fixed a race condition for rules that could prevent scheduled actions from being canceled when a previously inactive device became active again [MDM-21113] [RS-6091]
- Creation of new policy versions no longer fails completely if a single configuration is invalid [MDM-21265] [RS-6268]
- Fixed an error that could leave a VPP sync in a zombie state when an error with a message too large to be logged occurred [MDM-21429] [RS-6597]
- Assigned user is now correctly cleared when an iOS device is enrolled as a shared device [MDM-21257]
- Ensure the latest published policy versions are assigned to device when re-apply policy is used [MDM-21302]
- Resolve performance issues when retrieving auto enrollments [MDM-21347] [RS-6396]
- Fix prefilling of password field in the web portal, when a password manager was used [MDM-21162]
- Pressing enter on username field during login did not perform a login attempt, when password is already filled [MDM-21163]
- Password reset view was still visible after being logged in [MDM-21248] [RS-6604]
- Re-add the option to create a policy version, if the current version is already published [MDM-21274]
- Disable all fields in Windows Wi-Fi configuration if it was published previously [MDM-21333]
- Set android enterprise fully managed device mode as default for Android Enterprise enrollments [MDM-21379]
- Display issues on information page of an Android Enterprise device [MDM-21415]

Version 5.3.3

2022-08-06

Updates

- Add support for JMX based analysis of cluster environments [MDM-21462]

Fixes

- Fix transaction borders when handling user saved events, and skip some handlers not necessary for newly created users [MDM-21458]

Version 5.3.2

2022-07-27

Fixes

- Adjust configuration of PKCS 12 key store generation on OpenJDK version 11.0.12 and above. The default settings have been changed in this OpenJDK version and the new defaults currently result in broken PKCS 12 archives which are not accepted by Apple devices [MDM-21410] [RS-6567]
- Make Google Cloud Pub/Sub use the system proxy again [MDM-21405] [RS-6489]

Für Version 26.4.0

Version 5.3.1

2022-07-22

Fixes

- Fix Android Enterprise devices having no assigned policies any more after being inactive [MDM-20628] [RS-6512] [RS-6208] [RS-6074] [RS-5332] [RS-5296]

Version 5.3

2022-07-09

New

- Allow resizing table columns and save them in user's preferences [MDM-21047] [MDM-21052] [MDM-21126]
- Display list of devices on which a specific app is installed [MDM-18611] [MDM-21142] [RS-5851]
- Support combining multiple app compliance configurations on Apple device [MDM-20551]
- Add app compliance configuration for Windows devices [MDM-20407]
- Add Samsung Classroom Management configuration [MDM-21118]
- Support app installation for lessons on Android Enterprise devices [MDM-21124] [MDM-21267]
- Add Shared iPad settings configuration [MDM-21232]
- Display a custom JSON which can be used to enroll KME devices via Android Enterprise in the QR code view and enrollment details [MDM-21258] [RS-6005]
- Ensure that policies are only applied on devices which are using the supported Windows edition and version [MDM-21237]
- Extend app selection options for remove app action [MDM-20971]
- Add Windows BitLocker configuration, which allows controlling disk encryption [MDM-21012]
- Allow to define the certificate store in Windows certificate configuration [MDM-21089]
- Add Windows Hello configuration [MDM-21136]
- Apply actions on multiple devices with a single bulk request [MDM-21046]

Updates

- Add wipe action for Android Enterprise fully managed devices [MDM-20955]
- Add VPP licensed information to apps list and app details [MDM-21227]
- Show available placeholders in certificate templates view [MDM-21228]
- Support groups in CSV import for classes [MDM-20633] [RS-3586] [RS-5009] [RS-5884]
- Add support to deploy and remove Windows public apps [MDM-21100]
- Check MariaDB version requirement for 10.3 or newer during startup [MDM-21112]
- Require to explicitly set a password for exiting the Android Kiosk mode [MDM-21211]
- Fail VPP sync immediately when token expired, send no network requests [MDM-21229]
- Extend model of lesson device with information about its platform and enrollment type [MDM-21320]
- Add new properties on Windows Start Menu configuration - start layout and edge assets [MDM-20873]
- Make Windows Update Auto-Update time a dropdown selection field [MDM-21058]
- Add context menu actions "Use default device name from DEP profile" and "Use auto-assigned policies" to auto enrollment list [MDM-21067] [RS-5966]
- Rename whitelist and blacklist to allow list and block list [MDM-21121]
- Add CSV export to Windows account action and improve user interface [MDM-21125]
- Update Windows Update Configuration to use the list of available Windows versions [MDM-21221]
- Ensure Relution iOS client is always allowed if Relution Shared Device Configuration is active, especially when conflicting app compliance settings are present [MDM-21268] [RS-6261]

Fixes

Für Version 26.4.0

- Android Enterprise devices no longer stay non-compliant when all violations have been resolved [MDM-20944] [RS-5943] [RS-6034] [RS-5771]
- Fix issue with per app VPN connections not being associated correctly [MDM-21111]
- The CORS preflight request (OPTIONS) now also responds with a HTTP 200 message for clients that do not provide credentials [BR-1710]
- Deleting apps and weblinks referenced in a lesson or lesson template [MDM-21135] [RS-6084]
- Fix enable state for new remote desktop service configurations [MDM-21180]
- Show the missing icon for new device action state DELIVERY_CONFIRMED [MDM-21189]
- Fix Windows Wi-Fi Configuration Open authentication type creation [MDM-21217]
- Fix add app modal not closing after uploading a new app using drag and drop [MDM-21218]
- Fix device name change validation in device inventory list and edit device page error messages [MDM-21235]
- Fix multi tenant file upload for non file endpoints [MDM-21276] [RS-6305]
- Fix Android Enterprise Work Profile device deletion [MDM-21286]
- Fix formatting of battery level in device inventory [MDM-21327] [RS-6397]
- Fix incorrect active task count shown in health indicator after deleting a VPP token [MDM-21301]
- Fix potential endless recursion in VPP sync when multiple pending requests fail to send [MDM-21301]

Version 5.2.4

2022-06-30

Updates

- Change policy publishing mechanism to run in its own thread pool instead of the global one [MDM-21285]

Für Version 26.4.0

Fixes

- Extend REST endpoint to reactivate Windows devices by changing the Device ID for active devices as well [MDM-21247] [RS-6231]
- Add missing Android Enterprise platform option to policy prioritisation [MDM-21272]

Version 5.2.3

2022-06-24

Fixes

- Add a new REST endpoint to reactivate Windows devices which were marked as deleted due to Device IDs used by multiple devices [MDM-21247] [RS-6231]

Version 5.2.2

2022-06-18

Fixes

- Fix Android Enterprise platform migration for no longer needed policy configurations linked to violations [MDM-21239]

Version 5.2.1

2022-06-16

Updates

- Add defining initial Android Enterprise policies to enrollments [MDM-21222]

Fixes

- Allow soft deletion also for expired certificates [MDM-21219]

Version 5.2

2022-06-11

Für Version 26.4.0

New

- Make Android Enterprise a separate device platform. Devices and policies including configurations are migrated to the new platform automatically [MDM-20819]
- Add managed app configuration editor for Android Enterprise [MDM-20724]
- Add Android Enterprise system update policy [MDM-19756]
- Add custom device variables [MDM-19888] [MDM-20970] [RS-2838] [RS-3662] [RS-4242] [RS-5019]
- Add configuration to persist enrollment user in device's custom property on enrollment [MDM-20556]
- Allow deleting certificates [MDM-20695] [RS-5915]
- Delete device actions automatically after a configurable period, default two years (730 days) [MDM-20907]
- Add client widget for desktop browsers [MDM-20959]
- Add information box to policy details [MDM-19940]
- Add information card to device details [MDM-20160]
- Add Windows Defender scan action [MDM-20405] [MDM-20422]
- Show Windows Defender Antivirus health data in device details [MDM-20798]
- Add Action to add local accounts on Windows devices [MDM-21056]

Updates

- Renew iOS App Store push certificate, the previous one will expire on December, 13th 2021 [MDM-20704]
- Renew iOS MDM push certificate, the previous one will expire on November, 17th 2021 [MDM-20704]
- Give all users “User” and “Device User” permissions regardless of group membership [MDM-18356]
- Required apps, which refer to non-installable system apps, are not taken into account during compliance status detection [MDM-20714] [RS-5441]
- Adjust off-time mode for iOS devices: Allow Settings app only for devices during off-time instead of activating lost mode as this allows to change Wi-Fi even during off-time. [MDM-20818] [RS-4630]
- Enable remove app action for tvOS and macOS devices [MDM-20956] [RS-5852]
- Allow triggering supervised device actions only on supervised devices [MDM-16290]
- Adjust translation and information for DEP profile allow pairing setting [MDM-20884]
- Display hint if selected VPN type does not support per app and account VPN connections [MDM-20957]
- Add auto-scroll to column selector drop list [MDM-20958]
- Hide unneeded checkboxes in Android app compliance [MDM-20966]
- Removed contacts and calendar from Windows Email configuration [MDM-20979]
- Change password field in the Windows Exchange configuration to no longer be required [MDM-20998]
- Update validation of Windows Update configuration [MDM-21058]
- Extend device state filter with the option to filter devices in status “withdraw pending” in device inventory [MDM-21070]
- Extend add app options to allow selecting from both standard Google Play and the Android Enterprise managed Play Store [MDM-21076]
- Optimize IOT license metric gathering [MDM-21186] [RS-5695]

Fixes

- Fix installation of .pkg files [MDM-20845] [RS-5571] [RS-5380]
- Remove non-optimal JPQL to query parent groups when native SQL is not available and use legacy implementation instead [MDM-21057]
- Fix adding of new members to existing courses during CSV import [MDM-21104] [RS-5974]
- Hide the option to enable Secure Mail Gateway in Exchange configuration for Windows [MDM-21093]
- Prevent error log message occurring in rare cases on system shutdown [BR-1417]
- Hide confusing warning on startup when LDAP is not configured [MDM-20692]
- Prevent education content synchronisation for manually triggered LDAP synchronisation if LDAP education synchronisation is not configured. [MDM-20896]
- Fix saving the user profile with an empty phone number [MDM-21033]
- Improve performance of user and device inventory when performing select or deselect actions [MDM-19991] [MDM-19992]
- Fix overlapping device name pattern for Windows 10 devices [MDM-20908]
- Ignore deprecated user preferences for dashboard [MDM-20918]
- Disable autofocus on auto deployment search field in users and groups edit view [MDM-20934]
- Display the collected ethernet MAC address on macOS [MDM-21006] [RS-5874]
- Fix deploy action name shown for Microsoft Store application [MDM-21013]
- Fix disabled next button in app selectors [MDM-21027]
- Fix row selection with single click on tablet size screens [MDM-21065] [RS-5968]
- Add missing translations in auto enrollment inventory [MDM-21066] [RS-5964]

Für Version 26.4.0

Version 5.1.4

2022-05-31

Updates

- Add network rate-limiter to pub/sub and increase stability on large instances [MDM-21083]
- Add ability to restore pub/sub subscriptions that were deleted (due to inactivity) [MDM-21071] [RS-5527]

Version 5.1.3

2022-05-26

Updates

- Support meta data update of public macOS apps [MDM-21084]

Fixes

- Meta data update of public apps not working in some cases [MDM-21084]

Version 5.1.2

2022-05-25

Updates

- Optimize pub/sub poll for large instances with support for parallel poll requests [MDM-21078]

Für Version 26.4.0

Version 5.1.1

2022-05-19

Updates

- Replace CTE and native SQL resource files with string constants to avoid issues on some Windows installations [MDM-21035]

Fixes

- Fix initial state of checkbox in Android Enterprise Play Store management configuration [MDM-21038]
- Fix update script that removes duplicate Content Manager groups, which could produce a contraint violation in rare cases [MDM-20936]
- Fix saving organization administrator group, which incorrectly reported the administrator member as missing, preventing modifications such as adding new administrators [MDM-21034] [RS-5916]
- Fix configuration of authentication types in Windows Wi-Fi configuration [MDM-21025] [RS-5893]
- Fix persisting the automatic assignment of policies when being edited [MDM-21030] [RS-5898]
- Add missing indicator for already used email addresses when editing the user profile of users created before Relution 5 [MDM-21031]

Version 5.1

2022-05-12

New

- Add support for uploading modern Windows apps [MDM-20953] [MDM-20739] [MDM-20790] [MDM-20917]
- Add deploying modern Windows apps to devices [MDM-20952] [MDM-20759] [MDM-19789]
- Add removing modern Windows apps from devices [MDM-20954] [MDM-20760] [MDM-19790]
- Add selecting public applications from Windows App Store [MDM-20145]
- Add Windows Update policy [MDM-20401]
- Automatically renew education CA certificates when they will expire in the next 180 days [MDM-19930]
- Add global proxy configuration for Android Enterprise [MDM-20080]
- Allow multiple restriction configurations on Apple devices [MDM-20162]
- Prevent modification of LDAP groups and system groups [MDM-20384]
- Optimize new native client version notifications in notification center [MDM-20510]
- Add Android Enterprise Play Store management configuration [MDM-20394]

Updates

- Add full support for installation of .pkg files on macOS devices [MDM-20845] [RS-5571] [RS-5380]
- Allow ignoring auto-assigned policies also for auto-enrollment [MDM-20717]
- Add automatic refresh of notification center [MDM-20555]
- Make all failing permission checks respond with a 401 (Unauthorized) instead of 403 (Forbidden) status when no valid authentication is provided [BR-996]
- Update connection date of Apple devices only on MDM communication [MDM-17936]
- Add possibility to perform partial downloads of resources [MDM-20380]
- Add support for custom client names to SAML2 registrations and support additional attribute value formats [MDM-20691]
- Prohibit changing the password of a user, when the user is managed by a 3rd party user management system [MDM-20719]
- Add optional configuration for automatic removal of completed VPP tasks older than a defined period of time [MDM-20795]
- Do not include hidden ping actions in open action count [MDM-20871] [RS-5611] [RS-5669]
- Replace several dropdown filters in device inventory with a list of selectable options [MDM-20509]
- Optimize translations in app compliance configurations [MDM-20543]
- Add installed apps selection list for remove app action [MDM-20550]
- Update certificate lists to the standard list style [MDM-20711]
- Add Windows platform in app release workflow [MDM-20713]
- Show user's groups and group members for content manager [MDM-20718]
- Update compliance violation views to the standard list style [MDM-20726]
- Check if email is available when editing user details on the profile page [MDM-20774]
- Remove Windows Update configuration from Windows restrictions policy configuration as it will be available as a standalone configuration [MDM-20825]
- Improve performance when loading auto deployments [MDM-20705]

Fixes

Für Version 26.4.0

- Fix VPP sanity check in cluster environments on server startup and optimize its performance [MDM-20795]
- Fix removal of organizations with VPP publications [MDM-19989]
- Fix extracting bundle identifier of .pkg files with a different format [MDM-20666] [RS-5571] [RS-5380]
- Retry on VPP token upload when Apple responds with a temporary error, to avoid a 422 HTTP status [MDM-19826] [RS-5145] [RS-4388]
- Fix refresh device info actions being marked as an error on Shared iPads, even if all available information could be retrieved successfully [MDM-20639] [RS-5520]
- Fix calculation of file sizes and hashes when using MongoDB based GridFS [MDM-20927]
- Ensure that Windows devices can be enrolled by using the Device User group instead of a specific user [MDM-20941]
- Do not enable the update OS button for tvOS devices if no update is available [MDM-20226]
- Move selection labels into search field in app selector modals [MDM-20706]
- Prevent issues with translations using the same property name from a translation file, e.g. *apps* [MDM-20755]
- Fix policy export when using special characters in the passcode [MDM-20786] [RS-5519]
- Show correct available storage space units for a Windows device [MDM-20789]
- Showing line breaks in reason why action buttons are disabled [MDM-20860]
- Fix enrolling Windows 10 devices again after they have already been enrolled on the server before [MDM-20975]

Version 5.0.3

2022-04-27

Fixes

- Fix handling of illegal characters in certificate file names on Windows platform [MDM-20877] [RS-5619]

Für Version 26.4.0

Version 5.0.2

2022-04-13

Fixes

- Fix important security issue, same as 4.79.4 [MDM-20765]
- Fix database update on Microsoft SQL Server [MDM-20771]

Version 5.0.1

2022-04-12

New

- Serve the new Relution portal directly in `/` and fully replace the legacy portal [MDM-19864] [MDM-20563]
- Add support for assigning multiple policies to a device [MDM-19741] [MDM-19742] [MDM-19743] [MDM-20440] [MDM-20449] [MDM-20440] [MDM-20507] [MDM-20450]
- Add support for managing Windows 10 devices [MDM-19781] [MDM-19782] [MDM-19784] [MDM-19785] [MDM-19789] [MDM-19790] [MDM-19871] [MDM-19874] [MDM-19875] [MDM-19876] [MDM-19877] [MDM-19878] [MDM-19879] [MDM-19883] [MDM-19884] [MDM-20063] [MDM-20383]
- Show all configurations of applied policies in device details, not only those with a compliance status [MDM-20507]
- Replace default policy with more versatile automatic assignment to all devices or specific users or groups[MDM-20446]
- Use the managed Google Play Store to select apps to add into the Relution app store when Android Enterprise is configured in the organization [MDM-20079]
- Add a setting to make enrollments reusable which allows enrolling multiple devices with a single enrollment [MDM-20087]
- Add configuring managed accounts to use a specific VPN on Apple devices [MDM-20128] [MDM-20128]
- Add configuring managed apps to use a specific VPN on iOS and tvOS devices [MDM-20136]
- Require email addresses of users to be unique on the system [MDM-20564]
- Add device name configuration for supervised Apple devices [MDM-20447]
- Add time zone configuration for supervised iOS and tvOS devices [MDM-20582]
- Add the “Skip passcode” option also to Android Enterprise Work Profile enrollments [MDM-20526]

Updates

- Require Java version 11 or higher and, when using MySQL, version 8.0 or higher [MDM-20564]
- Reset the database baseline for version 5. Version 4.79 is required before updating to version 5 [MDM-19865]
- Migrate Spring Boot to 2.4.2 which also supports running with Java 15 [MDM-19894]
- Move all API endpoints to the unified `/api/` path, the previous endpoints are redirected [MDM-19950] [MDM-19951]
- Make table list headers sticky [MDM-20679]
- Remove Development Hub [MDM-19868]
- Remove App Store Ratings [MDM-19870]
- Add “untrusted apps policy” to Android Enterprise restrictions, replacing deprecated unknown sources setting [MDM-19997] [RS-5029] [RS-4596] [RS-5230]
- Optimize retrieval of devices with many installed apps [MDM-20635]
- Reorder dashboard widgets [MDM-19565]
- Add logging in as organization admin context menu action to system organization list [MDM-20445]
- Change default visibility of the platform and enrollment type column in the device list as all devices now have an enrollment type [MDM-20557]
- The members of a course are now sorted alphabetically [MDM-20596]
- Replace legacy icons [MDM-20640]
- Adjusted app compliance configurations to new list design [MDM-20543]
- Adjusted auto deployment list to new list design [MDM-20644]
- Automatically disassociate VPP licenses on device deletion also for tvOS and macOS [MDM-20553]
- Hide the link into the device in VPP license details when the current user does not have the permissions to access it [MDM-20549]
- Clean Up Windows Mobile implementation [MDM-19979]

Fixes

Für Version 26.4.0

- Fix persisting LDAP referenced fields in user preferences that could accidently be removed [MDM-20399] [RS-4960]
- Fix a problem causing Relution to forget the policy assigned to Android Enterprise devices [MDM-20628] [RS-5296] [RS-5332]
- Fix cloning policies on systems with MS SQL Server [MDM-20579] [RS-4993]
- Add missing translations to paginator [MDM-20665]
- Remove the words *in progress* from app history titles [MDM-20654]
- Sort VPP apps by name in the device VPP license list [MDM-20175]
- Hide issued certificates in the certificate view as there is a separate view for them [MDM-20597]
- Link from app settings to app categories [MDM-20600]
- Fix various elements where the default font size was not honored [MDM-20641]
- Fix header in VPP lists breaking the table layout [MDM-20642]
- Fix VPP association modal layout [MDM-20646]
- Fix empty state when no version was found in the current release state [MDM-20647]

Für Version 26.4.0

Bekannte Probleme

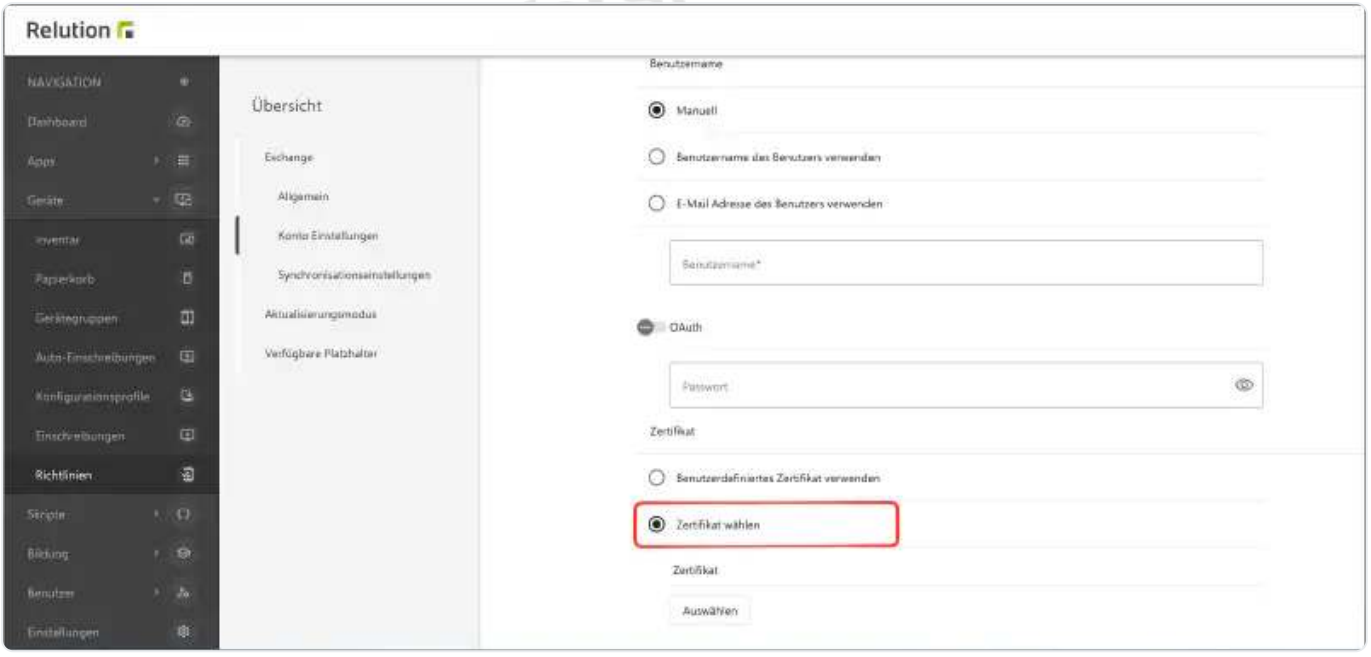
Exchange-Richtlinie: Kein Nutzerzertifikat des Subtyps Exchange

Beim Anwenden einer Richtlinie mit Exchange-Konfiguration schlägt die Aktion Richtlinie ändern in den Aktionen des Geräts fehl. Als Nachricht erscheint:

```
Mindestens eine Unteraktion ist fehlgeschlagen: ErrorCode: -, Message: Kein
Nutzerzertifikat des Subtyps Exchange für den Nutzer <Benutzername> gefunden.
```

Ursache ist die Einstellung Benutzerdefiniertes Zertifikat verwenden im Abschnitt Zertifikat der Exchange-Konfiguration. Mit dieser Option sucht Relution für den Benutzer des Geräts ein Nutzerzertifikat des Subtyps Exchange. Ist für den Benutzer kein solches Zertifikat vorhanden, kann das Konto nicht ausgerollt werden.

Lösung: In der angewendeten Exchange-Konfiguration wird im Abschnitt Zertifikat die Option Zertifikat wählen gesetzt. Ein Zertifikat muss dabei nicht ausgewählt werden; die Konfiguration kann direkt gespeichert werden.



Dasselbe gilt für die S/MIME-Zertifikate weiter unten in der Exchange-Konfiguration. Ist die S/MIME-Signierung bzw. -Verschlüsselung aktiviert, erscheinen dort die Abschnitte S/MIME Signierungszertifikat und S/MIME Verschlüsselungs-Zertifikat mit derselben Auswahl. Steht einer dieser Abschnitte auf Benutzerdefiniertes Zertifikat verwenden, sucht Relution zusätzlich ein Nutzerzertifikat des Subtyps S/MIME-Signierung bzw. S/MIME-Verschlüsselung, und die Aktion schlägt mit der entsprechenden Meldung fehl, wenn keines vorhanden ist. In diesem Fall wird auch in diesen Abschnitten die Option Zertifikat wählen gesetzt.

Weitere Informationen: Exchange-Konfiguration →

Kurzbefehle als Pflicht-App

Für die App `Kurzbefehle` wurde von Apple die Bundle-ID geändert. Das ältere VPP-Listing mit der Bundle-ID `is.workflow.my.app` lässt sich auf Geräten mit iOS 26 und neuer nicht mehr installieren, da iOS die Installation aktiv mit dem Fehler `AppBlacklisted` verweigert. Ist dieses ältere Listing in der Liste `Erforderliche Apps` hinterlegt, wird das Deployment fortlaufend neu angestoßen, ohne dass die Installation jemals erfolgreich abgeschlossen wird.

Typisches Fehlerbild:

- Betroffene iOS-Geräte werden im Geräte-Inventar als `nicht konform` angezeigt.
- Unter `Installierte Apps` ist `Kurzbefehle` korrekt vorhanden.
- Das Deployment der App startet wiederholt neu, wird aber nie erfolgreich abgeschlossen.
- Im Geräte-Log erscheint die Meldung `Diese App darf auf dieser Version des OS nicht mehr installiert werden.` zusammen mit dem Fehlercode `AppBlacklisted`.

Workaround: Die veraltete VPP-App mit der Bundle-ID `is.workflow.my.app` wird aus der Liste `Erforderliche Apps` entfernt und die zugehörige VPP-Zuweisung gelöscht.

> Die aktuelle App `Kurzbefehle` mit der Bundle-ID `com.apple.shortcuts` sollte derzeit nicht als Ersatz in die Liste `Erforderliche Apps` aufgenommen werden, da sie von Relution noch als nicht installierbare System-App behandelt wird. Fehlt `Kurzbefehle` auf einzelnen Geräten, kann die App stattdessen über die Verteilung von Apple-App-Store-Apps installiert werden (App-Store-Apps verwalten →).

Für Version 26.5.0

Update hängt bei GeneratedSelfSignedSignerKeyStore (Docker)

Bei Docker-Installationen mit veraltetem Host-Kernel kann das Update beim Erzeugen des selbstsignierten Signaturzertifikats (`GeneratedSelfSignedSignerKeyStore`) hängen bleiben.

Ursache und Lösung: Bekannte Fehlermeldungen der Docker-Installation →

Serverstart schlägt bei S3 mit selbstsigniertem Zertifikat fehl

Nach einem Update von einer Version vor 26.2 direkt auf Relution 26.4 oder neuer startet der Server nicht mehr, wenn der angebundene S3-Objektspeicher über TLS mit einem selbstsignierten oder unternehmensinternen Zertifikat erreichbar ist. Im Log erscheint folgender Fehler:

```
AccessDeniedException: software.amazon.awssdk.core.exception.SdkClientException: Unable
to execute HTTP request: (certificate_unknown) PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid
certification path to requested target (SDK Attempt Count: 3)
```

Ursache und Lösung — inklusive der erforderlichen erneuten Anmeldung aller Benutzer: Serverstart bei S3 mit selbstsigniertem Zertifikat →

Prometheus-Metriken werden nicht bereitgestellt

Seit Relution 26.4 wird aus Sicherheitsgründen standardmäßig nur der Health-Endpoint bereitgestellt; der Prometheus-Endpoint (`/actuator/prometheus`) ist deaktiviert. Ein Prometheus-Monitoring erhält daher keine Metriken, bis der Endpoint einmalig in der `application.yml` freigeschaltet wurde.

Ursache und Lösung: Prometheus-Metriken in Relution aktivieren →

Log-Level lassen sich nicht über das System-Portal ändern

Für Version 26.4.0

Seit Relution 26.4 wird aus Sicherheitsgründen standardmäßig nur der Health-Endpoint bereitgestellt. Das System-Portal zeigt daher nur noch den Bereich `Details`; die Bereiche `Logger`, `Environment`, `Metrics` und `Threads` erscheinen erst, nachdem die zugehörigen Endpoints einmalig in der `application.yml` freigeschaltet wurden. Unabhängig davon lassen sich Log-Level weiterhin über die Web API ändern.

Ursache und Lösung: Freischaltung der Actuator-Endpoints →

Datenbank-Update schlägt bei Update auf 26.1/26.2 fehl (MariaDB)

Beim Update von Relution 26.0.3 auf 26.1 oder 26.2 kann das automatische Datenbank-Update mit der Fehlermeldung `Cannot change column 'action_uuid': used in a foreign key constraint` fehlschlagen. Betroffen sind die MariaDB-Versionen 10.11.5–10.11.7 (bekanntes MariaDB-Problem).

Ursache und Lösung: Bekannte Fehlermeldungen bei Datenbank-Updates →

Fehler beim Update auf Relution 26.1

Nach einem Update auf Relution 26.1 startet der Docker-Container nicht mehr. Im Container-Log erscheint wiederholt folgender Fehler:

```
Exception in thread "main" java.lang.reflect.InvocationTargetException
Caused by: java.io.IOException: Permission denied
    at java.base/java.io.File.createTempFile(File.java:2184)
    at io.relution.boot.Main.checkTempDirectory(Main.java:291)
    at io.relution.boot.Main.main(Main.java:216)
```

Ursache und Lösung: Problem bei Update auf 26.1 →

OIDC + Entra ID

- Die OIDC-Authentifizierung mit Microsoft Entra ID wurde gemäß unserer Dokumentation neu konfiguriert. Die Konfiguration selbst ist korrekt, die Anmeldung funktioniert jedoch nicht direkt nach der Einrichtung. Benutzer erhalten nach der Anmeldung mit ihren Microsoft-Anmeldeinformationen eine Fehlermeldung:

Für Version 26.4.0

Lösung / Workaround

Erst nach einem Neustart des Relution-Servers funktioniert die OIDC-Anmeldung wie erwartet.

Backups mit iOS 26.4

- Beim Wiederherstellen von Backups von iOS 26.3 oder früher auf einem Gerät, auf dem iOS 26.4 installiert ist, geht der Status der Geräteverwaltung (Device Management) verloren.

Geteiltes iPad

- Auf Geteiltes iPad ist es seit iOS 26 nicht möglich, lokale Dateien zu erstellen oder abzuspeichern im Gast-Modus. Wir haben hierzu ein Case bei Apple eröffnet, um den Vorgang zu beschleunigen, gerne auch ein Case bei Apple anlegen → und unseren Support informieren.
  - Workaround: Dateien über eine angebundene Dateifreigabe erstellen und bearbeiten. paed.ML x Relution →

Apple ID Anmeldung

Das Problem ist von Apple mit iOS 26.2 gelöst.

- Anmeldung über System-Apps mit Apple ID möglich, obwohl in den Restriktionen Account modifizieren erlaubt deaktiviert ist.

Neue Apps

- Neue Apps und die Bundle IDs zum Blockieren
  - Preview → `com.apple.Preview`
  - Games → `com.apple.games`
  - Tipps → `com.apple.tips`

Für Version 26.4.0

Relution Agent 5.19.0

Das Problem (1) ist mit Relution Agent 5.19.2 gelöst. Die Version wurde von Apple freigegeben!

Aktuell gibt es mit dem Relution Agent in der Version 5.19.0 zwei Probleme.

1. Beim Login an Relution Shared Device kann es in einzelnen Fällen zu einem Fehler kommen. Dieser wird nach dem Login angezeigt. Die Fehlermeldung lautet `Bad state: Stream has already been listened to.`. Als Workaround kann einfach die Home-Taste auf dem iPad gedrückt werden. Der User sollte angemeldet sein und das Gerät normal nutzbar sein.

2. Im App Store werden alle Apps mit einem verfügbaren Update angezeigt. Hierbei handelt es sich um einen Anzeigefehler.

iOS Hintergrundbild

Das Problem ist von Apple mit iOS 18.5 gelöst.

Es gibt derzeit ein Problem mit der Bereitstellung von Hintergrundbildern. Das Problem kann auf allen iOS-Geräten auftreten, auf denen eine Richtlinie für Hintergrundbilder bereitgestellt wird. Das Problem kann nicht die ganze Zeit reproduziert werden, sondern tritt auf, wenn eine Richtlinienänderung auf dem Gerät erfolgt. Wir haben einen Workaround mit der Relution Server Version 5.29.1 erstellt, aber das Problem kann in einigen Fällen immer noch auftreten. Wir haben bereits ein Ticket bei Apple erstellt, um dieses Problem so schnell wie möglich zu lösen.

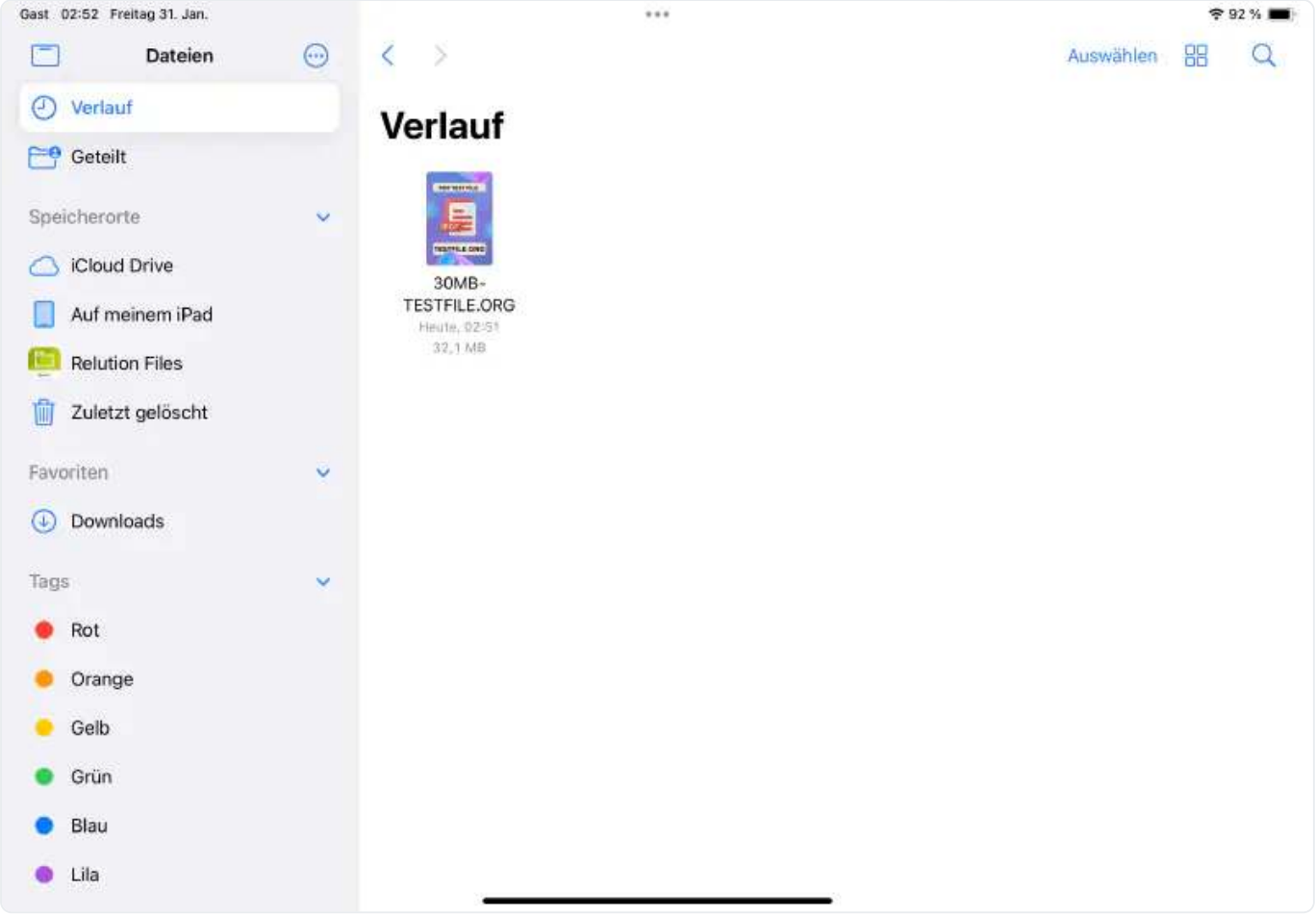
Die andere Lösung für das Problem wäre, eine Gerätegruppe zu erstellen, in der das Gerät nur für einen kurzen Moment ist und in der das Wallpaper bereitgestellt wird. Nach der Bereitstellung des Hintergrundbildes wird das Hintergrundbild nicht mehr vom Gerät entfernt, allerdings verschwindet dadurch die Richtlinie, die das Problem verursacht. Dies sollte nicht zu dem erwähnten Wallpaper-Problem führen.

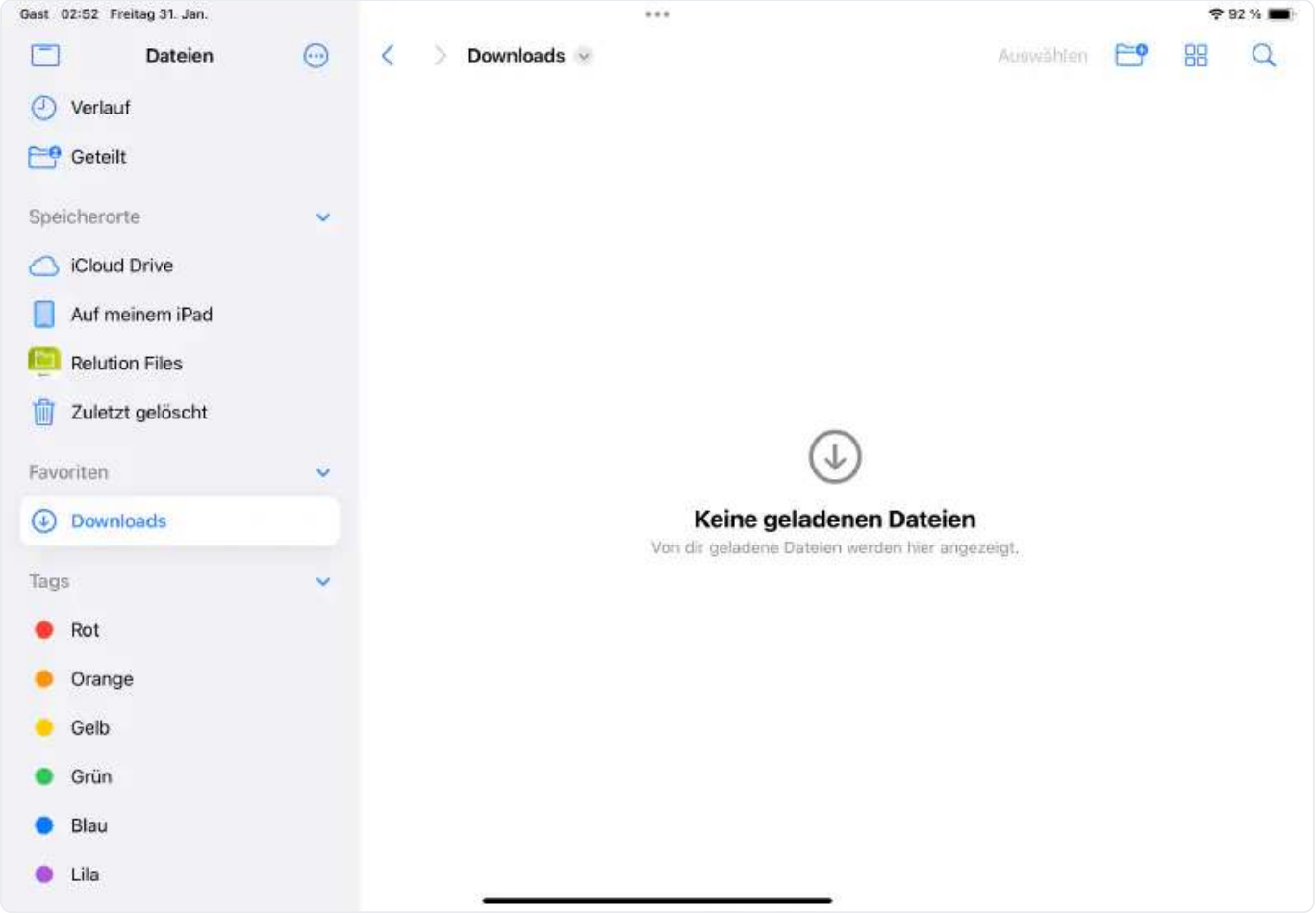
Apple Dateien App

Aktuell besteht ein Fehler in der Dateien-App auf Apple geteilten iPads (getestet mit iOS 18.2 und 18.3).

> Auf nicht geteilten Geräten funktionieren der Share und die Verwendung der Apple Dateien App.

Der Fehler macht sich auch dadurch bemerkbar, dass heruntergeladene Dateien im Downloads-Ordner fehlen. Wenn Daten geöffnet werden, sind diese bis zum Schließen und erneuten Öffnen der Apple-Files-App im Downloads-Ordner sichtbar.





Das Problem ist mit Relution Server 5.32 behoben. Hier kann in der Konfiguration für die Dateifreigaben ein neuer Parameter konfiguriert werden. Dazu die Art der Erweiterung von Modern auf Klassisch stellen.

Probleme mit SMB-Zugriffen in iOS 18

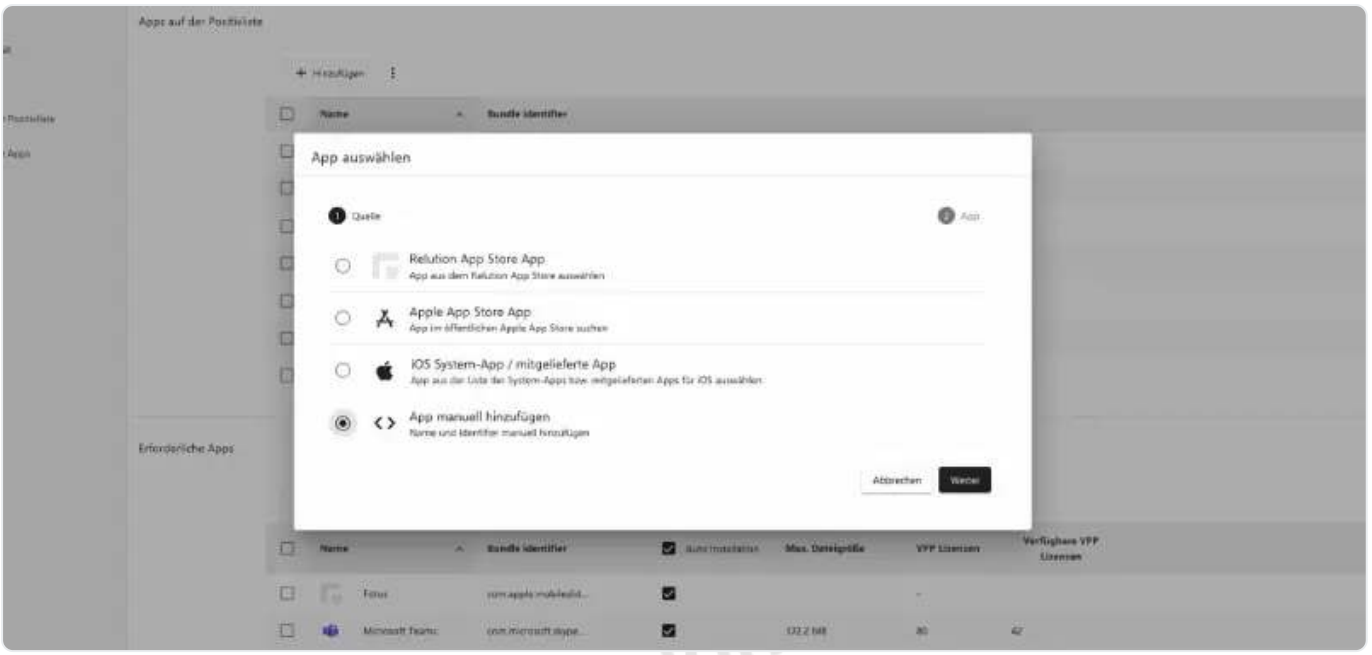
Mit iOS 18 gibt es aktuell ein bekanntes Problem, das beim Schreiben in SMB-Shares auftreten kann. Es handelt sich dabei um einen Fehler, der unabhängig von Relution auftritt und auf ein Problem innerhalb von iOS 18 selbst zurückzuführen ist. Apple ist sich dieses Problems bewusst, und wir empfehlen, die aktuellen Updates von Apple zu verfolgen, da eine Lösung möglicherweise mit einer zukünftigen iOS-Version bereitgestellt wird.

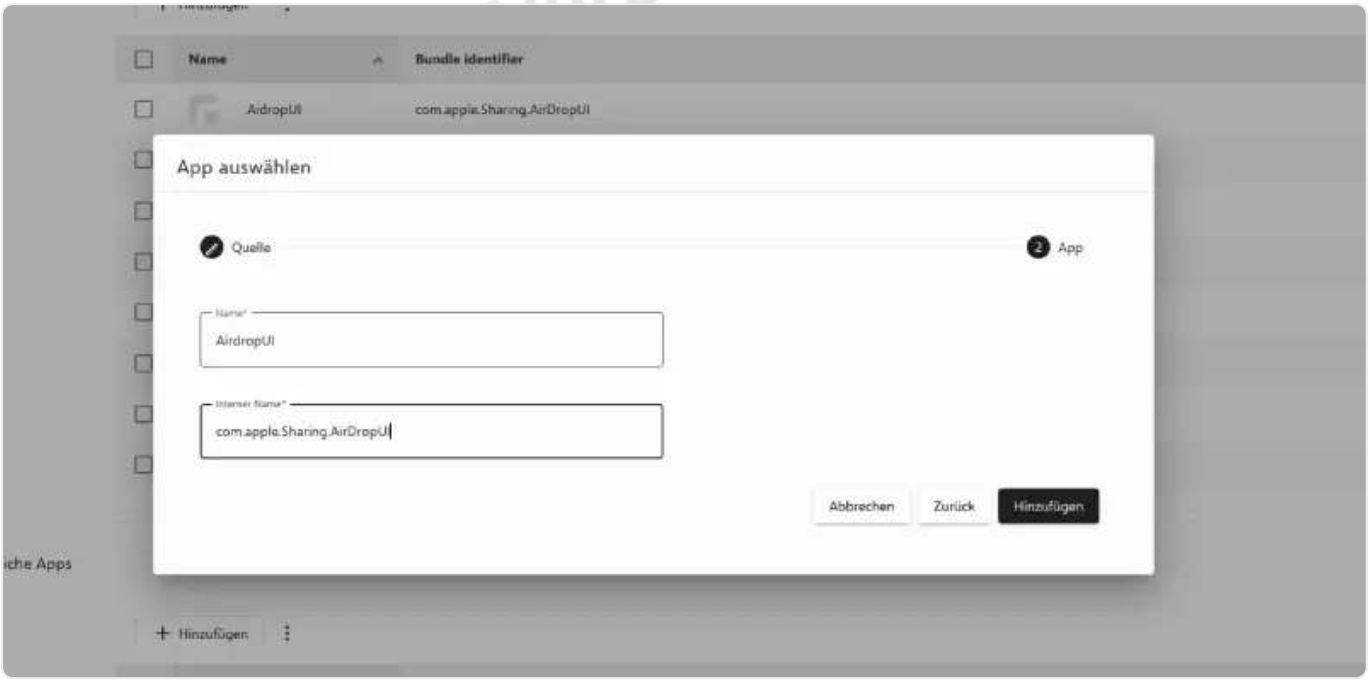
Airdrop

In iOS 18 kann es zu Schwierigkeiten mit Airdrop kommen, da der neue Bundle Identifier für das Airdrop-UI in der App-Konformität positiv hinterlegt werden muss. Der korrekte Identifier lautet:

```
com.apple.Sharing.AirDropUI
```

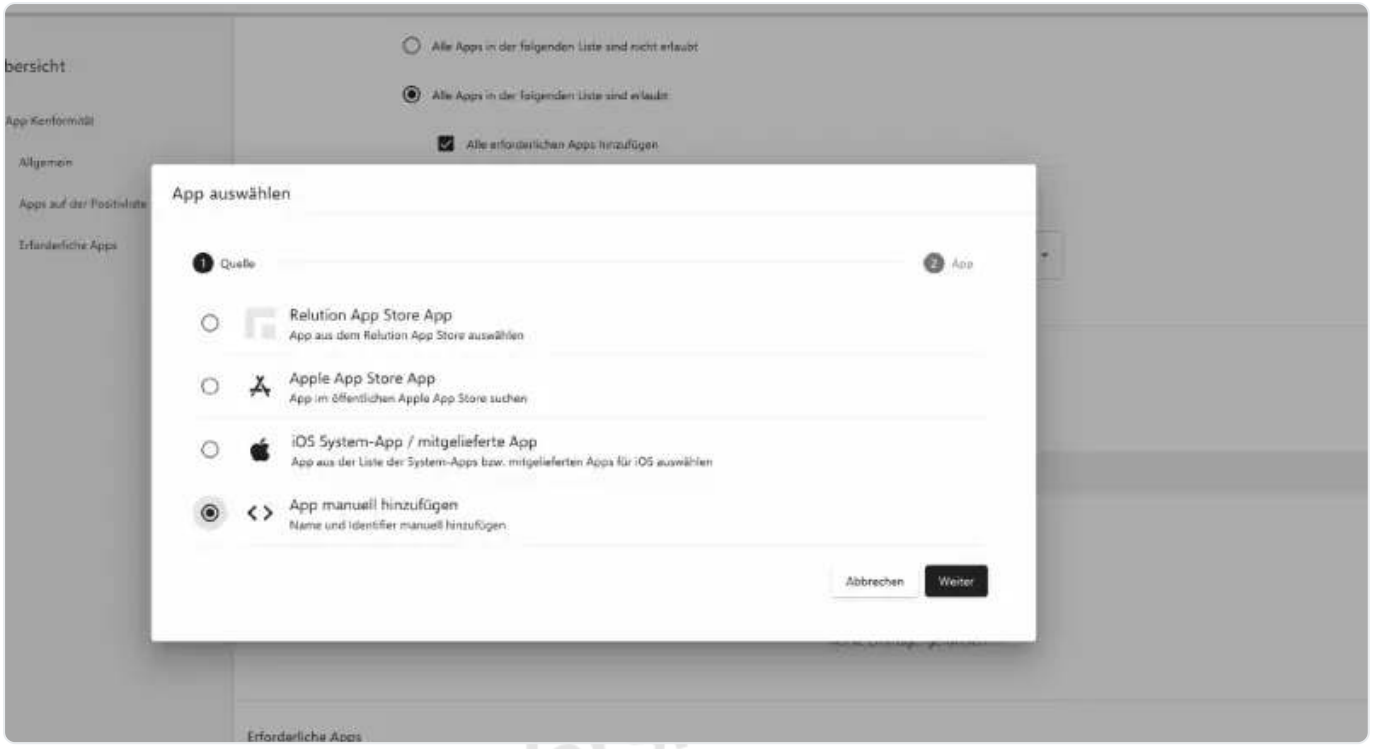
Es ist zu beachten, dass der Bundle Identifier case-sensitiv ist.

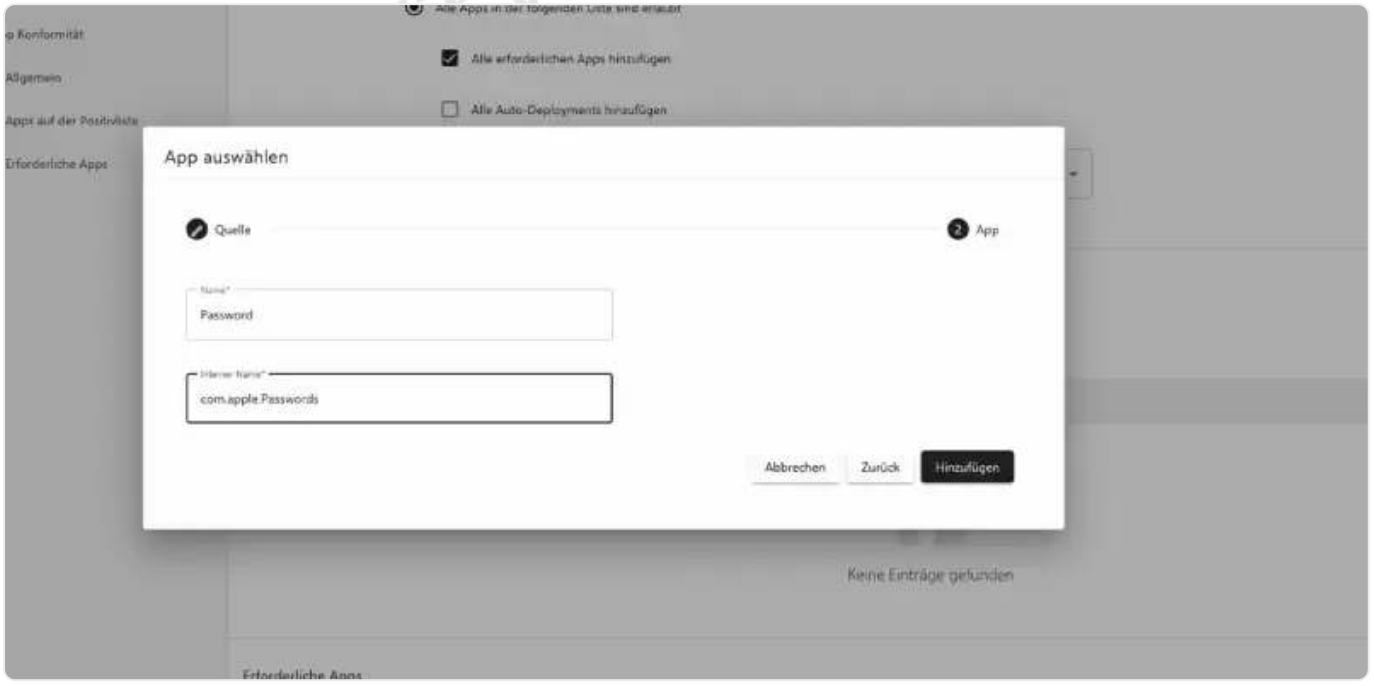




Passwort-App

Mit iOS 18 hat Apple eine neue System-App eingeführt, die als Passwort-Safe dient. Falls eine Positivliste freigegebener Apps über die App-Konformität definiert ist, muss auch hier der neue Bundle Identifier der Passwort-App hinterlegt werden, um sie korrekt zuzulassen.





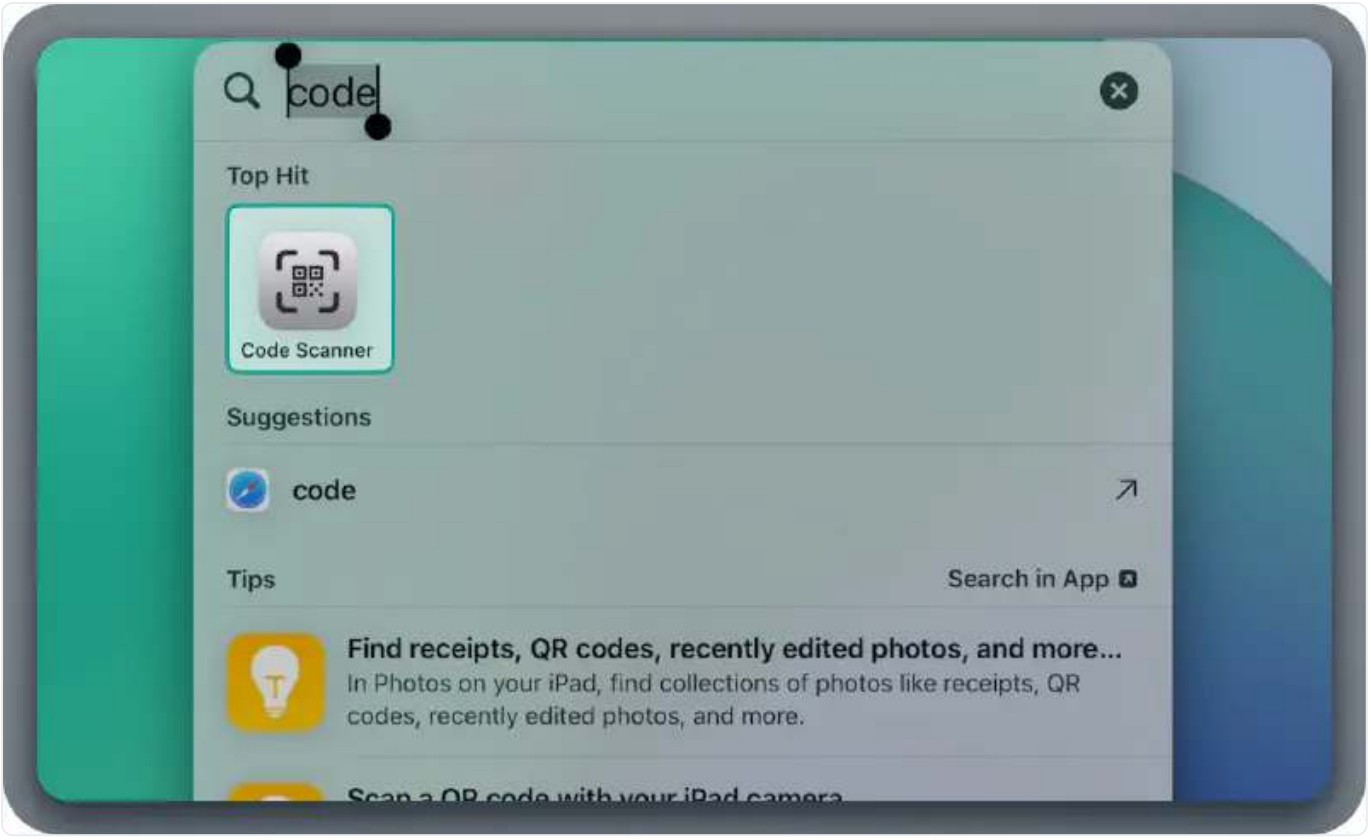
QR-Code-Scanner

Ein weiteres bekanntes Problem betrifft den QR-Code-Scanner in iOS 18 mit Geräten ab Generation 9. Hier wurde der Bundle Identifier verkürzt. Der aktuelle Identifier lautet:

```
com.apple.BarcodeScanner
```

Um dies zu beheben, muss in der App-Konformität die Positivliste manuell ergänzt werden. Der Name ist hierbei irrelevant; es ist lediglich wichtig, den oben genannten Bundle Identifier einzutragen.

Geräte kleiner Generation 9 müssen die separate App `Code Scanner` verwenden. Diese kann aufgerufen werden indem die Spotlight-Suche vom Homescreen aus von oben nach unten aufgerufen und nach `Code` gesucht wird.



Langsame Anmeldung bei geteilten iOS Geräten

Mit iOS 17.x bewirkt das Festlegen der Restriktionskonfiguration Synchronisierung des iCloud-Schlüsselbunds erlauben auf nein, dass die Anmeldung auf gemeinsam genutzten Geräten verlangsamt wird.

Um dieses Verhalten zu umgehen, muss in der angewendeten Restriktions-Konfiguration der Punkt Synchronisierung des iCloud-Schlüsselbunds erlauben auf ja gesetzt werden.

Fehlender Speicherplatz auf iOS Geräten

Auf iOS Geräten kann es trotz ausreichendem Speicher bei App-Installationen zu einem Hinweis kommen, dass nicht genügend Speicherplatz zur Verfügung steht. Dies wird auch entsprechend in den Systemeinstellungen angezeigt.

Das Problem entsteht durch die Anwendung der Richtlinienkonfiguration `Einstellungen geteiltes iPad`. Durch wiederholte An- und Abmeldungen von Gastbenutzern am geteilten Gerät kann es spontan zu diesem Fehler kommen.

Um das Auftreten dieses Problems zu vermeiden, empfiehlt es sich, die Richtlinie nicht zu verwenden. Alternativ sollten zumindest die beiden Punkte `Speicherplatzquota` und `Anzahl der Benutzer` vermieden werden.

Bei betroffenen Geräten ist es erforderlich, diese auf Werkseinstellungen zurückzusetzen.

Für Version 26.4.0

Schwachstellen-Offenlegung

1. Einleitung

Die Sicherheit unserer Produkte und Dienste sowie der Schutz der uns anvertrauten Kundendaten haben für Relution höchste Priorität. Unabhängige Sicherheitsforschende leisten einen wertvollen Beitrag, indem sie Schwachstellen aufdecken, die andernfalls unentdeckt bleiben könnten.

Diese Richtlinie beschreibt, wie sich autorisiert nach Schwachstellen suchen lässt, wie uns Erkenntnisse gemeldet werden können und was im Gegenzug von uns erwartet werden kann. Wir schätzen die Mitarbeit all jener, die in gutem Glauben dazu beitragen, unsere Plattform für alle sicherer zu machen.

Die Richtlinie kann von Zeit zu Zeit aktualisiert werden; Datum des Inkrafttretens und Versionsnummer werden dabei entsprechend angepasst. Vor Beginn der Tests bitte die jeweils aktuelle Fassung lesen.

2.1 Einbezogene Systeme

Für Version 26.4.0

Folgende Ressourcen fallen in den Geltungsbereich dieser Richtlinie:

- Die Relution-Plattform und die zugehörigen Dienste, die unter von Relution betriebenen Domains gehostet werden
- Von Relution unter `*.relution.io` betriebene Webanwendungen und Portale
- Die von Relution auf Docker Hub veröffentlichten Docker-Container
- Von Relution in offiziellen App Stores veröffentlichte mobile Anwendungen
- Öffentliche APIs, dokumentiert unter https://live.relution.io/web-api/index.html (Registrierung → erforderlich)
- Die Relution-Website → und zugehörige Webseiten wie der Relution Hub →

2.2 Ausgenommene Systeme

Folgende Ziele sind im Rahmen dieser Richtlinie nicht für Tests autorisiert:

- Relution-Software, die von unseren Kunden, Partnern oder Dritten betrieben wird
- Sonstige Systeme, Netzwerke oder Anwendungen unserer Kunden, Partner oder Dritter
- In unsere Plattform eingebundene Drittanbieterdienste (z. B. Zahlungsdienstleister, Identitätsanbieter, Analysedienste)
- Physische Räumlichkeiten und Einrichtungen der Relution GmbH

Falls unklar ist, ob ein Ziel in den Geltungsbereich fällt, bitte vor Beginn jeglicher Tests an security@relution.io → wenden.

3.1 Autorisierte Aktivitäten

Bei Einhaltung dieser Richtlinie sind folgende Aktivitäten ausdrücklich gestattet:

- Auswertung öffentlich zugänglicher Informationen zu unseren Systemen (z. B. DNS-Einträge, SSL-Zertifikate, öffentlich verfügbare Dokumentation)
- Tests auf gängige Schwachstellen in Webanwendungen (z. B. Injection-Schwachstellen, Authentifizierungsmängel, Zugriffskontrollprobleme, Sicherheitsfehlkonfigurationen)
- Untersuchung von API-Endpunkten auf Sicherheitslücken
- Analyse von clientseitigem Code, der über unsere Webanwendungen ausgeliefert wird
- Sofern die betreffenden Artefakte von Relution stammen und auf legitimem Weg über offizielle Distributionskanäle bezogen wurden:
  - Analyse von Docker-Containern und deren Inhalten
  - Reverse Engineering einschließlich Dekompilierung von mobilen Anwendungen sowie Java-Archiven und zugehörigen Klassendateien

---

3.2 Voraussetzungen für die Autorisierung

Um im Rahmen dieser Autorisierung zu handeln, ist Folgendes erforderlich:

1. In gutem Glauben handeln – mit dem alleinigen Ziel, Sicherheitslücken zu identifizieren und zu melden
2. Schäden minimieren: Handlungen vermeiden, die die Verfügbarkeit von Systemen, die Datenintegrität oder andere Nutzende beeinträchtigen könnten
3. Bei Entdeckung abbrechen: Sobald das Vorhandensein einer Schwachstelle bestätigt ist, weitere Tests einstellen und die Erkenntnisse melden; die Auswirkung nicht durch Zugriff auf weitere Daten oder Systeme demonstrieren
4. Daten schützen: Nicht auf Daten anderer Nutzender zugreifen und diese nicht kopieren, verändern oder löschen; bei versehentlichem Zugriff auf solche Daten sofort abbrechen, die Daten nicht speichern oder teilen und den Vorfall im Bericht vermerken
5. Vertraulichkeit wahren: Keine Details zu Schwachstellen an Dritte weitergeben, bevor wir angemessen Gelegenheit hatten, das Problem zu beheben, und eine koordinierte Offenlegung vereinbart wurde

Für Version 26.4.0

3.3 Untersagte Aktivitäten

Folgende Methoden und Verhaltensweisen sind unter keinen Umständen gestattet – auch nicht gegenüber einbezogenen Systemen:

- Jede Form von Social Engineering, Phishing, Vishing, Pretexting oder vergleichbaren Methoden gegenüber Beschäftigten oder Nutzenden von Relution
- Physisches Eindringen oder Versuche, sich physisch Zugang zu verschaffen
- Denial-of-Service-Angriffe (DoS/DDoS) oder Tests, die auf eine Beeinträchtigung der Dienstverfügbarkeit abzielen
- Automatisierte Schwachstellenscans in einem Umfang oder einer Häufigkeit, die die Systemleistung beeinträchtigen könnten
- Zugriff auf, Herunterladen oder anderweitiges Abgreifen von Kundendaten, personenbezogenen Daten oder vertraulichen Geschäftsinformationen
- Verändern oder Löschen von Daten in jeglichen Systemen
- Hochladen von Schadcode, Hintertüren oder Mechanismen für dauerhaften Zugriff
- Versuche, ausgehend von einer entdeckten Schwachstelle auf weitere Systeme oder Daten zuzugreifen
- Spam oder unaufgeforderte Massennachrichten
- Weitergabe von Zugangsdaten, Schwachstellendetails oder Proof-of-Concept-Code an Dritte
- Öffentliche Offenlegung von Schwachstellen, bevor eine koordinierte Offenlegung vereinbart wurde

---

4. Rechtliche Position

Gegenüber Sicherheitsforschenden, die diese Richtlinie vollständig einhalten, verpflichtet sich Relution:

- Keine zivilrechtlichen Schritte einzuleiten für Aktivitäten, die im Einklang mit dieser Richtlinie durchgeführt wurden
- Keine Strafanzeige zu erstatten für Aktivitäten, die im Einklang mit dieser Richtlinie durchgeführt wurden
- In gutem Glauben zusammenzuarbeiten bei der Bearbeitung gemeldeter Schwachstellen
- Auf Anfrage eine Autorisierungsbestätigung auszustellen, damit Forschende ihren Status vor Beginn der Tests dokumentieren können

Diese Richtlinie stellt eine Autorisierung durch Relution als Betreiberin der in Abschnitt 2.1 beschriebenen Systeme dar. Wir haben sie in gutem Glauben erstellt, um Forschende zu schützen, die ebenfalls in gutem Glauben handeln.

Diese Richtlinie kann und wird jedoch keine Immunität vor strafrechtlicher Verfolgung gewährleisten. Wir empfehlen daher dringend, alle Aktivitäten sorgfältig zu dokumentieren und bei Bedenken vor Beginn der Tests eine schriftliche Autorisierungsbestätigung bei uns einzuholen.

5. Verwendung personenbezogener Daten

Die im Rahmen der Schwachstellenmeldung übermittelten personenbezogenen Daten werden ausschließlich zur Untersuchung und Behebung der Schwachstelle verwendet und unterliegen den datenschutzrechtlichen Bestimmungen der Datenschutz-Grundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG).

Für Version 26.4.0

6.1 Meldung einreichen

Schwachstellenberichte bitte per PGP-verschlüsselter E-Mail senden an: security@relution.io →

Unser öffentlicher PGP-Schlüssel ist unter keys.openpgp.org → abrufbar. Der Fingerabdruck lautet: `3594163819E19D4D9FDA35F78BDAB6171E0A12DF`.

Darüber hinaus pflegen wir eine security.txt →.

6.2 Inhalt des Berichts

Damit wir das Problem rasch nachvollziehen und beheben können, bitten wir um folgende Angaben:

- Beschreibung der Schwachstelle und ihrer möglichen Auswirkungen
- Betroffene Systeme: URLs, Anwendungsnamen, Versionsnummern sofern zutreffend
- Schrittweise Reproduktionsanleitung
- Proof of Concept: Screenshots, Protokolle oder Codebeispiele, die die Schwachstelle belegen (ohne echte Nutzerdaten)
- Eigene Einschätzung zu Schweregrad und möglichen Auswirkungen
- Kontaktdaten für Rückfragen (pseudonyme Angaben sind möglich)
- Versehentlich eingesehene sensible Daten: Bei unbeabsichtigtem Zugriff auf personenbezogene oder vertrauliche Daten bitte das Gesehene beschreiben, ohne die Daten selbst aufzuführen

Berichte können auf Deutsch oder Englisch eingereicht werden.

6.3 Was der Bericht nicht enthalten sollte

- Keine tatsächlichen Kundendaten, personenbezogenen Daten oder Zugangsdaten beifügen
- Auf schadhafte Payloads oder funktionsfähigen Exploit-Code verzichten, der bei unsachgemäßer Handhabung Schaden verursachen könnte

7. Reaktion und Offenlegung

Nach Eingang des Berichts bestätigen wir den Empfang innerhalb von fünf Werktagen und beginnen mit der Validierung und Einstufung der gemeldeten Schwachstelle.

Für die Behebung wird angemessene Zeit benötigt: Wir bitten um eine Frist von mindestens 90 Tagen ab der Erstmeldung vor einer öffentlichen Offenlegung. Dies gibt uns Gelegenheit, das Problem zu validieren und zu beheben, die Korrektur zu verifizieren und auf allen Systemen bei allen Kunden auszurollen.

Bei Bedarf setzen wir uns über die etablierten Kanäle mit der meldenden Person in Verbindung, um zusätzliche Informationen einzuholen. Über den Fortschritt der Untersuchung und Behebung wird informiert.

Wird die Schwachstelle bestätigt, vergeben wir eine interne `RVD`-Kennnummer, die in der weiteren Kommunikation und in späteren Sicherheitshinweisen → als Referenz dient.

Nach Behebung der Schwachstelle werden Zeitpunkt und Details der Offenlegung gemeinsam mit der meldenden Person abgestimmt.

Für Version 26.4.0

8. Anerkennung und Vergütung

Wir betreiben derzeit kein monetäres Bug-Bounty-Programm. Die Einführung eines solchen Programms ist für die Zukunft nicht ausgeschlossen; diese Richtlinie wird in diesem Fall entsprechend aktualisiert.

Forschende, die im Einklang mit dieser Richtlinie eine bestätigte Schwachstelle melden, haben derzeit Anspruch auf:

- Öffentliche Anerkennung auf unserer Seite für Sicherheitshinweise → (mit Zustimmung der meldenden Person)
- Namentliche Erwähnung in Sicherheitshinweisen zur gemeldeten Schwachstelle (mit Zustimmung der meldenden Person)
- Ein Dankesschreiben, das sich für berufliche Portfolios eignet (auf Anfrage)

Anhang: Beispiele für Schwachstellen

Die folgenden Beispiele sollen veranschaulichen, welche Arten von Schwachstellen in den Geltungsbereich dieser Richtlinie fallen und welche nicht.

Qualifizierende Schwachstellen

- Remote Code Execution
- SQL-Injection und andere Injection-Schwachstellen
- Fehler in der Authentifizierung oder Sitzungsverwaltung
- Umgehung von Autorisierungsmechanismen und Rechteausweitung
- Cross-Site Scripting (XSS) mit nachgewiesener Auswirkung
- Cross-Site Request Forgery (CSRF) mit nachgewiesener Auswirkung
- Offenlegung sensibler Daten
- Sicherheitsfehlkonfigurationen mit erkennbarer Auswirkung
- Server-Side Request Forgery (SSRF)
- Unsichere direkte Objektreferenzen

Nicht qualifizierende Meldungen

Folgende Punkte gelten in der Regel nicht als qualifizierende Schwachstellen:

- Schwachstellen, die physischen Zugriff auf das Gerät eines Nutzenden erfordern
- Schwachstellen in Anwendungen oder Diensten von Drittanbietern
- Social-Engineering-Angriffe
- Denial-of-Service-Schwachstellen (bitte dennoch melden; aufgrund der Testbeschränkungen sind sie im Rahmen dieser Richtlinie jedoch nicht anerkennungsfähig)
- Durch automatisierte Scanner identifizierte Probleme ohne nachgewiesene Ausnutzbarkeit
- Fehlende Sicherheitsheader ohne nachgewiesene Auswirkung
- Clickjacking ohne nachgewiesene sicherheitsrelevante Aktion
- Self-XSS (Skriptausführung nur in der eigenen Sitzung möglich)
- CSRF bei nicht sicherheitsrelevanter Funktionalität
- Offenlegung nicht sensibler Informationen
- Offenlegung von Softwareversionen ohne zugehörige Schwachstelle
- Theoretische Schwachstellen ohne Proof of Concept
- Bereits bekannte oder zuvor gemeldete Schwachstellen

Für Version 26.4.0

Sicherheitshinweise

Diese Seite bietet eine Übersicht über Sicherheitslücken, die in unseren Produkten identifiziert wurden – einschließlich der internen RVD-Kennnummer, zugehöriger CVE-Kennungen (sofern vorhanden) und detaillierter Informationen zur Offenlegung. Wir folgen einem Verfahren zur koordinierten Offenlegung von Schwachstellen → und veröffentlichen vollständige Hinweise, sobald Patches verfügbar sind und das vereinbarte Offenlegungsfenster abgelaufen ist. Unser Ziel ist es, Transparenz zu schaffen, sichere Deployments zu unterstützen und unseren Kunden zu helfen, ihre Systeme durch regelmäßige Aktualisierungen geschützt zu halten.

Der Newsletter → informiert über Schwachstellen und andere wichtige Informationen.

Das Verfahren wird ab 2026 eingeführt; Hinweise, die in dessen Rahmen erstellt werden, veröffentlichen wir auf dieser Seite.

RVD-2026-6: Unauthentifizierter Zugriff im Relution Server

Angabe	Wert
Kennung	`RVD-2026-6`
CVE	nicht vergeben
Betroffene Komponente	Relution Server
Betroffene Versionen	bis `26.5.3`
Behoben in	`26.5.4`
Veröffentlicht	20.10.2026
Status	Update verfügbar

Relution Server 26.5.4 behebt eine Schwachstelle, die Zugriff ohne vorherige Authentifizierung ermöglichen kann.

Wir empfehlen allen Kunden mit On-Premises-Installationen, zeitnah auf Version **`26.5.4`** oder neuer zu aktualisieren.

Alle von Relution betriebenen Cloud-Instanzen wurden bereits aktualisiert; für Cloud-Kunden sind keine Maßnahmen erforderlich.

Weitere technische Einzelheiten veröffentlichen wir an dieser Stelle, sobald das Update breit ausgerollt ist.

RVD-2026-5: Brute-Force-Schwachstelle im Relution Server

Angabe	Wert
Kennung	`RVD-2026-5`
CVE	nicht vergeben
Betroffene Komponente	Relution Server
Betroffene Versionen	bis `26.5.1`
Behoben in	`26.5.2`
Veröffentlicht	19.10.2026
Status	Update verfügbar

Relution Server 26.5.2 behebt eine Schwachstelle, die unbefugten Zugriff durch automatisiertes Ausprobieren (Brute-Force) ermöglichen kann.

Wir empfehlen allen Kunden mit On-Premises-Installationen, zeitnah auf Version **`26.5.2`** oder neuer zu aktualisieren.

Alle von Relution betriebenen Cloud-Instanzen wurden bereits aktualisiert; für Cloud-Kunden sind keine Maßnahmen erforderlich.

Weitere technische Einzelheiten veröffentlichen wir an dieser Stelle, sobald das Update breit ausgerollt ist.

Für Version 26.4.0

RVD-2026-4: Schwachstelle beim Datenbankzugriff im Relution Server

Angabe	Wert
Kennung	`RVD-2026-4`
CVE	nicht vergeben
Betroffene Komponente	Relution Server
Betroffene Versionen	bis `26.5.2`
Behoben in	`26.5.3`
Veröffentlicht	16.10.2026
Status	Update verfügbar

Für Version 26.4.0

Relution Server 26.5.3 behebt eine Schwachstelle, die authentifizierten Benutzern unbefugten Zugriff auf Datenbankinhalte ermöglichen kann.

Wir empfehlen allen Kunden mit On-Premises-Installationen, zeitnah auf Version **`26.5.3`** oder neuer zu aktualisieren.

Alle von Relution betriebenen Cloud-Instanzen wurden bereits aktualisiert; für Cloud-Kunden sind keine Maßnahmen erforderlich.

Weitere technische Einzelheiten veröffentlichen wir an dieser Stelle, sobald das Update breit ausgerollt ist.

RVD-2026-3: Codeausführung im Relution Server

Angabe	Wert
Kennung	`RVD-2026-3`
CVE	nicht vergeben
Betroffene Komponente	Relution Server
Betroffene Versionen	bis `26.5.2`
Behoben in	`26.5.3`
Veröffentlicht	16.10.2026
Status	Update verfügbar

Relution Server 26.5.3 behebt eine Schwachstelle, die authentifizierten Benutzern unter bestimmten Umständen das Ausführen von Code ermöglichen kann.

Wir empfehlen allen Kunden mit On-Premises-Installationen, zeitnah auf Version **`26.5.3`** oder neuer zu aktualisieren.

Alle von Relution betriebenen Cloud-Instanzen wurden bereits aktualisiert; für Cloud-Kunden sind keine Maßnahmen erforderlich.

Weitere technische Einzelheiten veröffentlichen wir an dieser Stelle, sobald das Update breit ausgerollt ist.

Für Version 26.4.0

RVD-2026-2: Berechtigungsproblem im Relution Server

Angabe	Wert
Kennung	`RVD-2026-2`
CVE	nicht vergeben
Betroffene Komponente	Relution Server
Betroffene Versionen	bis `26.5.2`
Behoben in	`26.5.3`
Veröffentlicht	16.10.2026
Status	Update verfügbar

Relution Server 26.5.3 behebt eine Schwachstelle, die authentifizierten Benutzern unbefugten Zugriff ermöglichen kann.

Wir empfehlen allen Kunden mit On-Premises-Installationen, zeitnah auf Version **`26.5.3`** oder neuer zu aktualisieren.

Alle von Relution betriebenen Cloud-Instanzen wurden bereits aktualisiert; für Cloud-Kunden sind keine Maßnahmen erforderlich.

Weitere technische Einzelheiten veröffentlichen wir an dieser Stelle, sobald das Update breit ausgerollt ist.

Für Version 26.4.0

RVD-2026-1: Berechtigungsproblem im Relution Server [REL-13078]

Angabe	Wert
Kennung	`RVD-2026-1`
CVE	nicht vergeben
Betroffene Komponente	Relution Server
Betroffene Versionen	`5.32` - `26.4.1`
Behoben in	`26.4.2`
Veröffentlicht	13.08.2026
Status	Update verfügbar

Für Version 26.4.0

Relution Server 26.4.2 behebt ein Berechtigungsproblem, das authentifizierte Benutzer betreffen kann.

Wir empfehlen allen Kunden mit On-Premises-Installationen, zeitnah auf Version **`26.4.2`** oder neuer zu aktualisieren.

Alle von Relution betriebenen Cloud-Instanzen wurden bereits aktualisiert; für Cloud-Kunden sind keine Maßnahmen erforderlich.

Weitere technische Einzelheiten veröffentlichen wir an dieser Stelle, sobald das Update breit ausgerollt ist.

Sicherheitsoptimierungen

Relution ist ein mächtiges Werkzeug, mit dem Anwendende teilweise große Berechtigungen auf verwalteten Geräten haben. Daher sollte das System bestmöglich vor Fremdzugriff geschützt werden. Das Relution Portal lässt sich an verschiedenen Stellen mit eingebauten Funktionen sicherheitstechnisch optimieren. Hinzu kommt die gezielte Verteilung von notwendigen Berechtigungen.

Sicheres Kennwort verwenden

Wird ein neues Benutzerkonto in Relution angelegt, wird hier ein komplexes Kennwort vorgeschlagen. Dies kann übernommen oder auch abgeändert werden. Auf jeden Fall darauf achten, sich an die Komplexitätsempfehlung des BSI → zu halten.

Zweiten Faktor zur Authentifizierung hinzufügen

Relution unterstüzt die Anmeldung mit einem zweiten Faktor. Dies müssen Benutzer:Innen für ihren eigenen Account selbst konfigurieren. Hierzu oben rechts auf `Benutzername` → `Profil` klicken. Dort kann ein MFA-Token für eine Authenticator App oder eine E-Mail Verifizierung hinterlegt werden. Diese Funktion auf jeden Fall nutzen!

Für Version 26.4.0

Access Token verwenden

In Relution kann ebenfalls im Profil des Userkontos ein Access Token für die Nutzung der API hinterlegt werden. Dieses Token bietet den Vorteil, dass in Skripten keine Username/Passwort Kombination im Klartext hinterlegt werden müssen. Zudem kann das Token mit einem Ablaufdatum versehen werden, um sicherzustellen, dass es nicht länger aktiv ist als wirklich notwendig.

IP-Zugriffsregeln & Fail2Ban konfigurieren

In der Global Organisation kann unter `Einstellungen` → `Systemsicherheit` sowohl IP-Zugriffsregeln als auch Fail2Ban konfiguriert werden.

Damit lässt sich z. B. festlegen, dass eine IP-Adresse nach einer bestimmten Anzahl fehlgeschlagener Loginversuche (z. B. 10) für einen Zeitraum gesperrt wird.

IP-Zugriffsregeln steuern grundsätzlich, von welchen IP-Adressen oder Netzwerken aus eine Anmeldung erlaubt oder blockiert wird. Dabei können sowohl einzelne IPs als auch ganze Bereiche definiert werden.

> Vor der Konfiguration sollte geprüft werden, mit welcher eigenen IP-Adresse die Verbindung zum Server erfolgt, um ein versehentliches Aussperren zu vermeiden.

Bedeutung der Statuswerte

Erlaubt

- Anmeldung ist aktuell möglich
- Wird automatisch gesetzt, sobald ein Anmeldeversuch erfolgt (auch bei fehlgeschlagenen Versuchen)
- Dient hauptsächlich der Übersicht und Protokollierung

Dauerhaft erlaubt

- IP-Adresse ist explizit freigegeben
- Hat Vorrang vor anderen Regeln
- Bleibt dauerhaft bestehen
- Empfohlen für vertrauenswürdige Standorte (z. B. Büro oder VPN)

Blockiert

- IP-Adresse ist vorübergehend gesperrt
- Kann jederzeit wieder freigegeben werden

Dauerhaft blockiert

- IP-Adresse ist dauerhaft gesperrt
- Keine Anmeldung mehr möglich
- Sinnvoll bei eindeutig unerwünschten Zugriffen

Für Version 26.4.0

Verwendung von IP-Bereichen

Mit dem sogenannten CIDR-Präfix wird festgelegt, wie groß der IP-Bereich ist, auf den sich eine Regel bezieht.

Präfix	Bedeutung
`/32`	Genau eine einzelne IP-Adresse
`/24`	Ein typisches Netzwerk (z. B. Firmennetz)

Grundregel:
Je kleiner die Zahl, desto größer der abgedeckte IP-Bereich.

Beispiele CIDR

- `192.168.1.10/32`
  → Betrifft genau ein einzelnes Gerät
- `192.168.1.0/24`
  → Betrifft alle Geräte von `192.168.1.1` bis `192.168.1.254`

Vertrauenswürdige IPs definieren

- Eigene oder bekannte Netzwerke festlegen
- Diese als „Dauerhaft erlaubt“ konfigurieren
- Beispiele:
  - Büro-Netzwerk
  - VPN-Zugänge

Globale Blockregel erstellen

- Regel für alle übrigen IP-Adressen anlegen
- Beispiel: `0.0.0.0/0` (umfasst alle IPs weltweit)
- Status: „Dauerhaft blockiert“

Für Version 26.4.0

Vor Aktivierung der globalen Blockregel unbedingt sicherstellen, dass die eigene IP-Adresse korrekt als dauerhaft erlaubt hinterlegt ist.

Sicherheitsoptimierungen für Einschreibungen

Link und QR-Code einer Einschreibung wirken wie ein Zugangsschlüssel: Solange die Einschreibung gültig ist, lässt sich darüber ein Gerät in Relution einschreiben. Das Gerät erhält anschließend die mit der Einschreibung verknüpften Richtlinien und Regelwerke – unter Umständen also auch WLAN-Zugangsdaten, Zertifikate oder Zugänge zu Unternehmensdiensten. Offene Einschreibungen sollten daher so knapp wie möglich gehalten werden.

- Gültigkeit kurz halten: Beim Anlegen einer Einschreibung steht Gültig bis standardmäßig sieben Tage in der Zukunft. Der Zeitraum sollte nicht länger gewählt werden, als für die geplante Einschreibung tatsächlich nötig ist. Reicht die Zeit nicht aus, lassen sich noch nicht verwendete Einschreibungen über Einschreibungen verlängern nachträglich verlängern – vorsorglich lange Laufzeiten sind daher nicht notwendig.
- Einmal-Einschreibungen bevorzugen: Standardmäßig ist jede Einschreibung nur für ein einziges Gerät nutzbar. Über eine Mehrfach-Einschreibung lassen sich dagegen bis zum Ablaufdatum beliebig viele Geräte einschreiben, begrenzt nur durch die verfügbaren Lizenzen. Sie sollte deshalb nur gezielt für größere Rollouts eingesetzt und mit einer besonders kurzen Gültigkeit kombiniert werden.
- Nicht mehr benötigte Einschreibungen löschen: Offene Einschreibungen, die nicht mehr gebraucht werden – etwa nach Abschluss eines Rollouts oder wenn ein Gerät doch nicht eingeschrieben wird –, sollten unter `Geräte` → `Einschreibungen` gelöscht werden. Geräte, die bereits über eine Mehrfach-Einschreibung eingeschrieben wurden, bleiben dabei eingeschrieben. Bei Android Enterprise wird zusätzlich das zugehörige Einschreibungstoken bei Google gelöscht, sodass der QR-Code nicht mehr funktioniert.
- Links und QR-Codes nicht öffentlich teilen: Einschreibungslinks werden nur an die vorgesehenen Personen verschickt und nicht im Intranet, in Wikis oder über große E-Mail-Verteiler veröffentlicht. Ausgedruckte QR-Codes werden nach dem Rollout vernichtet.
- Einschreibungen regelmäßig prüfen: In der Liste unter `Geräte` → `Einschreibungen` lässt sich anhand von Status und Gültig bis erkennen, welche Einschreibungen noch offen sind. Zusätzlich lohnt ein Blick ins Geräte-Inventar, ob dort unerwartete Geräte aufgetaucht sind.
- macOS: Passwort zum Entfernen des Profils: Bei macOS-Einschreibungen kann Passwort zum Entfernen des Profils verwenden aktiviert werden. Das MDM-Profil lässt sich dann nur mit einem automatisch generierten Passwort vom Gerät entfernen.

Berechtigungen verwalten

Für Version 26.4.0

Relution bietet im Standard zwölf Berechtigungsvorkonfigurationen an. Prüfen, welche Funktionen in welchem Berechtigungspreset aktiv sind. Hierzu auf `Benutzer` → `Berechtigungen` klicken und auf die Einträge achten, die vom System angelegt wurden. Diese Rollen können nicht editiert werden. Es lassen sich jedoch jederzeit neue Berechtigungen anlegen und dort feingranular die notwendigen Funktionen für einzelne Benutzer:Innen freischalten. Die Berechtigungen korrelieren mit den Benutzergruppen, die von Relution angelegt wurden.

Organisationen anlegen

Relution ist mandantenfähig, d.h. eine realistische Abbildung von Schul- oder Firmenstrukturen ist möglich. Nach der Installation erfolgt die erste Anmeldung auf der globalen Organisationsebene. Von dort aus können weitere Mandanten angelegt werden.

In diesem Artikel wird Schritt für Schritt erklärt, welche Maßnahmen dafür erforderlich sind und worauf besonders zu achten ist.

Organisation anlegen

1. Mit dem angelegten Administrator `admin` und dem Passwort am System anmelden.
    - Bei der ersten Anmeldung eines Benutzers muss die EULA akzeptiert werden.
2. In der Global Organisation in der Seitenleiste zu `Organisationen` → `Hinzufügen` navigieren.

Allgemeine Angaben

- Organisationsdaten
    - Ist die eigene Organisation, Firma oder das Unternehmen nicht aufgeführt, die nächstgelegene verfügbare Adresse wählen.

Für Version 26.4.0

Organisation

- Name
    - Dient der allgemeinen Darstellung in Relution und kann nachträglich geändert werden.
- Eindeutige Bezeichnung der Organisation
    - Kann nachträglich nicht geändert werden (datenbankrelevant).
- Organisationstyp
    - Legt fest, ob die Organisation eigenständig (Eigenständig), als Meta-Organisation (Meta) oder als Unterorganisation einer bestehenden Meta-Organisation (Unterorganisation) angelegt wird. Bei Unterorganisation wird zusätzlich die übergeordnete Meta-Organisation ausgewählt. Details unter Meta-Organisationen →.
- Absenderadresse
    - E-Mail-Adresse, die der Server als Absender verwendet, wenn er E-Mails sendet (z. B. bei neuen Enrollments oder ablaufenden Zertifikaten).
- Antwortadresse
    - Optionale Adresse, die in das Feld „Reply-To“ eingetragen wird. Wenn ein Benutzer z. B. auf eine Registrierungs-Mail antwortet, wird diese Adresse (abhängig vom Mail-Client) als Empfänger verwendet.

Verwaltung

- Mitglieder verwalten
  - Bestehende Mitglieder der Organisation hinzufügen.
- Administrator anlegen
  - Neuen Administrator für diese Organisation anlegen.

Zusammenfassung

Eine Zusammenfassung aller eingegebenen oder ausgewählten Punkte wird angezeigt.

Lizenzen

- Ohne Limit kann die angelegte Organisation alle Lizenzen der globalen Instanz nutzen, bis diese aufgebraucht sind.
- Das Limit kann nachträglich gesetzt, entfernt oder angepasst werden. → Menü `?` → `Lizenzinformationen` (oben rechts neben dem Benutzernamen).

Für Version 26.4.0

Apple Geräte verwalten

Die Betriebssysteme iOS, macOS und tvOS wurden ausschließlich für Apple-Geräte entwickelt. Relution bietet eine Reihe von Funktionen, mit denen sich Apple-Geräte konfigurieren und steuern lassen. Im Folgenden mehr dazu, wie die Verwaltung von Apple-Geräten beginnt.

Zertifikate

Neu in 26.3

Vor der Einschreibung von Apple-Geräten sicherstellen, dass ein APNS-Zertifikat → (Apple Push Notification Service) auf dem Server konfiguriert ist.

Ab Relution 26.3.0 müssen Neuinstallationen ein eigenes APNS-Zertifikat bereitstellen, bevor Geräte eingeschrieben werden können. Der Self-Service-Assistent unter `Einstellungen` → `Organisationszertifikate` führt durch die Einrichtung. Bereits laufende Instanzen vor dieser Version werden vorerst weiterhin mit einem von Relution bereitgestellten Zertifikat betrieben.

APNS Push-Zertifikate einrichten →

Für Version 26.4.0

Einschreibung

Um ein Apple-Gerät verwalten zu können, muss es in Relution eingeschrieben werden. Hierzu wird ein sogenanntes MDM-Profil auf dem Gerät installiert. Für Apple-Geräte stehen drei unterschiedliche Arten der Einschreibung zur Verfügung.

iOS-Einschreibungen →
macOS-Einschreibungen →
tvOS-Einschreibungen →

Überwachter Modus/Supervised Mode

Der Überwachte Modus/Supervised Mode ermöglicht es, Apple-Geräte, die sich im Besitz des Arbeitgebers befinden, von persönlichen Geräten zu unterscheiden. Wir empfehlen für eine uneingeschränkte Verwaltung und die Nutzung aller MDM-Funktionen, die Geräte in den Überwachten Modus zu versetzen. So lassen sich viele für die Nutzung im Schul- oder Arbeitsumfeld nicht benötigte Funktionen durch Restriktionen deaktivieren. Der unten stehende Link führt zu weiteren Informationen dazu, wie sich Apple-Geräte in diesen Modus bringen lassen.

DEP-Geräte sind immer supervised. Geräte mit dem Apple Configurator ins DEP aufnehmen →

Relution Agent

Der Relution Agent wird während der Einschreibung immer automatisch auf den Apple-Geräten installiert. Er ist für die Verwaltbarkeit der Geräte nicht notwendig, liefert aber eine Vielzahl zusätzlicher nützlicher Funktionen für Benutzer.

Es ist zu empfehlen, eine ausreichende Anzahl an VPP-Lizenzen für die App vorzuhalten, dann kann die Installation vollautomatisch erfolgen. Ansonsten müssen sich die Nutzer mit Apple-Accounts auf den Apple-Geräten anmelden, damit keine VPP-Lizenzen für die App-Installation notwendig sind.

Dienstliche und persönliche Daten trennen

Verwaltete Apps: Apps, die über Relution auf Apple-Geräten bereitgestellt werden, werden als verwaltete Apps bezeichnet. Die Kontrolle über diese Apps bleibt dabei erhalten; sie und die damit verbundenen Daten lassen sich bei Bedarf entfernen. Bei iOS- und macOS-Geräten lassen sich verwaltete Apps über die Richtlinien-Konfiguration Verwaltete App (Managed App) konfigurieren.

Verwaltete Konten: Für iOS- und macOS-Geräte lassen sich mit Relution E-Mail- und andere Konten per MDM einrichten und unabhängig von persönlichen Konten verwalten. Mit Relution lassen sich folgende Konten konfigurieren:

- E-Mail
- Exchange
- CardDAV
- CalDAV
- Abonnierte Kalender
- Google Accounts (nur iOS-Geräte).

Die Datentrennung findet bei Apple innerhalb des Betriebssystems statt.

Für Version 26.4.0

Apps verwalten

Die Apps auswählen, die auf Apple-Geräten genutzt werden sollen, und die nicht relevanten Apps blockieren oder entfernen. Apps effizient auf einer Vielzahl von Apple-Geräten gleichzeitig verwalten, verteilen und entfernen.

App Management →

App-Lizenzen

Jede App, die auf Apple-Geräten über den Public App Store installiert wird, muss lizenziert werden. Es spielt keine Rolle, ob die App kostenfrei ist oder nicht. Die Lizenz kann entweder über den aktuell per Apple-ID angemeldeten Benutzer oder, falls ohne Apple IDs gearbeitet werden soll, über das Apple Volume Purchase Program (VPP) bezogen werden. Für VPP ist ein Zugang zu einem Apple School/Business Manager notwendig. Für native Apps ist dies nicht notwendig.

Die Apps lassen sich auf Apple-Geräten installieren, ohne dass Benutzer die Installation manuell initiieren, sofern die Apple-Geräte überwacht sind, sich also im Supervised Mode befinden.

App-Installation ohne Benutzereingabe →

VPP-Apps (Volume Purchase Program) können auf Apple-Geräten, die überwacht sind, ohne Zutun der Nutzer installiert werden. Weitere Informationen zu VPP:

VPP-Einrichtung in Relution →
VPP-Apps ausrollen →

Sperr- oder Positivliste für iOS und tvOS

Mit der Sperr- oder Positivliste-Funktion in Relution können Administratoren bestimmte Apps auf iPhones, iPads und Apple TVs blockieren und die Installation wichtiger Apps erlauben. Diese Funktion verhindert die Installation von unerwünschten Apps und verbirgt installierte Apps, welche sich bereits auf Geräten befinden, falls erforderlich vor Benutzer. Der unten stehende Link führt zu weiteren Informationen über das Block- oder Allowlisting von Apps.

App-Konformität für iOS →
App-Konformität für tvOS →

Einzel-App-Modus für iOS

Der Einzel-App-Modus (Single App Mode) kann auf iPhones und iPads aktiviert werden, wodurch die Geräte auf eine einzige App beschränkt und alle anderen blockiert werden. Es ist zu beachten, dass die Geräte überwacht (supervised) sein müssen, um den Einzel-App-Modus zu aktivieren.

Einzel-App-Modus für iOS →

Für Version 26.4.0

Weblink

Der Webclip sieht aus wie ein App-Symbol, das beim Anklicken auf eine Website verweist. Dafür sind lediglich eine Bezeichnung und eine URL anzugeben.

Weblinks über Richtlinie hinzufügen →
Weblinks hinzufügen und über das Homescreen Layout für iOS platzieren →

MDM-Profil vor Löschung schützen

Das Entfernen des MDM-Profils aus den Geräteeinstellungen lässt sich verhindern, indem die Geräte über das Apple Device Enrollment Program (DEP) eingeschrieben werden.

Konfigurationsprofil für ADE →
Automatische Einschreibung →

Netzwerk-Konfiguration und -sicherheit

Höchste Sicherheit im Netzwerk lässt sich durch geeignete Konfigurationen erreichen. Mit Relution lassen sich WLAN-Einstellungen für alle Apple-Betriebssysteme konfigurieren. Darüber hinaus können VPN- (Virtual Private Network) und Per-App-VPN-Einstellungen für iOS- und macOS-Geräte konfiguriert werden. Mobilfunk-Einstellungen (Access Point Network) lassen sich für iOS-Geräte konfigurieren.

Restriktionen

Die Richtlinien-Konfiguration der Restriktionen schränkt Apple-Geräte in der Funktionalität ein. Es ist wichtig, die Art der Einschreibung zu beachten, da viele Restriktionen nur auf überwachten Geräten (supervised) greifen.

Zu den Restriktionen →

System-Updates

Apple-Geräte lassen sich auf die neueste Betriebssystem-Version aktualisieren, sofern sie überwacht (supervised) sind.

Administratoren können Updates für überwachte Geräte auch bis zu 90 Tage aufschieben. Während dieses Zeitraums werden Benutzer nicht aufgefordert, Geräte auf die neueste Betriebssystem-Version zu aktualisieren. So können Organisationen nach Fehlern/Problemen suchen oder die Kompatibilität der bereitgestellten Anwendungen mit den neuesten Betriebssystem-Versionen prüfen.

Restriktionen →

Filter für Inhalte

Für Version 26.4.0

Mit der Funktion zur Filterung von Webinhalten lässt sich der Zugriff auf bestimmte Webseiten in der eigenen Organisation verhindern.

Filter für Inhalte →

Homescreen Layout für iOS

Apps lassen sich sowohl auf dem Homescreen des iPhones oder iPads wie auch im Dock anordnen und in Ordnern platzieren, die sich manuell oder automatisch erstellen lassen.

Homescreen Layout für iOS →

Android Enterprise verwalten

Android Enterprise ist eine Initiative von Google, die darauf abzielt, die Verwaltung und Sicherheit von Android-Geräten in Unternehmen zu verbessern. Es handelt sich um eine Reihe von Tools, APIs und Diensten, die es Unternehmen ermöglichen, Android-Geräte effizienter zu verwalten und die Sicherheit der Unternehmensdaten auf diesen Geräten zu gewährleisten.

Voraussetzung

Bevor Android-Geräte über Android Enterprise eingeschrieben werden können, muss die Relution-Organisation zunächst mit einer Google-Organisation verknüpft werden. Die Verknüpfung erfolgt unter `Einstellungen` → `Geräteplattformspezifisch` → `Android Enterprise`.

Organisation verknüpfen →

Einschreibung

Für Android Enterprise stehen mehrere Einschreibungsmöglichkeiten zur Verfügung. Geräte können manuell, mittels eines QR-Codes oder automatisch über Android Zero Touch oder bei Samsung über das Knox-Mobile-Enrollment (KME) → eingeschrieben werden.

Für Version 26.4.0

KME → und Zero Touch →
Einschreibungsarten →
Vollverwaltetes Gerät einschreiben →
Arbeitsprofil →
Vollverwaltetes Gerät mit persönlichem Profil →

Relution Agent und Relution Companion

Der Relution Agent und der Relution Companion werden während der Einschreibung immer automatisch auf den Android-Enterprise-Geräten installiert. Beide sind für die Verwaltbarkeit der Geräte nicht zwingend notwendig, liefern aber eine Vielzahl zusätzlicher nützlicher Funktionen für Benutzer. Mit dem Relution Companion für Android Enterprise ist es möglich, Zertifikate auf den Geräten zu installieren und eine Ortung der Geräte durchzuführen.

Dienstliche und persönliche Daten trennen

Android Enterprise bietet hervorragende Möglichkeiten, dienstliche und private Daten zu trennen. Hier steht den Benutzer ein Work Profile / Arbeitsprofil zur Verfügung, welches auf privaten Geräten installiert werden kann. Alternativ kann ein persönliches Profil auf vollverwalteten Geräten aktiviert werden, in welchem Benutzer eine Anmeldung mit einem privaten Google-Konto durchführen und das Gerät nahezu uneingeschränkt privat nutzen können, ohne dass vertrauliche und dienstliche Inhalte durcheinander geraten.

Apps verwalten

Mit Android Enterprise können keine nativen Apps auf Geräten installiert werden. Sämtliche Apps müssen aus dem Managed Google Play Store kommen. Eigene APKs können dort hochgeladen und in der eigenen Organisation verfügbar gemacht werden, solange der Paketname der App bei Google eindeutig ist.

Apps verwalten→

> Es gibt aktuell keine Möglichkeit, mit Android Enterprise kostenpflichtige Apps zu verteilen.

Über die Verwaltung der Apps lassen sich zudem Konfigurationen hinterlegen. Diese sind für die Vorkonfiguration einzelner Anwendungen; beispielsweise, um Mailprofile oder andere Einstellungen auszurollen. Die möglichen Konfigurationen wurden direkt vom App-Hersteller eingebaut. Wir können hier bei eventuellen Fehlfunktionen keinen Support leisten.

Homescreen Layout und Kiosk Modus

Relution bietet mit der Richtlinie für den Homescreen Layout die Aktivierung des Kiosk Modus mit einem von Relution eigens entwickelten Launcher. Dieser ermöglicht die Installation eines Hintergrundbildes sowie die Anordnung von Apps auf dem Homescreen oder in Ordnern.

Homescreen Layout und Kiosk Modus →

Für Version 26.4.0

Restriktionen

Auf Android Enterprise Geräten können mit Relution viele Restriktionen aktiviert werden.

> Es ist möglich, die Geräte mit Restriktionen nachhaltig unbrauchbar zu machen. Ein Verbot eines Factory Reset lässt sich z. B. nicht aushebeln.

Restriktionen →

Laufzeitberechtigungen

Über die Laufzeitberechtigungen können Benutzer das Beantworten von Berechtigungsfragen abgenommen werden. Hier lassen sich Standard- aber Benutzerdefinierte Berechtigungen konfigurieren.

Laufzeitberechtigungen →

Windows Geräte verwalten

In Relution lassen sich Geräte mit Windows 10/11 verwalten. Je nach Variante, stehen verschiedene Funktionen zur Verfügung. Der größte Funktionsumfang besteht bei Pro, Education oder Enterprise Lizenzen. Im Gegensatz zu Domänenrichtlinien kann Relution auf Windows-Geräten auch Aktionen ausführen und Richtlinien anwenden, wenn sich diese nicht im lokalen Netzwerk befinden. Hier reicht eine Internetverbindung aus.

Einschreibung

Bei Windows Geräten kann auf drei verschiedene Einschreibungsarten zurückgegriffen werden.

Manuelle Einschreibung →
Bulk Enrollment →
Auto Pilot Einschreibung →

Für Auto Pilot wird eine P2 Premium Lizenz in Microsoft Azure benötigt.

Für die manuelle Einschreibung und das Bulk Enrollment muss der User über administrative Berechtigungen verfügen.

Für Version 26.4.0

Relution Companion

Der Relution Companion wird während der Einschreibung immer automatisch auf Windows Geräten installiert. Dies funktioniert aus Gründen der limitierten Funktionen in Windows Home auf dieser Variante jedoch nicht. Der Relution Companion ermöglicht das Ausführen von Powershell-Skripten und die Installation von MSI- und EXE-Dateien.

Windows Companion →
Windows Home Limitierungen →

Apps verwalten

Mit Relution können Apps aus dem Windows Store und native Apps aus dem Relution App Store auf den Windows Geräten installiert werden. Native Apps müssen in Relution hochgeladen und, je nach Format, konfiguriert werden. MSIX- Dateien müssen selbst erstellt und mit einem Zertifikat signiert werden, um die Installation zu ermöglichen. EXE- und MSI-Dateien benötigen Installations- und Deinstallationsparameter. Diese lassen sich entweder auf der Webseite des Herstellers oder auf Techblogs finden.

MSIX Dateien erstellen→
EXE- und MSI Dateien in Relution nutzen →
SilentinstallHQ →

Das Herausfinden der richtigen Konfigurationsparameter ist häufig eine zeitaufwändige Prozedur. Der Relution Support kann hier nur sehr bedingt unterstützen.

Zertifikate

Zertifikate können über die entsprechende Richtlinienkonfiguration direkt auf das Windows-Gerät geladen werden. Hier ist es zudem möglich, den entsprechenden Zertifikatsspeicher zu wählen.

Zertifikate →

Restriktionen

Auf Windows Geräten können viele Restriktionen mit Relution aktiviert werden. Hier lässt sich auch festlegen, ob das MDM-Profil durch die Benutzer entfernt werden oder ob der Rechner zurückgesetzt werden darf.

Restriktionen →
MDM Profil schützen →

Weitere Konfigurationen

Es stehen noch weitere Konfigurationen zur Verfügung, zum Beispiel WLAN- und VPN Profile, der Kiosk Modus und die Konfiguration für Windows Shared PC →.

Für Version 26.4.0

Whiteboards verwalten

Die Verwendung von Whiteboards auf Android-Basis erfreut sich in Schulen, Unternehmen und weiteren Organisationen wachsender Beliebtheit. Um diese Geräte effizient zu verwalten, bietet Relution eine umfassende Lösung, die speziell für die zentralisierte Steuerung von Android-Whiteboards verschiedener Hersteller entwickelt wurde.

Herstellerabhängiger Funktionsumfang

Der Funktionsumfang zur Verwaltung der Whiteboards hängt von den vom jeweiligen Hersteller bereitgestellten Endpunkten ab. Diese Endpunkte bestimmen, welche Steuerungs- und Konfigurationsmöglichkeiten über Relution genutzt werden können.

Beispiele:

- Spezifische Einstellungen
- Firmware-Updates
- Sicherheitsrichtlinien

Die verfügbaren Funktionen richten sich nach den unterstützten Features des jeweiligen Herstellers.

Für Version 26.4.0

Einfache Integration mittels Android Classic

Whiteboards können manuell in die Relution-Plattform eingebunden werden. Hierfür wird der Relution Companion verwendet, mit dem die Geräte Schritt für Schritt eingeschrieben werden.

Sobald ein Gerät erfolgreich registriert ist, steht der umfassende Funktionsumfang von Relution zur Verfügung. Über die Plattform können Konfigurationen und Richtlinien flexibel eingerichtet und auf die Geräte angewendet werden.

Breite Unterstützung zahlreicher Hersteller

Eine Vielzahl an Herstellern wird bereits von Relution unterstützt. Eine vollständige Übersicht über die aktuell kompatiblen Hersteller ist hier→ zu finden.

Die Liste wird kontinuierlich erweitert, da weitere Hersteller in die Integration aufgenommen werden.

Erweiterte Möglichkeiten dank Android Enterprise

Neben der Unterstützung von Android Classic Whiteboards bietet Relution auch erweiterte Optionen mittels Android Enterprise.

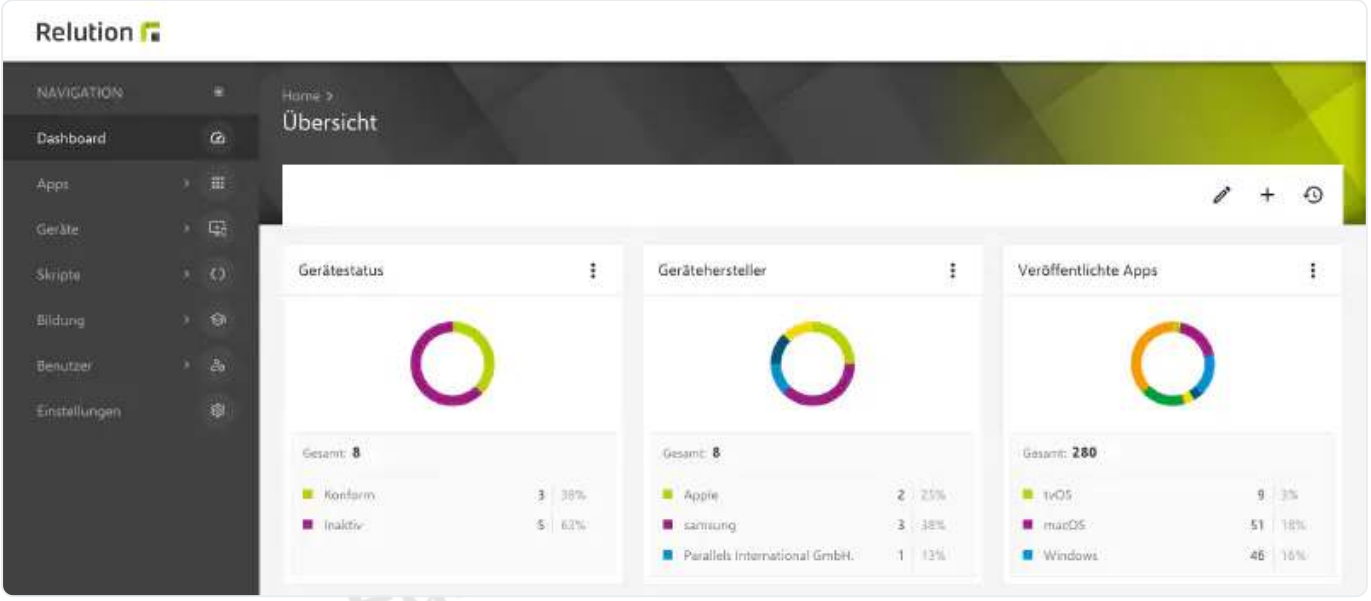
Diese Plattform ermöglicht zusätzliche, standardisierte Funktionen zur ganzheitlichen Verwaltung von Geräten.

Relution erweitert die Möglichkeiten der Android Enterprise Plattform speziell für interaktive Whiteboards und kombiniert die Standardfeatures mit herstellerspezifischen Whiteboard-Funktionen. Ein Überblick über die verfügbaren Android Enterprise Erweiterungen ist hier→ zu finden.

Dashboard

Das Dashboard ist die Startseite des Relution-Portals und fasst den aktuellen Zustand einer Organisation zusammen: Geräte, Apps, Richtlinien, Einschreibungen, Zertifikate und der Systemstatus werden als Kacheln dargestellt. In der Seitennavigation ist die Seite über Dashboard erreichbar.

Die einzelnen Kacheln werden als Widgets bezeichnet. Jedes Widget zeigt eine Auswertung als Diagramm, Tabelle oder Statusübersicht. Der Umfang des Dashboards ist nicht fest vorgegeben: Widgets können ergänzt, angepasst, verschoben und entfernt werden.



Gemeinsames Dashboard je Organisation

Ein Dashboard gehört zur Organisation, nicht zum einzelnen Benutzerkonto. Anpassungen am Layout, neu hinzugefügte oder gelöschte Widgets sind damit für alle Benutzer dieser Organisation sichtbar. Ein persönliches, nur für ein Konto sichtbares Dashboard ist nicht vorgesehen.

Beim Wechsel des Mandanten wird jeweils das Dashboard der aktiven Organisation geladen. Die dargestellten Werte beziehen sich immer auf die Organisation, in der sich die Anmeldung gerade befindet.

> Da das Dashboard organisationsweit gilt, wirken sich auch das Löschen eines Widgets und das Wiederherstellen des Standard-Dashboards auf alle Benutzer der Organisation aus.

Standard-Dashboard

Ohne eigene Anpassung wird ein vorkonfiguriertes Standard-Dashboard bereitgestellt. Welche Widgets es enthält, hängt von der Art der Organisation ab.

In jeder Organisation enthalten sind Gerätestatus, Gerätehersteller, Gerätemodelle, Betriebssysteme, Geräte, Geräte Eigentümerschaft, Geräte im Roaming-Modus nach Ländern, Richtlinien, Veröffentlichte Apps, Zertifikate, Systemzertifikate und Knox Service Plugin Feedback.

Abhängig von der Organisation kommen weitere Widgets hinzu:

- Ausstehende Einschreibungen — in allen Organisationen mit Ausnahme der globalen Organisation.
- Organisationen — in Organisationen mit untergeordneten Organisationen sowie in der globalen Organisation.
- Systemstatus — ausschließlich in der globalen Organisation.

Solange das Standard-Dashboard unverändert ist, ist die Aktion zum Wiederherstellen deaktiviert; ein Hinweistext weist darauf hin, dass bereits das Standard-Dashboard aktiv ist. Sobald das Layout gespeichert oder ein Widget geändert wurde, wird daraus ein eigenes Dashboard der Organisation.

Layout anpassen

Über das Symbol Widgets anordnen (Stift) wird der Bearbeitungsmodus aktiviert. In diesem Modus lassen sich Widgets per Maus verschieben und in der Größe verändern; das Raster ordnet die übrigen Kacheln automatisch neu an.

Die Übernahme erfolgt über Änderungen am Dashboard speichern, das Verwerfen über Änderungen am Dashboard verwerfen. Beide Aktionen werden mit einem Bestätigungsdialog abgesichert, da das Ergebnis für alle Benutzer der Organisation gilt. Liegt keine Änderung vor, weist ein Hinweis am Speichern-Symbol darauf hin, dass es keine Änderungen zum Speichern gibt.

Für Version 26.4.0

Widgets hinzufügen

Über Neues Widget hinzufügen öffnet sich der Dialog Widget erstellen. Er gliedert sich in die Bereiche Diagrammtyp auswählen für eigene Auswertungen und Vordefinierte Widgets für fest vorgegebene Kacheln.

Eigene Widgets aus Metriken

Den Ausgangspunkt bildet die Darstellungsform. Im Bereich Diagrammtyp auswählen stehen Balkendiagramm, Gestapeltes Balkendiagramm, Kreisdiagramm und Tabellendiagramm zur Verfügung.

Nach der Auswahl öffnet sich das Widget-Formular mit dem Abschnitt Widget-Konfiguration. Alle dort angezeigten Felder sind Pflichtfelder:

- Name — die Bezeichnung der Kachel.
- Entität — die Datenquelle: Geräte, Apps, Gerätegruppen, Einschreibungen oder Richtlinien. Zur Auswahl stehen nur die Entitäten, für die im aktuellen Benutzerkonto eine Leseberechtigung vorliegt; die übrigen erscheinen nicht in der Liste.
- Feld — das Merkmal, nach dem gruppiert wird, etwa Betriebssystem oder Hersteller. Bei Tabellendiagrammen entfällt dieses Feld.
- Entitäten anzeigen nach — nur beim gestapelten Balkendiagramm: das zweite Merkmal, aus dem sich die Reihen ergeben. Es muss sich von Feld unterscheiden.
- Spalten — nur bei Tabellendiagrammen: die Auswahl der angezeigten Spalten.

Im Abschnitt Metrik Filter lässt sich die Datenbasis zusätzlich einschränken, etwa auf eine Plattform oder einen Gerätestatus.

Über die Schaltfläche Vorschau wird das Ergebnis der Konfiguration bereits vor dem Speichern neben den Feldern angezeigt; der Name muss dafür noch nicht vergeben sein. Liefert die gewählte Kombination keine Werte, erscheint oberhalb der Felder der Hinweis, dass keine passenden Daten gefunden wurden.

Vordefinierte Widgets

Im Bereich Vordefinierte Widgets stehen Auswertungen bereit, die sich nicht über die Metrik-Konfiguration abbilden lassen:

- Systemstatus — Verfügbarkeit der Relution-Systemkomponenten, dargestellt als Aktiv oder Inaktiv.
- Organisationen — Übersicht der zugänglichen Organisationen, aus der heraus sich der Mandant wechseln lässt.
- Knox Service Plugin Feedback — Rückmeldungen aus dem Knox Service Plugin.
- Systemzertifikate — Ablaufdatum des APNs-Push-Zertifikats der Organisation für die Verwaltung von Apple-Geräten und des integrierten Push-Zertifikats des Relution Agent (siehe APNS Push Zertifikate →).

Angeboten werden nur die vordefinierten Widgets, für die die erforderlichen Leseberechtigungen vorliegen (siehe Berechtigungen). Deren Auswertung ist fest vorgegeben und lässt sich nicht über das Widget-Formular anpassen. Jeder Typ kann nur einmal auf dem Dashboard liegen; eine bereits verwendete Kachel ist im Dialog deaktiviert und mit Bereits hinzugefügt gekennzeichnet.

Widgets bearbeiten, aktualisieren und entfernen

Jede Kachel besitzt das Menü Widget-Optionen. Es umfasst Löschen, Bearbeiten und Aktualisieren: Aktualisieren lädt die Daten des Widgets neu, Bearbeiten öffnet die Konfiguration im Widget-Formular, Löschen entfernt die Kachel vom Dashboard. Bei vordefinierten Widgets und beim Widget Zertifikate entfällt Bearbeiten, da deren Auswertung nicht konfigurierbar ist. Löschen und Bearbeiten erscheinen nur mit der Berechtigung zum Aktualisieren von Dashboards, auf dem Standard-Dashboard zusätzlich nur mit der Berechtigung zum Erstellen. Im Bearbeitungsmodus steht das Menü nicht zur Verfügung, ebenso wenig bei Widgets, für deren Daten keine Leseberechtigung besteht.

Für Version 26.4.0

Das Entfernen wird mit einem Dialog bestätigt. Widget und Konfiguration werden dabei endgültig und für alle Benutzer der Organisation gelöscht; ein Wiederherstellen des einzelnen Widgets ist nicht möglich. Das Widget Zertifikate wird im Dialog Widget erstellen nicht angeboten und lässt sich nach dem Löschen nur über das Wiederherstellen des Standard-Dashboards zurückholen.

Standard-Dashboard wiederherstellen

Über Standard-Dashboard wiederherstellen wird die Ausgangskonfiguration zurückgeholt. Alle angepassten Widgets werden dauerhaft gelöscht. Auch diese Aktion kann nicht rückgängig gemacht werden und betrifft alle Benutzer der Organisation.

Von Widgets in die Listen navigieren

Widgets sind mit den zugehörigen Übersichten verknüpft. Ein Klick auf ein Diagrammsegment öffnet die passende Liste — etwa die Inventarübersicht → — und wendet die angeklickte Auswahl dort als Filter oder als Suchbegriff an. Beim gestapelten Balkendiagramm werden beide Merkmale des angeklickten Segments übernommen. Bei Tabellen-Widgets führt ein Klick auf eine Zeile zur Detailseite des jeweiligen Objekts, sofern für diesen Datentyp eine Detailansicht vorhanden ist. Im Widget Zertifikate öffnet ein Klick auf eine Zeile die Zertifikatsliste mit dem Namen des Zertifikats als Suchbegriff.

Im Bearbeitungsmodus ist diese Navigation deaktiviert, damit das Verschieben von Kacheln nicht versehentlich einen Seitenwechsel auslöst.

Liefert ein Widget keine Daten, bietet die Kachel neben dem Hinweis eine passende Schaltfläche an, etwa Einschreibungen erstellen, Gerätegruppe erstellen, Richtlinie erstellen, App Store oder beim Widget Zertifikate Zertifikat hinzufügen. Die Schaltfläche erscheint nur mit der Berechtigung für die jeweilige Aktion.

Berechtigungen

Der Zugriff auf das Dashboard und seine Bearbeitung wird über die Berechtigungen im Bereich Dashboard gesteuert:

- Für die Anzeige des Dashboards ist die Berechtigung Lesen erforderlich.
- Das Bearbeiten des Layouts, das Speichern von Änderungen, das Hinzufügen von Widgets sowie das Bearbeiten und Löschen einzelner Widgets setzen die Berechtigung Aktualisieren voraus.
- Solange das Standard-Dashboard aktiv ist, entsteht mit der ersten Anpassung ein eigenes Dashboard der Organisation. Dafür ist zusätzlich die Berechtigung Erstellen erforderlich.
- Das Wiederherstellen des Standard-Dashboards erfordert die Berechtigung Löschen.

Fehlt eine dieser Berechtigungen, ist das zugehörige Symbol in der Kopfzeile des Dashboards deaktiviert; ein Hinweis am Symbol nennt die fehlende Berechtigung. Fehlen alle drei Berechtigungen Erstellen, Aktualisieren und Löschen, entfällt die Kopfzeile vollständig. Die Vergabe der Berechtigungen ist im Artikel Berechtigungen → beschrieben.

Unabhängig davon werden in den Widgets nur Daten dargestellt, für die eine Leseberechtigung besteht. Ist das nicht der Fall, erscheint anstelle der Auswertung ein Hinweis mit der Empfehlung, die erforderlichen Berechtigungen bei der Administration anzufragen; bei eigenen Widgets nennt er die betroffene Entität.

Die vordefinierten Widgets setzen jeweils eine eigene Leseberechtigung voraus. Sie entscheidet darüber, ob das Widget im Dialog Widget erstellen angeboten wird und ob es auf dem Dashboard Daten anzeigt:

Für Version 26.4.0

Widget	Erforderliche Berechtigung
Systemstatus	Lesen im Bereich Systemzustand (nur globale Organisation)
Organisationen	Lesen im Bereich Organisationen (globale Organisation) oder Untermandanten (Meta-Organisation)
Knox Service Plugin Feedback	Lesen im Bereich Richtlinien
Systemzertifikate	Lesen im Bereich Organisationszertifikate

Einschränkungen

Bei der Planung eines eigenen Dashboards sind folgende Grenzen zu berücksichtigen:

- Ein Dashboard je Organisation. Benutzerspezifische Dashboards innerhalb derselben Organisation sind nicht möglich.
- Begrenzte Anzahl Widgets. Je Dashboard sind standardmäßig 30 Widgets zulässig. Ist die Grenze erreicht, nennt ein Hinweis am Symbol zum Hinzufügen die aktuelle sowie die maximale Anzahl.
- Begrenzte Anzahl Filter je Widget. Je Widget sind standardmäßig 20 Filter zulässig. Überschreitet die Filterkonfiguration diesen Wert, lässt sich das Widget nicht speichern, bis Filter entfernt wurden.
- Vordefinierte Widgets sind unveränderlich und können jeweils nur einmal hinzugefügt werden.
- Knox Service Plugin Feedback setzt eine konfigurierte Android-Enterprise-Anbindung voraus; andernfalls bleibt das Widget ohne Daten.
- Organisationsbezug der Daten. Ausgewertet werden die Daten der aktiven Organisation.
- Löschvorgänge sind endgültig. Weder ein entferntes Widget noch ein durch Wiederherstellung ersetztes Dashboard lässt sich zurückholen.

Die beiden zahlenmäßigen Grenzen sind Standardwerte und lassen sich serverseitig anpassen. In einer abweichend konfigurierten Installation nennen die Hinweise im Portal die dort gültigen Werte.

Für Version 26.4.0

Agent

Der Relution Agent überwacht den Konformitätsstatus jedes Geräts, stellt Apps über den Relution Store bereit und bietet Unterstützung für den Mehrbenutzermodus (iOS) auf verschiedenen Geräten. Diese umfassenden Funktionen ermöglichen ein reibungsloses und zentrales Management aller Geräte, sei es im Schulbetrieb oder in einem anspruchsvollen Unternehmensumfeld.

Durch die nahtlose Integration dieser Features schafft der Relution Agent eine effiziente Plattform, die sowohl die Sicherheit als auch die Produktivität in der Verwaltung mobiler Geräte optimiert.

Relution Agent für iOS

Der Relution Agent wird automatisch auf sämtlichen verwalteten Geräten installiert und fungiert als zentrale Anwendung für die umfassenden Funktionen des Mobile Device Management (MDM). Eine wichtige Sicherheitsmaßnahme besteht darin, dass der Relution Agent vom Benutzer nicht vom Gerät entfernt werden kann, solange das MDM-Profil installiert ist. Dies gewährleistet eine konstante Präsenz und Zuverlässigkeit der MDM-Funktionen.

> Die Relution Agent App ist Teil der Relution-Plattform und nur mit der Relution Backend-Komponente sowie entsprechenden Zugangsdaten nutzbar. Die Installation sollte in Abstimmung mit den IT-Administratoren der Organisation erfolgen.

Für Version 26.4.0

Funktionen der App

- Anzeige des Konformitätsstatus des Gerätes
- Installieren und Aktualisieren relevanter Apps
- Deinstallieren nicht benötigter Apps
- Anzeige, Anfordern und Hinzufügen von Apps und Weblinks
- Relution Shared Device (bei benutzerübergreifenden Geräten)
- iBeacon, GeoFence und Zonen-Erkennung
- Nachrichten über das MDM-System auf dem Gerät anzeigen
- Anmeldung am Gerät mit QR-Code / MFA-Token
- Geräteinformationen anzeigen
- Push-Benachrichtigungen aktivieren
- Biometrische Authentifizierung für den Geräte-Login aktivieren

Hinweise im Portal

Für iOS-Geräte können im Portal zwei agentenrelevante Hinweise angezeigt werden, sichtbar in der Richtlinienansicht des Geräts in der Zeile Geräte Standard:

1. `Relution Client App-Verbindung` – `Relution Agent ist nicht installiert`
2. `Push-Dienst` – `Push muss für die Relution App aktiviert sein`

Der Hinweis `Relution Client App-Verbindung` wird gelöst, sobald der Relution Agent installiert ist und in der App-Liste des Geräts erscheint. Fehlt die App, stößt Relution bei der nächsten Geräteaktualisierung die Installation automatisch erneut an. Der Hinweis `Push-Dienst` wird behoben, indem die Relution Agent App geöffnet und Mitteilungen zugelassen werden. Gelöste Hinweise entfernt Relution aus der Ansicht.

Relution Agent für Android Enterprise

Die Relution Agent App ist ein integraler Bestandteil der Relution-Plattform und nur in Verbindung mit der Relution Backend-Komponente nutzbar. Der Agent wird automatisch auf allen verwalteten Geräten installiert und fungiert als zentrale Anwendung für die MDM-Funktionen. Er ist gegen Deinstallation geschützt und wird von Relution automatisch mit den Verbindungsdaten des Geräts vorkonfiguriert.

Funktionen der App

- Anzeige des Konformitätsstatus des Gerätes
- Installieren und Aktualisieren relevanter Apps
- Deinstallieren nicht benötigter Apps
- Anzeige verfügbarer Apps aus dem Google Managed Play Store
- Nachrichten über das MDM-System auf dem Gerät anzeigen
- Anmeldung am Gerät mit QR-Code / MFA-Token
- Geräteinformationen anzeigen
- Push-Benachrichtigungen aktivieren
- Biometrische Authentifizierung für den Geräte-Login aktivieren

Für Version 26.4.0

Relution Agent für Windows

Der für Microsoft Windows entwickelte Relution Agent bietet grundlegende Funktionen und ist im Windows Store verfügbar. Benutzer mit den erforderlichen Berechtigungen (mindestens `Appstore User`) können die vom Administrator über das Relution Portal bereitgestellten Windows-Apps einsehen. Administratoren können App-Anfragen bearbeiten. Wird der Agent über Relution aus dem Store verteilt, schreibt Relution die Verbindungskonfiguration automatisch in die Registry des Geräts (`HKLM\SOFTWARE\Relution\Relution Agent`).

Relution Agent für macOS

Mit Relution 5.25.0 → wurde der Relution Agent für macOS bereitgestellt. Damit können Informationen direkt an Benutzer verwalteter Geräte bereitgestellt werden.

Wie bei iOS kann der Relution Agent aus dem App Store installiert werden. Auf verwalteten macOS-Geräten installiert Relution den Agent automatisch, wenn für die App Lizenzen über Apps und Bücher (im Portal: VPP) vorhanden sind. Fehlt der Agent später auf dem Gerät, installiert Relution ihn erneut. Ohne Lizenzen installiert Relution den Agent auf macOS nicht automatisch.

Funktionen der App

- Anzeige des Konformitätsstatus des Gerätes
- Installieren und Aktualisieren relevanter Apps (verwaltete Geräte)
- Nachrichten über das MDM-System auf dem Gerät anzeigen
- Geräteinformationen anzeigen
- Push-Benachrichtigungen aktivieren

Apps über den Relution Agent installieren

Damit die Installation und Anzeige von Apps über den Relution Agent erfolgen kann, muss dem Endgerät ein Benutzer zugewiesen sein. Dieser Benutzer kann auch ein Dummy User sein, falls nur die App-Funktion bereitgestellt werden soll.

Der Benutzer muss Mitglied der Systemgruppe `[ORGA] Appstore User` oder `[ORGA] Device Manager` sein, direkt oder über eine Gruppe, die selbst Mitglied ist (z. B. Teacher, Developer, App Reviewer, Content Manager, Administrator). Alternativ kann eine entsprechende Berechtigung erstellt und zugewiesen werden.

Welche Apps im Agent erscheinen, legen die Berechtigungen der einzelnen App fest; die Gruppenmitgliedschaft allein reicht nicht. Standardmäßig tragen neue Apps die Gruppen Appstore User und Device Manager in der Rolle Benutzer. Ist unter `Einstellungen` → `App Store` eine eigene Vorlage aktiv, gelten deren Gruppen (App Store Standard-Berechtigungen →). Mitglieder der Gruppe `[ORGA] Student` sehen Apps im Agent nur, wenn sie zusätzlich Mitglied von Appstore User sind oder in der Berechtigung der App eingetragen sind.

Für Version 26.4.0

Neue Benutzer

Benutzerverwaltung → Beim Erstellen des Benutzers kann dieser direkt einer Gruppe oder Berechtigung zugewiesen werden.

Bestehende Benutzer via Systemgruppe

Die Zuweisung von Mitgliedern zur Gruppe `Appstore User` erfolgt unter: `Benutzer` → `Gruppen` → `[ORGA] Appstore User` ([ORGA] = Eindeutiger Name der Organisation in Großbuchstaben)

Bestehende Benutzer via Berechtigung

Berechtigungen →

Companion & Daemon

Die Companion App von Relution ist für verschiedene Plattformen verfügbar. Sie erweitert nicht nur den Funktionsumfang, sondern erleichtert auch die unkomplizierte Inbetriebnahme von Geräten. Als verbindendes Element schlägt die App eine funktionale Brücke zwischen den Betriebssystemen und der Relution-Plattform.

Auf macOS-Geräten übernimmt diese Aufgabe der macOS Companion. Auf dem Mac läuft er als Dienst Relution Daemon.

Welche Versionen der Companion-Apps auf den Geräten installiert werden, ist unter `Einstellungen` → `Relution Client Apps` einsehbar. Dort werden auch der macOS Companion (Schalter macOS Companion aktivieren) und der Gerätebenutzerwechsel des Windows Companion (Schalter Gerätebenutzerwechsel aktivieren) ein- und ausgeschaltet.

Companion für Android (Legacy)

Android Legacy ist eine ältere Methode für das Management von Android-Geräten, zuvor als `Geräteadministrator` bekannt. Für die Einschreibung und Konfiguration von Android Legacy-Geräten ist der Relution Companion unverzichtbar: Er wird vor der Einschreibung aus Google Play oder als APK installiert, und die Einschreibung läuft über ihn, siehe Manuelle Einschreibung →.

Die App erweitert nicht nur den Funktionsumfang, sondern stellt auch grundlegende Mobile Device Management (MDM)-Funktionen bereit. Durch diese Integration wird eine nahtlose Verwaltung älterer Android-Geräte ermöglicht, wodurch Bedienkomfort und Effizienz gesteigert werden.

Ist unter `Einstellungen` → `Geräteverwaltung` die Option Verwaltung auf älteren Android-Geräte entfernen, falls dem Geräteadministrator die Berechtigung nicht erteilt wird aktiviert, entfernt Relution den Companion und damit die Verwaltung, wenn die Berechtigung Geräteadministrator nicht erteilt oder später widerrufen wird. Auf Android-basierten Whiteboards hat die Option keine Wirkung.

Für Version 26.4.0

> Mit der Einführung fortschrittlicherer Ansätze wie Android Enterprise wird das Legacy-Modell nicht mehr als bevorzugte Methode für das Management von Android-Geräten angesehen.

Companion für Android Enterprise

Der Relution Companion für Android Enterprise wird bei der Einschreibung automatisch installiert und ist für den Einschreibungsprozess zwingend erforderlich. Seine Installationsart lässt sich in der Richtlinie nicht überschreiben.

Der Companion erweitert die Funktionalitäten der Geräte um zusätzliche Features, wie zum Beispiel die Ortung verlorener Geräte.

Darüber hinaus ermöglicht er die Verteilung von Zertifikaten an die Geräte über das Relution Portal (siehe Zertifikat →). Über den Companion setzt Relution außerdem das Hintergrundbild → und stellt das Stammzertifikat für Relution Decon (Inhaltsfilter) → bereit.

Companion für Windows

Der Relution Companion für Windows stellt einen exklusiven Windows-Dienst dar, der auf allen von Relution verwalteten Windows-Geräten automatisch installiert wird, ausgenommen Geräte mit Windows Home Edition und Geräte, deren Edition nicht erkannt wird (siehe Windows Companion →).

Anders als herkömmliche Anwendungen ist diese App weder im Windows App Store noch im Relution App Store verfügbar. Mit Administratorrechten ausgestattet, richtet sich der Relution Companion ausschließlich an Administratoren und arbeitet unbemerkt im Hintergrund, ohne direkte Interaktion mit Endanwendern.

Bei der Konfiguration von Windows-Geräten werden standardmäßig sogenannte Configuration Service Provider (CSP) eingesetzt, die den Zugriff auf spezifische Einstellungen im Windows-System ermöglichen. Trotz ihrer Nützlichkeit weisen diese CSPs gewisse Einschränkungen bei den Konfigurationsmöglichkeiten auf.

Der Relution Companion für Windows überwindet diese Einschränkungen, indem er die Konfigurationsoptionen signifikant erweitert und somit eine umfassendere Anpassung ermöglicht.

Das Verhalten des Companion (u. a. Detaillevel der Log-Ausgabe, Zeitlimits für Aktionen und App-Installationen, Server-Kommunikation und Benutzerwechsel beim Anmelden) wird über die Richtlinienkonfiguration Windows Companion gesteuert, siehe Companion konfigurieren →.

Companion für Whiteboards

Für Version 26.4.0

Für Whiteboards stellt Relution je nach Verwaltungsart eigene Companion-Apps bzw. Erweiterungen bereit.

Android Classic

Dank des Relution Companions besteht die Möglichkeit, Whiteboards unterschiedlicher Hersteller auf Android-Basis effizient zu verwalten. Dies erfolgt durch die manuelle Einschreibung der Geräte über den Relution Companion.

Anschließend können die Whiteboards zentral über Richtlinien und Aktionen durch Relution gesteuert werden.

Der Funktionsumfang orientiert sich dabei an den bereitgestellten Endpunkten des jeweiligen Herstellers.

Eine Übersicht über alle Android Classic-Integrationen ist unter Hersteller → zu finden.

Android Enterprise

Relution bietet ebenfalls die Möglichkeit, interaktive Whiteboards über Android Enterprise zu verwalten. Um die Zusatzfunktionen der Whiteboards nutzen zu können, ist eine der EDLA-Erweiterungen erforderlich.

Eine Übersicht der EDLA-Erweiterungen ist unter EDLA-Erweiterungen → zu finden.

macOS Companion (Relution Daemon)

Der macOS Companion (auf dem Gerät als Relution Daemon installiert) wurde speziell für macOS-Geräte entwickelt, um die Ausführung von Skripten und die Installation von .dmg-Dateien zu ermöglichen.

Der Daemon wird automatisch installiert, sobald ein Gerät eingeschrieben ist. Voraussetzungen:

- Unter `Einstellungen` → `Relution Client Apps` ist macOS Companion aktivieren eingeschaltet (Standard: aktiviert).
- Der Mac läuft mit macOS 12 oder neuer.
- Der Mac ist nicht benutzerseitig eingeschrieben (User Enrollment).

Auf anderen Macs lassen sich keine Skripte ausführen und keine .dmg-Dateien installieren. Wird die Option deaktiviert, wird der Daemon von allen eingeschriebenen Macs deinstalliert.

Fehlt der macOS Companion auf einem Mac, der diese Voraussetzungen erfüllt, vermerkt Relution beim Gerät einen Konformitätsverstoß mit dem Hinweis `Der macOS-Companion ist nicht installiert!`.

Die Richtlinienkonfiguration Script und die Aktion Shell-Skript ausführen stehen nur bei aktiviertem macOS Companion zur Verfügung, siehe Verfügbare Konfigurationen → und Native macOS-Apps installieren →.

Für Version 26.4.0

Assets

Die Relution Assets App ermöglicht die einfache Rücknahme ausgeliehener Geräte per QR-Code-Scan. Dazu muss auf dem Trägergerät (z. B. Smartphone oder Tablet des Administrators) die Relution Assets App installiert sein. Auf dem ausgeliehenen Gerät muss die Relution Agent App vorhanden sein.

Die Anmeldung in der Assets App erfolgt mit einem Relution-Benutzerkonto der Organisation; ist für das Konto eine Mehrfaktor-Authentifizierung eingerichtet, wird sie dabei abgefragt. Das Konto benötigt Leserechte für Geräte sowie Lese- und Bearbeitungsrechte für Ausleihen. Für Shared Logout + zurücknehmen ist zusätzlich das Recht zum Bearbeiten von Geräten erforderlich, für das Zurücksetzen auf Werkseinstellungen das Recht, diese Geräteaktion auszuführen.

Schritt-für-Schritt-Anleitung zur Rücknahme

Um ein verliehenes Gerät zurückzunehmen, muss Folgendes durchgeführt werden:

Verliehenes Gerät

1. Relution Agent App öffnen
2. Seitenmenü (Hamburger-Menü) öffnen
3. Geräteinformationen auswählen
4. QR-Code muss sichtbar sein

Für Version 26.4.0

Trägergerät

1. Relution Assets App öffnen
2. QR-Code des ausgeliehenen Geräts scannen
3. Nach dem Scan stehen bis zu 3 Optionen bereit, abhängig davon, ob es sich um 1:1-Geräte oder Geräte mit Relution Shared Device handelt:

- Gerät zurücknehmen: Beendet die Ausleihe ohne weitere Änderungen
- Gerät auf Werkseinstellungen zurücksetzen + Gerät zurücknehmen: Setzt das Gerät vollständig zurück und beendet die Ausleihe
- Shared Logout + zurücknehmen: Nur bei Geräten mit der Richtlinie Relution Shared Device → verfügbar, auf denen gerade ein Benutzer angemeldet ist. Meldet diesen Benutzer ab, entfernt damit die Benutzerzuordnung des Geräts und beendet die Ausleihe.

Nach der Rückgabe

Nach erfolgreicher Ausführung wird die Ausleihe im Relution Portal als nicht mehr aktiv angezeigt (Spalte Aktiv); das Rückgabedatum steht in der Spalte Zurückgegeben.

Mehr zum Ausleihe-System in Relution unter folgendem Link: Ausleihe →

Files

Die Relution Files App ist eine mobile App für iOS- und Android-Geräte, die es ermöglicht, lokale Dateifreigaben zu integrieren. Diese Dateifreigaben können über die Protokolle SMB und WebDAV bereitgestellt werden.

Die App ist insbesondere für Unternehmen und Schulen interessant, die ihre Daten sicher und zentral verwalten möchten. Durch die Integration von lokalen Dateifreigaben können Benutzer auf relevante Dokumente und Inhalte zugreifen.

Mit der Relution Files App lässt sich auf Freigaben zugreifen, die über das Relution Portal eingerichtet wurden. Alternativ lassen sich zusätzliche Freigaben auch direkt in der App konfigurieren. Durch den integrierten Dateiexplorer besteht Zugriff auf Verzeichnisse, und verschiedene Dateien lassen sich in den Systemanwendungen öffnen.

Darüber hinaus besteht die Möglichkeit, die integrierte Kamera der Relution Files App zu verwenden, um Bilder direkt auf dem Netzlaufwerk zu speichern, anstatt sie im integrierten Fotoalbum von Apple abzulegen. Dies trägt zur Erhöhung des Datenschutzes bei.

Manuelle Einrichtung

Die manuelle Einrichtung der Dateifreigabe in der Relution Files App ist intuitiv und einfach durchzuführen. Es müssen nur ein paar Pflichtfelder ausgefüllt werden; nach der Eingabe kann die Verbindung über den Testen-Button geprüft und verbunden werden.

Für Version 26.4.0

Feld	Beschreibung
Anzeigename	Beliebiger Anzeigename für die Freigabe
URL	WebDAV- oder SMB-URL für die Dateifreigabe
Benutzername	Benutzername des Benutzers für die Dateifreigabe
Passwort	Passwort des Benutzers für die Dateifreigabe
Extension Type	Art der Integration in die Apple Files App (nur iOS)

Ausschließlich für iOS: der Extension Type `Modern` oder `Classic` muss gewählt werden. Je nach iOS-Version und Geräteverwendung (Shared) kann es innerhalb der Apple Dateien App zu einer fehlenden Darstellung kommen.
Files Bug →

Verwaltete Einrichtung

Die Dokumentation für die verwaltete Einrichtung ist unter Relution Files für iOS → und Relution Files für Android → zu finden.

Bei der verwalteten Einrichtung über die Richtlinienkonfiguration Relution Dateifreigaben ist als Art der Erweiterung (nur iOS) standardmäßig Modern voreingestellt. Unter Android installiert Relution die App automatisch als Pflicht-App, sobald eine Android-Enterprise-Richtlinie diese Konfiguration enthält.

Anwendung durch den Benutzer

Nach erfolgreicher Einrichtung der Dateifreigabe lässt sich in der App der Dateibrowser für die Navigation verwenden. Es besteht die Möglichkeit, neue Ordner innerhalb der Freigabe hinzuzufügen oder zu bearbeiten.

Zudem kann die integrierte Kamera genutzt werden, um Bilder datenschutzkonform auf der Freigabe zu speichern.

Ist die Dateifreigabe einmal eingerichtet, lässt sie sich sowohl auf iOS-Geräten als auch auf Android-Geräten direkt über die integrierte Dateien App nutzen.

Für Version 26.4.0

Parent

Die Relution Parent App ermöglicht es Eltern, die Geräte ihrer Kinder zu verwalten – ohne dass Schulen die Kontrolle verlieren. Die Schuladministration behält jederzeit die Möglichkeit, den Einrichtungsprozess der Relution Parent App individuell zu gestalten oder die Verbindung zwischen der Parent App und dem Schülergerät zu unterbinden.

Eltern können mithilfe der Relution Parent App die Nutzung installierter Apps auf dem Gerät ihres Kindes einschränken oder wieder freigeben.

Kompatibilität der Parent App

Die Relution Parent App ist kompatibel mit iOS- und Android Enterprise-Geräten der Eltern. Die zu steuernden Schülergeräte können ebenfalls Android Enterprise- oder iOS-Geräte sein.

Ein besonderes Highlight ist die plattformübergreifende Funktionalität: Eltern mit Android Enterprise-Geräten können iOS-Geräte verwalten – und umgekehrt. Das bedeutet maximale Flexibilität bei der Nutzung unterschiedlicher Gerätekombinationen.

Einrichtung

Für Version 26.4.0

Die Relution Parent App ist mit dem Relution Server ab Version `5.23.0` kompatibel. Damit ein Schülergerät verbunden werden kann, muss:

- das Gerät ein iOS- oder Android Enterprise-Gerät sein,
- der Relution Agent → mindestens in Version `5.15.0` installiert sein,
- das Gerät supervised sein,
- und der Benutzer des Schülergeräts die Berechtigung zur Kopplung besitzen.

Diese Berechtigung findet sich unter: `Relution Parent App` → `Kopplung erlauben` → `Erstellen` Sie kann einer bestehenden Rolle hinzugefügt oder über eine neue Rolle vergeben werden.

Für die Verwaltung der Kopplungsanfragen benötigt der Administrator im Bereich Einstellungen die Berechtigung Parent App Links: Lesen zum Anzeigen, Aktualisieren zum Freigeben und Bearbeiten, Löschen zum Entfernen von Einträgen.

Verknüpfung der Schülergeräte mit der Parent App

Damit nur autorisierte Eltern eine Kopplung durchführen können, muss jede Verbindung vom Administrator genehmigt werden. Ein Freitextfeld ermöglicht es, individuelle Kopplungsprozesse abzubilden (z. B. Schul-ID, Klassenname etc.).

Schülergerät

Auf dem Gerät des Kindes wird in der Relution Agent App der Bereich `Geräteinformationen` → `Parent App` geöffnet. Dort wird ein QR-Code generiert, der von der Relution Parent App der Eltern gescannt wird.

02:19 Donnerstag 11. Dez.
100 %
Geräte Information
Gerät
Service
Parent App
Standortverfolgung
Parent App
Scannen Sie den unten stehenden QR-Code mit der Relution Parent App
Erstellen Sie einen Link für dieses Gerät, um eine Verbindung mit die Parent App herzustellen

> Wird die Parent App-Sektion nicht angezeigt, ist entweder der Agent älter als Version `5.15.0`, das Gerät kein iOS- oder Android-Enterprise-Gerät oder dem Benutzer des Schülergeräts fehlt die Berechtigung `Relution Parent App` → `Kopplung erlauben`.

QR-Code und Einladung sind 24 Stunden ab Erstellen des QR-Codes gültig.

Je Schülergerät sind maximal 5 Einträge unter `Parent App Links` möglich. Mitgezählt werden alle Einträge außer denen mit dem Status Abgelaufen, also auch Offen, Eingeladen, E-Mail bestätigt, Verbunden und Vom Elternteil gelöscht. Ein QR-Code, dessen Gültigkeit von 24 Stunden verstrichen ist, behält den Status Offen und zählt weiter mit. Ist das Limit erreicht, muss der Administrator zuvor einen Eintrag unter `Parent App Links` löschen.

Eltern

Eltern laden die Relution Parent App aus dem Google Play Store oder Apple App Store herunter. Nach Zustimmung zur Datenschutzbestimmung kann die App sofort verwendet werden.

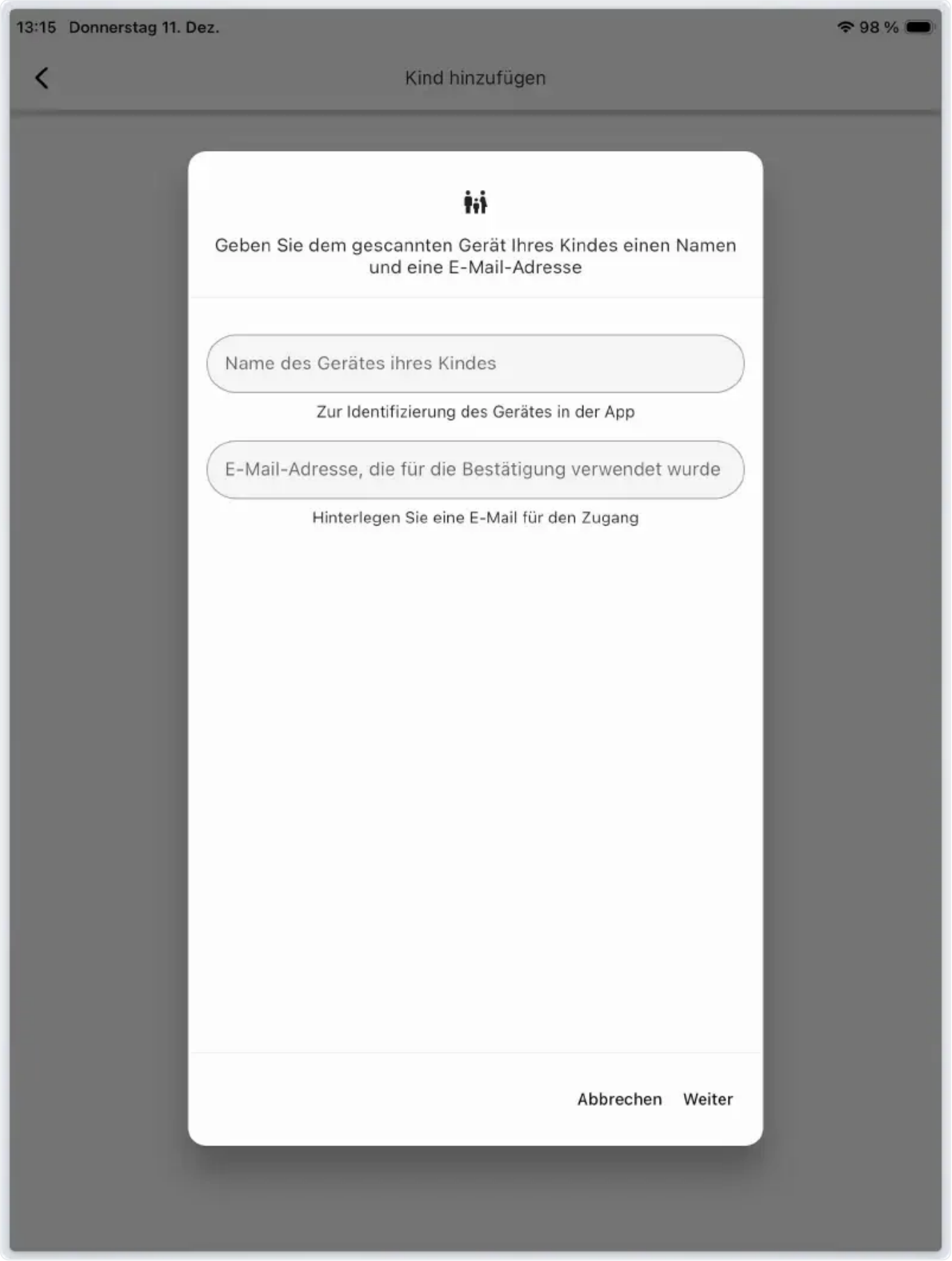
Der QR-Code wird mit dem integrierten Scanner der Parent App oder einer beliebigen QR-Code-App (z. B. Kamera-App) eingescannt.

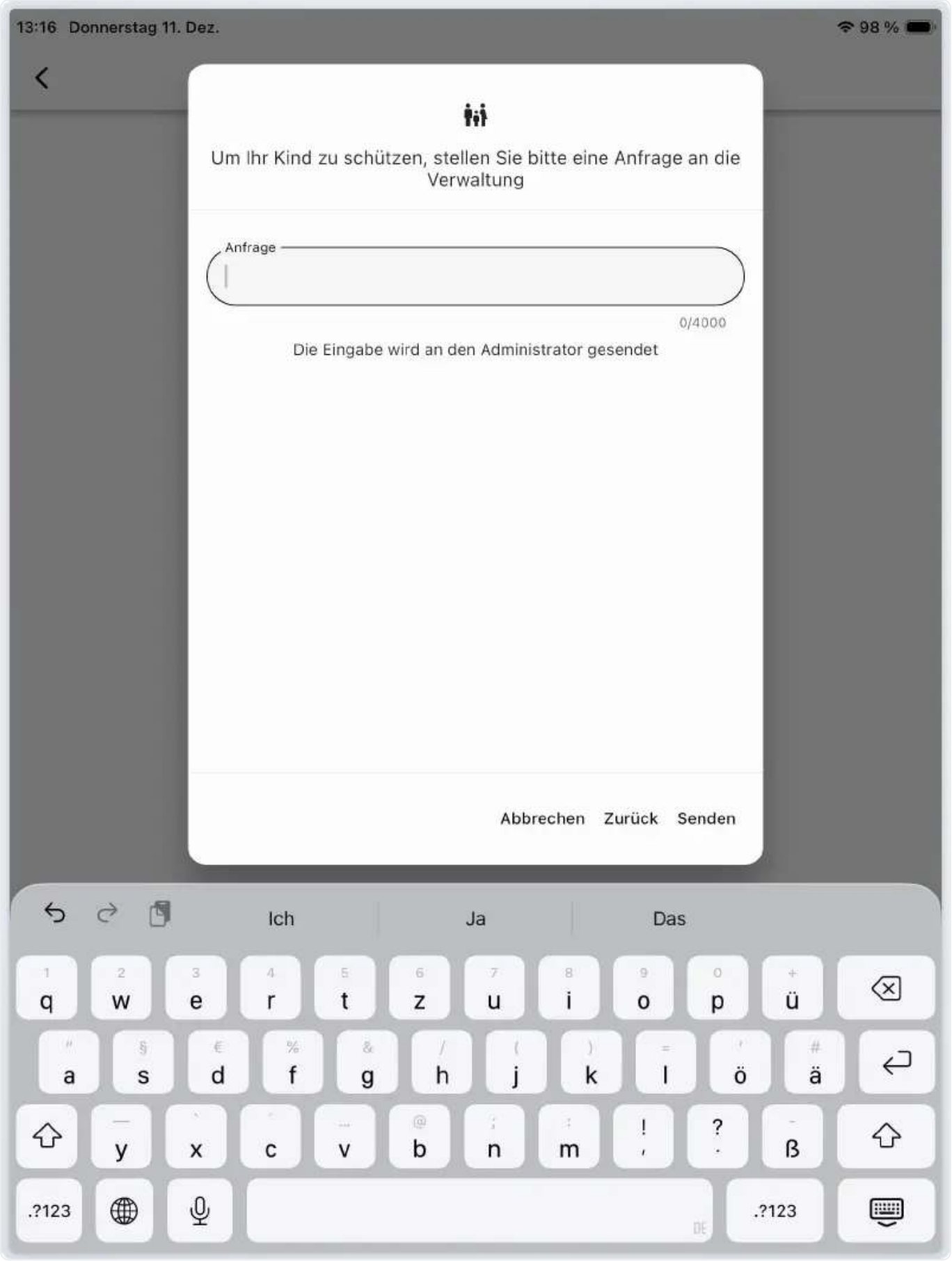
Für Version 26.4.0

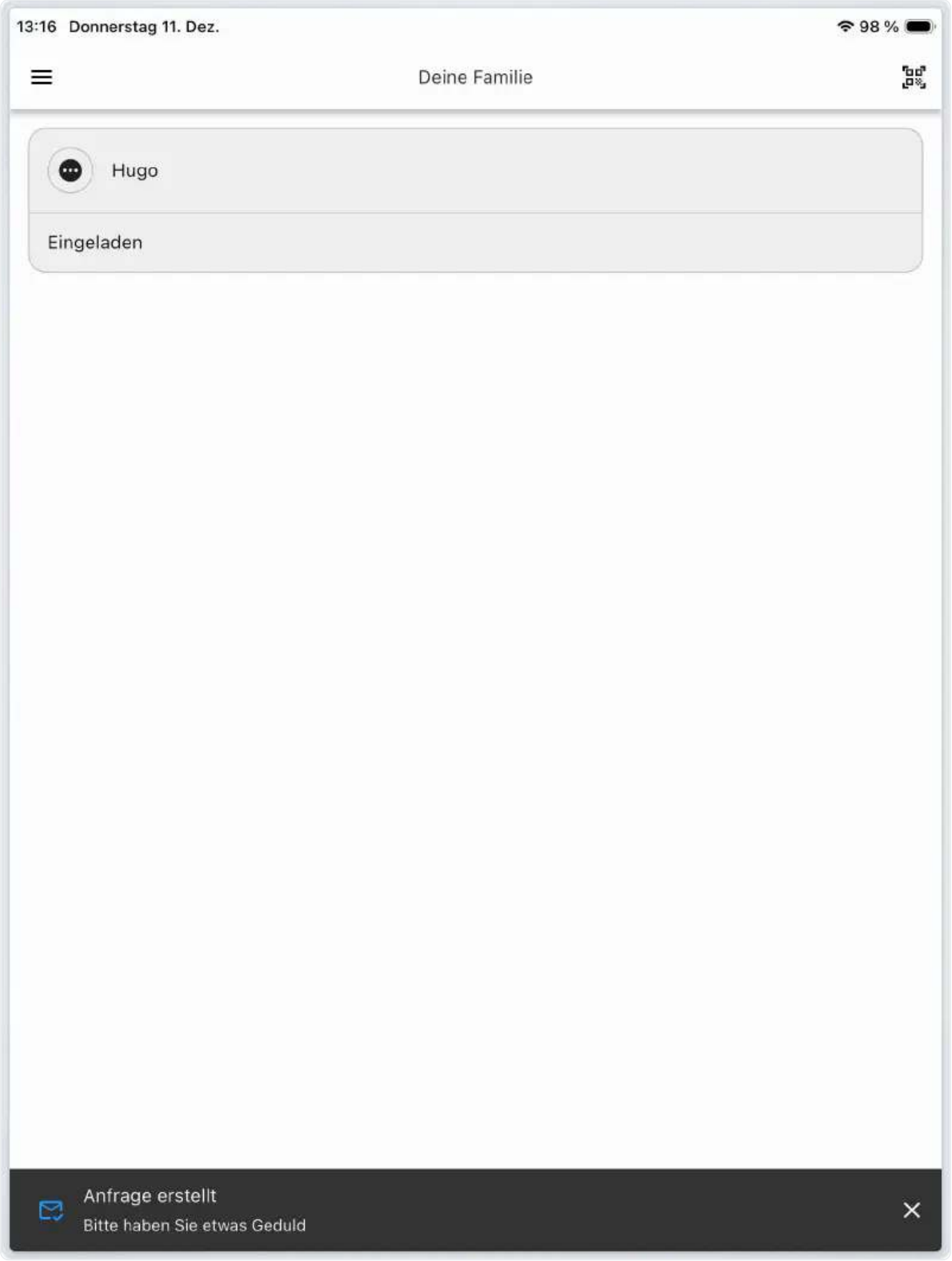
Nach dem Scan müssen Eltern:

- dem Gerät einen Namen geben,
- eine gültige E-Mail-Adresse angeben (muss bestätigt werden),
- optional einen Freitext für zusätzliche Informationen hinzufügen.

Für Version 26.4.0


13:15 Donnerstag 11. Dez.
98 %
Kind hinzufügen
Geben Sie dem gescannten Gerät Ihres Kindes einen Namen und eine E-Mail-Adresse
Name des Gerätes ihres Kindes
Zur Identifizierung des Gerätes in der App
E-Mail-Adresse, die für die Bestätigung verwendet wurde
Hinterlegen Sie eine E-Mail für den Zugang
Abbrechen
Weiter


13:16 Donnerstag 11. Dez.
98 %
Um Ihr Kind zu schützen, stellen Sie bitte eine Anfrage an die Verwaltung
Anfrage
0/4000
Die Eingabe wird an den Administrator gesendet
Abbrechen
Zurück
Senden
Ich
Ja
Das

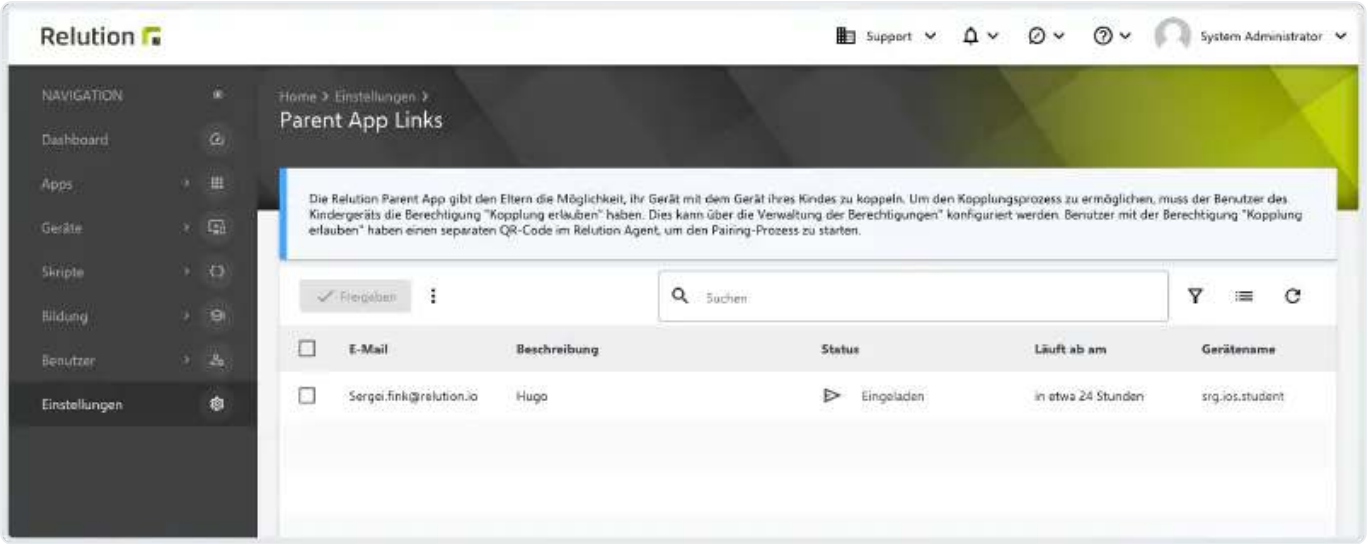

13:16 Donnerstag 11. Dez.
98 %
Deine Familie
Hugo
Eingeladen
Anfrage erstellt
Bitte haben Sie etwas Geduld

Wenn beim Absenden der Anfrage ein Fehler auftritt, ist der QR-Code möglicherweise abgelaufen oder bereits verwendet. In diesem Fall sollte die Parent App-Sektion im Relution Agent des Kindes aktualisiert werden.

Nach dem Absenden erhalten die Eltern eine E-Mail mit einem achtstelligen Bestätigungscode und einem Bestätigungslink. Nach erfolgreicher Bestätigung wechselt der Status auf E-Mail bestätigt. Wird der Bestätigungscode zehnmal falsch eingegeben, erhält der Eintrag den Status Abgelaufen und kann nicht mehr bestätigt werden.

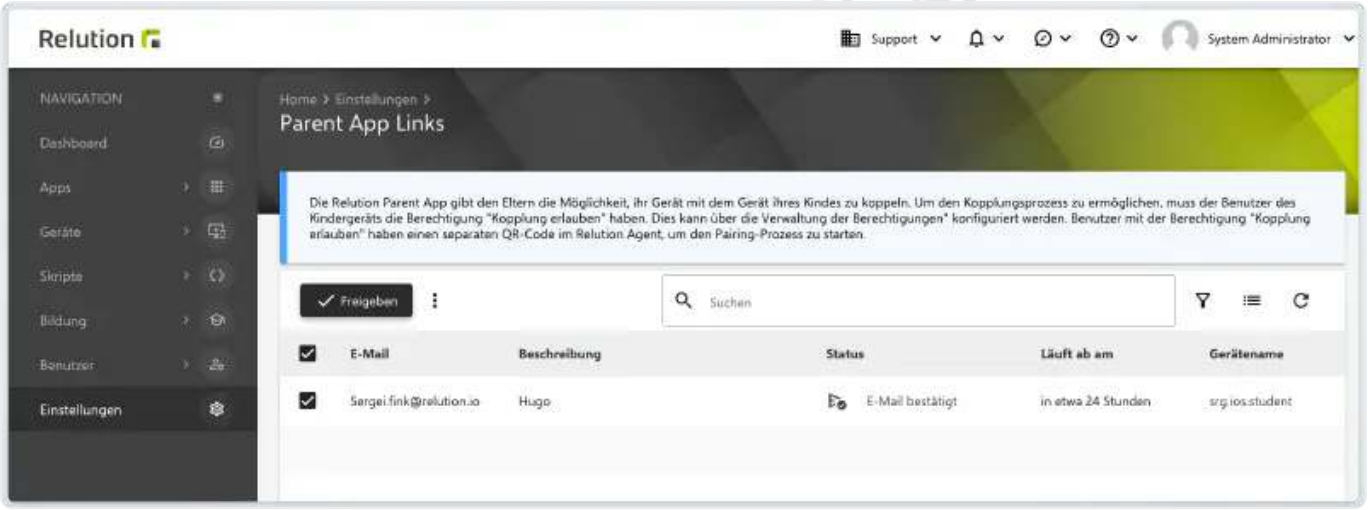
Administration

Alle Kopplungsanfragen werden unter `Einstellungen` → `Geräteverwaltung` → `Parent App Links` angezeigt. Die Kopplungen eines einzelnen Geräts sind zusätzlich in der Gerätedetailansicht unter `Geräte` → `Inventar` im Reiter Parent App Links einsehbar (nur iOS und Android Enterprise).



Die Spalte Läuft ab am zeigt für Einträge mit dem Status Offen und Eingeladen den Ablaufzeitpunkt. Nach Ablauf behält der Eintrag den Status Offen bzw. Eingeladen, kann aber nicht mehr weitergeführt werden. Einträge mit dem Status Abgelaufen blendet der Standardfilter der Liste aus.

Sobald die Eltern ihre E-Mail-Adresse bestätigt haben (Status E-Mail bestätigt), kann der Administrator die Kopplung über Freigeben genehmigen. Die Freigabe ist auch für mehrere ausgewählte Einträge gleichzeitig möglich, sofern alle den Status E-Mail bestätigt haben. Über Bearbeiten im Kontextmenü eines Eintrags lässt sich die Beschreibung anpassen.



Eine eigene Aktion zum Ablehnen gibt es nicht: Eine Anfrage wird abgelehnt, indem der Eintrag über Löschen entfernt wird. Auch eine bestehende Kopplung lässt sich jederzeit löschen. Dadurch verliert das Elternteil die Berechtigung, das Gerät des Kindes zu steuern. Besteht für das Gerät danach keine weitere Kopplung mit dem Status Verbunden, werden alle von Eltern gesetzten Sperren aufgehoben. Dasselbe gilt, wenn die Eltern die Kopplung in der Parent App entfernen.

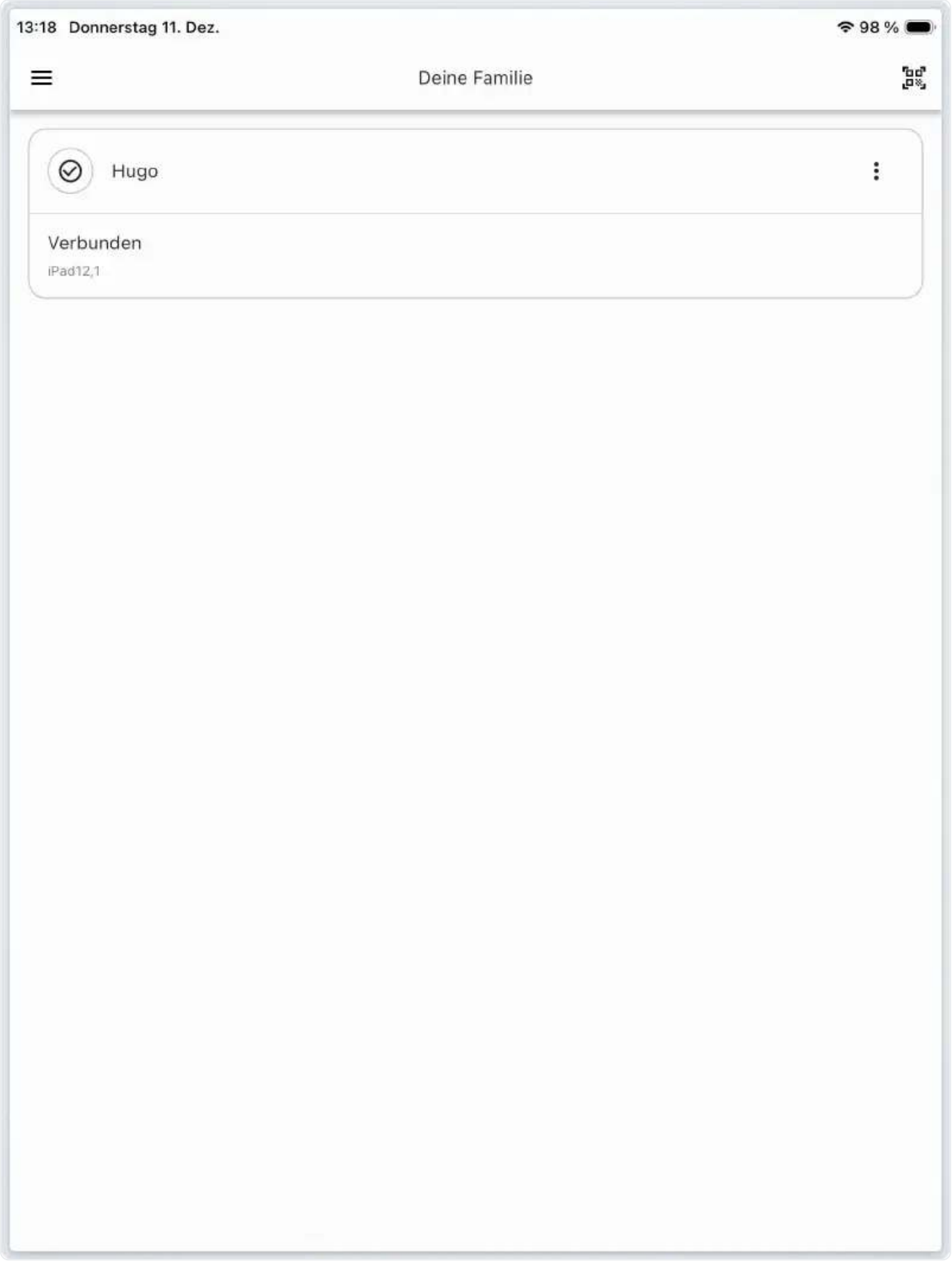
Mögliche Kopplungszustände

Status	Beschreibung
Offen	QR-Code wurde erstellt, aber noch nicht gescannt.
Eingeladen	QR-Code wurde gescannt, E-Mail aber noch nicht bestätigt.
E-Mail bestätigt	E-Mail wurde bestätigt, Freigabe durch Admin steht aus.
Verbunden	Kopplung wurde vom Administrator genehmigt.
Abgelaufen	Die E-Mail-Bestätigung ist zu oft mit einem falschen Bestätigungscode fehlgeschlagen (10 Versuche). Die Kopplung kann nicht mehr bestätigt werden.
Vom Elternteil gelöscht	Kopplung wurde von den Eltern entfernt.

Anwendung der Parent App

Nach dem Start der App sehen Eltern auf der Startseite alle verknüpften Geräte. Unter dem vergebenen Gerätenamen ist der aktuelle Status der Kopplung ersichtlich.

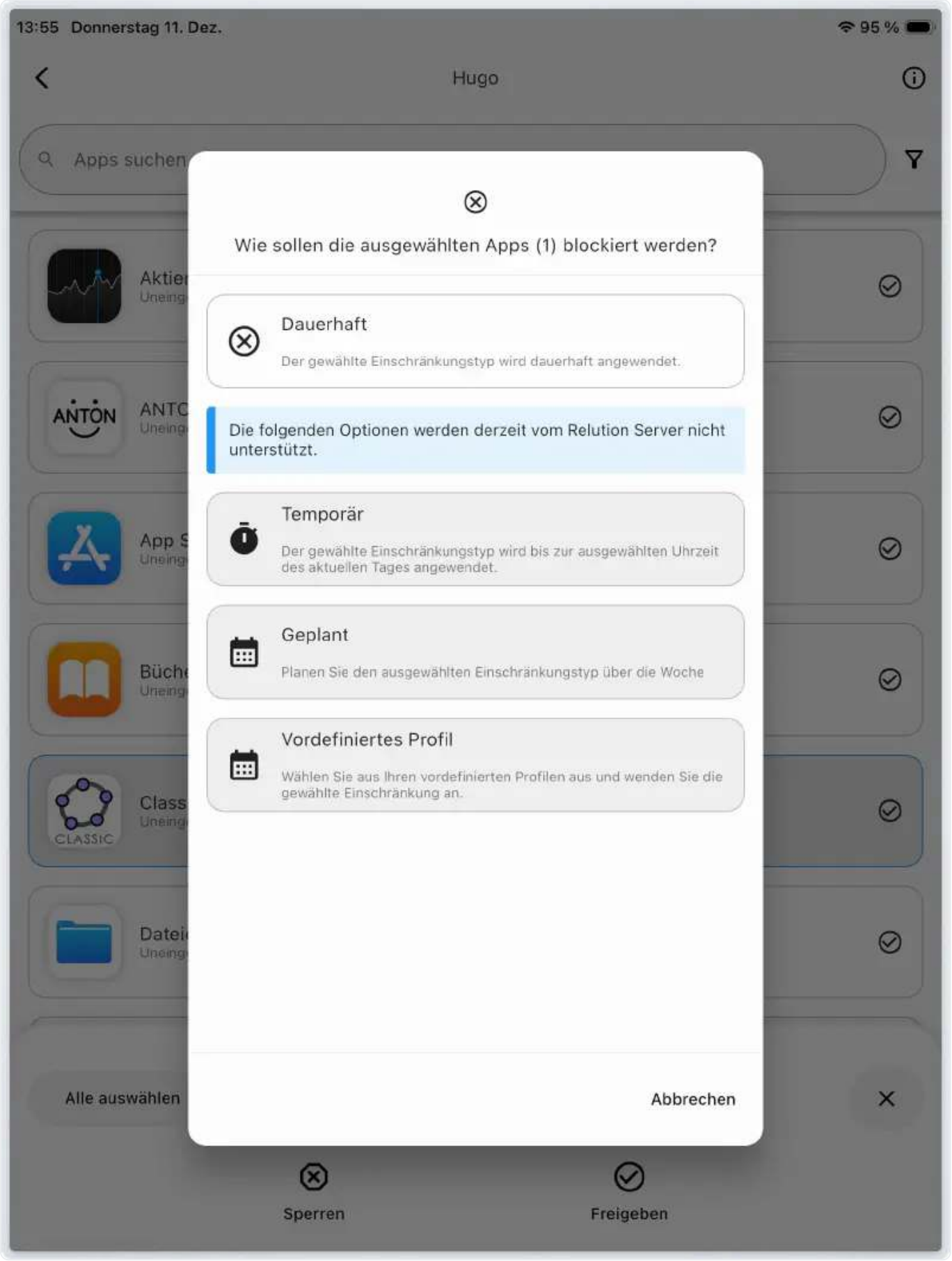
Für Version 26.4.0



Sobald die Schule die Verbindung freigegeben hat, können Eltern:

- die installierten Apps auf dem Kindergerät einsehen,
- einzelne Apps blockieren oder freigeben,
- einzelne Apps temporär oder geplant blockieren und freigeben
  Ab Relution 26.0.0
- die Änderungen per Bestätigung anwenden.

Für Version 26.4.0


13:55 Donnerstag 11. Dez.
95 %
Hugo
Apps suchen
Wie sollen die ausgewählten Apps (1) blockiert werden?
Dauerhaft
Der gewählte Einschränkungstyp wird dauerhaft angewendet.
Die folgenden Optionen werden derzeit vom Relution Server nicht unterstützt.
Temporär
Der gewählte Einschränkungstyp wird bis zur ausgewählten Uhrzeit des aktuellen Tages angewendet.
Geplant
Planen Sie den ausgewählten Einschränkungstyp über die Woche
Vordefiniertes Profil
Wählen Sie aus Ihren vordefinierten Profilen aus und wenden Sie die gewählte Einschränkung an.
Abbrechen
Alle auswählen
Sperren
Freigeben

Wenn sich eine Eltern-Restriktion mit einer Unterrichts-Restriktion überschneidet, hat der Unterricht immer Vorrang.

Anwendung der Restriktion

Ab Relution Server 26.0.0 in Kombination mit Relution Parent 26.0.0 können Eltern Restriktionen nun flexibel zeitlich steuern. Dafür stehen drei unterschiedliche Arten der zeitlichen Beschränkung zur Auswahl:

1. Dauerhaft
    - Die Restriktion wird dauerhaft, ohne zeitliche Begrenzung, angewendet und ersetzt die zuvor ausgewählte Restriktion vollständig – inklusive ihres Typs.
    - Diese Option eignet sich für langfristige, feste Regeln zur Gerätesteuerung.
2. Temporär
    - Diese Restriktion gilt bis zum angegebenen Zeitpunkt des aktuellen Tages. Falls der Zeitpunkt im aktuellen Tag in der Vergangenheit liegt, so wird der nächste Tag genommen.
    - Temporäre Beschränkungen überschreiben ausschließlich andere temporäre Restriktionen und sorgen anschließend für eine nahtlose Rückkehr zur ursprünglichen Einstellung.
    - Ideal für situative Einschränkungen, z. B. während Lern- oder Ruhezeiten.
3. Eingeplant
    - Die Restriktion gilt für den angegebenen Zeitplan; außerhalb dieses Zeitfensters wird die invertierte Restriktion angewendet.
    - Zeitpläne können in Relution Parent als Profile gespeichert und flexibel wiederverwendet werden, um wiederkehrende Muster schnell anzuwenden.
    - Änderungen am Profil haben keinen Einfluss auf bereits angewendete Restriktionen und müssen erneut auf die gewünschten Applikationen angewendet werden.

Für Version 26.4.0

Die aktuelle zeitliche Einschränkung wird als Symbol sowie in textueller Form für jede App angezeigt.

Hinweise

- Ist auf einem iOS-Schülergerät eine Allowlist aktiv, hat diese Vorrang vor der Parent App. Die Allowlist kann aus der Konfiguration App Konformität (Listenart Alle Apps in der folgenden Liste sind erlaubt) oder aus der Konfiguration Restriktionen (App Bundle ID Positivliste) stammen.
- Auch ein aktiver Unterricht hat Vorrang vor den von Eltern gesetzten Beschränkungen.
- Die Relution-Apps auf dem Schülergerät (z. B. Relution Agent, Relution Companion, Relution Teacher) können von Eltern nicht gesperrt werden.
- Ab iPadOS 26 des Kindgerätes werden System-Applikationen (z. B. Safari, Books) der Parent App zur Verfügung gestellt. Für frühere iPadOS-Versionen ist diese Möglichkeit nicht verfügbar.

Fehlermeldungen

- Fehlermeldung 500
  Hier ist der E-Mail-Versand vom Relution Server aus nicht möglich. Der E-Mail-Versand wird in der `Global`-Organisation unter `Einstellungen` → `E-Mail Konfiguration` eingerichtet und dort im Bereich E-Mail-Konfiguration testen geprüft (siehe Mail Versand →).

Für Version 26.4.0

Teacher

Die Relution Teacher App (iOS, Android & Windows, ab Relution 5.24 auch als Web App) erlaubt es Lehrkräften, unterrichtsspezifische Profile zu erstellen, mit denen sich Apps, Gerätefunktionen und Weblinks für den Unterricht vorbereiten und verwalten lassen.

Zudem ermöglicht sie, Teilnehmerkreise zu definieren und den Unterricht zu steuern.

Dank der Integration mit Apple Classroom und Samsung Classroom Management → (separate Lizenz erforderlich) ist eine umfassende Steuerung auch während des Unterrichts möglich – ganz ohne Apple Account auf den Schülergeräten.

Voraussetzungen für die Nutzung

Um die Relution Teacher App verwenden zu können, ist eine Relution Education Lizenz erforderlich.

Zudem sollten Klassen mit den dazugehörigen Schülern und Lehrkräften angelegt sein (`Bildung` → `Klassen`).

Die Lehrkraft benötigt mindestens die Berechtigung `Bildung` → `Teacher App verwenden`. Sie ist in der Systemgruppe [Eindeutiger Name der Organisation] Teacher (z. B. `UIT Teacher`) enthalten, die im Benutzerkonto unter Gruppen & Berechtigungen im Feld Gruppen zugewiesen wird; alternativ lässt sie sich über eine Rolle im Feld Berechtigungen vergeben.

Als Schülergeräte werden iOS-, Android-Enterprise- und ChromeOS-Geräte unterstützt.

Für Version 26.4.0

Aufbau

Der Inhalt für das Schülergerät wird durch ein Profil festgelegt. Zusätzlich werden die Teilnehmer definiert und die Laufzeit festgesetzt. Danach lässt sich der Unterricht starten.

Profile

In den Profilen wird definiert, womit das Gerät für den Unterricht ausgestattet wird.

Die Lehrkraft hat die Möglichkeit, zwischen privaten und öffentlichen Profilen zu wählen. Letzteres darf von allen Lehrkräften der Organisation verwendet werden. Das Bearbeiten und Löschen bleiben dem Ersteller vorbehalten.

Bei dem Prüfungsprofil (iOS, ChromeOS) wird zusätzlich das Hintergrundbild gesetzt.

Apps, Weblinks und System Apps sowie bestimmte Einschränkungen lassen sich im Profil definieren.

Apps sollten nicht erst mit dem Profil installiert werden, um die Rüstzeit für den Unterricht zu minimieren. Wenn der Prüfungsmodus verwendet wird, sollte ein Standard-Hintergrundbild in einer separaten Richtlinie festgelegt werden. Um Schüler z. B. permanent im WLAN zu halten oder das Deaktivieren von Bluetooth zu verhindern, bietet sich ebenfalls eine separate Richtlinie an.

Teilnehmer verwalten

Für den Unterricht kann eine hinterlegte Klasse ausgewählt werden. Fehlende Schüler lassen sich hier direkt vom Unterricht herausnehmen. Somit wird das Profil nur auf die Geräte der Anwesenden verteilt.

Alternativ lässt sich auch eine Ad-hoc-Klasse erstellen. Hier stehen dann alle Schüler der Organisation zur Auswahl.

Für wiederkehrende Ad-hoc-Gruppen empfiehlt es sich, über das Portal eigene Klassen zu definieren oder Schüler mehreren Klassen zuzuordnen.

Unterrichtsdauer festlegen

Ein Profil ist zeitlich begrenzt – z. B. bis zum Ende der aktuellen Unterrichtsstunde.

Unter Unterrichtseinstellungen → lassen sich die einzelnen Stunden festlegen.

Unterricht starten und steuern

Je Lehrkraft kann nur ein Unterricht gleichzeitig laufen. Beim Start eines Unterrichts werden andere nicht beendete Unterrichte derselben Lehrkraft beendet bzw. gelöscht. Nehmen Schüler bereits an einem anderen aktiven Unterricht teil, erscheint ein Hinweis; wird der Unterricht trotzdem gestartet, werden sie aus dem anderen Unterricht herausgenommen.

Ist in den Unterrichtseinstellungen → die Option Unterricht auf Stundenplan begrenzen aktiv, lässt sich Unterricht außerhalb des Stundenplans nicht starten.

Für Version 26.4.0

Während eines laufenden Unterrichts können Lehrkräfte Teilnehmer anpassen, die verbleibende Zeit ändern und den Unterricht manuell beenden. Beim Beenden lassen sich geteilte iPads (Shared iPad) abmelden; im laufenden Unterricht ist das auch für einzelne geteilte Geräte möglich.

Das Profil wird nach dem Ablauf der definierten Zeit oder nach dem Beenden von den Schülergeräten entfernt.

Beim manuellen Beenden sendet Relution die Änderungen sofort an die Schülergeräte, nach Ablauf der definierten Zeit innerhalb von etwa einer Minute. Gesperrte Websites und Einschränkungen des Unterrichts werden aufgehoben, sobald die Änderung das Gerät erreicht. Ist ein Gerät zu diesem Zeitpunkt nicht erreichbar, erhält es die Änderung, sobald es wieder erreichbar ist. Für den Unterricht installierte Apps werden dabei nicht deinstalliert.

> Die Anordnung der Apps und Ordner kann nicht gespeichert werden, da sich durch das Entfernen der Profile die Strukturen des Homescreens verändern und abgeglichen werden.

Unterrichtsvorlage erstellen

Unterrichtseinheiten lassen sich als persönliche oder geteilte Vorlagen abspeichern, um sie schnell wiederzuverwenden.

Eine Unterrichtsvorlage umfasst die folgenden Einstellungen:

Typ der Unterrichtsvorlage

- Persönliche Vorlage (privat)
- Verwendung nur für den Ersteller der Vorlage
- Geteilte Vorlage (geteilt)
- Verwendung der Vorlage für alle Lehrkräfte

Private Vorlagen ohne Besitzer (z. B. nach dem Löschen der Lehrkraft) werden täglich um 01:00 Uhr automatisch gelöscht.

Prüfungsmodus (iOS, ChromeOS)

- Prüfungsmodus
- Setzt auf iOS- und ChromeOS-Geräten der Schüler ein lila Hintergrundbild mit dem Schriftzug „Klausur“ (bei englischer Server-Standardsprache „Exam“), damit sich auf einen Blick erkennen lässt, ob das Gerät im gewünschten Zustand ist.
- Auf iOS lässt sich das Hintergrundbild während der Prüfung nicht ändern, und die Spotlight-Suche zeigt keine Internetergebnisse an.
- Nach Ende der Prüfung setzt Relution ein Standard-Hintergrundbild. Auf iOS entfällt das, wenn eine Richtlinie bereits ein Hintergrundbild für Sperr- und Home-Bildschirm festlegt.

Für Version 26.4.0

Einzel-App-Modus

- Versetzt das Gerät (Android oder iOS) in den Single-App-Modus-Betrieb.
- Dafür muss im Unterricht genau eine App ausgewählt sein.
- Zusätzlich lassen sich Gerätefunktionen im Einzel-App-Modus einschränken, unter iOS z. B. Touch, Drehung, Lautstärketasten, Klingelschalter, Standby-Taste und automatische Sperre, unter Android z. B. Ein/Aus-Taste, Systemnavigation, Statusleiste, Geräteeinstellungen sowie das Anlassen des Displays beim Laden.

Apps, die während des Unterrichtes genutzt werden dürfen

- Hier kann eine Auswahl an Apps erfolgen, die den Schülern für die Dauer des Unterrichtes zur Verfügung stehen.

Gerätefunktionen während des Unterrichtes

- Kamera erlauben (Android + iOS)
- Screenshot erlauben (Android + iOS)
- Safari und Weblinks anzeigen (iOS)
- Weblinks verwenden, um Webinhalte zu filtern (iOS)
- Nachrichten-App anzeigen (iOS)
- Rechtschreibhilfen erlauben (iOS)
- AirDrop erlauben (iOS)
- Bluetooth erzwingen (iOS)

Alternativ lässt sich festlegen, dass für den Unterricht keine unterrichtsspezifischen Einschränkungen angewendet werden.

Weblinks und Surfeinschränkungen

Neu in 26.5

Weblinks lassen sich in einer Unterrichtsvorlage auf zwei unabhängig voneinander konfigurierbaren Wegen einsetzen:

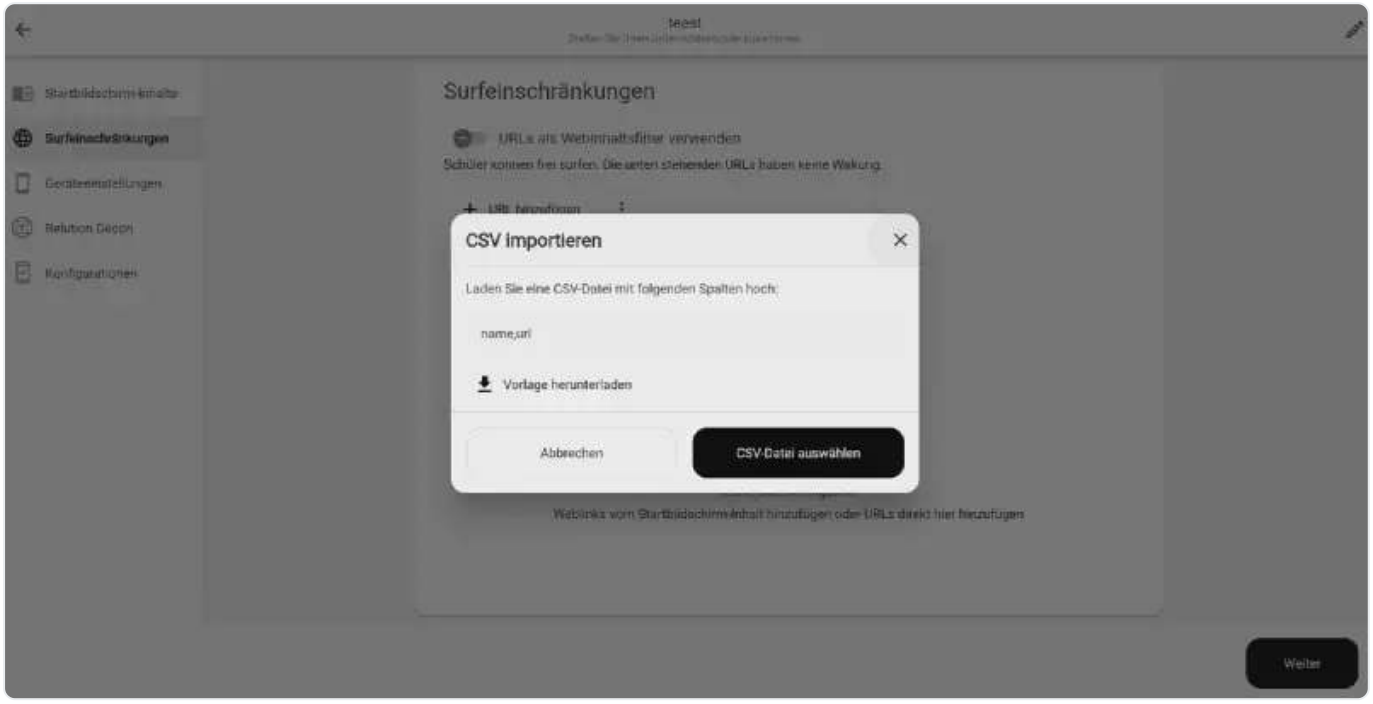
- Unter Startbildschirm-Inhalte werden Weblinks für die Dauer des Unterrichts als Verknüpfung auf dem Startbildschirm der Schülergeräte abgelegt. Über Hinzufügen lassen sich weitere Weblinks aufnehmen.
- Unter Surfeinschränkungen dienen URLs als Positivliste für den Webinhaltsfilter (iOS). Der Schalter URLs als Webinhaltsfilter verwenden aktiviert die Filterung. Ist er ausgeschaltet, kann frei gesurft werden und die aufgeführten URLs haben keine Wirkung.

In der Liste der Surfeinschränkungen legt je URL die Spalte Aktiv fest, ob die URL im Webinhaltsfilter erlaubt ist, und die Spalte Startbildschirm, ob sie zusätzlich als Verknüpfung auf dem Startbildschirm erscheint. Ein Eintrag kann so ausschließlich als erlaubte URL dienen, ohne auf dem Startbildschirm aufzutauchen. Bei eingeschaltetem Webinhaltsfilter erscheint eine nicht aktive URL auch nicht auf dem Startbildschirm. Über URL hinzufügen lassen sich URLs direkt ergänzen; bereits unter Startbildschirm-Inhalte angelegte Weblinks können ebenfalls übernommen werden.

Für Version 26.4.0

Weblinks per CSV importieren

Über das 3-Punkte-Menü → CSV importieren lässt sich eine Liste von Weblinks als CSV-Datei hochladen. Die Datei enthält die Spalten `name` und `url`; eine passende Vorlage steht über Vorlage herunterladen bereit.



```
name,url
Wikipedia,https://wikipedia.org
```

App Store Einstellungen

- Google Play Store erlauben (Android)
- App Store anzeigen (iOS)
- iTunes Store anzeigen (iOS)

Relution Decon

- Relution Decon aktivieren (lizenzpflichtig. Zudem muss Schüler-Geräten in Relution eine Decon-Richtlinie zugewiesen sein)
- BPjM-Liste
- Sichere Suche
- Filter Typ
  - Aus
  - Altersbeschränkung
    - 0+
    - 6+
    - 12+
    - 16+
  - Kategorien
    - Erwachseneninhalte
    - Werbung
    - Kommunikation
    - Soziale Medien
    - Unterhaltung
    - Musik
    - Nachrichten
    - Einkaufen
    - Arbeit
    - Bildung
    - Generative KI
    - Phishing
    - Sonstiges

Für Version 26.4.0

Mehr zu Relution Decon →

Zusätzlich lassen sich im Unterricht eigene Listen erlaubter und gesperrter Websites hinterlegen. Die aktiven Weblinks des Unterrichts werden automatisch als erlaubte Websites übernommen. Voreingestellt sind der Filtertyp Kategorien und die Altersstufe 12+.

Hinweis: Für die Dauer der Unterrichtsstunde wird die sonst gültige Decon-Konfiguration überschrieben.

Konfigurationen

Als Konfigurationen werden in Relution Teacher die Bildungsgruppen bezeichnet, die im Portal angelegt und mit Richtlinien versehen wurden: Bildungsgruppen →.

In der Unterrichtsvorlage lassen sich im Bereich Konfigurationen eine oder mehrere Konfigurationen auswählen; zu jeder werden Name, Beschreibung und die verknüpften Richtlinien angezeigt. Beim Start des Unterrichts werden die verknüpften Richtlinien auf die Schülergeräte angewendet und beim Beenden wieder entfernt.

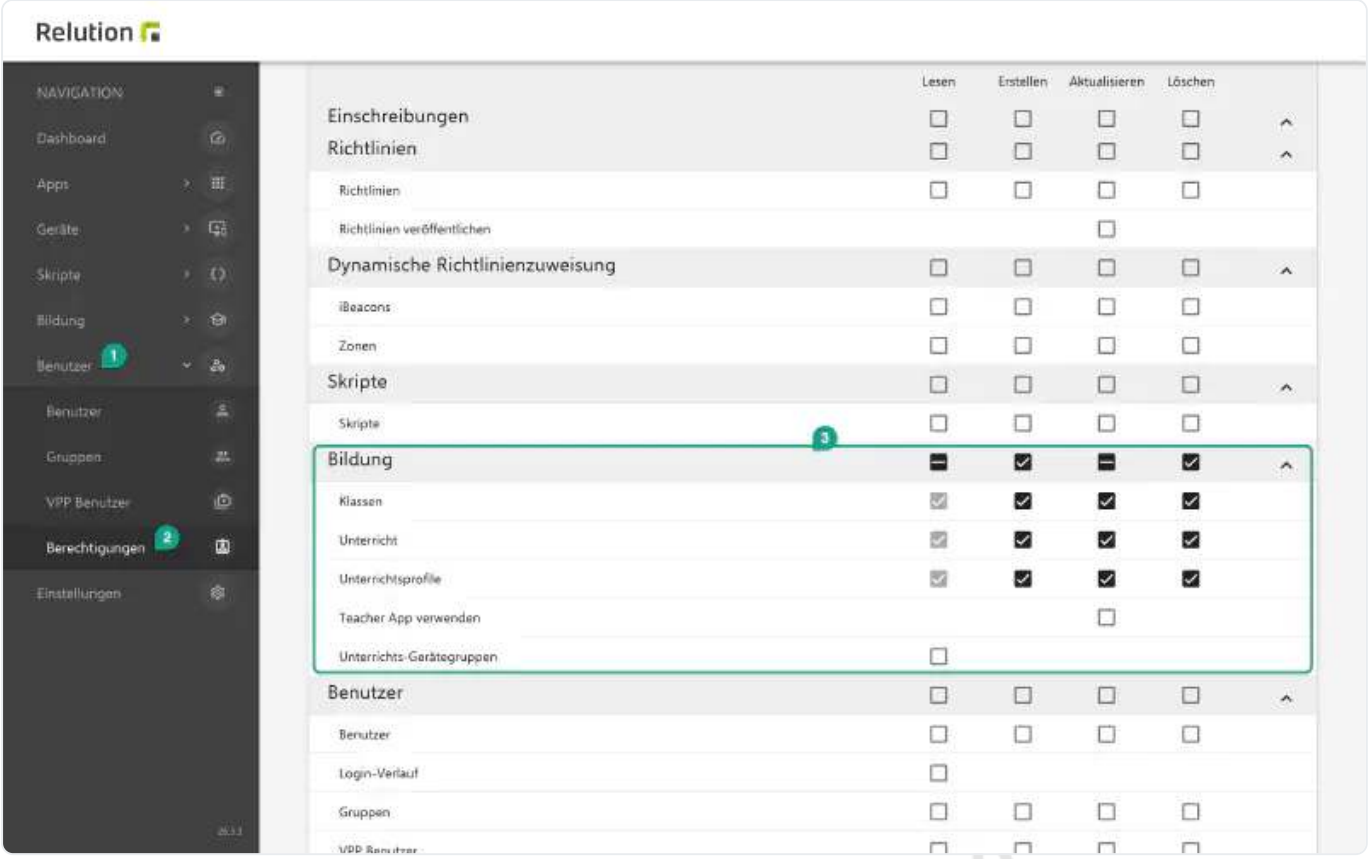
Die Auswahl setzt die Leseberechtigung `Bildung` → `Unterrichts-Gerätegruppen` voraus. Ohne diese Berechtigung werden keine Konfigurationen angezeigt.

Admin-Modus für den Unterrichtseinblick

Für die Admin-Ansicht in der App ist mindestens die Leseberechtigung `Bildung` → `Unterricht` notwendig.

Der Admin hat Zugriff auf alle Unterrichte seiner Organisation. Diese können eingesehen und im Problemfall weitere Informationen gewonnen werden.

Mit der Berechtigung Aktualisieren für `Bildung` → `Unterricht` lässt sich der Unterricht bearbeiten (Schüler hinzufügen/entfernen) und vorzeitig beenden.



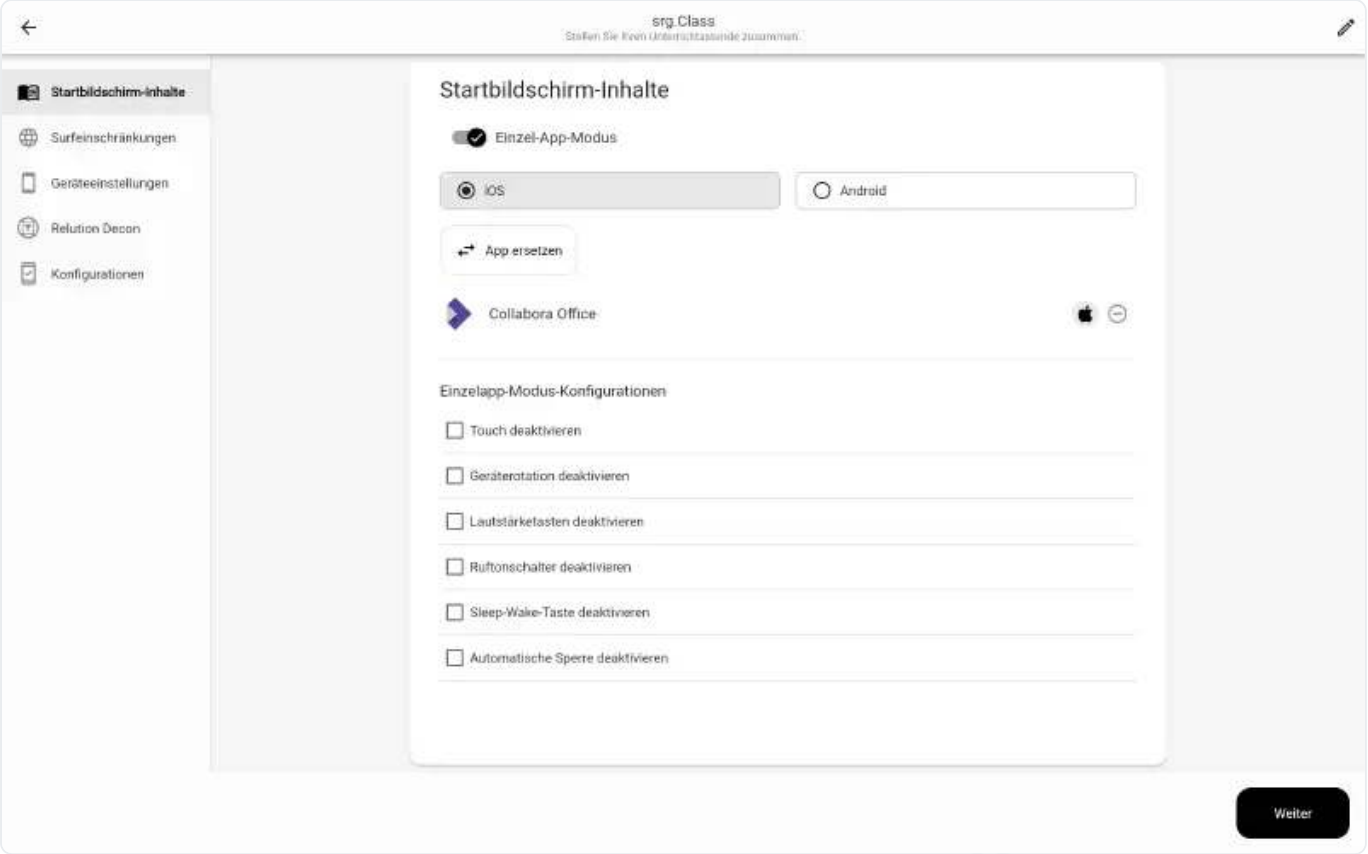
Für Version 26.4.0

Relution Teacher als Web-App

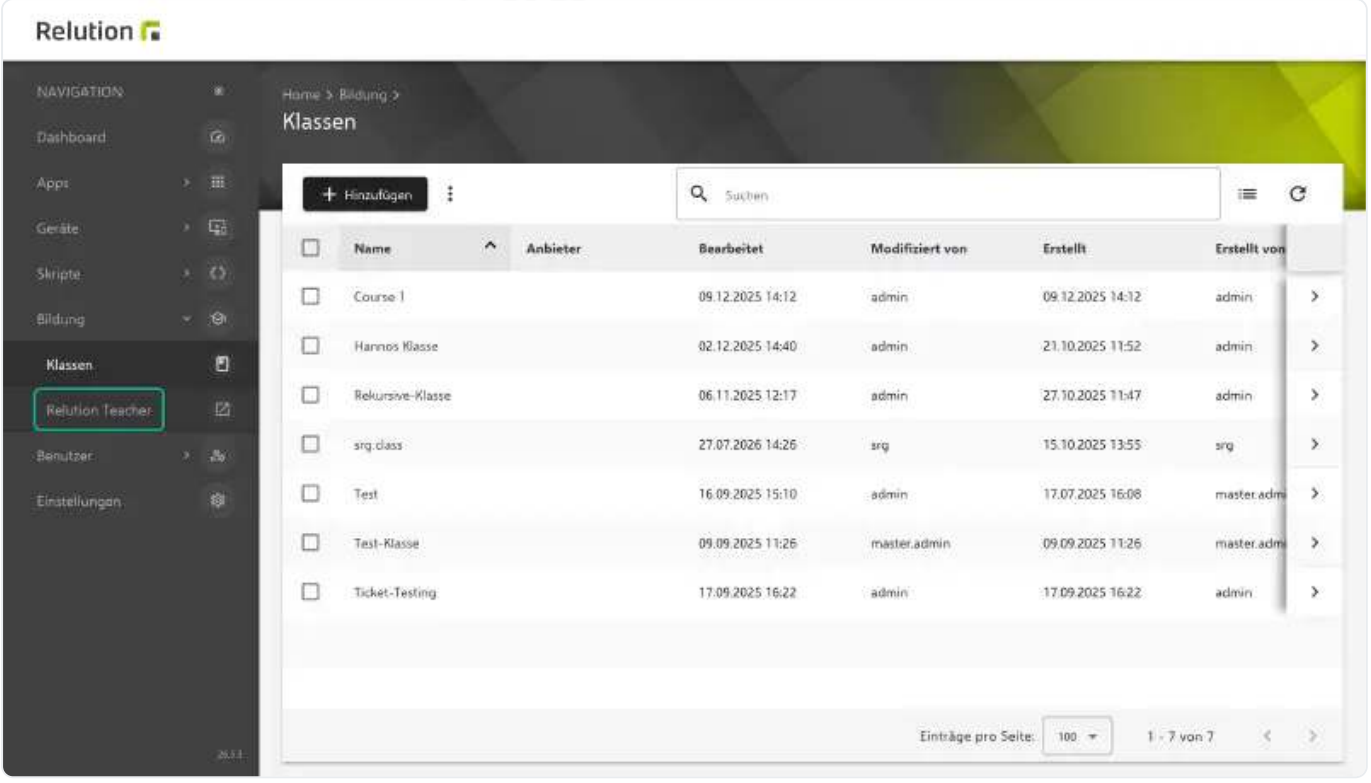
Seit Relution Server 5.24 steht die Relution Teacher Web-App zur Verfügung.

Nun können Lehrkräfte in gleicher Weise wie auf iOS und Android Unterrichtseinheiten direkt aus einem Browserfenster heraus erstellen, starten und steuern.

Diese nahtlose Integration ermöglicht eine reibungslose und effiziente Unterrichtsorganisation, die den Anforderungen moderner Bildungsumgebungen gerecht wird.



Die Web-App ist im Navigationsmenü unter `Bildung` → `Relution Teacher` zugänglich und öffnet sich in einem neuen Browser-Tab. Der Menüeintrag erscheint nur mit der Berechtigung `Bildung` → `Teacher App verwenden`.



Multitenant-Funktion für Lehrkräfte mit mehreren Schulen

Die Multimandantenfähigkeit von Relution Teacher ermöglicht es Lehrkräften, die Funktionalität von Relution Teacher auf mehrere Organisationen auszuweiten.

Dies ist besonders hilfreich, wenn Lehrkräfte an mehreren Schulen tätig sind, die ihre Schülergeräte über dieselbe Relution-Instanz verwalten.

Konfiguration

Um den Zugriff auf mehrere Relution-Organisationen zu ermöglichen, sind folgende Schritte notwendig:

- Die Anmeldung erfolgt in der Organisation `Global`.
- Im Relution-Portal wird im Bereich `Benutzer` der entsprechende Benutzer (Lehrkraft) gesucht und bearbeitet.
- Der Benutzer wird den Systembenutzergruppen der zusätzlichen Organisation(en) hinzugefügt, z. B. der Gruppe [Eindeutiger Name der Organisation] Teacher.

Nach der Konfiguration kann in der Relution Teacher App sowie im Relution Teacher Web-Interface über das Seitenmenü die gewünschte Organisation ausgewählt werden. Zur Auswahl stehen nur Organisationen, in denen die Lehrkraft die Berechtigung `Bildung` → `Teacher App verwenden` besitzt.

Zusätzlich zeigt in der Organisation `Global` unter `Bildung` → `Klassen` die Spalte Organisation, zu welcher Relution-Organisation eine Klasse gehört.

Für Version 26.4.0

Hinweis

Beim Anwenden eines Unterrichtes über Relution Teacher wird das individuelle Homescreen-Layout vom Benutzer verworfen.

Technisch gibt es aktuell keine Möglichkeit, die App-Anordnung vom Benutzer zu speichern und nach Beendigung des Unterrichtes wieder anzuwenden.

Es gibt die Möglichkeit, via Home Screen Layout Konfiguration zentral ein Layout vorzugeben, sodass ein einheitlicher Stand über alle Geräte hinweg vorgegeben werden kann.

Homescreen Layout →

Unterrichtseinstellungen

Unter `Einstellungen` → `Bildung` → `Unterrichtseinstellungen` wird der zeitliche Rahmen festgelegt, innerhalb dessen Lehrkräfte über die Teacher App → Unterricht starten können. Die Seite ist nur mit einer Education- oder Free-Lizenz sichtbar.

Erforderlich ist die Berechtigung Unterrichtseinstellungen im Bereich Einstellungen: Lesen zum Anzeigen, Aktualisieren zum Ändern. Ohne Aktualisieren ist die Seite schreibgeschützt. Hinzugefügte, bearbeitete und gelöschte Schulstunden werden erst mit Speichern der Seite übernommen.

Schulstunden

Die Schulstunden werden als Liste mit Name, Beschreibung, Startzeit und Endzeit gepflegt. Name ist ein Pflichtfeld, die Beschreibung ist optional. Schulstunden dürfen sich zeitlich nicht überschneiden, das gilt auch beim Bearbeiten. Auch eine Startzeit, die genau auf das Ende einer anderen Schulstunde fällt, gilt als Überschneidung, daher ist mindestens eine Minute Abstand nötig. Die Endzeit muss nach der Startzeit liegen.

Ab Werk ist die Liste mit 14 Schulstunden (1. Stunde bis 14. Stunde, 07:45 bis 21:05 Uhr) vorbelegt, als Unterrichtstage sind Montag bis Freitag gesetzt, die Zeitzone steht auf UTC und die Begrenzung auf den Stundenplan ist ausgeschaltet.

Für Version 26.4.0

Allgemeine Einstellungen

- Systemweite Einstellungen überschreiben: Nur bei Mandanten-Organisationen sichtbar. Erlaubt es, von den systemweiten Unterrichtseinstellungen abzuweichen. Ist die Option ausgeschaltet, sind alle Felder gesperrt und Schulstunden lassen sich weder hinzufügen noch bearbeiten; Änderungen in der System-Organisation werden automatisch übernommen. Beim Zurückschalten auf die systemweiten Einstellungen gelten wieder die Werte der System-Organisation.
- Zeitzone: Zeitzone, auf die sich die konfigurierten Schulstunden beziehen.
- Unterricht auf Stundenplan begrenzen: Ist diese Option aktiviert, lässt sich in der Teacher App nur an den gewählten Unterrichtstagen Unterricht starten, und zwar frühestens zu Beginn der ersten und mit einer geplanten Endzeit spätestens zum Ende der letzten Schulstunde. Pausen zwischen einzelnen Schulstunden werden nicht gesperrt.
    - Unterrichtstage: Wird bei aktivierter Begrenzung zur Pflichtangabe. Legt fest, an welchen Wochentagen Unterricht stattfinden darf.

Zugriff auf Profilbilder für Apple Education-Konfigurationen

Steuert, ob Relution auf die Profilbilder der Benutzer zugreifen darf, um die gemeinsame Anmeldung (Shared iPad) und Apple Classroom mit den hinterlegten Profilbildern zu versorgen. Standardmäßig aktiviert. Bei Deaktiviert liefert Relution keine Profilbilder an Shared iPad und Apple Classroom aus.

Die Profilbilder werden nur an Geräte mit einer Apple-Education-Konfiguration ausgeliefert, und nur für Benutzer, die Mitglied einer Klasse dieser Konfiguration sind.

Homescreen

Die Relution Homescreen App ist ein Launcher, mit dem Administratoren den Startbildschirm vollständig verwalteter Android-Enterprise-Geräte aus der Ferne anpassen können. Die App ersetzt den vorinstallierten Launcher und wird zentral über die Konfiguration Relution Homescreen Layout in einer Android-Enterprise-Richtlinie konfiguriert. Sobald die Richtlinie angewendet wird, wird sie automatisch auf den Geräten installiert.

Den vorinstallierten Launcher ersetzt die App nur auf vollständig verwalteten Geräten (Device Owner). Bei den übrigen Android-Enterprise-Einschreibungen erhält die App das konfigurierte Layout, wird aber nicht als Launcher gesetzt. Für Android Legacy gibt es diese Konfiguration nicht.

Die App bietet eine Vielzahl von Funktionen, um den Startbildschirm individuell zu gestalten:

- Anpassung des Themes
- Auswahl des Wallpapers
- Auswahl und Anordnung der angezeigten Apps

Konfiguration

Die Konfiguration Relution Homescreen Layout umfasst folgende Einstellungen:

- Layout: Theme (Light als Standard oder Dark), Rastergröße (Auto, 4x4, 5x4 (Standard), 6x4) und Bildschirmausrichtung (Automatisch als Standard, Landscape, Portrait).
- Hintergrundbild: Bilddatei sowie optional ein Text auf dem Hintergrundbild mit Farbe des Textes (Hex-Wert, Standard `#ffffff`).
- Einschränkungen → Erlaubte Apps: Nur Apps aus dem Layout anzeigen (Standard) oder Alle Apps anzeigen. Bei Nur Apps aus dem Layout anzeigen sind auf dem Gerät nur die Apps aus dem Layout verfügbar.
- Im Layout-Editor werden Apps, Ordner und Weblinks per Drag & Drop auf Seiten und im Dock angeordnet; im Dock sind keine Ordner möglich. Apps lassen sich auch manuell über den Paketnamen hinzufügen, das neue Element erscheint dann auf der ersten Seite. Auf dem Gerät ist das Layout gesperrt und kann vom Benutzer nicht verändert werden.

Für Version 26.4.0

Weitere Details zur Konfiguration enthält der Artikel Android Kiosk Modus →.

> Die Konfiguration Relution Homescreen Layout steht nur zur Verfügung, wenn keine Konfiguration Kiosk-Modus angewendet wird. Es ist nicht möglich, beide Konfigurationen gleichzeitig zu nutzen. Innerhalb einer Richtlinie lässt sich nur eine der beiden hinzufügen; bei mehreren Richtlinien entscheidet die Richtlinienpriorität.

Bei Relution Education setzt der Server auf Android-Enterprise-Schülergeräten während eines Unterrichts die Homescreen App automatisch mit den Apps des Unterrichts ein, auch ohne eigene Konfiguration. Ausgenommen sind Unterrichte im Einzel-App-Modus.

Nicht verwaltete Geräte

Die Relution Homescreen Layout App ist auch für nicht verwaltete Geräte kostenlos im Google Play Store verfügbar.

Google Play Store Link →

Relution Decon

Ab Version 5.27 ermöglicht Relution für iOS die Einrichtung eines DNS-basierten Inhaltsfilters. Diese Funktion sorgt für einen sicheren und fokussierten Internetzugang, indem der Zugriff auf ausgewählte Webseiten und Apps eingeschränkt wird. Dank der KI-gestützten Kategorisierung von Inhalten bietet Relution Decon einen umfassenden Jugendschutzfilter mit erweiterten Einstellungsmöglichkeiten.

Was ist Relution Decon?

Relution Decon ist ein KI-gestütztes Add-on für iOS, iPadOS, macOS und Android Enterprise, das Inhalte in Echtzeit filtert und ein sicheres digitales Umfeld schafft. Mithilfe der DNS-basierten Inhaltskontrolle blockiert Decon unerwünschte Webseiten und Apps, sodass Nutzer in einem geschützten, ablenkungsfreien Raum arbeiten und lernen können.

Relution Decon nutzt einen DNS-Proxy, um alle Anfragen an den Decon-Server weiterzuleiten. Dort werden Webseiten klassifiziert und gemäß den Richtlinien entweder erlaubt oder blockiert. Dank SSL-Verschlüsselung bleiben alle Datenübertragungen sicher, und die Nutzeraktivitäten geschützt.

Decon App

Für Version 26.4.0

Die Decon-App wird bei der Richtlinieninstallation automatisch auf iOS-, iPadOS-, macOS- und Android-Enterprise-Geräten bereitgestellt. Sie überwacht die DNS-Anfragen des Geräts und stellt sicher, dass nur zugelassene Inhalte aufgerufen werden können.

Funktionen der App:

- Aktiviert einen systemweiten DNS-Proxy, der vom Benutzer nicht deaktiviert werden kann
- Zeigt den aktuellen Status von Relution Decon an
- Gibt Einsicht in blockierte Webseiten und die angewendeten Filterkategorien

> Empfehlenswert: Für Apple-Geräte vor der Verteilung ausreichend Lizenzen über Apps und Bücher (im Portal: VPP) für die App bereitstellen.

VPP konfigurieren →
Relution Decon im Apple App Store →

Decon Richtlinie

In der Geräte-Richtlinie wird die Konfiguration über `Hinzufügen` → `Relution Decon` angelegt. Mit dieser Richtlinie wird die Decon-App automatisch auf den Geräten installiert und fungiert als Proxy für alle DNS-Anfragen.

Die Konfiguration wird mit der Veröffentlichung der Richtlinie abgeschlossen. Ohne gültige Relution-Decon-Lizenz zeigt das Formular einen Hinweis, und die Konfiguration lässt sich nicht speichern. Unter macOS steht die Konfiguration nur bei Geräteregistrierung zur Verfügung.

Enthält eine iOS- oder macOS-Richtlinie bereits eine Konfiguration DNS Proxy, richtet Relution Decon keinen eigenen DNS-Proxy ein; das Gerät erhält dazu einen Compliance-Hinweis.

Die Einstellungen im Detail beschreiben die Plattformartikel Relution Decon für iOS →, Relution Decon für macOS → und Relution Decon für Android Enterprise →.

Hierarchie der Richtlinienkonfiguration (höchste zu niedrigste Priorität)

1. Apps auf der Positivliste (nur iOS/iPadOS und macOS)
2. Apps auf der Sperrliste (nur iOS/iPadOS und macOS)
3. Erlaubte Domains
4. Gesperrte Domains
5. Filter-Typ (gesperrte Kategorien oder Altersstufe)

Die Relution-Apps (Relution Agent, Relution Teacher, Relution Files, Relution Assets, Relution Decon) sowie die Adressen des Relution Servers und des Decon-Servers sind immer erlaubt.

Decon in Relution Teacher

Decon kann mit Relution Server 5.32.0 und Relution Agent 5.19.0 in Unterrichtsprofilen ausgewählt und gesteuert werden. Voraussetzung: Schülergeräte müssen mit einer Decon-Richtlinie versehen sein.

Teacher →

Hinweis: Für die Dauer der Unterrichtsstunde wird die sonst gültige Decon-Konfiguration überschrieben.

Für Version 26.4.0

Filtern

Im Abschnitt Filtern wird über das Pflichtfeld Filter-Typ festgelegt, wonach Webseiten gefiltert werden:

- Aus: Es wird weder nach Kategorien noch nach Altersstufe gefiltert.
- Kategorien (Standard): Die zu blockierenden Kategorien werden einzeln gewählt (siehe Tabelle).
- Altersstufe: Gefiltert wird nach einer Altersstufe (0+, 6+, 12+ oder 16+, Standard 12+).

Zusätzlich stehen die Schalter BPJM-Liste und Sichere Suche zur Verfügung. Einträge unter Erlaubte Domains können den Zugriff auf Inhalte ermöglichen, die von der BPjM als unzulässig eingestuft wurden.

Werden auf einem Gerät mehrere Decon-Konfigurationen verwendet, kommt automatisch die stärkste Filterung zum Tragen: Filter nach Altersstufe gehen Filtern nach Kategorien vor, Konfigurationen ohne Filterung werden ignoriert. Blockierte Kategorien werden zusammengeführt (eine Kategorie ist blockiert, sobald eine Konfiguration sie blockiert); bei mehreren Altersstufen gilt die strengste. Domain- und App-Listen werden ebenfalls zusammengeführt.

Klassifizierung nach Kategorien

Relution Decon ordnet Webseiten automatisch einer Kategorie zu. Beim Filter-Typ Kategorien legen Administratoren unter Gesperrte Kategorien fest, welche Kategorien blockiert werden. Standardmäßig ist nur Nicht jugendfreie Inhalte blockiert.

Kategorie	Beschreibung	Beispiele
Nicht jugendfreie Inhalte	Nicht für Jugendliche geeignete Seiten	Pornografie, Gewalt, Waffen, Drogen, Gambling, Adult Entertainment, Adult Shopping, Dating, Google Safe Search
Werbung	Werbeseiten	Ad Providers
Kommunikation	Kommunikationsdienste	Email, Messenger, (Video) Calling
Soziale Medien	Social-Media-Inhalte	Facebook, Instagram, TikTok, etc.
Unterhaltung	Unterhaltung, z. B. Streaming oder Spiele	Movies, Games, Videos
Musik	Musik-Streaming-Anbieter	Spotify, Tidal, etc.
Nachrichten	Nachrichten und Magazine	News, Wetter
Shopping	Online-Shops (außer adult content)	Amazon, eBay, etc.
Arbeit	Arbeitsrelevante Webseiten	Office, File Sharing, Intranet
Bildung	Lerninhalte	Wikipedia, Google Scholar
Generative KI	KI-spezifische Webseiten	ChatGPT, Perplexity.ai, etc.
Phishing	Potenzielle Phishing-Webseiten	Potential scams, Data theft
Sonstiges	Alles Andere	Rest

Positiv- und Sperrlisten

- Erlaubte Domains / Gesperrte Domains: Spezifische Domains gezielt freigeben oder sperren (keine Pfadunterscheidung). Möglich sind Domains mit Platzhaltern sowie IPv4- und IPv6-Adressen. Die Anzahl der gesperrten Domains sollte auf etwa 500 begrenzt werden.
- Apps auf der Positivliste / Apps auf der Sperrliste: Internetzugang für Apps gezielt steuern, Basisfunktionen bleiben erhalten. Die App-Listen stehen nur in Richtlinien für iOS/iPadOS und macOS zur Verfügung, nicht bei Android Enterprise.

Zusätzlich übernimmt Relution die organisationsweit unter `Einstellungen` → `Relution Decon Anfragen` erlaubten und gesperrten Domains in jede Decon-Konfiguration. Während eines Unterrichts mit Decon gelten diese Domains nicht.

Erweiterte DNS-Konfiguration

Die erweiterte DNS-Konfiguration steht in Android-Enterprise-Richtlinien nicht zur Verfügung.

DNS-Server auf dem Gerät: Alternative DNS-Server können hinterlegt werden, falls Relution Decon DNS nicht erreichbar ist. Fallback: Cloudflare Families DNS (1.1.1.3).

DNS-Server auf dem Relution Decon Server: Ersetzt den Standard-DNS für den Decon-Server. IP-Adressen (UDP) oder DNS-over-HTTPS (DoH) wie Zero oder Quad9 sind möglich.

Datenschutz

In Android-Enterprise-Richtlinien steht im Abschnitt Datenschutz die Option Datenweitergabe automatisch akzeptieren zur Verfügung. Sie akzeptiert die Datenweitergabe in der Decon-App im Namen des Benutzers.

Limitierungen

- Zwischenspeicherung: Blockierungen und Richtlinienänderungen können bis zu 1 Minute verzögert umgesetzt werden.
- Pfadunabhängigkeit: DNS arbeitet auf Domain-Ebene, keine Unterscheidung von Unterseiten.
- App-Blockierung: Nur Internetzugang wird gesperrt, Basisfunktionen und zwischengespeicherte Inhalte bleiben verfügbar.

Für Version 26.4.0

App-Verwaltung

Relution bietet eine umfassende Mobile App Management (MAM)-Funktion, mit der sich alle unterstützten Apps zentral verwalten lassen – plattformübergreifend und effizient.

Unterstützte Plattformen und App-Formate:

- iOS & iPadOS: Apps aus Apps und Bücher (im Portal: VPP) sowie native Apps (`.ipa`)
- macOS: Apps aus Apps und Bücher sowie native Apps (`.dmg`, `.pkg`)
- Android: Google Play Store Apps, Managed Google Play Store Apps (Android Enterprise) sowie native Apps (`.apk`)
- Windows: Microsoft Store-Apps sowie Installationspakete in den Formaten `.msix`, `.msixbundle`, `.appx`, `.appxbundle`, `.msi`, `.exe` und über Winget
- Weblinks: können ebenfalls zentral verwaltet und bereitgestellt werden

So ermöglicht Relution eine einheitliche und flexible Verwaltung sämtlicher Applikationen innerhalb einer Organisation.

Für native Apps ist die Nutzung des Relution App Stores obligatorisch, während Apps aus Apps und Bücher oder aus Hersteller-Stores optional darüber verwaltet werden können.

Aufbau des Apps-Menüs

Für Version 26.4.0

Das Apps-Menü in Relution ist in folgende Bereiche unterteilt:

- App Store - Der Relution-eigene App Store für alle oben genannten und unterstützten Apps.
- Anfragen - App-Anfragen von Endbenutzern, die durch Administratoren oder Verantwortliche freigegeben werden können.
- Kategorien - Ermöglicht das Kategorisieren von Apps in Kategorien, z. B. für Unterrichtszwecke.
- Gekaufte Apps - Übersicht aller Apps aus Apps und Bücher inklusive VPP-Tokens und der Möglichkeit zur Synchronisierung.
- Medien - Übersicht aller über Apps und Bücher bezogenen Bücher sowie selbst hochgeladener Dateien, z. B. PDFs.

App Store erklärt

Der Relution App Store ist ein zentraler Sammelbereich für alle unterstützten Apps und deren Plattformen. Er bietet eine Übersicht der verfügbaren Apps nach Name, Plattformen, Status, Bearbeitet und weiteren Kriterien. Zusätzliche Spalten können über das Hamburger-Menü eingeblendet werden.

Über den Hinzufügen-Button können Apps aus den jeweiligen Hersteller-Stores eingebunden oder nativ hochgeladen werden. Folgende Quellen stehen zur Auswahl: Native App, Weblink, Windows Store App, Google Play Store App, Managed Google Play Store App (Android Enterprise), Apple App Store App und Winget Store App. Die Quelle Managed Google Play Store App (Android Enterprise) erscheint nur, wenn Android Enterprise in der Organisation verbunden ist.

Bereiche im App Store

Beim Öffnen einer hinzugefügten App erweitern sich die verfügbaren Konfigurationsmöglichkeiten sowie die eigentlichen MAM-Funktionen.

- Informationen
  - Übersicht mit aktuellem Status und Version (Entwicklung, Prüfung, Produktiv, Archiv)
  - Beschreibung der App (bezogen aus dem jeweiligen Hersteller-Store)
  - Changelog der App (bezogen aus dem jeweiligen Hersteller-Store)
  - Zusätzliche Informationen wie z. B. interner App-Name oder Version
- Einstellungen
  - Allgemein
    - Automatische Updates – nur bei Store-Apps; bezieht sich auf die Metadaten aus dem jeweiligen Hersteller-Store (wöchentliche Aktualisierung)
    - Kategorien – ermöglicht das Kategorisieren der App, z. B. für Unterrichtszwecke
    - Verantwortlicher – zuständige Person oder Rolle für die App
    - Support-Kontakt – Kontaktadresse für App-Support
  - Rechte
    - Eigentümer – Eigentümer der App
    - Prüfer – Berechtigung zur App-Prüfung
    - Entwickler – Berechtigung zur App-Entwicklung
    - Benutzer – hier freigegebene Benutzer oder Gruppen können die App verwenden oder installieren
- Auto-Deployments – Benutzer oder Gruppen festlegen, die diese App automatisch erhalten sollen. Der Reiter erscheint erst, wenn eine Version im Status Produktiv vorhanden ist; bei macOS nur für Apps aus Apps und Bücher.
- Skripte – nur bei Windows-Apps im Format `.msi` oder `.exe`
- Versionszuordnungen und App Berechtigungen – nur in der Global-Organisation für lokale Apps
- Historie – Verlauf der App-Aktualisierungen und Versionen
- Geräte mit dieser App – Übersicht aller Geräte, auf denen diese App installiert ist

Für Version 26.4.0

Anfragen

Über den Relution Agent → oder das Portal können Benutzer gewünschte Apps anfragen. Damit hat der berechtigte Benutzer oder Administrator die Möglichkeit, Apps freizugeben, Anfragen zu löschen, den Status anzupassen und bei Bedarf Lizenzen aus Apps und Bücher zu beschaffen.

Voraussetzung ist der Schalter App Requester aktiviert unter `Einstellungen` → `Allgemeine Organisations-Einstellungen` im Bereich App Requester. Er ist standardmäßig aktiv und steht in der Global-Organisation nicht zur Verfügung. Ist er ausgeschaltet, fehlt der Menüpunkt Anfragen und es können keine Apps angefragt werden.

Kategorien

Admins und berechtigte Benutzer können hier Kategorien für Apps erstellen und entsprechende Apps hinzufügen, damit diese in der Relution Teacher App leichter und schneller zu finden sind.

Gekaufte Apps

Spezielle Übersicht für Apps aus Apps und Bücher für iOS, iPadOS und macOS, inklusive der Funktion zum manuellen Sync bei Bedarf. Bietet die Möglichkeit, nach VPP-Token zu filtern und eine Übersicht über die gesamte Lizenzanzahl, verfügbare Lizenzen und vergebene Lizenzen zu erhalten.

Über einen Klick auf eine bestimmte App können Lizenzen direkt Geräten, Benutzern oder Gruppen zugewiesen werden. Über das Kontextmenü App kaufen lassen sich weitere Lizenzen erwerben.

Bei einem öffentlichen VPP-Token beziehen sich die angezeigten Zuweisungen nur auf die aktuelle Organisation, die Gesamtzahl der Lizenzen dagegen auf alle Organisationen.

Medien

Spezielle Übersicht für Medien aus Apps und Bücher für iOS, iPadOS und macOS, inklusive der Funktion zum manuellen Sync bei Bedarf. Bietet die Möglichkeit, nach VPP-Token zu filtern und eine Übersicht über die gesamte Lizenzanzahl, verfügbare Lizenzen und vergebene Lizenzen zu erhalten.

Über einen Klick auf ein bestimmtes Medium können Lizenzen direkt Geräten, Benutzern oder Gruppen zugewiesen werden.

Zusätzlich können weitere Medien, wie z. B. PDF oder EPUB, verteilt werden. Sie werden über Neues PDF oder ePUB hochladen hinzugefügt und über Medieninhalte aktualisieren ersetzt. Das Hochladen ist nur möglich, wenn in der Organisation ein VPP-Token vorhanden ist. Über Bücher im Apple Store kaufen lassen sich weitere Bücher erwerben.

App-Anfragen bearbeiten

Angefragte Apps landen im Status Prüfung. Ohne aktiven App-Freigabeprozess können Eigentümer und Prüfer der App, standardmäßig also die Mitglieder der Gruppe App Reviewer, die angefragte Version direkt freigeben oder ablehnen. Benutzer mit Löschrecht können die Anfrage entfernen. Optional lässt sich ein mehrstufiger Freigabeprozess einrichten, dessen Schritte sich auf angefragte Apps beschränken lassen.

Für Version 26.4.0

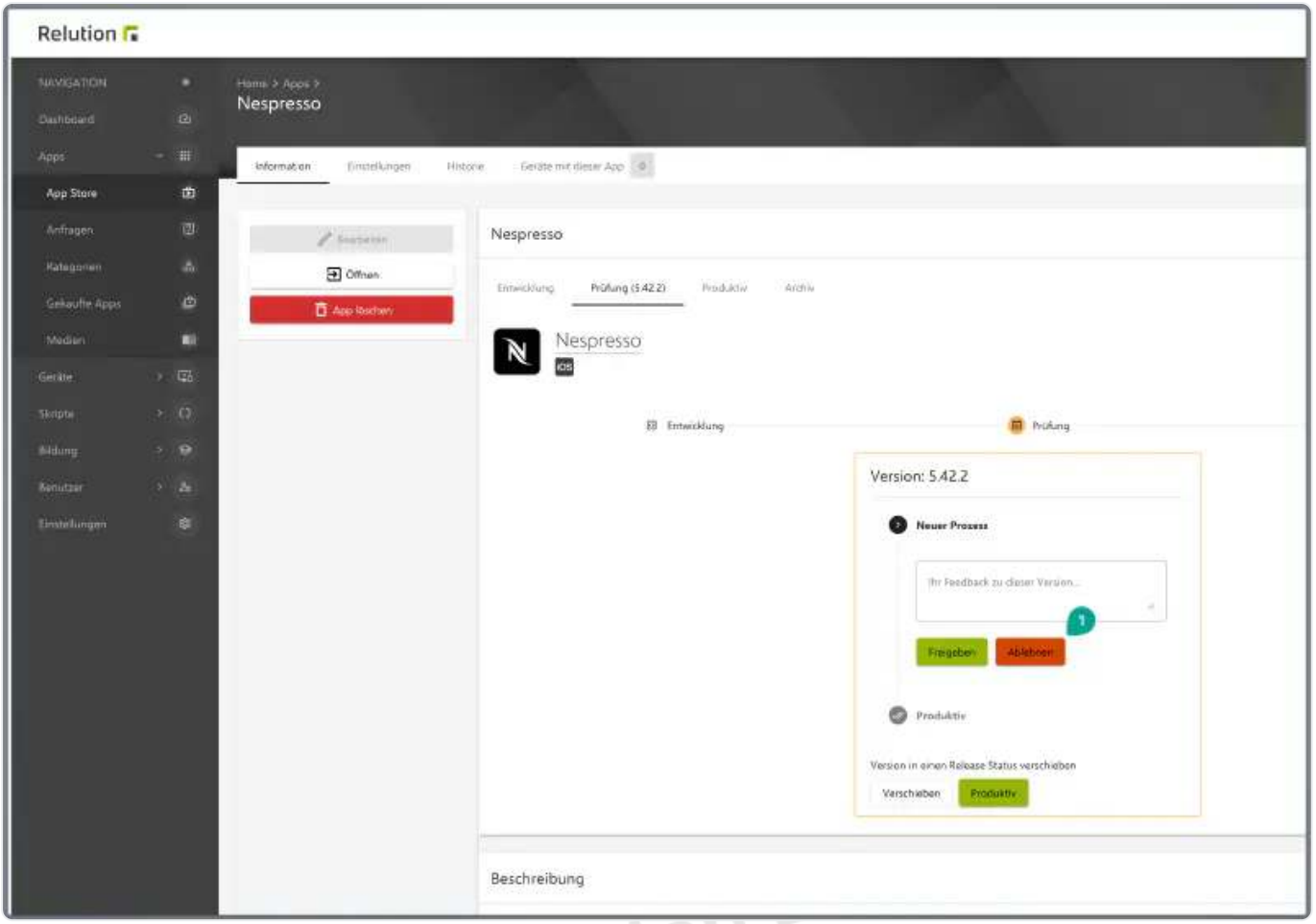
Einrichtung des Prozesses

Die Konfiguration eines optionalen Freigabeprozesses erfolgt unter `Einstellungen` → `App-Freigabeprozess`. Details zu den einzelnen Freigabeschritten, Zuständigkeiten und der automatisierten Terminfindung finden sich unter App-Freigabeprozess →.

Verwaltung von App-Anfragen

Angefragte Apps lassen sich über die Seitenleiste unter folgendem Menüpunkt verwalten: `Apps` → `Anfragen`

Dort können die vorliegenden Anfragen geprüft und anschließend freigegeben oder abgelehnt werden.



Für Version

App Store Standard-Berechtigungen für neue Apps

In Relution können unter `Einstellungen` → `App Store` die Standard-Berechtigungen für neue Apps definiert werden. Dies ist besonders sinnvoll, wenn Apps standardmäßig explizit nur für eine bestimmte Gruppe von Benutzern verfügbar sein sollen.

Standard-Konfiguration für neue Apps

Solange der Schalter Aktivieren ausgeschaltet ist, erhalten neue Apps folgende Standardzuordnung:

- Benutzer: Appstore User und Device Manager
- Entwickler: Developer
- Prüfer: App Reviewer

Nach dem Einschalten sind alle Rollen zunächst leer und müssen über Hochladender Benutzer bzw. Benutzer oder Gruppe zuweisen befüllt werden. Ohne Zuweisung in der Rolle Benutzer sind neue Apps für Appstore-Benutzer nicht verfügbar. Nach dem Aus- und erneuten Einschalten des Schalters ist die Vorlage wieder leer.

> Wenn diese Option aktiv ist, ist es dem App-Uploader nicht erlaubt, individuelle Berechtigungen für eine hochgeladene App zu vergeben. Es werden stattdessen automatisch die definierten Standard-Berechtigungen angewendet.

Ausgenommen sind Benutzer mit der Rolle Appstore Manager (auch Administratoren): Bei deren Uploads sind die Standard-Berechtigungen nur vorbelegt und können beim Hochladen individuell angepasst werden.

Beispiel: Konfiguration für die Rolle Benutzer

Innerhalb der Einstellungen stehen für die Zuweisung folgende Optionen zur Verfügung:

1. Hochladender Benutzer: Wenn aktiv, wird der hochladende Benutzer automatisch dieser Rolle zugeordnet. Wird ein Benutzer als Eigentümer hinterlegt, besitzt dieser die Berechtigung, alle weiteren Einstellungen der App zu verändern.

2. Benutzer oder Gruppe zuweisen: Alternativ kann gezielt ein bestimmter Benutzer oder eine vordefinierte Gruppe für die Verwendung der App festgelegt werden.

Für Version 26.4.0

App-Freigabeprozess

Unter `Einstellungen` → `App-Freigabeprozess` lässt sich festlegen, welche Schritte eine App-Version durchlaufen muss, bevor sie den Status Produktiv erreicht. Der Prozess gilt für Versionen im Status Prüfung. Ohne aktiven Prozess kann jeder Benutzer mit dem Recht Eigentümer oder Prüfer an der App eine Version direkt freigeben. In den Standard-App-Rechten ist als Prüfer die System-Gruppe App Reviewer der Organisation eingetragen.

Freigabeschritte anlegen

Ein Freigabeprozess besteht aus beliebig vielen, frei sortierbaren Schritten. Für jeden Schritt lassen sich folgende Angaben machen:

- Name und Beschreibung
- Typ:
  - Standard – ein regulärer Freigabeschritt.
  - Go-Live Datum ermitteln – fügt der Version einen Terminfindungs-Schritt hinzu (siehe unten).
- Verantwortliche Person oder Gruppe: Wird niemand hinterlegt, ist automatisch der App-Eigentümer verantwortlich. Wird ein als verantwortlich hinterlegter Benutzer gelöscht, geht die Verantwortung auf die Gruppe Appstore Manager der Organisation über.
- Diesen Schritt erzwingen: Ist diese Option aktiv, muss die Version diesen Schritt zwingend durchlaufen. Solange dieser Schritt oder ein späterer Schritt erzwungen ist, lässt sich die Version nicht direkt von Prüfung auf Produktiv setzen. Ausgenommen sind App-Eigentümer mit der Rolle Appstore Manager, die Administratoren automatisch besitzen.
- Bedingungen: Ein Schritt kann auf bestimmte Apps (Für bestimmte Apps), App-Typen (Nativ, Public, Weblink), Plattformen (iOS, Android, macOS, Windows, tvOS), den Kosten-Typ (Kostenpflichtig/Kostenfrei), bestimmte App-Operationen (Erstellen/Aktualisieren) oder ausschließlich auf angefragte Apps (Nur angefragte Apps) eingeschränkt werden. Sind bestimmte Apps ausgewählt, entfallen die Bedingungen App-Typ, Plattform, Kosten-Typ und Nur angefragte Apps. Ist Nur angefragte Apps aktiv, entfällt die Auswahl der App-Typen.

Für Version 26.4.0

> Ein Schritt, dem bereits Versionen zugeordnet sind, kann weder bearbeitet noch gelöscht werden.

Wird der letzte Freigabeschritt gelöscht, wird der Freigabeprozess automatisch deaktiviert.

Freigabe bei aktivem Prozess

Ist der Freigabeprozess aktiv, wird jede Version im Status Prüfung dem ersten passenden Schritt zugeordnet. Den aktuellen Schritt freigeben können nur die verantwortliche Person bzw. die Mitglieder der verantwortlichen Gruppe sowie App-Eigentümer. Nach der Freigabe wechselt die Version in den nächsten passenden Schritt.

Ist der letzte Schritt freigegeben, wird die Version veröffentlicht und erhält den Status Produktiv. Ist für die Version ein Go-Live Datum in der Zukunft hinterlegt, erfolgt die Veröffentlichung automatisch zu diesem Termin.

Bei nativen Apps lässt sich für Versionen im Status Entwicklung oder Prüfung im Feld Go-Live Datum ein Wunschtermin angeben. Während ein Schritt vom Typ Go-Live Datum ermitteln läuft, kann das Datum nicht geändert werden.

Go-Live Datum ermitteln

Enthält der Prozess einen Schritt vom Typ Go-Live Datum ermitteln, schlagen Uploader und zuständige Person in der App-Detailansicht der jeweiligen Version gemeinsam ein Veröffentlichungsdatum vor. Haben beide Seiten zugestimmt, wird das Datum als Go-Live Datum übernommen. Folgen im Prozess weitere Schritte, durchläuft die Version zunächst diese. Nach Abschluss des Prozesses wird sie zum vereinbarten Termin automatisch veröffentlicht.

Prozess aktivieren/deaktivieren

Über das 3-Punkte-Menü lässt sich der gesamte Freigabeprozess aktivieren oder deaktivieren:

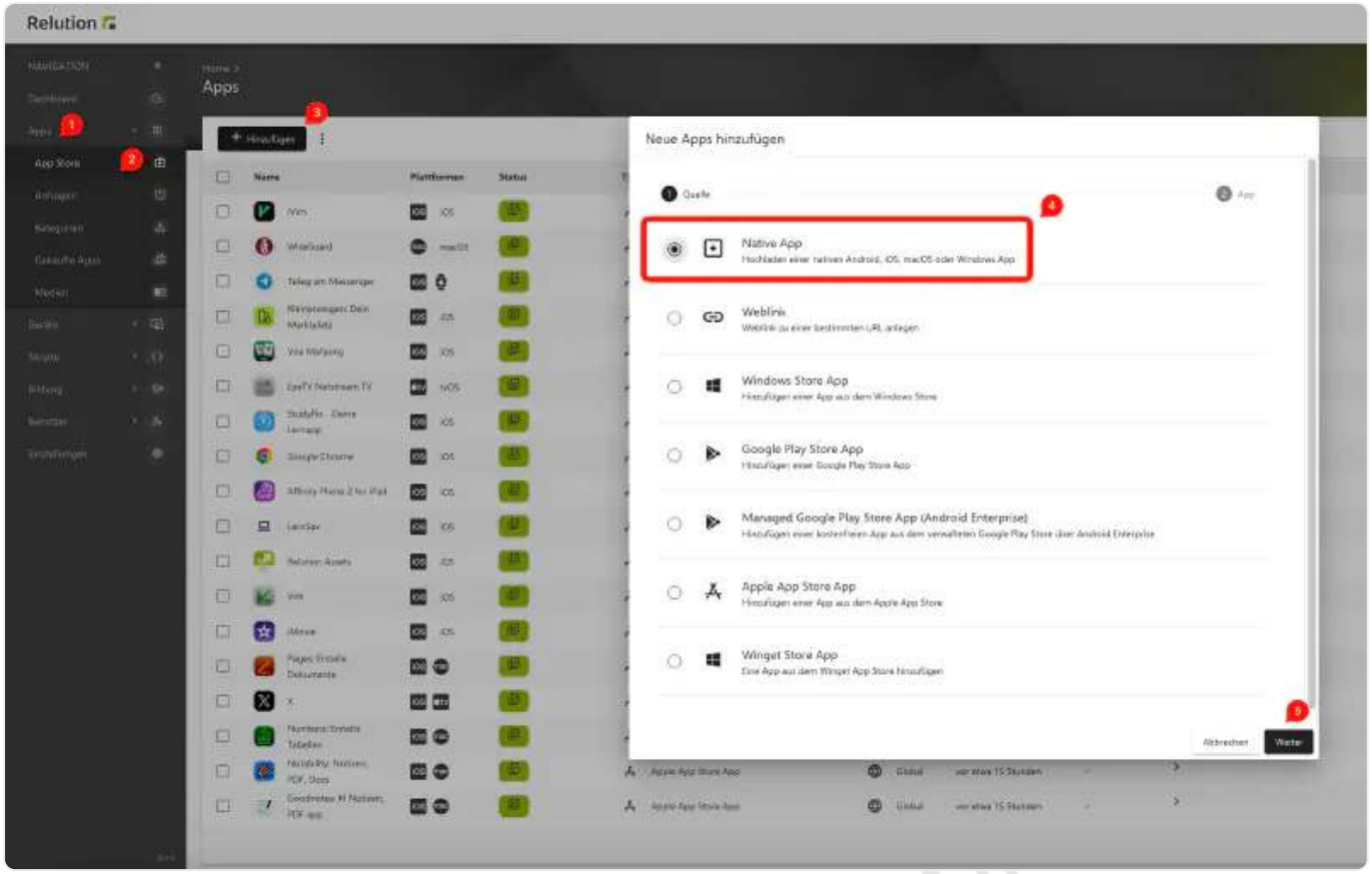
- Freigabeprozess aktivieren: Alle Versionen im Status Prüfung werden in den ersten passenden Freigabeschritt verschoben. War eine Version bereits zuvor in einem Schritt, wird ihre Freigabe-Historie wiederhergestellt. Eine Aktivierung ist erst möglich, sobald mindestens ein Schritt angelegt wurde.
- Freigabeprozess deaktivieren: Eigentümer und Prüfer der App, standardmäßig also auch die Mitglieder der Gruppe App Reviewer, können Versionen wieder direkt freigeben.

Native App im Relution App Store bereitstellen

Für Version 26.4.0

Relution ermöglicht die Bereitstellung nativer Apps und Installationspakete, beispielsweise IPA-, PKG-, DMG-, APK-, MSIX-, MSIXBUNDLE-, APPX-, APPXBUNDLE-, MSI- und EXE-Dateien. Dadurch können auch unterschiedliche Versionen einer App, etwa Entwickler- oder Testversionen, gezielt bereitgestellt und vorab getestet werden.

Unter `Apps` → `App Store` wird über Hinzufügen die Quelle Native App gewählt und mit Weiter bestätigt.

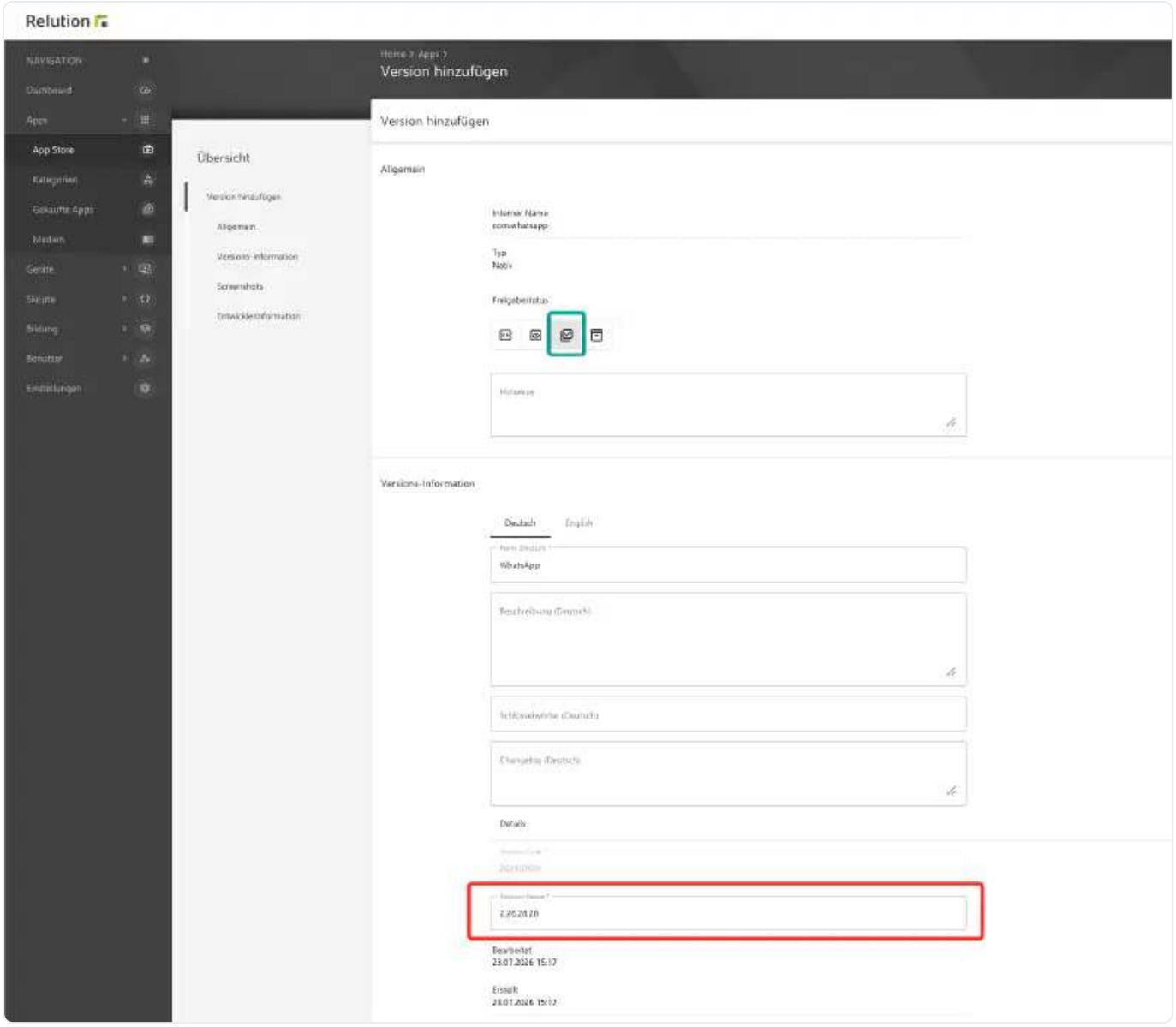


Über Auswählen wird das gewünschte Installationspaket hochgeladen.

Sobald das Installationspaket – in diesem Beispiel die WhatsApp-APK – hochgeladen wurde, wird über Details hinzufügen das Formular geöffnet. Im Abschnitt Allgemein wird im Feld Freigabestatus der Status Produktiv ausgewählt. Der Statusname erscheint als Tooltip am jeweiligen Symbol. Der Status Produktiv steht nur App-Eigentümern zur Verfügung. Eine direkt im Status Produktiv angelegte Version durchläuft keinen Freigabeprozess.

Apps mit dem Freigabestatus Produktiv können von allen berechtigten Benutzern über den Relution App Store heruntergeladen werden.

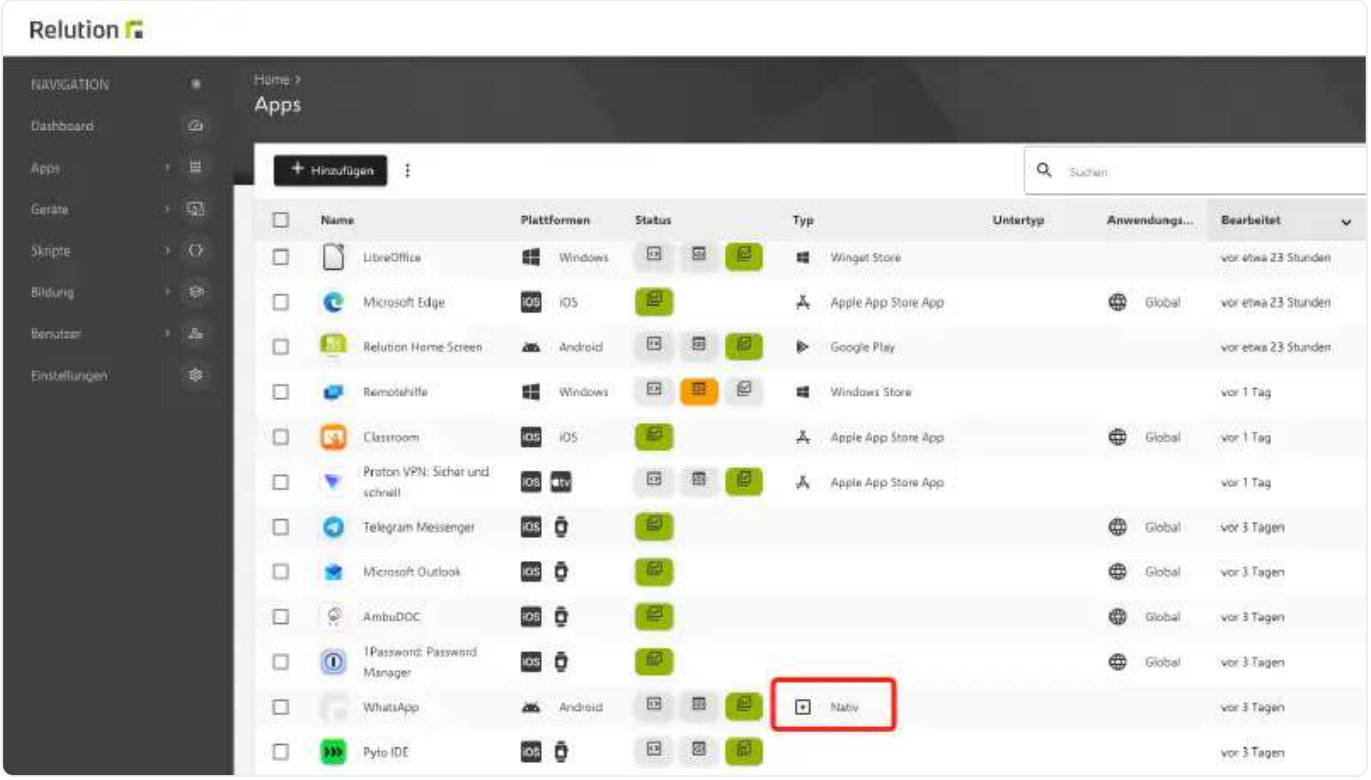
In diesem Bereich sind außerdem der Versionsname sowie das Erstellungs- und Bearbeitungsdatum der App einsehbar.



Abschließend werden die Angaben oben rechts über Speichern übernommen.

Nach dem Speichern wird eine Gesamtübersicht der hinterlegten App angezeigt. Dort sind unter anderem die Plattform, für die die App verfügbar ist, sowie weitere Informationen und Einstellungen ersichtlich.

Auch im Relution App Store ist ersichtlich, um welche Art von App es sich handelt und für welche Plattform sie bereitgestellt wird.

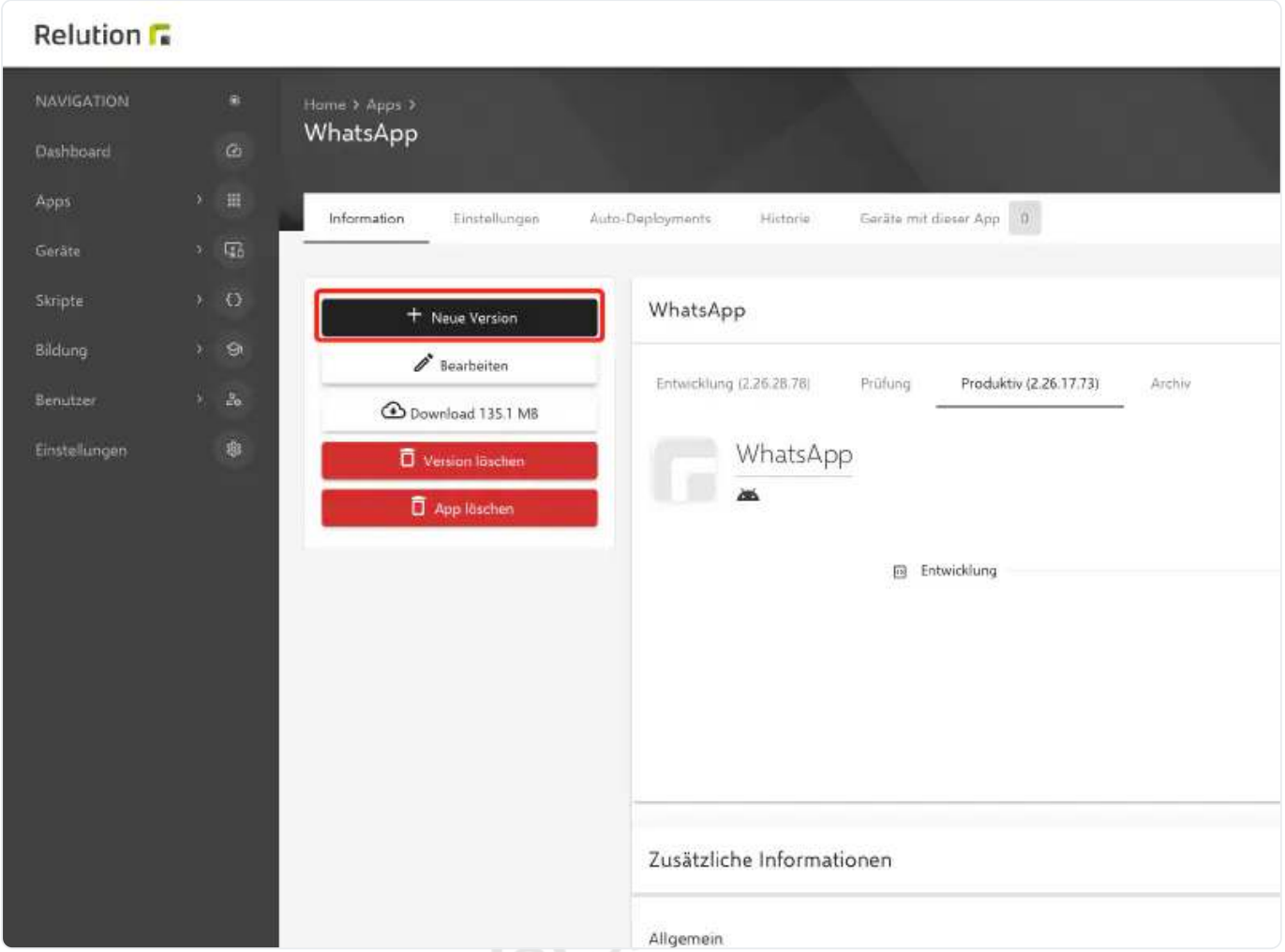


Entwickler- oder Testversion für bestimmte Benutzer bereitstellen

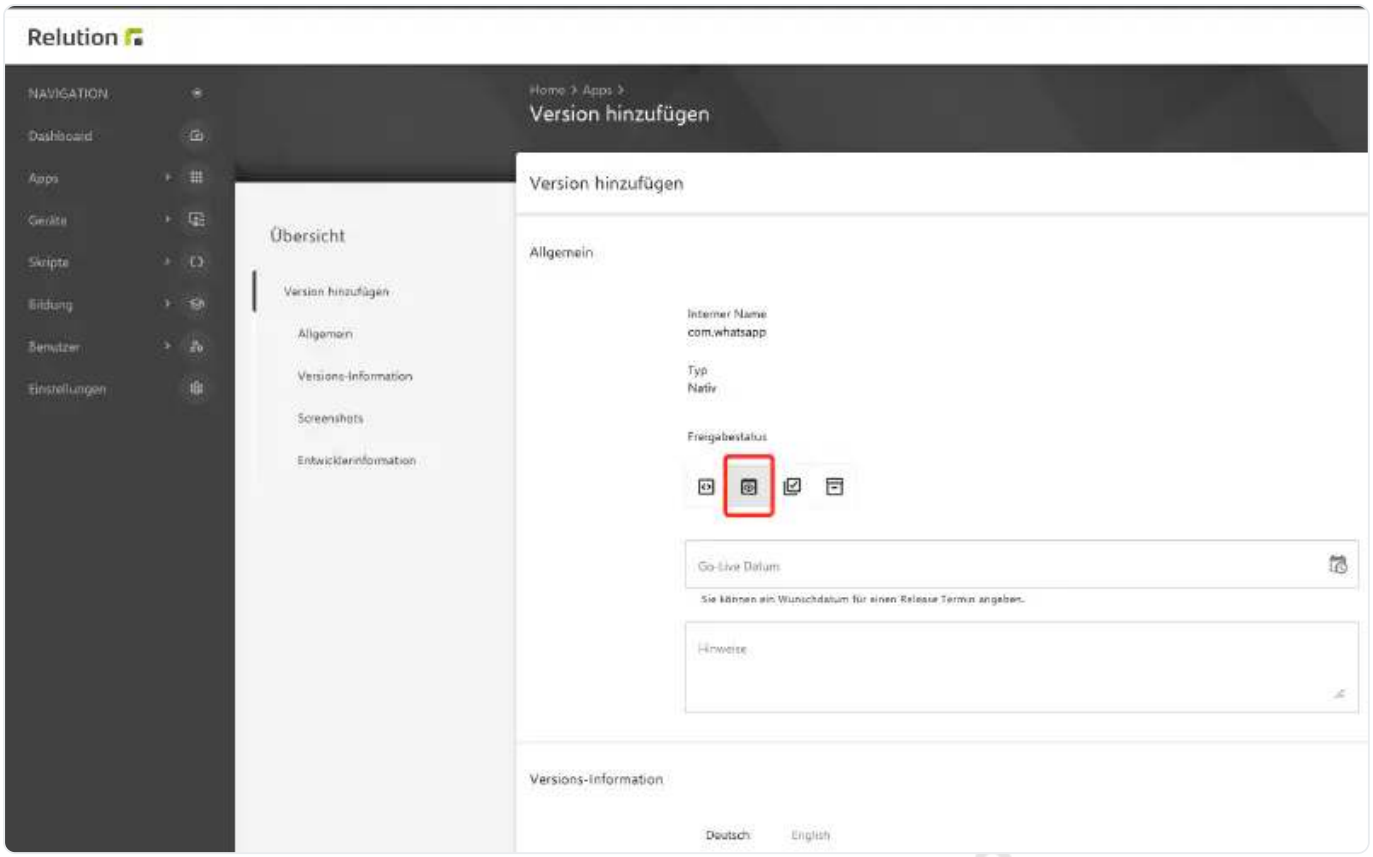
Für Version 26.4.0

Soll eine weitere Version derselben App – beispielsweise eine Entwickler- oder Testversion – nur für bestimmte Benutzer bereitgestellt werden, wird sie im Status Prüfung angelegt.

Die gewünschte App wird im Relution App Store geöffnet und über Neue Version eine neue Version angelegt.



Die neue Version wird anschließend wie oben beschrieben als native App hochgeladen. Im Abschnitt Allgemein wird im Feld Freigabestatus der Status Prüfung ausgewählt und die Änderungen werden gespeichert.



Dadurch ist die Version für normale App-Store-Benutzer nicht sichtbar. Prüfversionen sehen nur Personen mit dem Recht Eigentümer, Prüfer oder Entwickler an der App sowie Administratoren. Die Freigabe gilt immer für alle Prüfversionen der App, nicht für eine einzelne Version.

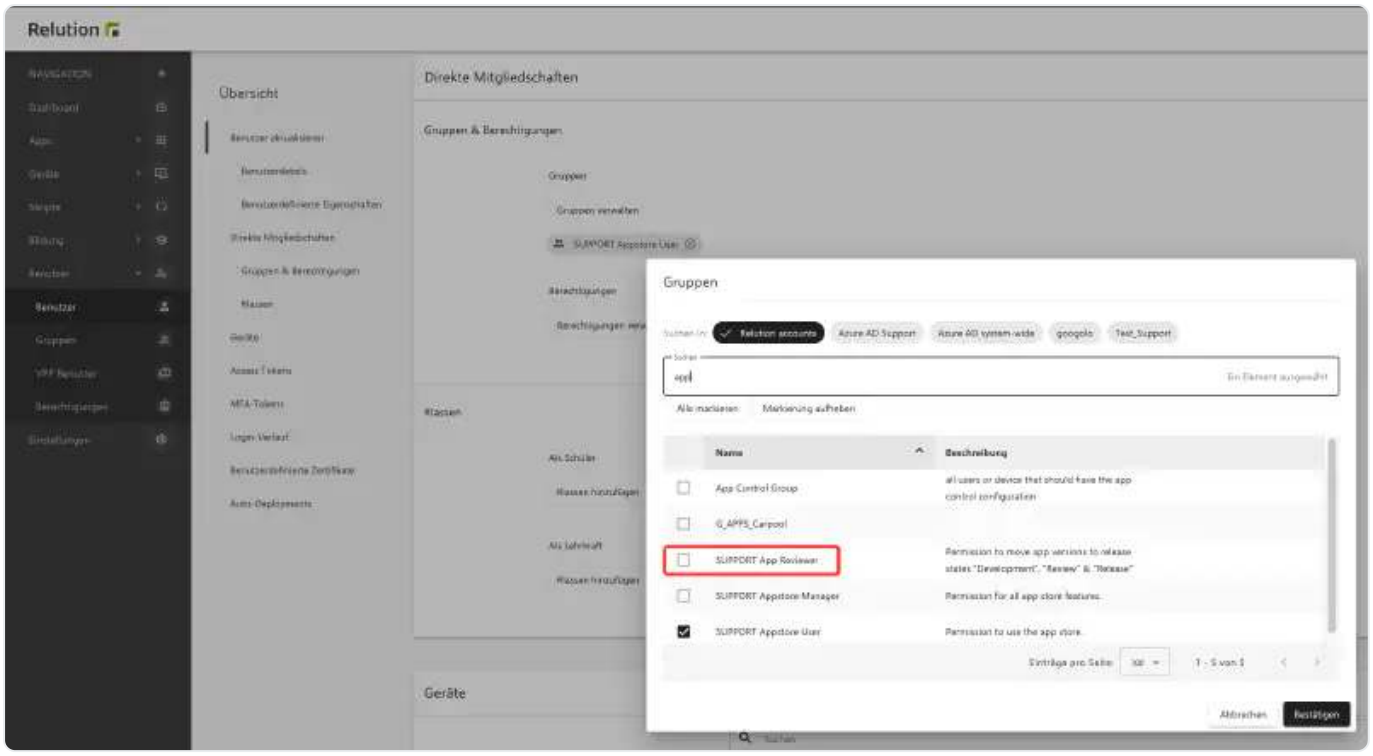
Für Version 26.4.0

Zugriff über die Rechte der App

Einzelne Testpersonen erhalten den Zugriff gezielt über die App selbst: Im Reiter Einstellungen der App wird die Person im Abschnitt Rechte über Benutzer und Gruppen bei Prüfer oder Entwickler eingetragen. Als Entwickler sieht sie Prüfversionen, darf sie aber nicht freigeben. Sie kann jedoch Prüf- und Entwicklungsversionen bearbeiten und die App löschen. Der Abschnitt Rechte steht App-Eigentümern zur Verfügung.

Zugriff über die Gruppe App Reviewer

Alternativ wird der Benutzer der System-Gruppe App Reviewer der Organisation hinzugefügt. Dazu wird unter `Benutzer` → `Benutzer` der entsprechende Benutzer geöffnet und im Abschnitt Gruppen & Berechtigungen die Schaltfläche Gruppen verwalten ausgewählt. Dort wird die Gruppe zugewiesen. Ihr Name beginnt mit dem Organisationsnamen. Im Screenshot heißt die Organisation „Support“, die Gruppe daher Support App Reviewer.

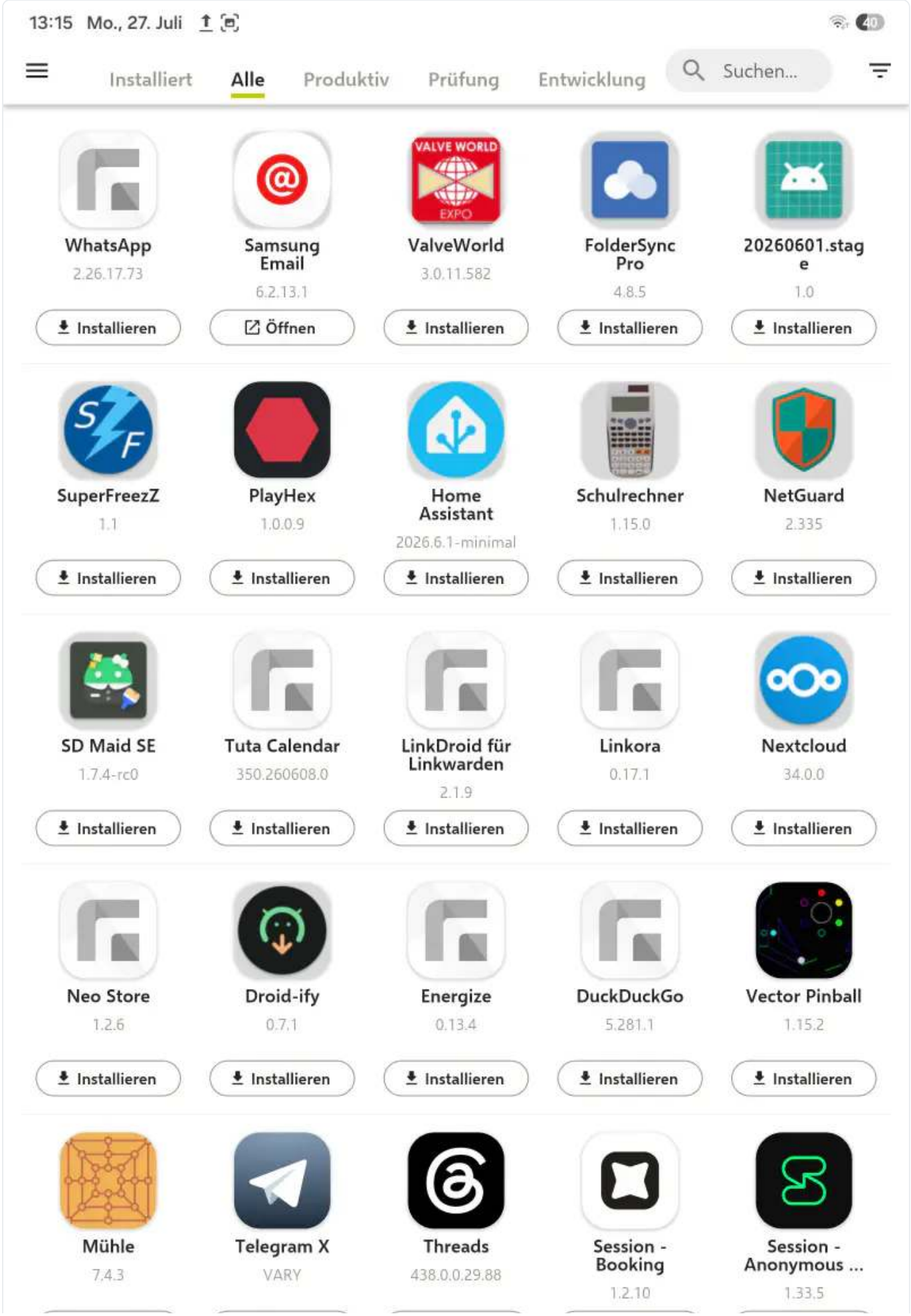


Mitglieder dieser Gruppe sind in den Standard-App-Rechten als Prüfer eingetragen. Sie sehen damit die Prüfversionen aller Apps, deren Rechte die Gruppe enthalten. Ist unter `Einstellungen` → `App Store` eine Vorlage für die Standard-Berechtigungen aktiv, gilt das nur, wenn die Gruppe darin enthalten ist (App Store Standard-Berechtigungen →).

> Als Prüfer dürfen die Mitglieder der Gruppe App Reviewer Versionen dieser Apps auch freigeben, also von Prüfung auf Produktiv oder Entwicklung verschieben. Ist kein App-Freigabeprozess aktiv, geht das ohne weitere Prüfung. Für einzelne Testpersonen ist das Recht Entwickler an der App deshalb der gezieltere Weg.

Für Version 26.4.0

Benutzer ohne eines dieser Rechte sehen ausschließlich Versionen mit dem Status Produktiv. Benutzer mit Zugriff auf Prüfversionen sehen im Relution App Store zusätzlich den Bereich Prüfung in der oberen Leiste.


13:15 Mo., 27. Juli
40
Installiert
Alle
Produktiv
Prüfung
Entwicklung
Suchen...
WhatsApp
2.26.17.73
Installieren
Samsung Email
6.2.13.1
Öffnen
ValveWorld
3.0.11.582
Installieren
FolderSync Pro
4.8.5
Installieren
20260601.stage
1.0
Installieren
SuperFreezZ
1.1
Installieren
PlayHex
1.0.0.9
Installieren
Home Assistant
2026.6.1-minimal
Installieren
Schulrechner
1.15.0
Installieren
NetGuard
2.335
Installieren
SD Maid SE
1.7.4-rc0
Installieren
Tuta Calendar
350.260608.0
Installieren
LinkDroid für Linkwarden
2.1.9
Installieren
Linkora
0.17.1
Installieren
Nextcloud
34.0.0
Installieren
Neo Store
1.2.6
Installieren
Droid-ify
0.7.1
Installieren
Energize
0.13.4
Installieren
DuckDuckGo
5.281.1
Installieren
Vector Pinball
1.15.2
Installieren
Mühle
7.4.3
Telegram X
VARY
Threads
438.0.0.29.88
Session - Booking
1.2.10
Session - Anonymous ...
1.33.5

Siehe auch App-Anfragen bearbeiten → für die anschließende Prüfung angefragter Apps.

Für Version 26.4.0

Benutzerverwaltung

Relution verfügt über eine interne Benutzerverwaltung, die es erlaubt, Benutzerkonten manuell anzulegen oder durch externe Provider hinzuzufügen. Einige Besonderheiten und wichtige Hinweise werden im Folgenden erläutert.

Benutzer allgemein

- Jeder Benutzer wird in einer Organisation in Relution angelegt.
- Ein Benutzer kann nicht in mehreren Organisationen gleichzeitig hinterlegt sein.
- Für administrative Accounts ist Multimandantenfähigkeit konfigurierbar, jedoch verbleibt das Benutzerkonto immer im Ursprungsmandanten.
- Jedes Benutzerkonto wird in der Datenbank gespeichert.
- E-Mail-Adressen müssen eindeutig sein; geprüft wird über alle Organisationen des Servers hinweg. Benutzernamen müssen innerhalb einer Organisation eindeutig sein.

Hinzufügen von Benutzerkonten

Für Version 26.4.0

Es gibt mehrere Möglichkeiten, Benutzerkonten hinzuzufügen:

1. Manuelles Anlegen
2. Upload einer CSV-Datei mit Benutzerinformationen
3. Anbindung an externe Provider (z. B. LDAP → oder Microsoft Entra ID →)

Über das Kontextmenü der Benutzerliste stehen außerdem Benutzer einladen (Einladung per E-Mail) und Mehrere Benutzer erstellen zur Verfügung. Beide Einträge erfordern das Recht, Benutzer zu erstellen.

1. Manuelles Anlegen von Benutzerkonten

- Im Abschnitt Benutzer öffnet ein Klick auf Hinzufügen die Eingabemaske.
- Alle Pflichtfelder müssen ausgefüllt werden: Benutzername, Passwort, Vorname, Nachname (je bis zu 50 Zeichen) und E-Mail-Adresse.
- Mit der Option Passwortbasierte Authentifizierung deaktivieren entfällt das Passwort. Die Anmeldung ist dann nur über einen externen Identitätsanbieter (z. B. OpenID Connect oder SAML) oder ein API-Token möglich. Die Option lässt sich nur beim Anlegen setzen und nachträglich nicht mehr zurücknehmen.
- Im Abschnitt Benutzerdefinierte Eigenschaften (standardmäßig eingeklappt) stehen 15 Felder mit je bis zu 255 Zeichen zur Verfügung. Die Felder 1–10 können als Platzhalter `${user.custom1}` bis `${user.custom10}` in Richtlinien-Konfigurationen verwendet werden; die Felder 11–15 werden gespeichert, aber nicht als Platzhalter ersetzt.
- Berechtigungen und Gruppen sollten definiert werden.
- Weitere Informationen zu Berechtigungen finden sich im Artikel Berechtigungen →.

Über Mehrere Benutzer erstellen lassen sich bis zu 50 Benutzerkonten auf einmal anlegen. Der Benutzername muss den Platzhalter `%N` enthalten, der durch eine aufsteigende Nummer ersetzt wird (Standard `user-%N`); der Startwert wird im Feld Start von %N festgelegt.

2. Upload einer CSV-Datei

Für den Import mehrerer Benutzerkonten steht die CSV-Import-Funktion zur Verfügung. Der vollständige Ablauf inklusive Vorlage, Vorschau und optionaler Gruppen- bzw. Berechtigungszuweisung ist im Artikel CSV-Import → beschrieben.

> In der CSV hinterlegte Passwörter müssen die Passwortrichtlinie unter `Einstellungen` → `Verwaltung der Anmeldedaten` erfüllen, insbesondere die **Minimale Passwortlänge**. Zeilen mit nicht konformen Passwörtern werden nicht importiert.

3. Anbindung an externe Provider

- Bei angebundenen Providern (z. B. LDAP →, Microsoft Entra ID →) ist der externe Provider das führende System.
- Inhalte, die importiert werden, werden aktualisiert, wenn sie auf Provider-Seite geändert werden.
- Die Felder Benutzername, Vorname, Nachname, E-Mail-Adresse, Position, Telefon und Land sind im Portal gesperrt, da sie bei der nächsten Synchronisation überschrieben werden.
- Bei Login authentifiziert Relution immer gegen das konfigurierte LDAP →. Ist die Verbindung nicht verfügbar, kann der Benutzer sich nicht anmelden.

Die Konfiguration der Anbindung wird in den Artikeln zu den einzelnen Providern ausführlich erklärt. Für Schulen stehen zusätzlich die Anbindungen OneRoster Schnittstelle → und SchulConnex Import → zur Verfügung.

Für Version 26.4.0

Benutzergruppen

Benutzergruppen werden unter `Benutzer` → `Gruppen` verwaltet. Gruppen fassen Benutzerkonten zusammen — etwa zur Vergabe von Berechtigungen über die Gruppenzugehörigkeit. Berechtigungsrollen → können sowohl einzelnen Benutzern als auch Gruppen zugewiesen werden — Mitglieder erhalten die Berechtigungen ihrer Gruppen.

- Gruppe anlegen: Eine neue Gruppe wird über Hinzufügen in der Gruppenübersicht erstellt.
- Mitglieder verwalten: Mitglieder werden über Mitglieder verwalten in den Gruppendetails hinzugefügt oder entfernt. Mitglieder einer Gruppe können sowohl Benutzerkonten als auch andere Gruppen sein (verschachtelte Gruppen). Bei Gruppen, die von einem Provider synchronisiert werden (z. B. aus LDAP), sind die Mitglieder schreibgeschützt.
- Löschen: Nicht mehr benötigte Gruppen können in der Gruppenliste gelöscht werden.
- Systemgruppen: Sie können nicht gelöscht werden; Name und Beschreibung sind nicht bearbeitbar, und andere Systemgruppen lassen sich nicht als Mitglieder hinzufügen.

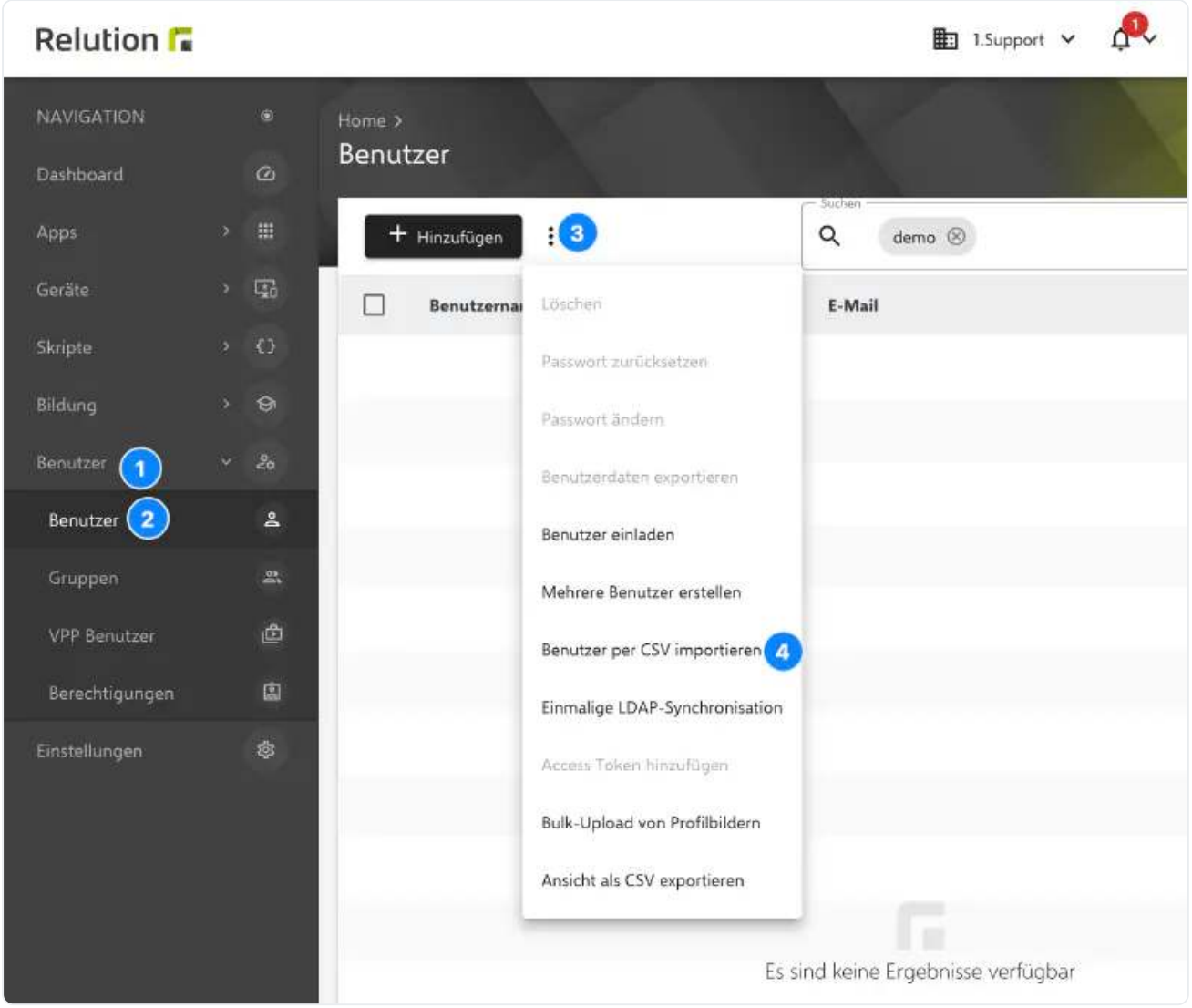
Die Gruppenzugehörigkeiten eines einzelnen Benutzers können auch direkt in den Benutzerdetails im Bereich Direkte Mitgliedschaften unter Gruppen & Berechtigungen über Gruppen verwalten bearbeitet werden.

CSV-Import

Um eine größere Anzahl an Benutzern effizient zu verwalten, lässt sich die Import-Funktion über eine CSV-Datei nutzen. Voraussetzung sind die Berechtigungen zum Erstellen und zum Aktualisieren von Benutzern. Dafür sind folgende Schritte nötig:

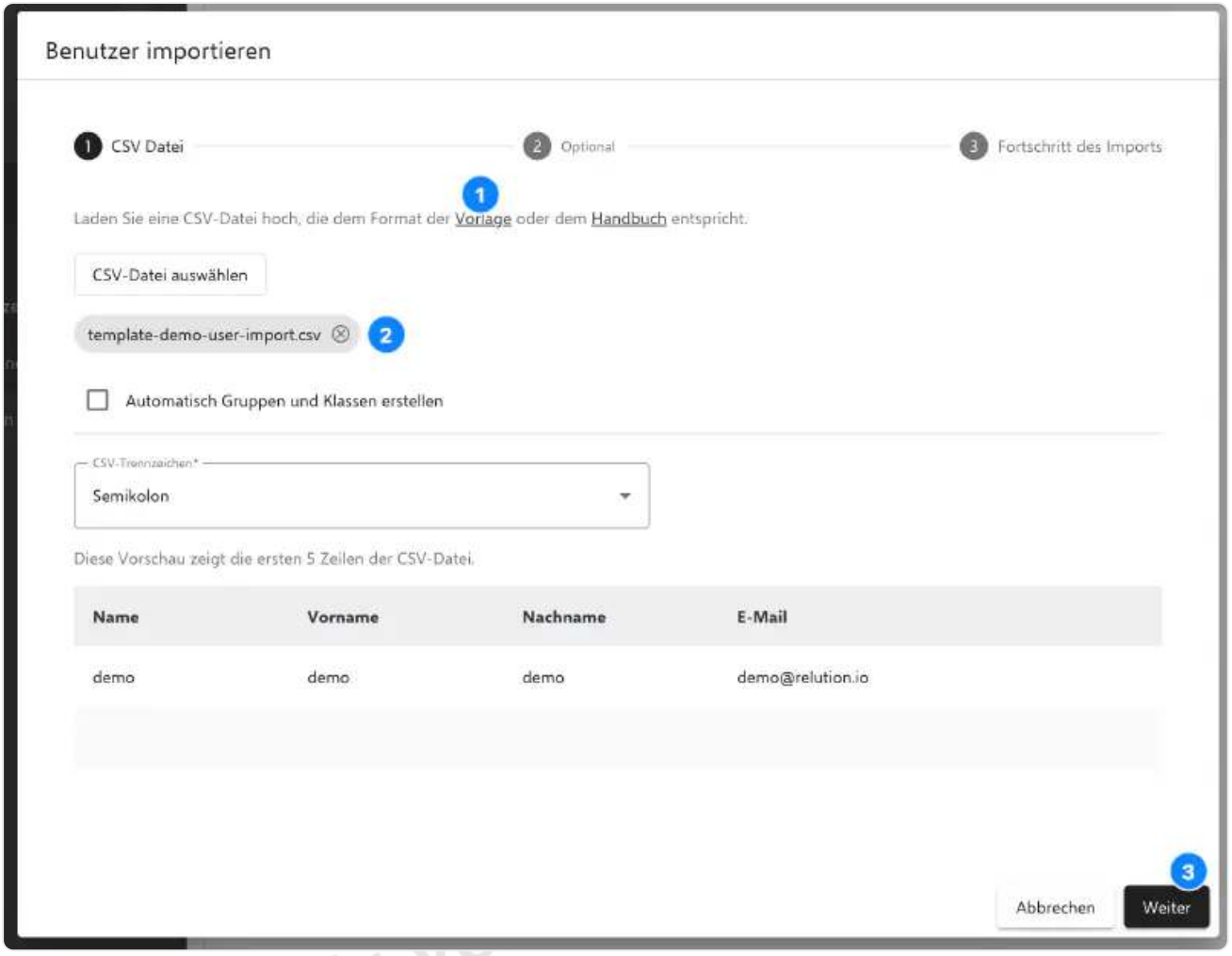
Für Version 26.4.0

1. Menü aufrufen: In Relution den Navigationspunkt Benutzer öffnen.
2. Import starten: Das 3-Punkte-Menü wählen und auf Benutzer per CSV importieren klicken.

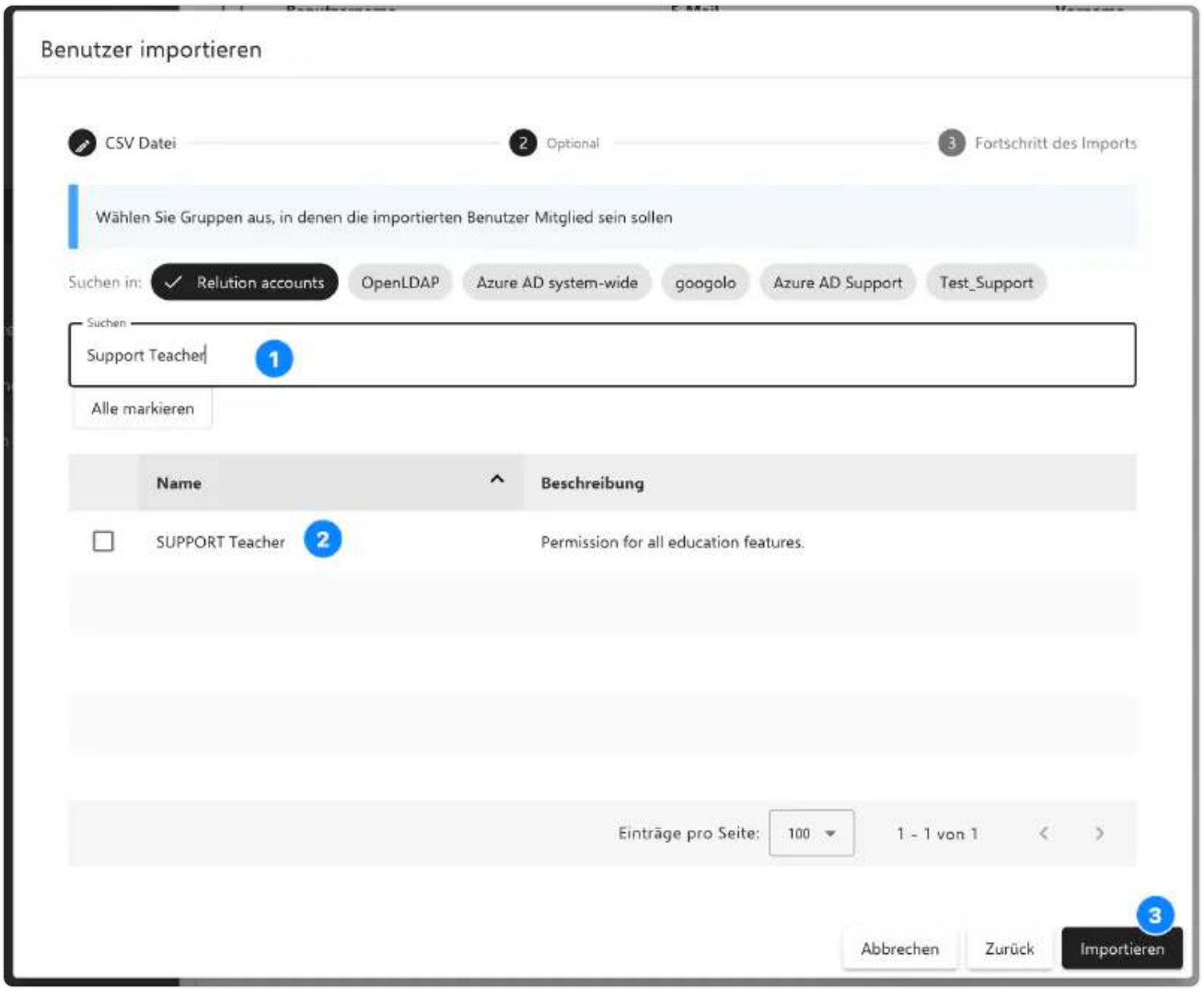


3. Vorlage nutzen: Die bereitgestellte CSV-Vorlage herunterladen. Die Vorlage verwendet das im Feld CSV-Trennzeichen gewählte Trennzeichen (Komma oder Semikolon) und enthält die Spalten `name`, `email`, `givenName`, `surname`, `password`, `disablePasswordAuthentication`, `phone`, `position`, `country`, `managedAppleId`, `locale`, `permissions`, `memberOfGroups`, `teacherOfClasses` und `studentOfClasses`.
4. Daten bearbeiten: Die Datei in einem Editor der Wahl öffnen und die erforderlichen Werte eintragen.
5. Datei hochladen: Die editierte CSV-Datei im Schritt CSV Datei wieder in Relution hochladen. Dort befindet sich auch die Option Automatisch Gruppen und Klassen erstellen (siehe unten).

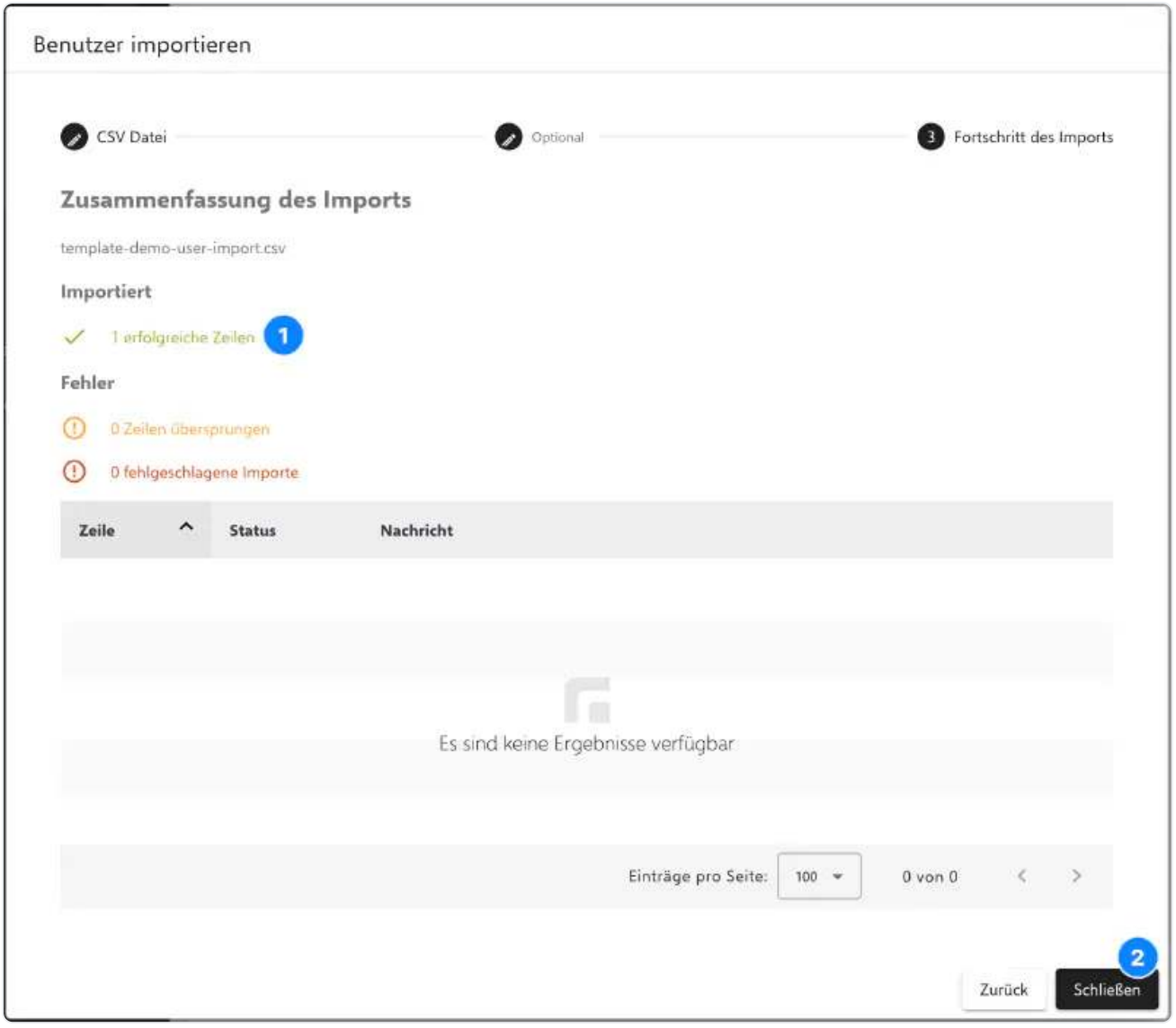
6. Prüfung: Die Vorschau prüfen (hierbei werden die ersten 5 Zeilen zur Kontrolle angezeigt).



7. Zuweisung (Optional): Die Nutzer lassen sich während dieses Prozesses direkt zu bestehenden Gruppen hinzufügen. Dieser Schritt wird nur mit der Berechtigung zum Lesen von Gruppen angezeigt.



8. Abschluss: Der Import-Fortschritt zeigt den aktuellen Status an. Die Zusammenfassung unterscheidet erfolgreiche, übersprungene und fehlgeschlagene Zeilen und führt zu jeder Zeile die Meldung auf.



Wichtige Hinweise zur Konfiguration

- Passwort-Richtlinien: Bei der Hinterlegung fester Kennwörter müssen diese der Passwortrichtlinie der jeweiligen Organisation entsprechen. Schreibt die Richtlinie beispielsweise mindestens 8 Zeichen vor, schlägt der Import für alle Benutzer mit kürzeren Passwörtern fehl.
- Klassenzuweisung: Lehrkräfte und Schüler werden Klassen über die Spalten `teacherOfClasses` und `studentOfClasses` zugewiesen. Mehrere Klassen in einer Zelle werden durch `|` getrennt. Die Mitgliedschaft in einer Gruppe (z. B. `UIT Teacher`) ordnet niemanden einer Klasse zu. Eine Klasse wird nur gespeichert, wenn sie danach mindestens eine Lehrkraft und mindestens einen Schüler hat; bei bestehenden Klassen zählen die bisherigen Mitglieder mit. Ist das nicht der Fall, wird diese Klasse im Import-Bericht als übersprungen aufgeführt, die Benutzer selbst werden trotzdem importiert. Eine noch nicht vorhandene Klasse wird nur angelegt, wenn die Option Automatisch Gruppen und Klassen erstellen aktiviert ist, sonst wird die Zeile als fehlgeschlagen gemeldet.
- Gruppenzuweisung: Gruppen (z. B. die Systemgruppen `UIT Teacher` und `UIT Student`) werden über die Spalte `memberOfGroups` zugewiesen, Berechtigungen aus `Benutzer` → `Berechtigungen` (z. B. `Self service portal - read access`) über die Spalte `permissions`. Maßgeblich ist jeweils der exakte Name. Die Systemgruppen der Organisation tragen deren eindeutigen Namen als Präfix, z. B. `UIT Teacher`; selbst angelegte Gruppen werden mit ihrem eigenen Namen eingetragen. Steht der Name einer Berechtigung in `memberOfGroups`, schlägt der Import für diese Zeile mit der Meldung fehl, dass die Gruppe nicht gefunden wurde; ist Automatisch Gruppen und Klassen erstellen aktiviert, entsteht stattdessen eine neue, leere Gruppe mit diesem Namen.
- Aktualisierung bestehender Benutzer: Der CSV-Import kann auch für bereits vorhandene Benutzerkonten verwendet werden. Übereinstimmende Konten werden anhand der Spalte `name` (Benutzername) innerhalb derselben Organisation erkannt und mit den Werten aus der CSV-Datei aktualisiert, anstatt doppelt angelegt zu werden. Die E-Mail-Adresse spielt für diese Zuordnung keine Rolle. Benutzer, die von einem externen Anbieter (z. B. einem Verzeichnisdienst) verwaltet werden, werden übersprungen. Importierte Benutzer werden stets aktiviert.
- Leere Spalten bei einer Aktualisierung: Ist eine Spalte in der CSV-Datei vorhanden, ihr Wert für eine Zeile jedoch leer, wird das entsprechende Feld beim bestehenden Benutzer geleert. Ausgenommen davon sind die Spalten `permissions`, `memberOfGroups`, `teacherOfClasses` und `studentOfClasses`: Eine leere Zelle lässt die bestehenden Zuordnungen unverändert. Ein eingetragener Wert ersetzt die bisherigen Zuordnungen dagegen vollständig; nicht aufgeführte Berechtigungen und Gruppen werden entfernt, ebenso nicht aufgeführte Klassen, in denen der Benutzer als Lehrer bzw. Schüler eingetragen ist. Die im Import-Dialog zusätzlich gewählten Gruppen werden in jedem Fall hinzugefügt. Bei allen anderen Spalten gilt: Spalten, deren vorhandene Werte unverändert bleiben sollen, werden aus der CSV-Datei vollständig entfernt, statt sie nur leer zu lassen.
- Passwort bei einer Aktualisierung: Bleibt die Spalte `password` bei einem bereits bestehenden Benutzer leer oder wird sie ganz weggelassen, bleibt dessen aktuelles Passwort unverändert erhalten. Bei neu angelegten Benutzern ohne Passwort-Angabe wird kein Passwort automatisch vergeben; für diese Benutzer wird ein erstes Passwort in einem separaten Schritt hinterlegt.
- Nur Anmeldung per SSO: Die Spalte `disablePasswordAuthentication` wirkt nur beim Anlegen eines Benutzers; bei einer Aktualisierung bleibt der bisherige Wert erhalten.

Für Version 26.4.0

Verhalten in der Praxis

Einige konkrete Beispiele zur Aktualisierung bestehender Benutzer über die CSV-Datei:

- Die Spalte `email` ist vorhanden, aber für eine Zeile leer gelassen: Die vorhandene E-Mail-Adresse des Benutzers wird dadurch gelöscht. Soll sie unverändert bleiben, muss die Spalte `email` vollständig aus der CSV-Datei entfernt werden.
- Die Spalte `memberOfGroups` ist vorhanden, aber für eine Zeile leer gelassen: Die bestehenden Gruppenmitgliedschaften des Benutzers bleiben unverändert. Enthält die Zelle dagegen `UIT Teacher`, ist der Benutzer danach nur noch Mitglied dieser Gruppe und der im Import-Dialog gewählten Gruppen.
- Woran wird ein bestehender Benutzer beim Update erkannt: Ausschließlich anhand der Spalte `name` (Benutzername) innerhalb derselben Organisation — die E-Mail-Adresse spielt dabei keine Rolle.
- Die Spalte `password` bleibt leer: Bei einem bereits bestehenden Benutzer bleibt das aktuelle Passwort unverändert erhalten, unabhängig davon, ob die Spalte fehlt oder nur leer ist. Bei einem neu angelegten Benutzer wird in diesem Fall kein Passwort automatisch vergeben.

Beispiel für die Benennung:

- Name der Organisation: `User-Import-Test`
- Eindeutiger Name der Organisation: `UIT`
- Zuzuweisende Gruppen: `UIT Student`, `UIT Teacher`

Eine CSV-Datei mit einer Lehrkraft und einem Schüler, denen über die Spalte `memberOfGroups` jeweils eine Gruppe und über `teacherOfClasses` bzw. `studentOfClasses` die Klasse `10a` zugewiesen wird, sieht beispielsweise wie folgt aus:

```
name;email;givenName;surname;permissions;memberOfGroups;teacherOfClasses;studentOfClass
es
lehrer1;lehrer1@uit-schule.de;Lena;Lehrer;;UIT Teacher;10a;
schueler1;schueler1@uit-schule.de;Sam;Schueler;;UIT Student;;10a
```

Mehrere Gruppen, Berechtigungen bzw. Klassen innerhalb derselben Zelle werden durch ein Pipe-Zeichen (`|`) getrennt, zum Beispiel `UIT Teacher|UIT Student`. Das gilt für die Spalten `memberOfGroups`, `permissions`, `teacherOfClasses` und `studentOfClasses`. Ein Semikolon ist innerhalb der Zelle ebenfalls als Trennzeichen möglich; da dieses je nach gewähltem CSV-Trennzeichen jedoch bereits die Spalten selbst trennt, wird zur eindeutigen Unterscheidung die Verwendung von `|` empfohlen. Ein Komma trennt innerhalb einer Zelle nicht.

Automatisches Anlegen von Gruppen und Klassen

Relution ist in der Lage, noch nicht vorhandene Klassen und Benutzergruppen während des Imports automatisch zu erstellen. Voraussetzung ist, dass im ersten Schritt (CSV Datei) die Option Automatisch Gruppen und Klassen erstellen aktiviert wird. Die Option ist standardmäßig deaktiviert und lässt sich nur mit den Berechtigungen zum Erstellen von Gruppen und Klassen aktivieren. Ohne diese Option werden Zeilen mit nicht vorhandenen Gruppen oder Klassen als fehlgeschlagen gemeldet. Berechtigungen aus der Spalte `permissions` werden nie automatisch angelegt; sie müssen bereits existieren. Dabei sind folgende Punkte zu beachten:

- Präzision: Maßgeblich ist die exakte Schreibweise des Namens; eine abweichende Schreibweise führt zu einer neuen Gruppe bzw. Klasse.
- Leerzeichen: Führende und abschließende Leerzeichen um Gruppen-, Klassen- und Berechtigungsnamen werden beim Import automatisch entfernt.
- Verwaltete Klassen: Klassen, die von einem externen Anbieter synchronisiert werden, werden beim Import übersprungen.

Häufige Ursachen für einen fehlgeschlagenen Import

Ein häufiger Grund für einen fehlgeschlagenen CSV-Import ist eine E-Mail-Adresse, die bereits einem anderen Benutzerkonto auf dem Server zugeordnet ist. E-Mail-Adressen müssen serverweit eindeutig sein, unabhängig davon, welcher Organisation der jeweilige Benutzer angehört.

Für Version 26.4.0

Bildungsfunktion

Mit der innovativen Bildungsfunktion von Relution wird die Vorbereitung von Klassen erleichtert, indem sie nahtlos in die Relution Teacher App integriert werden können. Diese Funktion ermöglicht es Lehrkräften, Klassen einfach zu starten und zu verwalten. Die Relution-Klassen setzen sich aus Lehrkräften und Schülern zusammen, die jeweils spezifische Berechtigungen haben. Durch die klare Struktur und die benutzerfreundliche Oberfläche der Relution-Plattform wird die Organisation und Durchführung des Unterrichts effizienter gestaltet. Weitere Informationen über die Bildungsfunktion und andere Möglichkeiten von Relution sind auf der Website unter www.relution.io zu finden.

> Der Menüpunkt Bildung wird nur in Organisationen mit gültiger Education- oder Free-Lizenz angezeigt. Er enthält die Einträge Klassen und Relution Teacher; über Relution Teacher wird die Teacher-Web-App direkt geöffnet.

Benutzer erstellen

Neue Benutzer werden im Menüpunkt Benutzer angelegt und mit den entsprechenden Berechtigungen versehen. Die verfügbaren Anlage-Methoden (manuelles Anlegen, CSV-Upload, LDAP-Synchronisation) sowie die Regel zur eindeutigen E-Mail-Adresse sind im Artikel zur Benutzerverwaltung beschrieben.

Benutzerverwaltung →

Für Version 26.4.0

Berechtigungen zuweisen

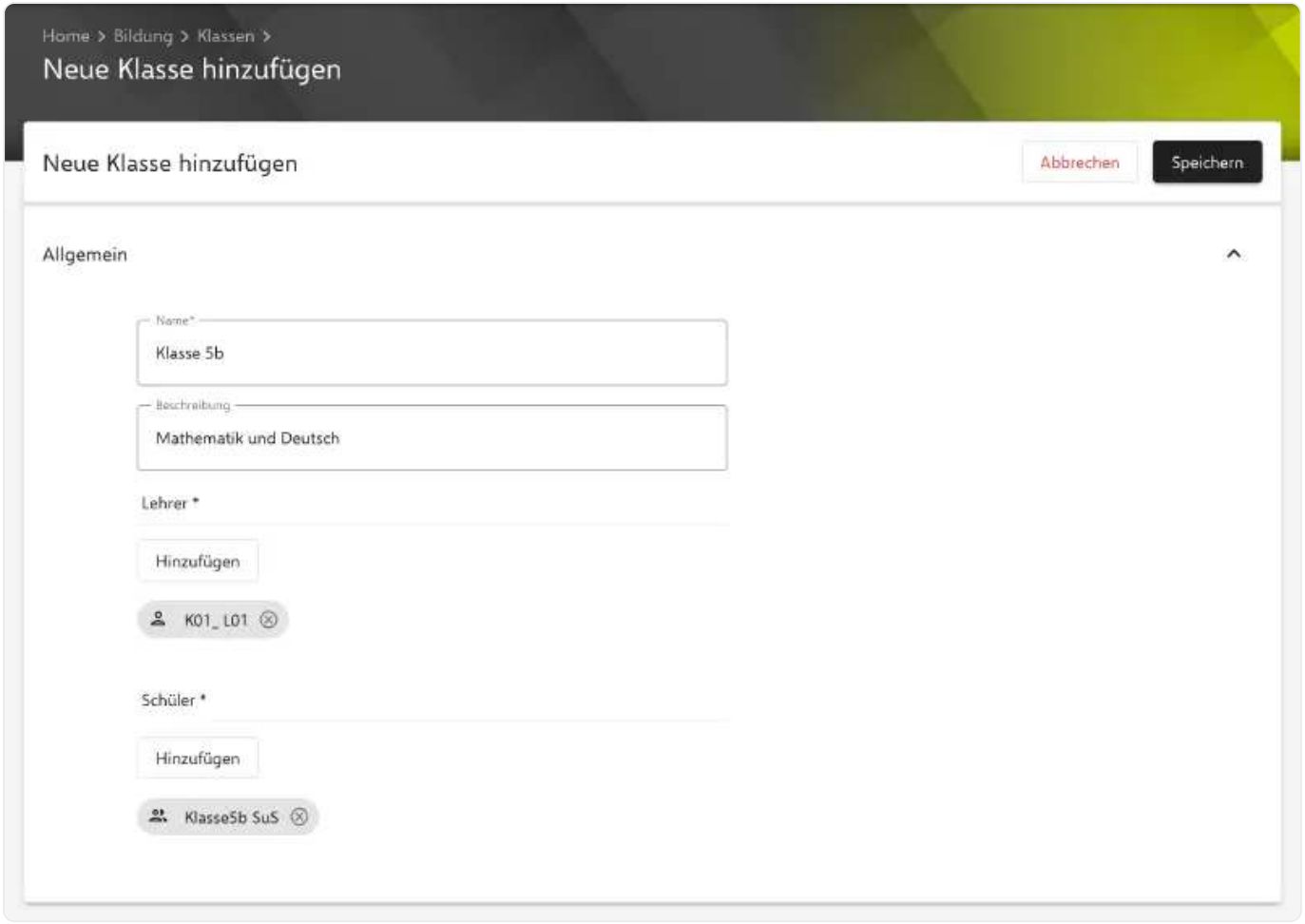
Im Menüpunkt `Benutzer` → `Gruppen` besteht die Möglichkeit, bestehenden Benutzern Gruppen zuzuweisen. Dabei sind bereits zwei wichtige Standardgruppen hinterlegt: `<ORGANISATION> Teacher` und `<ORGANISATION> Student`. Der Gruppenname beginnt mit dem eindeutigen Namen der Organisation in Großbuchstaben, z. B. `SCHULE Teacher`. In der Systemorganisation werden diese Gruppen nicht angelegt.

Die beiden Gruppen unterscheiden sich sowohl in ihren Rechten als auch im Umfang ihrer Funktionen. Beispielsweise ist der Start eines Unterrichts über die Relution Teacher App der Gruppe Teacher vorbehalten; Schüler (Gruppe Student) haben dieses Recht nicht. Die Systemgruppen `Device Manager` und `Appstore Manager` und damit auch `Administrator` sind Mitglied der Gruppe Teacher und erben deren Rechte. Diese klare Unterscheidung erleichtert die Verwaltung von Benutzern und gewährleistet eine gezielte Zuweisung von Rechten entsprechend den jeweiligen Aufgaben und Verantwortlichkeiten.

Sollen mehrere Benutzerkonten gleichzeitig mit `Teacher` oder `Student` ausgestattet werden, kann die Zuweisung auch direkt beim CSV-Import erfolgen, siehe CSV-Import →.

Klassen erstellen

Im Menüpunkt `Bildung` → `Klassen` besteht die Möglichkeit, Klassen manuell zu erstellen und den Benutzern entsprechend ihrer Rolle zuzuweisen. Pflichtfeld ist der Name; in der globalen Organisation wird zusätzlich die Zielorganisation gewählt. Lehrkräfte und Schüler lassen sich als einzelne Benutzer oder als ganze Gruppen zuweisen. Dabei ist zu beachten, dass eine Klasse aus mindestens einem Lehrer und einem Schüler (jeweils als Benutzer oder Gruppe) bestehen muss, um ordnungsgemäß angelegt zu werden.



Für eine effiziente Verwaltung besteht die Option, mehrere Klassen mithilfe der CSV-Upload-Funktion schnell und unkompliziert zu kreieren. Am komfortabelsten ist die Synchronisation der Klassen aus einem externen System, da sie eine automatische Aktualisierung und eine einheitliche Verwaltung der Klassen ermöglicht. Neben LDAP stehen dafür folgende Schnittstellen zur Verfügung:

- SchulConnex Import →
- OneRoster Schnittstelle → (z. B. für Untis/WebUntis)
- Apple School Manager Import →

Klassen, die über eine solche Schnittstelle synchronisiert werden, sind im Portal schreibgeschützt und werden ausschließlich im Quellsystem gepflegt.

Verwendung mit Relution Teacher und/oder Apple Classroom

Die erstellten Klassen lassen sich mühelos für den Unterricht mittels der Relution Teacher App vorbereiten. Nähere Einzelheiten zu diesem Prozess sind im Artikel über die Relution Teacher App zu finden.

Teacher →

Um während des Unterrichts die Geräte zu steuern, bietet sich zusätzlich die Verwendung der Apple Classroom App an. Weitere Informationen dazu sind dem Artikel über die Apple Classroom App zu entnehmen.

Apple Classroom →

Zusammenfassend kann festgehalten werden, dass die Relution Teacher App zur Vorbereitung von Unterrichtsstunden dient, während die Apple Classroom App die Steuerung während des Unterrichts ermöglicht.

Für Version 26.4.0

Berechtigungen

Relution ermöglicht es, Berechtigungen sehr präzise und feingranular zu konfigurieren. So kann für jeden Anwendungsfall ein spezielles Berechtigungsset erstellt werden, ohne dass Benutzer mehr Funktionen erhalten als nötig.

Über eine Berechtigung lässt sich zudem eine Multi-Faktor-Authentifizierung (MFA) für alle Benutzer erzwingen, die diese Berechtigung besitzen. Darüber hinaus lassen sich Berechtigungen aus der Global-Organisation für alle Organisationen und aus einer Meta-Organisation für alle Untermandanten bereitstellen.

Standard-Berechtigungsvorlagen

Unter `Benutzer` → `Berechtigungen` sind bereits Standardberechtigungen hinterlegt, z. B. Administrator, Teacher oder Student. Sie gelten global für alle Organisationen, entsprechen den Systemgruppen und sind mit diesen verknüpft. In der Liste sind sie in der Spalte System markiert. Diese Standardberechtigungen werden automatisch verwaltet und können weder geändert noch gelöscht oder exportiert werden.

Es ist jedoch jederzeit möglich, neue, benutzerdefinierte Berechtigungen anzulegen.

> Berechtigungen sind additiv. Das bedeutet, dass alle einem Benutzerkonto zugewiesenen Berechtigungen zusammengeführt werden.

Für Version 26.4.0

Berechtigungen konfigurieren

In der Kategorie Berechtigungen kann über Hinzufügen ein neuer Eintrag erstellt werden. Pflichtfeld ist der Name (bis zu 255 Zeichen), optional ist eine Beschreibung (bis zu 4000 Zeichen). Nahezu jede Funktion im Relution-Portal kann hier einzeln berechtigt werden.

In der Regel stehen vier Optionen zur Verfügung: Lesen, Erstellen, Aktualisieren und Löschen. Setzt eine Option eine andere voraus, wird diese automatisch mit aktiviert und ist dann gesperrt, z. B. setzt Erstellen das Recht Lesen voraus.

Beispiel: Ein Benutzer kann ein Konto mit Nur-Lese-Berechtigungen erhalten, sodass er keine Änderungen im System vornehmen kann.

Auch Geräteaktionen lassen sich einzeln konfigurieren:

- Beispiel: Alle Aktionen sind erlaubt außer Geräteortung.
- Ein weiteres Beispiel: Ein Benutzer darf nur die Token für Apps und Bücher (im Portal: VPP) und für die Automatische Geräteregistrierung (ADE, im Portal: DEP) erneuern, sonst aber keine Änderungen vornehmen. Für Apps und Bücher ist dafür im Eintrag Volume Purchase Programm (VPP) die Option Aktualisieren nötig, für ADE im Eintrag Apple Automated Device Enrollment die Option Erstellen. Eine Option Aktualisieren gibt es für ADE nicht; mit Erstellen kann der Benutzer auch neue ADE-Server-Konten anlegen.

Multi-Faktor-Authentifizierung erzwingen

Mit der Option Multi-Faktor-Authentifizierung wird für die Rolle erzwungen müssen sich alle Benutzer mit dieser Berechtigung per MFA anmelden. Der Abschnitt Multi-Faktor-Authentifizierung erscheint nur, wenn unter `Einstellungen` → `Verwaltung der Anmeldedaten` mindestens eine MFA-Methode aktiviert ist. Da sich die Standardberechtigungen nicht ändern lassen, wird dafür eine eigene Berechtigung benötigt. Details enthält der Artikel Multi-Faktor-Authentifizierung →.

Anwendungsbereich

Die Spalte Anwendungsbereich zeigt, wo eine Berechtigung gilt: Lokal (nur in der eigenen Organisation), Meta (in allen Untermandanten einer Meta-Organisation) oder Global (in allen Organisationen). Neue Berechtigungen werden lokal angelegt.

In der Global-Organisation macht der Kontextmenüeintrag Global verfügbar machen ausgewählte Berechtigungen in allen Organisationen verfügbar, in einer Meta-Organisation der Eintrag Meta-weit verfügbar machen in allen Untermandanten. Die Berechtigung wird dadurch niemandem zugewiesen, sondern steht dort nur zur Auswahl.

Berechtigungen exportieren und importieren

Über das Kontextmenü der Liste lassen sich ausgewählte Berechtigungen mit Berechtigungen exportieren als JSON-Datei sichern und über Berechtigungen importieren wieder einlesen, z. B. in einer anderen Organisation. Importierte Berechtigungen werden immer lokal angelegt. Standardberechtigungen lassen sich nicht exportieren.

Für Version 26.4.0

Verknüpfung von Berechtigungen mit Benutzerkonten

Im Benutzerkonto wird eine Berechtigung im Bereich Direkte Mitgliedschaften unter Gruppen & Berechtigungen zugewiesen: Die Schaltfläche Berechtigungen verwalten im Feld Berechtigungen öffnet die Auswahl.

Auf dieselbe Weise lassen sich Berechtigungen auch einer Gruppe zuweisen. Alle Mitglieder der Gruppe erhalten sie dann, auch über verschachtelte Gruppen.

Berechtigungen beim CSV-Import zuweisen

Berechtigungen lassen sich auch beim Anlegen mehrerer Benutzerkonten über den CSV-Import zuweisen. Der eigentliche Import-Vorgang ist im Artikel CSV-Import → beschrieben.

Die Zuweisung kann auf drei Wegen erfolgen:

- In der Spalte `permissions` der CSV-Vorlage werden pro Zeile Berechtigungen über ihren exakten Namen eingetragen, z. B. `Teacher` oder `Student`. Mehrere Einträge werden durch `|` getrennt.
- In der Spalte `memberOfGroups` werden Gruppen über ihren exakten Namen eingetragen, z. B. die Systemgruppe `[Organisation] Teacher`. Die Berechtigungen der Gruppe erhält das Benutzerkonto über die Gruppenmitgliedschaft.
- Im optionalen Schritt Gruppen des Import-Dialogs werden eine oder mehrere bestehende Gruppen ausgewählt. Alle importierten Benutzerkonten werden zusätzlich zu den Gruppen aus `memberOfGroups` Mitglied dieser Gruppen. Der Schritt ist nur sichtbar, wenn Leserecht auf Gruppen besteht.

Ein unbekannter Name in `permissions` führt dazu, dass die betroffene Zeile nicht importiert wird. Für `memberOfGroups` gilt das ebenso, sofern die Option Automatisch Gruppen und Klassen erstellen nicht aktiv ist; mit der Option wird eine neue, leere Gruppe ohne Berechtigungen angelegt.

> Die Namen der Systemgruppen enthalten den eindeutigen Namen der jeweiligen Organisation, z. B. [Organisation] Teacher oder [Organisation] Student. Die zugehörigen Standardberechtigungen heißen ohne dieses Präfix, z. B. Teacher oder Student.

Für Version 26.4.0

Self-Service Portal

Ab Version 5.22 verfügt Relution über ein Self-Service Portal. Hier haben Relution User die Möglichkeit, ihre eigenen Geräte einzusehen, einzelne Aktionen auszuführen und Details abzufragen.

Anforderungen

Für die Nutzung des Self-Service Portals stehen zwei Standardberechtigungen zur Verfügung. Sie werden bei einem Update auf Relution 5.22 oder bei der Erzeugung der Datenbank automatisch angelegt. Um das Self-Service Portal den Usern zur Verfügung zu stellen, müssen sie über die entsprechenden Berechtigungen verfügen und mindestens ein Gerät mit ihrem User Account verknüpft haben.

Erteilen der Berechtigung

Unter `Benutzer` → `Berechtigungen` stehen `Self service portal - full access` sowie `Self service portal - read access` als Vorlagen zur Verfügung. Diese müssen, je nach Anforderung, mit den gewünschten Accounts verknüpft werden.

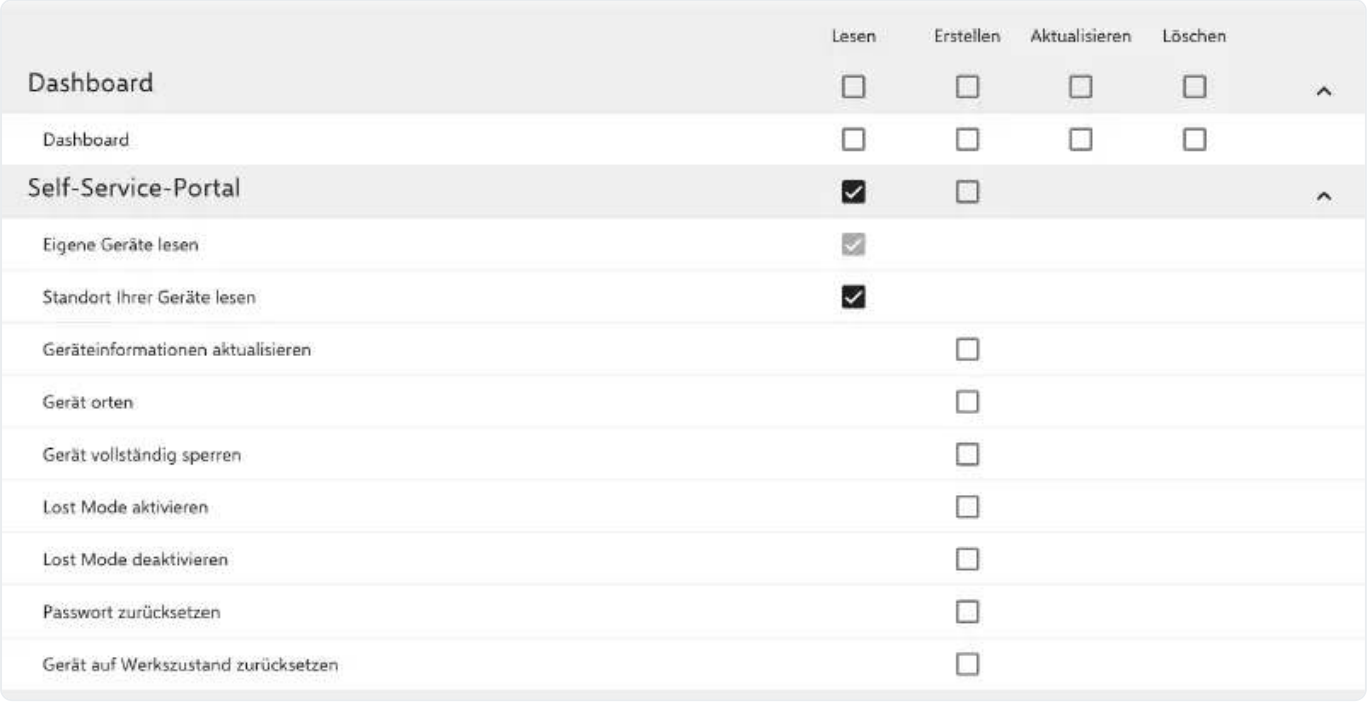
- `Self service portal - read access` erlaubt nur, die eigenen Geräte einzusehen und deren Geräteinformationen zu aktualisieren.
- `Self service portal - full access` erlaubt zusätzlich, den Standort zu lesen, das Gerät zu orten, den Lost Mode zu aktivieren und zu deaktivieren, das Gerät zu sperren, das Passwort zurückzusetzen sowie das Gerät auf den Werkszustand zurückzusetzen oder zu löschen.

Für Version 26.4.0

Für eigene Berechtigungen stehen in der Kategorie Self-Service-Portal die Rechte einzeln zur Verfügung, z. B. Eigene Geräte lesen, Standort Ihrer Geräte lesen und je Aktion ein eigenes Recht.

Die Zuweisung erfolgt folgendermaßen:

1. Unter `Benutzer` → `Benutzer` wird das entsprechende Benutzerkonto geöffnet.
2. Im Bereich Direkte Mitgliedschaften unter Gruppen & Berechtigungen öffnet Berechtigungen verwalten im Feld Berechtigungen die Auswahl.
3. Dort wird eine der o. g. Berechtigungen ausgewählt.
4. Mit Speichern wird die Zuweisung übernommen.



Verknüpfung eines Geräts mit dem Benutzerkonto

Die Verknüpfung eines Benutzerkontos mit einem Gerät kann entweder über den Import einer CSV-Datei, durch entsprechende Konfiguration der Einschreibung vor der Einschreibung oder manuell geschehen.

Für den manuellen Weg ist es lediglich nötig, das Gerät aus dem Inventar auszuwählen und aus der Symbolleiste das Icon für Benutzer ändern zu selektieren.

Für Version 26.4.0

Das Self-Service Portal

Loggt sich eine Person mit dem entsprechenden Benutzerkonto auf dem Relution Portal ein, steht die Self-Service Funktion zur Verfügung. Benutzer, die nur Self-Service-Rechte besitzen, landen nach der Anmeldung direkt auf der Seite Ihre Geräte; Administratoren erreichen sie über das Profilmenü oben rechts.

Seit Relution 26.5.0 läuft die Anmeldung am Self-Service Portal über einen eigenen Geltungsbereich (`/api/selfService/`). Wird sie per OpenID Connect mit scoped Redirect-URIs genutzt, muss die zugehörige Redirect-URI beim Identity Provider registriert sein, siehe OIDC mit Entra → bzw. OIDC mit Workspace →.

Pro Gerät werden grundlegende Informationen angezeigt, z. B. Akkustand, Status, letzte Verbindung, Plattform, Eigentümer, Modell, Seriennummer, Betriebssystem, Einschreibungsdatum und Lost-Mode-Status. Außerdem sind folgende Funktionen vorhanden:

- Lost Mode aktivieren / deaktivieren
- Gerät orten
- Standort auf einer Karte anzeigen
- Gerät auf Werkszustand zurücksetzen
- Gerät vollständig sperren
- Passwort zurücksetzen

Gerät auf Werkszustand zurücksetzen öffnet den Dialog Entfernen. Dort wird zwischen dem Zurücksetzen auf den Werkszustand und Löschen (Gerät aus dem MDM entfernen) gewählt. Über die Schaltfläche Geräteinformationen aller sichtbaren Geräte aktualisieren auf der Seite Ihre Geräte werden die Informationen aller angezeigten Geräte neu abgefragt; eine erneute Abfrage ist standardmäßig frühestens 5 Minuten nach der letzten Aktualisierung möglich.

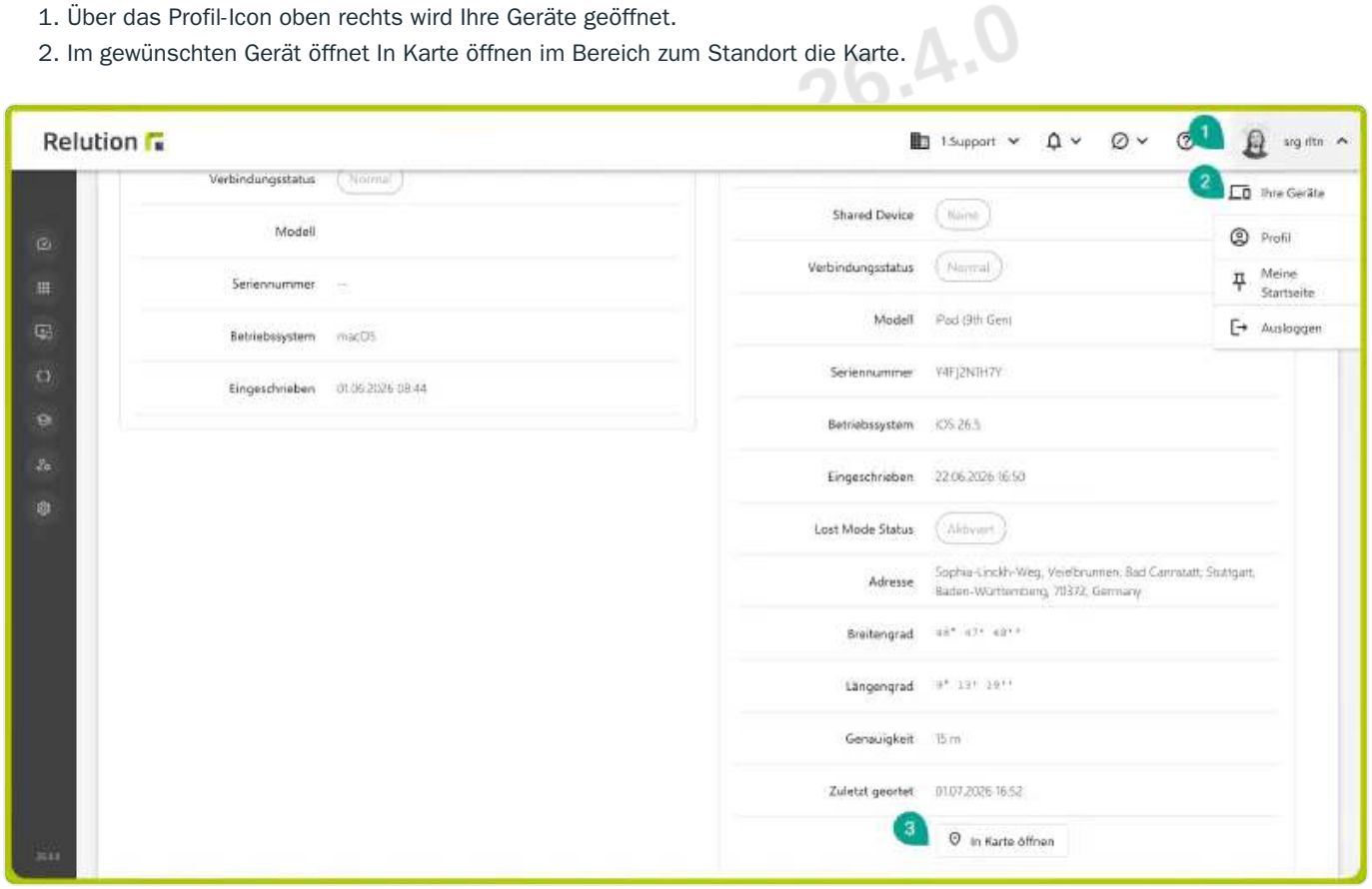
Die verfügbaren Funktionen können je nach Geräteplattform variieren. Auf iOS-Geräten stehen Lost Mode und Gerät orten nur bei betreuten Geräten zur Verfügung, Gerät orten zudem nur bei aktivem Lost Mode. Wird ein Gerät gerade gelöscht oder zurückgezogen, sind die Aktionen gesperrt. Zudem lassen sich die Funktionen über Berechtigungen einschränken.

Standort auf einer Karte anzeigen

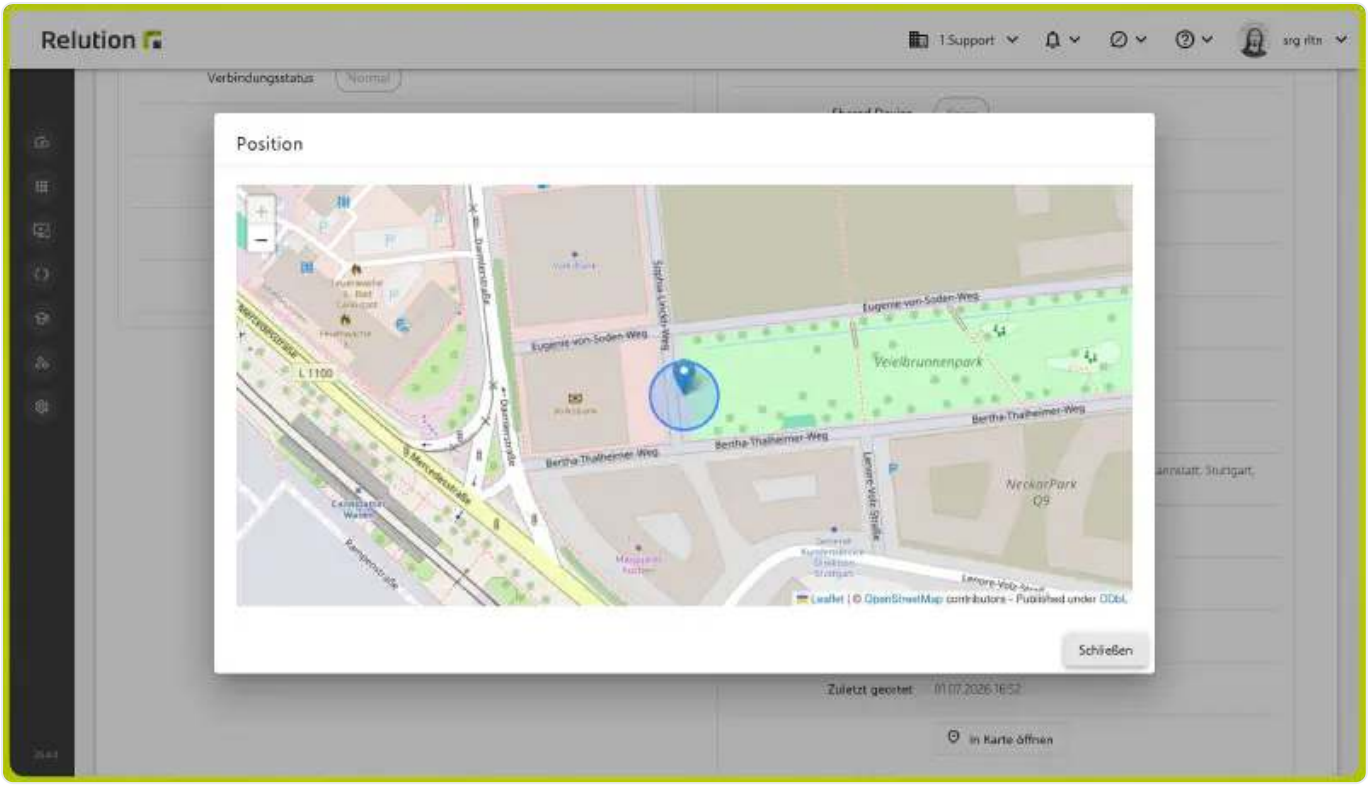
Neu in 26.4

Berechtigte Benutzer können sich den zuletzt ermittelten Standort ihres Geräts direkt auf einer Karte anzeigen lassen.

1. Über das Profil-Icon oben rechts wird Ihre Geräte geöffnet.
2. Im gewünschten Gerät öffnet In Karte öffnen im Bereich zum Standort die Karte.



Der zuletzt bekannte Standort wird daraufhin in einer Kartenansicht angezeigt.



Voraussetzung ist die Berechtigung Standort Ihrer Geräte lesen. Sie ist in `Self service portal - full access` enthalten, nicht aber in `Self service portal - read access`. Fehlt sie, wird der Standortbereich nicht angezeigt. Der Standortbereich steht für iOS-, Android- (inkl. Android Enterprise) und Windows-Geräte zur Verfügung, bei iOS-Geräten nur, wenn das Gerät betreut ist und der Lost Mode aktiv ist. Für macOS- und ChromeOS-Geräte wird kein Standort angezeigt.

Für Android Enterprise-Geräte sind zudem aktivierte Standortdienste sowie die entsprechende Berechtigung des Relution Companions Voraussetzung, siehe Android Gerät orten → und Standort Dienste →.

Für Version 26.4.0

Erweiterte Platzhalter

Platzhalter wie `${user.email}` oder `${device.model}` werden an mehreren Stellen in Relution genutzt, u. a. bei Gerätenamen, Zertifikaten, Exchange-Konten oder App-Konfigurationen. Über die zugrunde liegende Template-Engine `FreeMarker` stehen dabei zusätzliche Funktionen zur Verfügung, mit denen Platzhalter weiter angepasst werden können.

Teilzeichenfolgen (Substring)

Mit der Notation `[start..*länge]` wird nur ein Ausschnitt eines Werts verwendet: ab Position `start` höchstens `länge` Zeichen. Die Zählung beginnt bei `0`. Ist der Wert kürzer, wird entsprechend weniger eingesetzt, bei leerem Wert nichts. Voraussetzung ist, dass `start` nicht hinter dem Ende des Werts liegt; andernfalls schlägt die Ersetzung wie bei `[start..ende]` fehl (siehe Hinweis unten).

- `${user.givenName[0..*1]}` → erster Buchstabe des Vornamens
- `${device.model[0..*2]}` → erste zwei Zeichen des Gerätemodells

Beispiel:
`${user.givenName[0..*1]}${user.surname[0..*1]}-${device.model[0..*2]}-${(device.custom1)!"00000"}` ergibt bei einem Benutzerkonto „Max Mustermann“ mit einem `custom1`-Wert von `00042` auf einem `iPad12,1` beispielsweise `MM-iP-00042`.

> Die ebenfalls mögliche Notation `[start..ende]` (z. B. `[0..0]`) setzt voraus, dass der Wert mindestens bis zur Position `ende` reicht. Ist der Wert gesetzt, aber kürzer oder leer, schlägt die Ersetzung fehl und keiner der Platzhalter im betroffenen Text wird ersetzt. Dasselbe gilt für `[start..*länge]`, wenn `start` größer als die Länge des Werts ist.

Für Version 26.4.0

Standardwert bei nicht gesetztem Feld

Ist ein Feld nicht gesetzt, kann mit dem `!`-Operator ein Standardwert hinterlegt werden: `${(device.custom1)!"00000"}`. Ist das benutzerdefinierte Feld `custom1` nicht gesetzt, wird stattdessen `00000` verwendet, anstatt dass der Platzhalter leer bleibt. Ein gesetzter, aber leerer Wert gilt dagegen als vorhanden: Der Standardwert greift dann nicht, und der Platzhalter bleibt leer.

Groß-/Kleinschreibung und Zeichen ersetzen

Über `?lower_case` bzw. `?upper_case` wird ein Wert vollständig in Klein- oder Großbuchstaben umgewandelt. Mit `?replace("alt", "neu")` lassen sich einzelne Zeichen oder Zeichenfolgen ersetzen, beispielsweise um Umlaute für Systeme aufzulösen, die keine Sonderzeichen im Benutzernamen zulassen:

```
${user.surname?lower_case?replace("ä","ae")?replace("ö","oe")?replace("ü","ue")?replace("ß","ss")}
```

Diese Funktion ist besonders bei macOS-Einschreibungen mit Benutzerauthentifizierung relevant, da Sonderzeichen im lokalen Kontonamen zu fehlschlagenden Skript-Deployments führen können.

Lokalen Teil einer E-Mail-Adresse verwenden

Um aus `${user.name}` (bzw. `${user.email}`) nur den Teil vor dem `@`-Zeichen zu verwenden, stehen mehrere Varianten zur Verfügung:

- `${user.name?keep_before("@")}`
- `${user.name?split("@")[0]}`
- `${user.name[0..user.name?index_of("@")-1]}`

Enthält der Wert kein `@`, liefern die ersten beiden Varianten den vollständigen Wert, während die dritte fehlschlägt. Empfohlen wird daher `?keep_before`.

Benutzerzertifikate

Neu in 26.5

Für Version 26.4.0

Über Platzhalter der Form `${user.certificate.…}` werden die im Benutzerprofil hinterlegten Zertifikate (Abschnitt Benutzerdefinierte Zertifikate) als base64-kodierte Zeichenkette in eine Konfiguration eingefügt — zum Beispiel in eine Managed App Konfiguration, deren Felder ein Zertifikat als base64-String erwarten. Aufgelöst wird der Platzhalter beim Übertragen der Konfiguration anhand des Benutzers, der dem jeweiligen Gerät zugewiesen ist.

Drei Auswahlformen stehen zur Verfügung:

Platzhalter	Auflösung
`${user.certificate.EXCHANGE}`	Zertifikat des Subtyps mit der längsten Restlaufzeit
`${user.certificate.EXCHANGE["mein-zertifikat"]}`	Zertifikat mit exakt diesem Namen (Groß-/Kleinschreibung wird beachtet); bei mehreren gleichnamigen das mit der längsten Restlaufzeit
`${user.certificate.EXCHANGE[device.serialnumber]}`	Zertifikatsname wird aus einem anderen Platzhalter berechnet

Als Subtyp wird die Kategorie angegeben, die im Benutzerprofil für das Zertifikat ausgewählt ist. Beim Subtyp spielt die Groß-/Kleinschreibung keine Rolle.

Kategorie im Benutzerprofil	Subtyp
Allgemeines Zertifikat	`GENERAL_CERTIFICATE`
WLAN	`WIFI`
Exchange	`EXCHANGE`
VPN und Apps	`VPN`
S/MIME-Verschlüsselung	`SMIME_ENCRYPTION`
S/MIME Signierung	`SMIME_SIGNING`

Zertifikatsname in eckigen Klammern

Bei berechneten Namen wird der innere Platzhalter ohne umschließendes `${…}` geschrieben, also `[device.serialnumber]` statt `[${device.serialnumber}]` — verschachtelte `${…}`-Ausdrücke werden nicht unterstützt. Für Namen, die nur aus Buchstaben, Ziffern und Unterstrichen bestehen, funktioniert auch die Punktform `${user.certificate.EXCHANGE.iPhone}`.

Für Version 26.4.0

> Zertifikatsnamen mit anderen Zeichen (z. B. Bindestrich oder Leerzeichen) müssen in der Klammerform mit Anführungszeichen angegeben werden. Ein Ausdruck wie `${user.certificate.EXCHANGE.mein-zertifikat}` wird als Rechenoperation interpretiert und führt dazu, dass die gesamte Konfiguration ohne ersetzte Platzhalter ausgeliefert wird.

Passwort für PKCS#12-Zertifikate

Für passwortgeschützte PKCS#12-Zertifikate (z. B. eine S/MIME-Identität) wird das Importpasswort über den reservierten Schlüssel `password` mitgeliefert:

- `${user.certificate.SMIME_SIGNING.password}`
- `${user.certificate.SMIME_SIGNING["mein-zertifikat"].password}`

Bei Zertifikaten, die kein PKCS#12-Container sind, bleibt der Wert leer. Da `password` ein reservierter Schlüssel ist, kann ein Zertifikat, das selbst den Namen `password` trägt, nicht über Platzhalter ausgewählt werden — sowohl die Punkt- als auch die Klammerform liefern in diesem Fall das Passwort. Für solche Zertifikate sollte ein anderer Name verwendet werden.

Ausgabeformat

Unabhängig vom hochgeladenen Dateiformat (PEM oder DER) liefert der Platzhalter immer die base64-kodierte DER-Form des Zertifikats. PKCS#12-Container werden unverändert base64-kodiert ausgeliefert, sodass sie zusammen mit dem Passwort direkt von der empfangenden App importiert werden können. Andere Zertifikatstypen werden ebenfalls so ausgeliefert, wie sie gespeichert sind.

Beispiel einer Managed App Konfiguration für einen E-Mail-Client mit S/MIME-Signatur:

```
<key>SMIMECertificate</key>
<string>${user.certificate.SMIME_SIGNING}</string>
<key>SMIMECertificatePassword</key>
<string>${user.certificate.SMIME_SIGNING.password}</string>
```

Verfügbarkeit

Benutzerzertifikat-Platzhalter sind für Konfigurationen vorgesehen, deren Inhalt an das Gerät des zugewiesenen Benutzers übertragen wird, insbesondere Managed App Konfigurationen (iOS/macOS, Android Enterprise), Knox-Konfigurationen (Android Enterprise, Samsung KNS), eigene Konfigurationsprofile (`.mobileconfig`) und Windows Custom CSP. In diesen Konfigurationen führt das Portal sie auch unter Verfügbare Platzhalter auf. Nicht aufgelöst werden sie (der Platzhalter bleibt leer) in Gerätenamen, also beim Umbenennen von Geräten und in Gerätename-Konfigurationen für Apple und Windows, unter Android Enterprise in Sperrbildschirm- und Supportnachrichten, bei der Arbeitskonto-Einrichtung und in Setup-Aktionen sowie in Skript-Umgebungsvariablen und in Webhook-Aktionen von Gerätegruppen. Für Linux-Konfigurationen werden sie nicht unterstützt. In eigenen Konfigurationsprofilen (`.mobileconfig`) ist der Platzhalter nur in String-Feldern möglich, nicht in data-Feldern; in Managed App Konfigurationen funktioniert beides.

Für Version 26.4.0

Kann kein Zertifikat ermittelt werden — etwa bei unbekanntem Subtyp, nicht vorhandenem Namen oder fehlender Benutzerzuweisung —, bleibt der Platzhalter leer und die Konfiguration wird dennoch ausgeliefert. Details zur Ursache werden im Serverlog protokolliert.

Hinweise

> Funktionsnamen und Groß-/Kleinschreibung müssen exakt wie beschrieben verwendet werden. Das Relution-Portal zeigt keine Vorschau des aufgelösten Werts an; ein Test der Kombination an einem Testgerät vor dem Rollout der Konfiguration empfiehlt sich daher.

Welche Basis-Platzhalter (z. B. `${user.email}`, `${device.serialnumber}`) in einer bestimmten Konfiguration zur Verfügung stehen, wird im Konfigurationsformular bzw. im jeweiligen Dialog im Abschnitt Verfügbare Platzhalter angezeigt. Ein Klick auf einen Eintrag kopiert ihn in die Zwischenablage.

Nicht gesetzte Werte werden als leere Zeichenfolge eingesetzt. Schlägt dagegen die Auswertung eines Ausdrucks fehl — etwa bei einem Ausschnitt `[0..0]` aus einem gesetzten, aber leeren Wert oder einem unbekannten Funktionsnamen —, betrifft das nicht nur den einzelnen Platzhalter: Der gesamte Text des Felds bzw. der Konfiguration wird unverändert ausgeliefert, also mit allen nicht ersetzten `${…}`-Ausdrücken. Die Ursache wird im Serverlog protokolliert.

OneRoster Schnittstelle

Ab Relution 26.2 ist die OneRoster Schnittstelle für Benutzer im Portal implementiert. Diese ermöglicht die Synchronisation von Benutzern und Klassen, beispielsweise aus Untis oder WebUntis, mit Relution. Die Funktion ist unter `Einstellungen` → `Benutzerverwaltung` → `OneRoster` zu finden.

> Aktuell unterstützen Untis/WebUntis nur eine Organisation/Mandanten in Relution. Daher ist es sinnvoll, die OneRoster Schnittstelle direkt auf dem Zielmandanten einzubinden. Alternativ kann die Schnittstelle auch auf der globalen Organisation eingebunden werden, wobei Schulen über IDs gemappt werden können. Dies erfordert jedoch Unterstützung durch die Benutzerverwaltungsapplikation.

Einrichtung der OneRoster Schnittstelle

Eine neue Verbindung wird in der Übersicht `Einstellungen` → `Benutzerverwaltung` → `OneRoster` über Hinzufügen angelegt.

Allgemeine Einstellungen

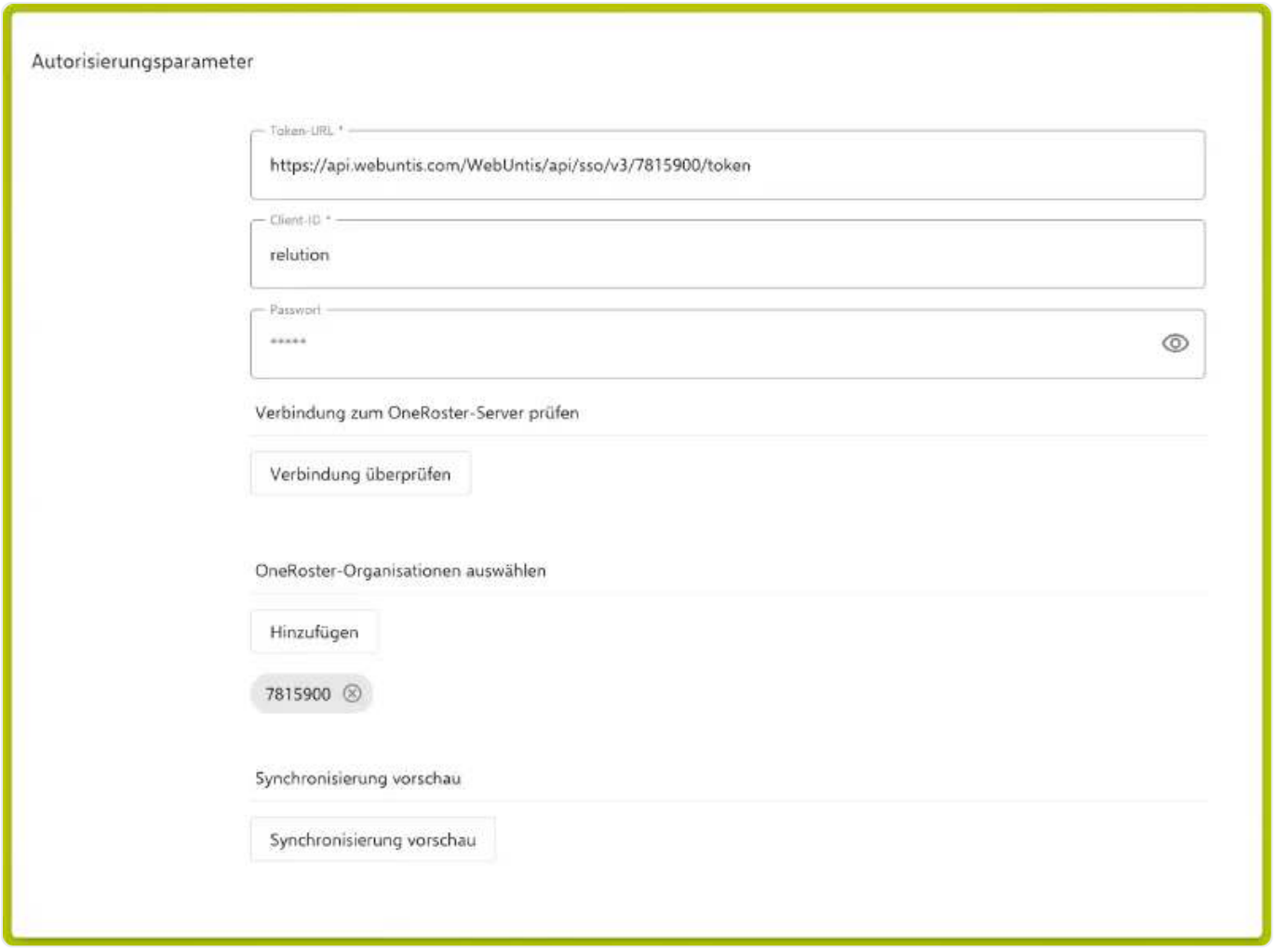
Für Version 26.4.0

1. Name des Anbieters: Eindeutiger Name für die Verbindung. Der Name darf bei keiner anderen Anbieter-Konfiguration vergeben sein und lässt sich nach dem Speichern nicht mehr ändern.
2. Aktiviert: Über diesen Schalter wird die Schnittstelle eingeschaltet. Bei einer neuen Verbindung ist er ausgeschaltet; solange er deaktiviert ist, findet keine Synchronisation statt.
3. Host: URL des OneRoster-Servers.

Autorisierungsparameter

- Token-URL: URL für die Token-Authentifizierung.
- Client-ID: Client-ID für die Authentifizierung.
- Passwort: Zugehöriges Client-Secret. Bei einer gespeicherten Verbindung ist das Feld mit `*****` vorbelegt; bleibt es leer, gilt weiterhin das hinterlegte Passwort. Werden Host oder Token-URL geändert, muss das Passwort erneut eingegeben werden, sonst lehnt Relution Verbindungstest und Speichern ab.

Über die Schaltfläche Verbindung überprüfen lässt sich die Verbindung zum OneRoster-Server testen, sobald alle Pflichtfelder ausgefüllt sind.



Organisationen auswählen

- In einem Mandanten werden im Abschnitt Autorisierungsparameter bei OneRoster-Organisationen auswählen über Hinzufügen die OneRoster-Organisationen gewählt, die synchronisiert werden sollen. Die Schaltfläche ist aktiv, sobald alle Pflichtfelder ausgefüllt sind.
- In der globalen Organisation oder einer Meta-Organisation gibt es stattdessen den Abschnitt Organisationszuordnungen. Dort werden OneRoster-Organisationen den einzelnen Relution-Organisationen zugeordnet.
- Über die Synchronisierungsvorschau lassen sich die zu synchronisierenden Klassen mit ihren Lehrern und Schülern vorab prüfen. Die Vorschau steht zur Verfügung, sobald mindestens eine Organisation ausgewählt bzw. zugeordnet ist.

Ohne ausgewählte OneRoster-Organisation schlägt die Synchronisation fehl.

Synchronisationseinstellungen

- Klassen synchronisieren: Importiert Klassen aus OneRoster. Die Option ist standardmäßig aktiviert.
- Aktion bei fehlenden Benutzern: Legt fest, was mit bereits synchronisierten Benutzern geschieht, die der OneRoster-Server nicht mehr liefert: `Keine` (Standard), `Deaktivieren` oder `Löschen`. Die Aktion gilt immer, auch wenn Klassen synchronisieren deaktiviert ist.
- Aktion bei fehlenden Klassen: Legt fest, was mit bereits synchronisierten Klassen geschieht, die in OneRoster nicht mehr vorhanden sind: `Keine` (Standard) oder `Löschen`. Die Aktion greift nur, wenn Klassen synchronisieren aktiviert ist.

Liefert eine Synchronisation gar keine Benutzer bzw. gar keine Klassen, führt Relution die jeweilige Aktion nicht aus. So werden bei einem Verbindungs- oder Konfigurationsfehler nicht alle Objekte deaktiviert oder gelöscht.

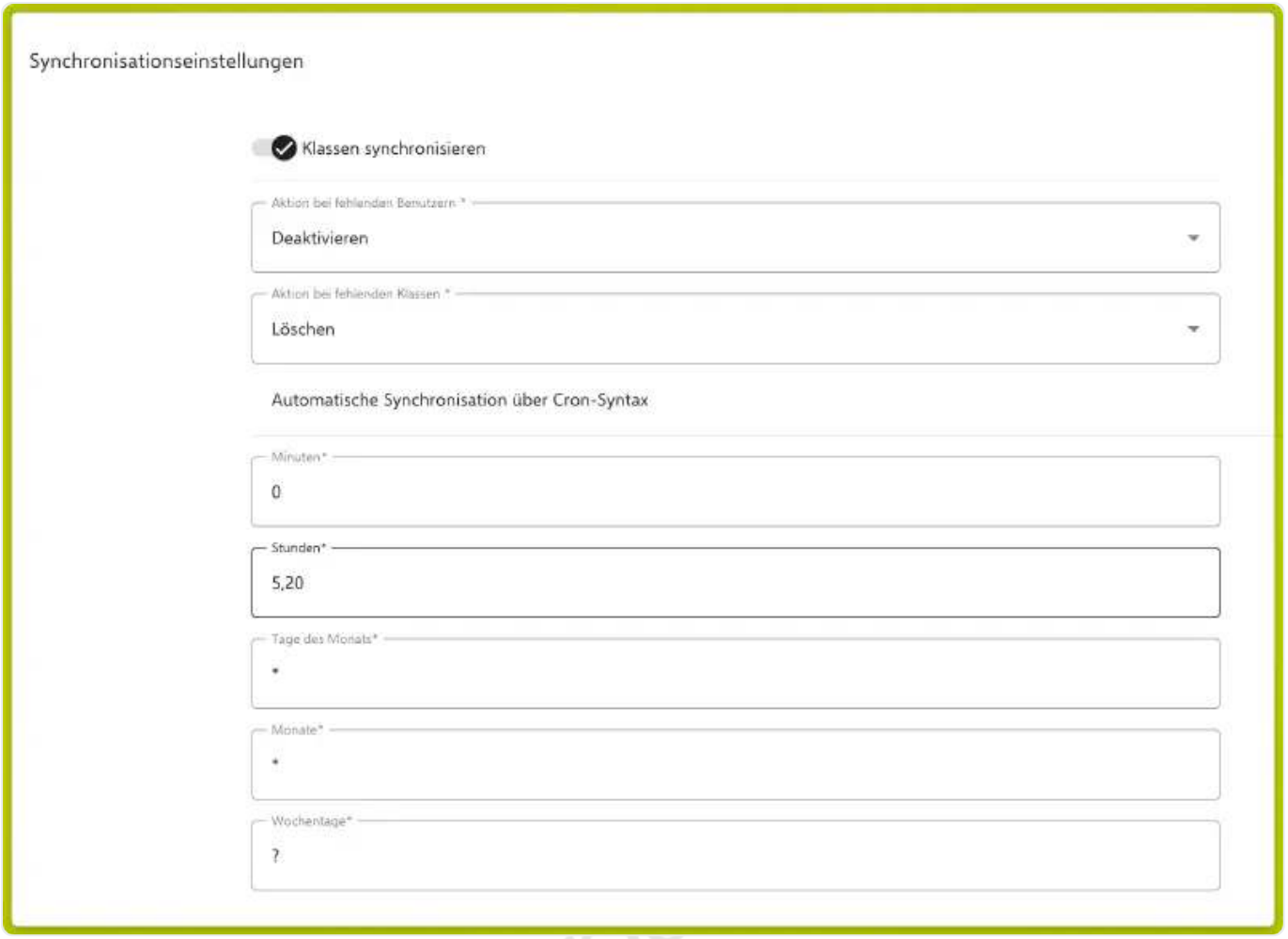
Synchronisierte Benutzer werden automatisch der Systemgruppe `<ORGANISATION> Teacher` bzw. `<ORGANISATION> Student` der Organisation sowie einer Gruppe des Anbieters zugeordnet. Als Anmeldename verwendet Relution den Benutzernamen aus OneRoster, ersatzweise die E-Mail-Adresse oder eine Kennung aus OneRoster.

Automatische Synchronisation

Die automatische Synchronisation wird über Cron-Syntax festgelegt. Standardmäßig läuft sie täglich um 5:00 und 20:00 Uhr.

- Minuten: Minute, zu der die Synchronisation ausgeführt wird.
- Stunden: Stunde der Synchronisation.
- Tage des Monats, Monate, Wochentage: Weitere Einschränkungen des Synchronisationsintervalls.

Für Version 26.4.0



Für Versi

Synchronisation prüfen

Nachdem die Verbindung gespeichert wurde, lässt sie sich in der Übersicht öffnen. Die Detailansicht listet die Sync-Ergebnisse getrennt für Benutzer und Klassen auf: Sie zeigt, wann die nächste geplante Synchronisierung ansteht und wann zuletzt synchronisiert wurde, ob die Synchronisierung erfolgreich war, die Statusmeldung sowie die Anzahl der synchronisierten, fehlenden und fehlgeschlagenen Objekte. Ein Klick auf die Anzahl unter Synchronisierungsfehler zeigt die einzelnen Fehler und damit deren Ursache.

In der Kopfzeile der Detailansicht stößt das Symbol Synchronisieren jederzeit einen manuellen Sync-Lauf an (erfordert die Berechtigung zum Bearbeiten von Benutzern oder Klassen). Daneben stehen Bearbeiten und Löschen zur Verfügung.

> Die meisten Synchronisationsfehler entstehen durch fehlende Benutzer in einer Klasse. Relution benötigt mindestens einen Schüler und einen Lehrer, um eine Klasse zu erstellen. Zudem werden Benutzer bei der Synchronisation übersprungen, wenn ihr Benutzername in der Organisation oder ihre E-Mail-Adresse in Relution bereits vergeben ist oder ihnen eine E-Mail-Adresse fehlt.

SchulConnex Import

Relution unterstützt die Synchronisation von Identitäten und Bildungskontextdaten über SchulConnex. Die Funktion ist unter `Einstellungen` → `Benutzerverwaltung` → `SchulConnex` zu finden und synchronisiert Benutzer, Gruppenrollen und Klassen/Kurse automatisch mit der zugrunde liegenden Schulverwaltungssoftware. In der Übersicht SchulConnex Importe wird eine neue Konfiguration über Hinzufügen angelegt.

SchulConnex dient ausschließlich dem Import. Die Anmeldung der importierten Benutzer an Relution erfolgt über eine andere Anmeldemethode, z. B. einen Identitätsanbieter.

Allgemein

1. Name des Anbieters: Eindeutiger Name für die Konfiguration. Der Name darf bei keiner anderen Anbieter-Konfiguration vergeben sein und lässt sich nach dem Speichern nicht mehr ändern.
2. Aktiviert: Schaltet die Synchronisation ein. Bei einer neuen Konfiguration ist der Schalter ausgeschaltet; solange er deaktiviert ist, findet keine Synchronisation statt.
3. Host: URL des SchulConnex-Servers.

Autorisierungsparameter

- Autorisierungs-URL: URL für die OAuth-Authentifizierung.
- Kunden-ID: Client-ID für die Authentifizierung.
- Passwort: Client-Secret des SchulConnex-Clients. Bei einer gespeicherten Konfiguration ist das Feld mit `*****` vorbelegt; bleibt es leer, gilt weiterhin das hinterlegte Secret. Werden Host oder Autorisierungs-URL geändert, muss das Secret erneut eingegeben werden, sonst lehnt Relution Speichern, Verbindungstest und Sync-Vorschau ab.

Über die Schaltfläche Verbindung überprüfen (Beschriftung SchulConnex-Verbindung prüfen) lässt sich die Verbindung testen, sobald alle Pflichtfelder gültig ausgefüllt sind.

Für Version 26.4.0

Home > Einstellungen >

SchulConnex

SchulConnex

Abbrechen | Speichern

Allgemein

Name des Anbieters *

SchulConnex

Aktiviert

Host *

https://api.schulconnex.example.org

Autorisierungsparameter

Autorisierungs-URL *

https://login.schulconnex.example.org/token

Kunden-ID *

relution-schule-01

Passwort *

••••••••••••••••••••

SchulConnex-Verbindung prüfen

Verbindung überprüfen

Wählen Sie die SchulConnex-Organisationen aus, die in diese Organisation eingegliedert werden sollen.

Hinzufügen

Sync-Vorschau anzeigen

Sync-Vorschau anzeigen

Organisationszuordnung

- Auf einer normalen Organisation werden direkt die SchulConnex-Organisationen ausgewählt, die in diese Organisation eingegliedert werden sollen (1:1-Zuordnung).
- Auf der globalen Organisation oder einer Meta-Organisation lassen sich stattdessen mehrere Relution-Organisationen gleichzeitig verwalten: Für jede Relution-Organisation wird per Zuordnungs-Assistent eine eigene Auswahl von SchulConnex-Organisationen festgelegt. Jede SchulConnex-Organisation und jede Relution-Organisation lässt sich dabei nur einmal zuordnen.

Über Sync-Vorschau anzeigen lässt sich vorab prüfen, welche Klassen/Kurse mit wie vielen Lehrern und Schülern importiert würden.

Synchronisationseinstellungen

- Klassen synchronisieren: Aktiviert den Import von Klassen/Kursen (Standard: aktiviert).
- Aktion, wenn ein Benutzer in SchulConnex entfernt wird: Legt fest, was passiert, wenn ein zuvor synchronisierter Benutzer in SchulConnex nicht mehr vorhanden ist: `Keine` (Standard), `Deaktivieren` oder `Löschen`.
- Aktion, wenn eine Klasse in SchulConnex entfernt wird: Legt fest, was mit Klassen geschieht, die in SchulConnex entfernt wurden: `Keine` (Standard) oder `Löschen`.
- Automatische Synchronisation: Zeitplan über Cron-Syntax (Minuten, Stunden, Tage des Monats, Monate, Wochentage). Standardmäßig läuft die Synchronisation zweimal täglich um 5 und 20 Uhr.

Zusätzlich zur automatischen Synchronisation kann in der Detailansicht der Konfiguration jederzeit manuell über das Symbol Synchronisieren in der Kopfzeile ein Sync-Lauf angestoßen werden (erfordert die Berechtigung zum Bearbeiten von Benutzern oder Klassen).

Für Version 26.4.0

Rollenzuordnung

SchulConnex-Gruppenrollen werden beim Import automatisch auf die Systemgruppen `<ORGANISATION> Teacher` bzw. `<ORGANISATION> Student` der Organisation abgebildet:

- Lehrer: Rollen `LEHR`, `KLLEIT`, `FOERD`, `VLEHR`, `GLEIT`
- Schüler: Rollen `LERN`, `GMIT`

Ausgewertet werden nur SchulConnex-Gruppen vom Typ Klasse oder Kurs. Die Rolle `SCHB` wird keiner Gruppe zugeordnet. Zusätzlich werden alle importierten Benutzer einer Gruppe des Anbieters zugeordnet.

Synchronisation prüfen

Nach einem Sync-Lauf lassen sich die Ergebnisse in der Detailansicht der Konfiguration einsehen. Sie zeigt getrennt für Benutzer und Klassen die nächste geplante Synchronisierung, den Zeitpunkt des letzten Abschlusses, ob die Synchronisierung erfolgreich war, die Statusmeldung sowie die Anzahl der synchronisierten, fehlenden und fehlgeschlagenen Objekte. Ein Klick auf die Anzahl unter Synchronisierungsfehler zeigt die einzelnen Fehler.

Eine Klasse/ein Kurs wird nur angelegt, wenn mindestens ein Schüler und ein Lehrer enthalten sind. Übersprungene Klassen werden als Fehler gezählt.

Ist bei einer Person keine E-Mail-Adresse hinterlegt, wird als Login stattdessen die SchulConnex-Personen-ID verwendet. Existiert bereits ein Benutzer mit derselben E-Mail-Adresse oder demselben Benutzernamen, wird der Import für diese Person übersprungen und als Fehler ausgewiesen.

Schlägt die Authentifizierung fehl (z. B. abgelaufenes Secret), wird der gesamte Sync-Lauf der Konfiguration abgebrochen, da die Zugangsdaten für alle zugeordneten Organisationen gemeinsam gelten.

Andere Fehler, etwa eine Zeitüberschreitung, brechen nur die Synchronisation der betroffenen zugeordneten Organisation ab. Für diese Organisation werden die Aktionen für entfernte Benutzer und Klassen nicht ausgeführt, die übrigen Organisationen werden vollständig synchronisiert. Der Sync-Lauf gilt in diesem Fall als fehlgeschlagen.

Für Version 26.4.0

Profilbilder

Relution ermöglicht das Hinterlegen von Bildern für bestehende Benutzer in der Plattform. Diese Funktion bietet insbesondere in der Apple-Welt Vorteile, etwa für die Classroom-App oder die vereinfachte Anmeldung an Shared iPads.

Wenn ein Benutzer ein Profilbild hinterlegt hat, wird es Lehrkräften ermöglicht, Schüler anhand der Bilder in der Apple Classroom-App leichter zu identifizieren. Darüber hinaus erleichtert die Funktion die Anmeldung an Shared iPads: Benutzer können ihre Klasse auswählen und auf das Profilbild klicken, um sich anzumelden.

Es ist wichtig zu beachten, dass die Profilbilder auf den Servern von Relution gespeichert bleiben und nicht mit den Servern von Apple synchronisiert werden.

Voraussetzungen

- Angelegte Benutzer in Relution
- Quadratische Bilder (empfohlen: `256x256` oder `512x512` Pixel)
- Die maximale Größe der Bilder beträgt `300 KB`

Konfiguration

Für Version 26.4.0

- Die Bilder werden nach dem Benutzernamen des jeweiligen Benutzers benannt. Maßgeblich ist der Dateiname ohne Endung; er muss exakt einem Benutzernamen entsprechen.
- Alle Bilder werden in einer `.zip`-Datei zusammengefasst. macOS-Metadateien (`._*`) werden ignoriert.
- Unter Benutzer öffnet das 3-Punkte-Menü die Option Bulk-Upload von Profilbildern. Dafür ist das Recht zum Aktualisieren von Benutzern erforderlich.
- Nach dem Hochladen der `.zip`-Datei zeigt eine Zusammenfassung für jedes Bild, ob es gültig ist und welche Verstöße vorliegen, z. B. kein oder mehrere passende Benutzer gefunden, Bild nicht quadratisch oder zu groß.
- Nur gültige Bilder werden zugeordnet; ein vorhandenes Profilbild wird dabei überschrieben. Ungültige Bilder werden verworfen.

Einzelne Profilbilder (JPEG oder PNG) lassen sich auch in den Benutzerdetails im Feld Profilbild hochladen. Benutzer können ihr eigenes Profilbild im Profil über das Bearbeiten-Symbol am Avatar ändern.

Hinweise

Damit Benutzer von Lehrkräften in der Classroom-App gesteuert werden können, müssen Klassen in Relution definiert werden. Dies ist auch notwendig, wenn Benutzer sich vereinfacht an einem Shared iPad anmelden sollen. Für die Nutzung der Shared iPad-Variante sind zudem verwaltete Apple Accounts (im Portal: Managed Apple ID) erforderlich, um die Anmeldung zu ermöglichen.

Profilbilder werden nur ausgeliefert, wenn unter `Einstellungen` → `Bildung` → `Unterrichtseinstellungen` im Abschnitt Zugriff auf Profilbilder für Apple Education-Konfigurationen der Zugriff auf Aktiviert steht (Standard) und der Benutzer Mitglied einer Klasse der Apple-Education-Konfiguration des Geräts ist, siehe Unterrichtseinstellungen →.

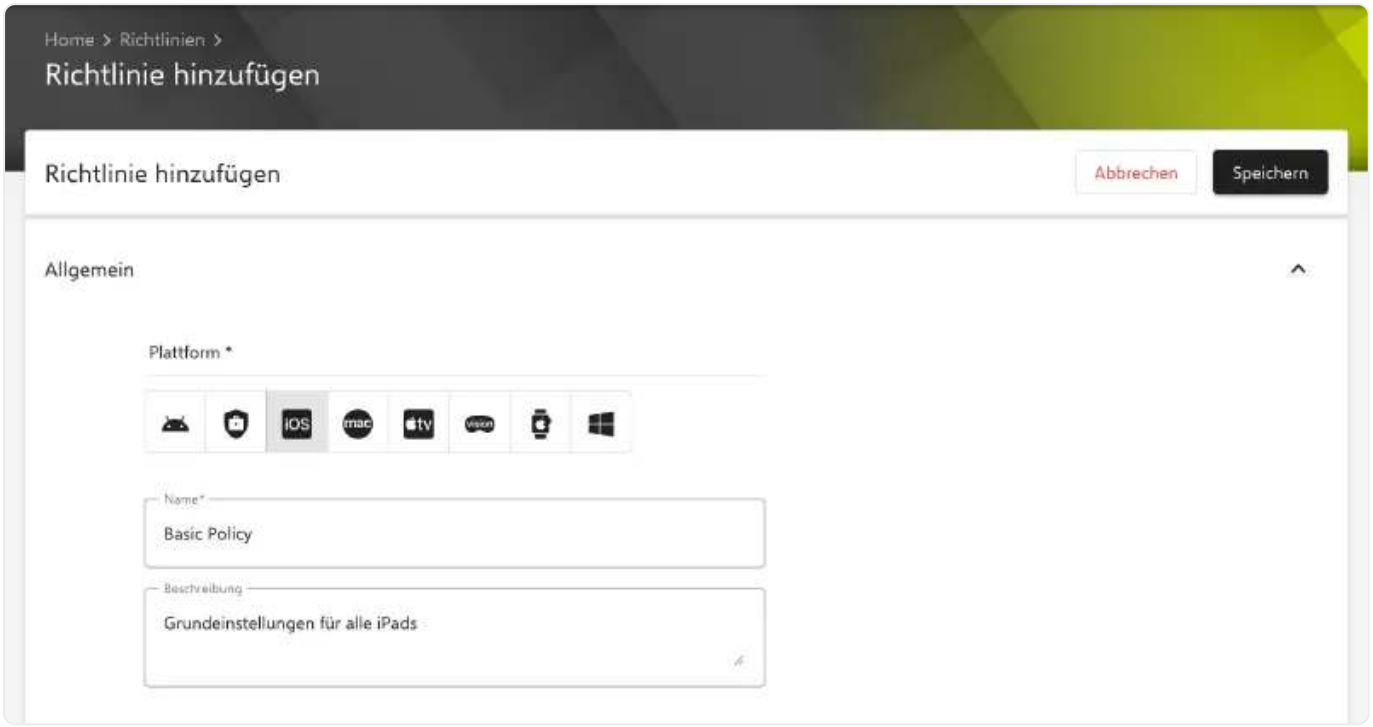
Richtlinien erklärt

Eine Richtlinie ist eine Sammlung einer oder mehrerer Konfigurationen. Jede Richtlinie kann auf einem oder auf mehreren Geräten gleichzeitig angewendet werden. Zudem können mit jedem Gerät eine oder mehrere Richtlinien verknüpft sein.

Erstellen

Richtlinien sind plattformabhängig. Bei der Erstellung muss darauf geachtet werden, für welche Plattform eine Richtlinie erstellt wird. Eine iOS-Richtlinie kann z.B. nicht nachträglich auf eine Android- oder Windows-Richtlinie umgestellt werden. Auch innerhalb der Apple-Betriebssysteme wird nach iOS-, macOS-, tvOS-, visionOS- und watchOS-Richtlinien unterschieden und kann ebenfalls nachträglich nicht umgestellt werden.

Im Seitenmenü unter `Geräte` → `Richtlinien` findet sich die Übersicht der bereits erstellten Richtlinien. Über die Schaltfläche Hinzufügen lässt sich eine neue Richtlinie erstellen. Dabei müssen das Zielsystem und ein Name angegeben werden.

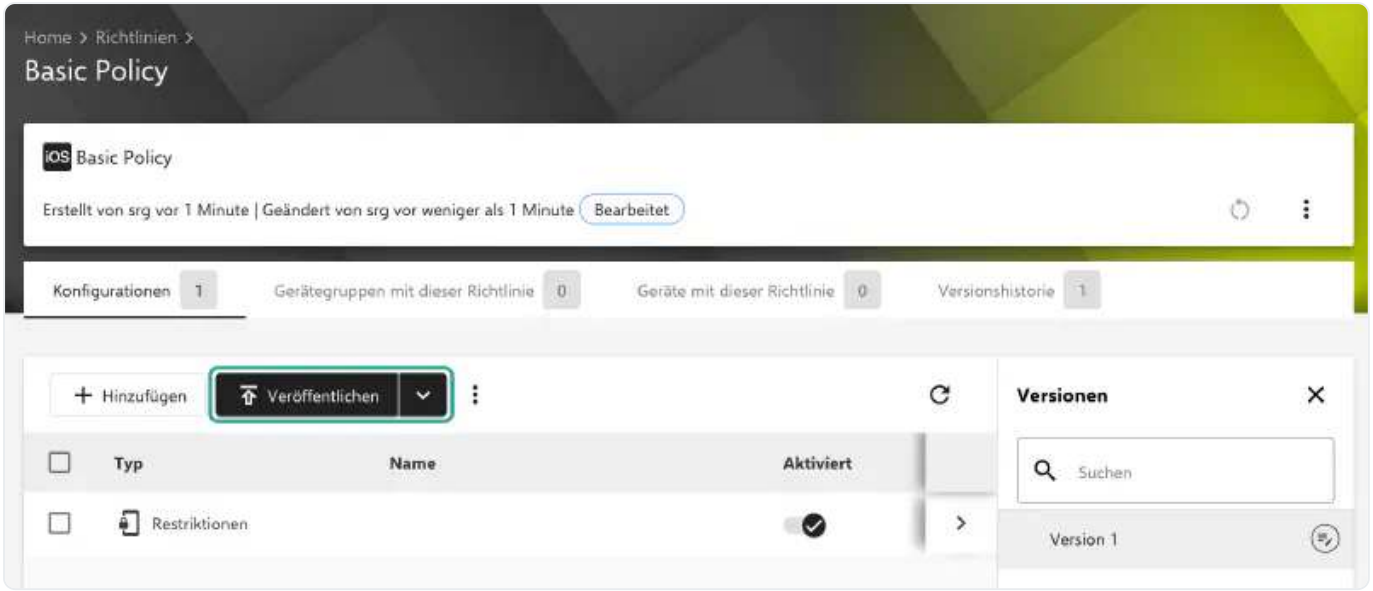


Durch Klick auf Speichern wird die neue Richtlinie angelegt.

Richtlinien-Versionierung

Alle Änderungen an einer Richtlinie werden erst nach einer Veröffentlichung wirksam. Dieser Prozess ermöglicht es, sämtliche Konfigurationen vorzunehmen und auf Vollständigkeit zu prüfen, ohne dass die Änderungen direkt auf verknüpften Geräten aktiv werden.

Sobald alle Änderungen vorgenommen wurden und diese auf den Geräten angewendet werden sollen, wird die Version über die Schaltfläche Veröffentlichen veröffentlicht. Die Schaltfläche befindet sich in der Aktionsleiste der Konfigurationsliste rechts neben Hinzufügen. Veröffentlicht werden kann nur eine Version, die seit ihrer Anlage geändert wurde und mindestens eine aktivierte Konfiguration enthält.



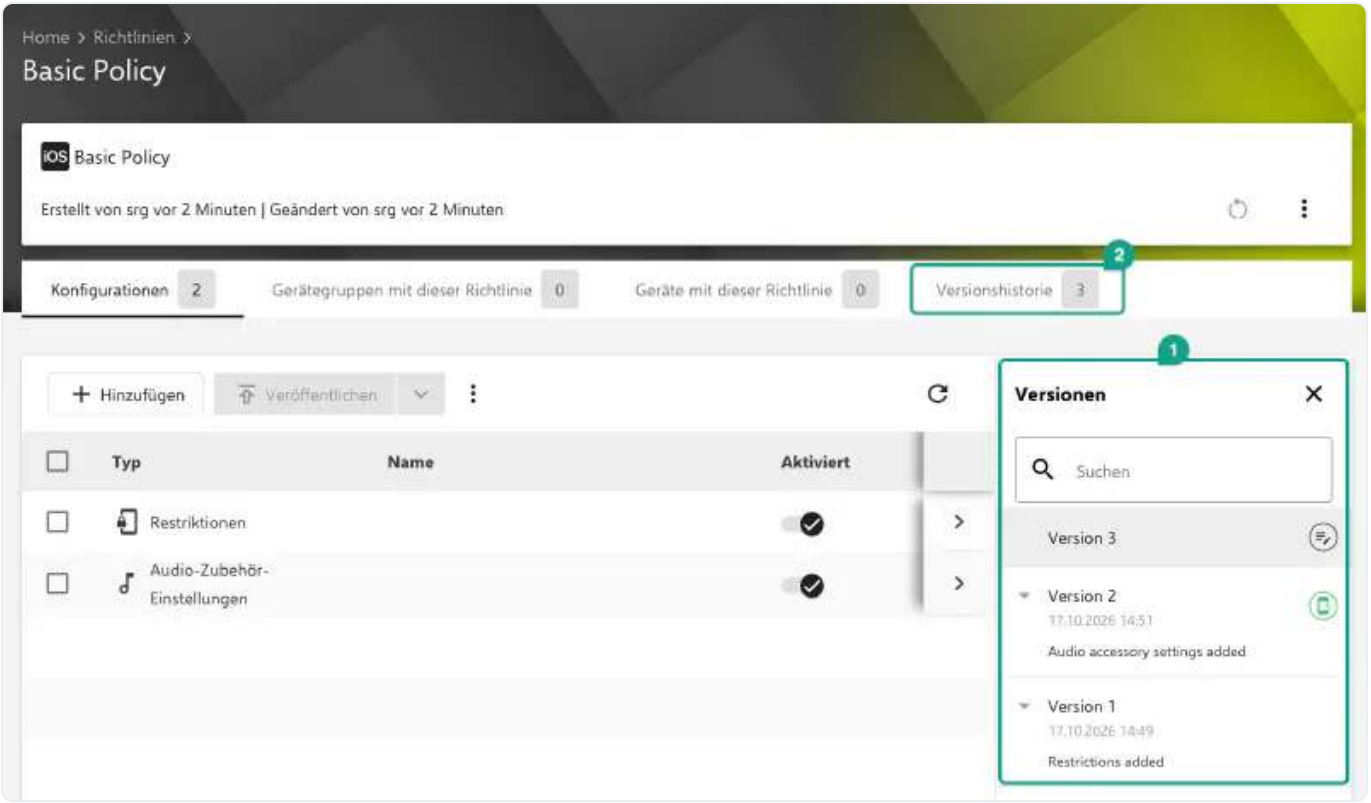
Über das Menü der Schaltfläche Veröffentlichen stehen zwei Varianten zur Verfügung:

- Auf allen Geräten veröffentlichen: Die Version wird auf allen Geräten angewendet, denen die Richtlinie zugewiesen ist.
- Auf Testgeräten veröffentlichen: Die Version wird als Testversion (Status Test) veröffentlicht und nur auf den Geräten der Gerätegruppen angewendet, die die Testversion verwenden. Diese Gerätegruppen werden im anschließenden Dialog ausgewählt, sofern noch keine Gerätegruppe die Testversion verwendet. Alle übrigen Geräte behalten die bisher veröffentlichte Version. Eine Testversion kann später über Veröffentlichen auf allen Geräten übernommen werden.

Für Version 26.4.0

Die Versionen-Sidebar

Die Versionen-Sidebar dient zur schnellen Einsicht in bereits veröffentlichte Richtlinien.



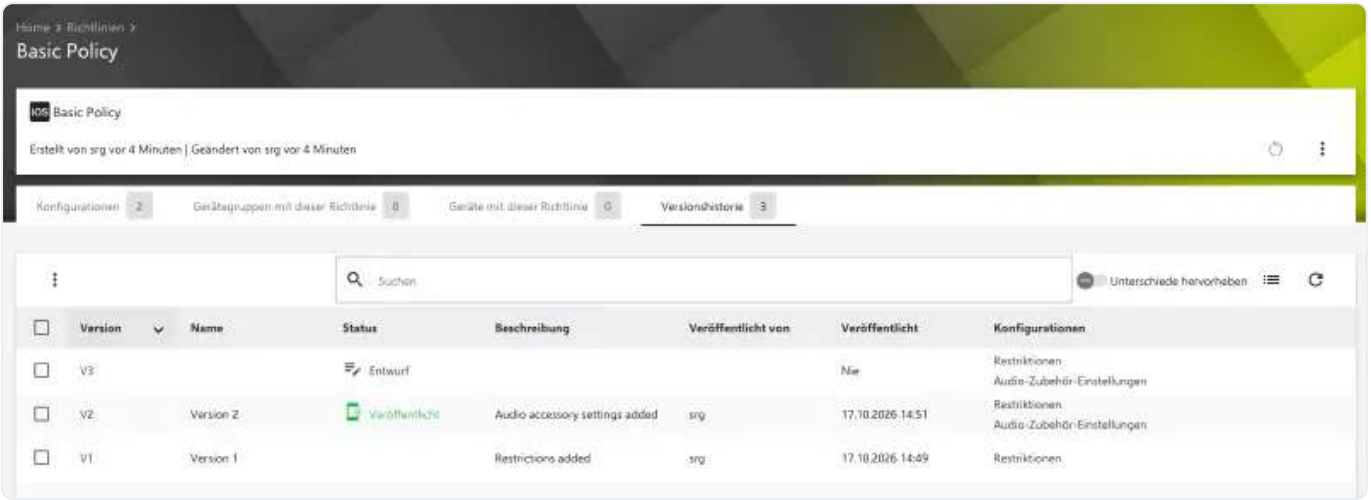
Dabei gelten folgende Hinweise:

- Bleistift-Symbol (Stift): Markiert den aktuellen Entwurf – dies ist die jüngste, aber noch unveröffentlichte Version der Richtlinie.
- Grünes Handy-Symbol: Kennzeichnet die aktuell veröffentlichte und somit auf den Geräten angewendete Richtlinie.
- Blaues Kolben-Symbol: Kennzeichnet eine Testversion, die nur auf den ausgewählten Testgerätegruppen angewendet wird.
- Versionsinformation: Beim Veröffentlichen einer neuen Version können ein Name und ein Hinweis (Beschreibung) angegeben werden. Diese werden direkt in der Sidebar angezeigt, um Änderungen schnell dokumentieren und nachverfolgen zu können.

Für Version 26.4.0

Versionshistorie

Zur detaillierten Nachverfolgung aller Änderungen gibt es zusätzlich den Reiter Versionshistorie.



In dieser Übersicht sind alle Versionen der Richtlinie übersichtlich gelistet, inklusive folgender Details:

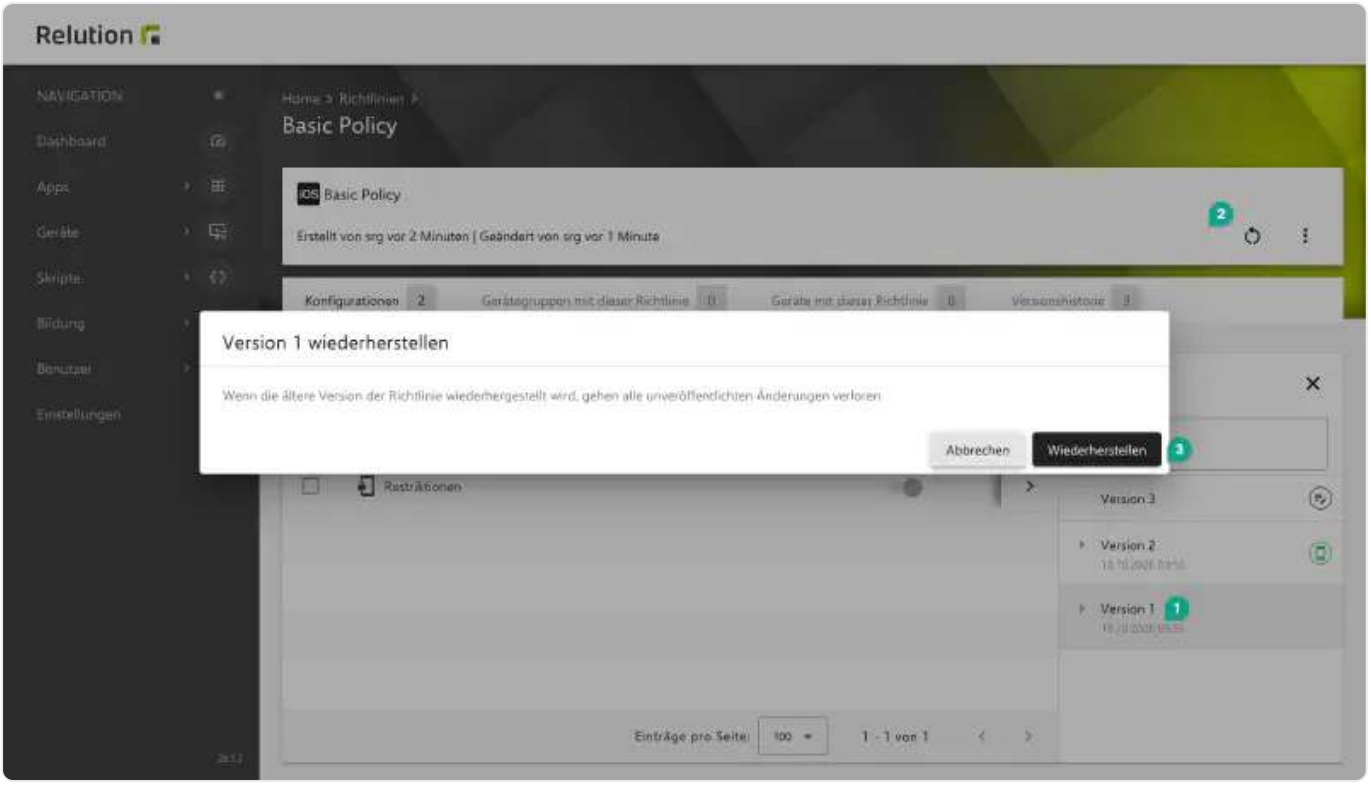
Spalte	Beschreibung
Version	Die eindeutige Kennung der Version (z. B. V4).
Name	Der vergebene Versionsname.
Status	Der Status der Version: Entwurf, Veröffentlicht oder Test. Bei veralteten Versionen bleibt die Spalte leer.
Beschreibung	Der beim Veröffentlichen hinzugefügte Hinweis/Kommentar zu den Änderungen.
Veröffentlicht von	Der Benutzer, der die Version veröffentlicht hat.
Veröffentlicht	Datum und Uhrzeit der Veröffentlichung.
Konfigurationen	Alle Konfigurationen dieser Version. Mit dem Schalter Unterschiede hervorheben werden gegenüber der Vorversion hinzugefügte, geänderte und entfernte Konfigurationen markiert.

Die Spalten Modifiziert von und Bearbeitet am sind standardmäßig ausgeblendet und lassen sich über die Spaltenauswahl einblenden.

Für Version 26.4.0

Richtlinien wiederherstellen

Eine ältere Version einer Richtlinie wird in der Versionen-Sidebar ausgewählt (1) und über die Schaltfläche Wiederherstellen als Entwurfsversion (2) im Kopfbereich der Richtlinie als neuer Entwurf wiederhergestellt. Alternativ steht die Funktion im Reiter Versionshistorie zur Verfügung. Nach der Bestätigung mit Wiederherstellen (3) wird der aktuelle Entwurf durch eine Kopie der ausgewählten Version ersetzt; alle unveröffentlichten Änderungen gehen dabei verloren. Voraussetzung ist, dass die Richtlinie neben dem Entwurf mindestens eine weitere Version besitzt.



Prioritäten

Für Version 26.4.0

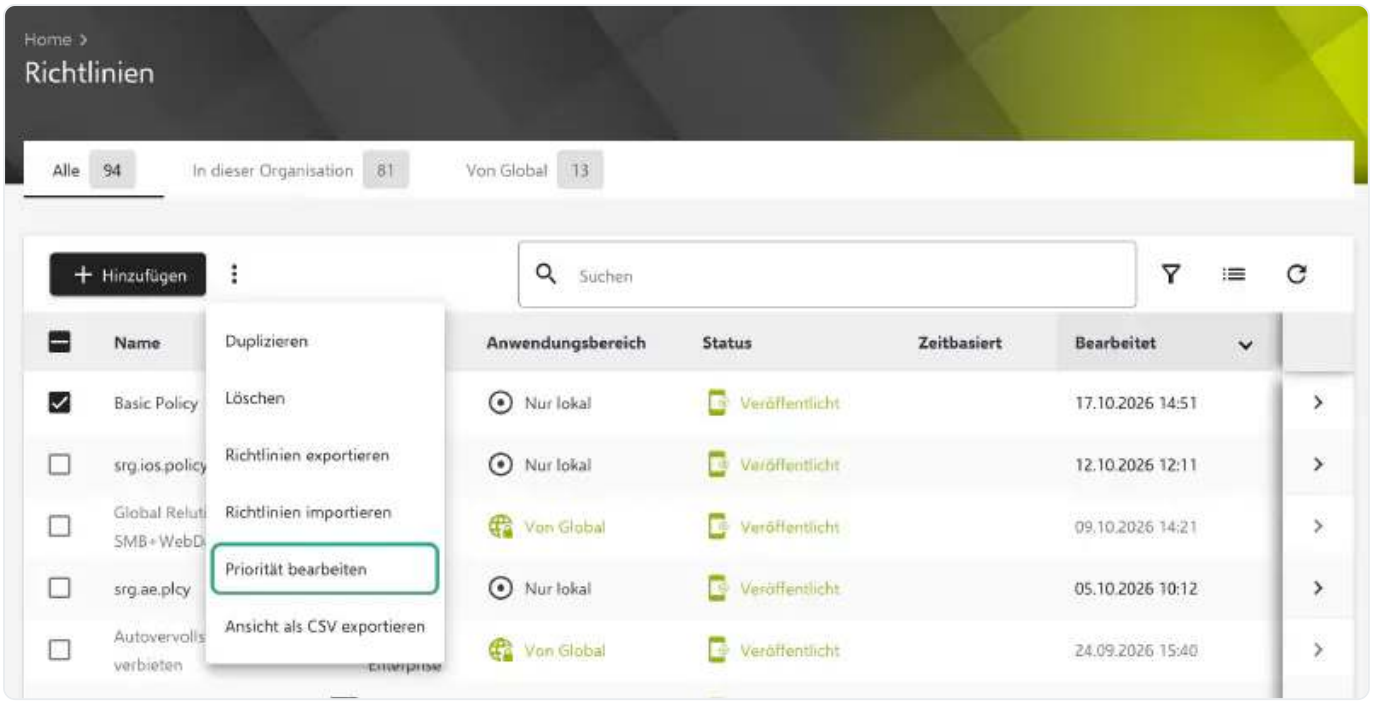
Richtlinien haben Prioritäten. Die niedrige Zahl sticht die höhere. Priorität 2 gewinnt also gegen Priorität 3. Die Prioritätszahl gilt dabei nur innerhalb derselben Ebene: Globale Richtlinien → haben immer Vorrang vor Richtlinien, die eine Meta-Organisation → teilt, und diese wiederum vor den Richtlinien der Organisation selbst. Eine lokale Richtlinie mit Priorität 1 überstimmt eine globale Richtlinie also nicht.

Jede Plattform hat ihre eigene Prioritäten-Liste. Es kann also Richtlinien mit der Priorität 1 mehrfach geben - jeweils für iOS, macOS, tvOS, visionOS, watchOS, `Android Classic/ Legacy`, `Android Enterprise` und Windows.

Kommt ein Konfigurationstyp, der nur einmal pro Richtlinie angelegt werden kann (z. B. die Restriktionen unter `Android Classic/ Legacy`, `Android Enterprise` und Windows), in mehreren Richtlinien unterschiedlicher Priorität vor, wird nur die Konfiguration aus der Richtlinie mit der höchsten Priorität übernommen. Die Konfigurationen der niedriger priorisierten Richtlinien werden nicht ergänzt, sondern vollständig ignoriert. Ist eine Funktion in den Restriktionen einer Richtlinie mit der Priorität 2 erlaubt, in einer mit der Priorität 4 aber verboten, bleibt sie erlaubt.

Einige dieser Konfigurationstypen werden dagegen aus allen Richtlinien zusammen an das Gerät übertragen, z. B. die Restriktionen unter iOS, macOS und tvOS; das Gerät wendet dann jeweils die restriktivere Einstellung an. Konfigurationen, die mehrfach angelegt werden können (z. B. WLAN oder Zertifikate), werden aus allen Richtlinien kombiniert. Kollidieren zwei Einträge (z. B. WLAN-Profile mit gleicher SSID), gilt der aus der Richtlinie mit der höheren Priorität.

Die Prioritäten werden in der Richtlinien-Übersicht über das 3-Punkte-Menü und den Eintrag Priorität bearbeiten geändert.



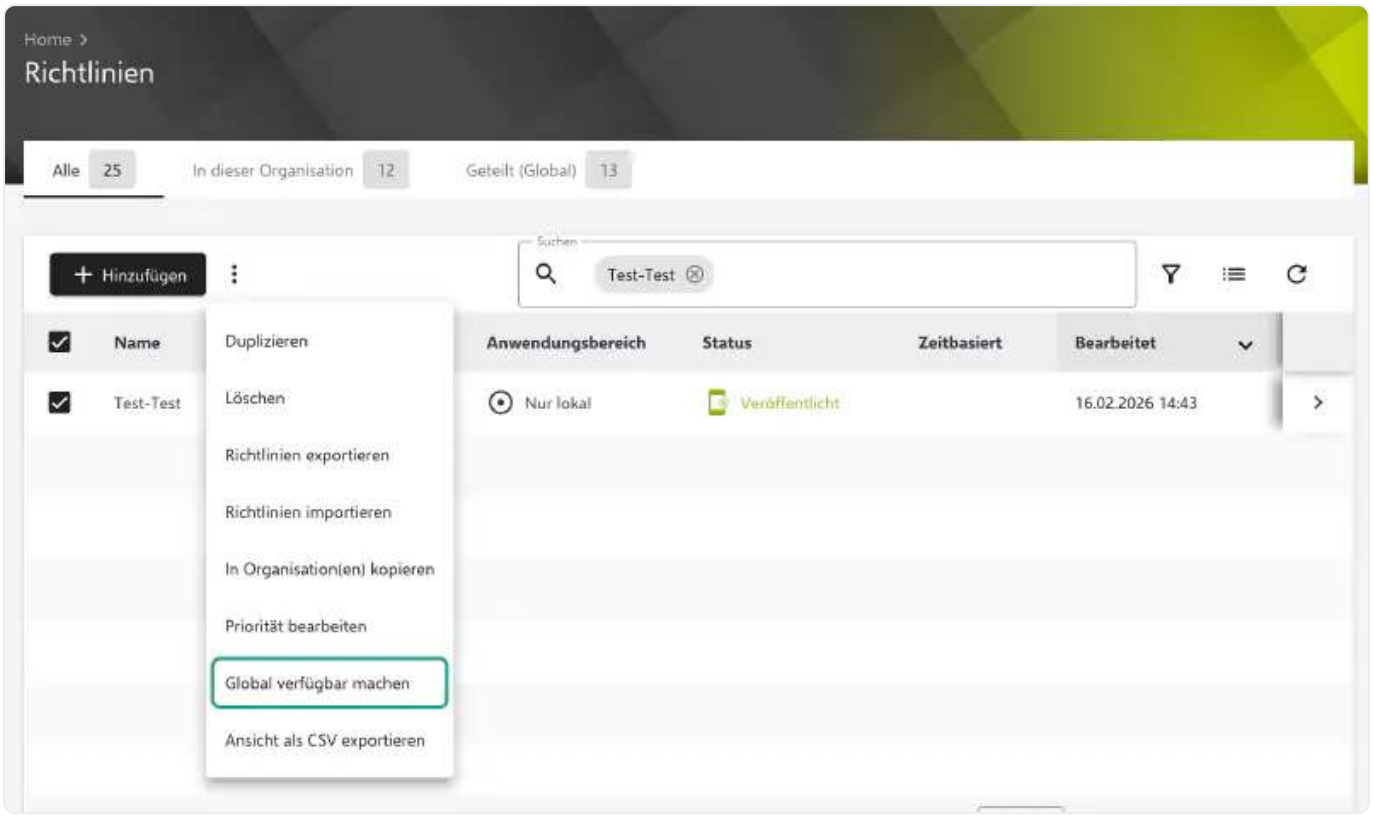
Globale Richtlinien

Für Version 26.4.0

Hin und wieder kann es sinnvoll sein, identische Konfigurationen in mehreren Organisationen von Relution anwenden zu können. Hierzu lassen sich in der Global-Organisation → globale Richtlinien erstellen und freigeben. Diese Richtlinien können in der Global-Organisation ganz normal bearbeitet werden, stehen aber in den anderen Organisationen nur schreibgeschützt zur Verfügung.

Voraussetzung für die Freigabe ist eine veröffentlichte Version der Richtlinie. Anschließend wird die Richtlinie in der Übersicht ausgewählt und über das 3-Punkte-Menü mit Global verfügbar machen freigegeben (in der Detailansicht der Richtlinie: Richtlinie öffentlich verfügbar machen). Diese Freigabe kann nicht rückgängig gemacht werden. In Meta-Organisationen → steht entsprechend Meta-weit verfügbar machen zur Verfügung; die Richtlinie ist dann in allen untergeordneten Organisationen schreibgeschützt verfügbar.

Globale Richtlinien sind für Android Enterprise nicht verfügbar.



In der Übersicht zeigt die Spalte Anwendungsbereich, ob eine Richtlinie freigegeben ist: In der Global-Organisation sind freigegebene Richtlinien mit Geteilt gekennzeichnet, in den übrigen Organisationen mit Von Global (bzw. Von Meta bei Richtlinien einer Meta-Organisation). Nicht freigegebene Richtlinien sind mit Nur lokal gekennzeichnet.

Für Version 26.4.0

Richtlinien deaktivieren

Ab Relution 5.33 ist es möglich, Richtlinien für einzelne Geräte zu deaktivieren. Mussten bisher immer Gerätegruppen geklont und angepasst werden, um ein Gerät kurzzeitig aus der Zuweisung einer Richtlinie zu entfernen, ist dies jetzt einfach über `Navigation` → `Geräte` → `Inventar` → `gewünschtes Gerät` → `Richtlinie` möglich. Dazu muss die entsprechende Richtlinie ausgewählt und kann über das 3-Punkte-Menü de-/aktiviert werden.

Richtlinienstatus

Der Richtlinienstatus wird in der Gerätedetail Seite in der Header Box angezeigt. Folgende Status können hierbei vorkommen:

- `UNKNOWN = Problem`
  - Der Status der Geräterichtlinie ist unbekannt
- `NONE = Keine`
  - Auf dem Gerät ist keine Richtlinie angewendet
- `SENT = Keine`
  - Dem Gerät wurde eine Richtlinie zugewiesen, die jedoch noch nicht angewendet wurde
- `APPLIED = Aktiv`
  - Eine Richtlinie wird auf dem Gerät angewendet
- `UPDATE = Aktiv`
  - Eine neue Version der Richtlinie wurde an das Gerät gesendet, das Gerät hat die Aktualisierung jedoch noch nicht durchgeführt
- `CHANGE = Info`
  - Eine andere Richtlinie wurde an das Gerät gesendet, das Gerät hat die Richtlinie jedoch noch nicht geändert
- `REMOVED = Info`
  - Die Zuweisung der Richtlinie zum Gerät wurde aufgehoben, das Gerät hat die Richtlinie jedoch noch nicht entfernt

Für Version 26.4.0

Gerätegruppen

Mit Relution Version 5.21.0 ist die Funktion der Gerätegruppen verfügbar. Hiermit lassen sich Geräte aufgrund diverser Geräte-Eigenschaften automatisch in Gruppen zuweisen. Über die Gerätegruppen können dann Richtlinien zugewiesen werden, die automatisch ausgeliefert werden.

Zugriff auf Gerätegruppen

Die Gerätegruppen sind unter dem Menüpunkt `Geräte` → `Gerätegruppen` zu finden. Hier steht eine Übersicht der bestehenden Gruppen zur Verfügung, zudem lassen sich neue Gruppen erstellen.

Eine Gerätegruppe ist eine Verknüpfung zwischen Geräten und Richtlinien. Diese Verknüpfung lässt sich entweder manuell oder aufgrund von bestimmten Geräteeigenschaften automatisch erstellen.

Richtlinien werden ausschließlich über Gerätegruppen mit Geräten verknüpft; eine direkte Verknüpfung ist nicht mehr möglich. Über Gerätegruppen lassen sich außerdem Aktionen ereignis- oder zeitgesteuert auslösen: Aktionen mit Gerätegruppen →

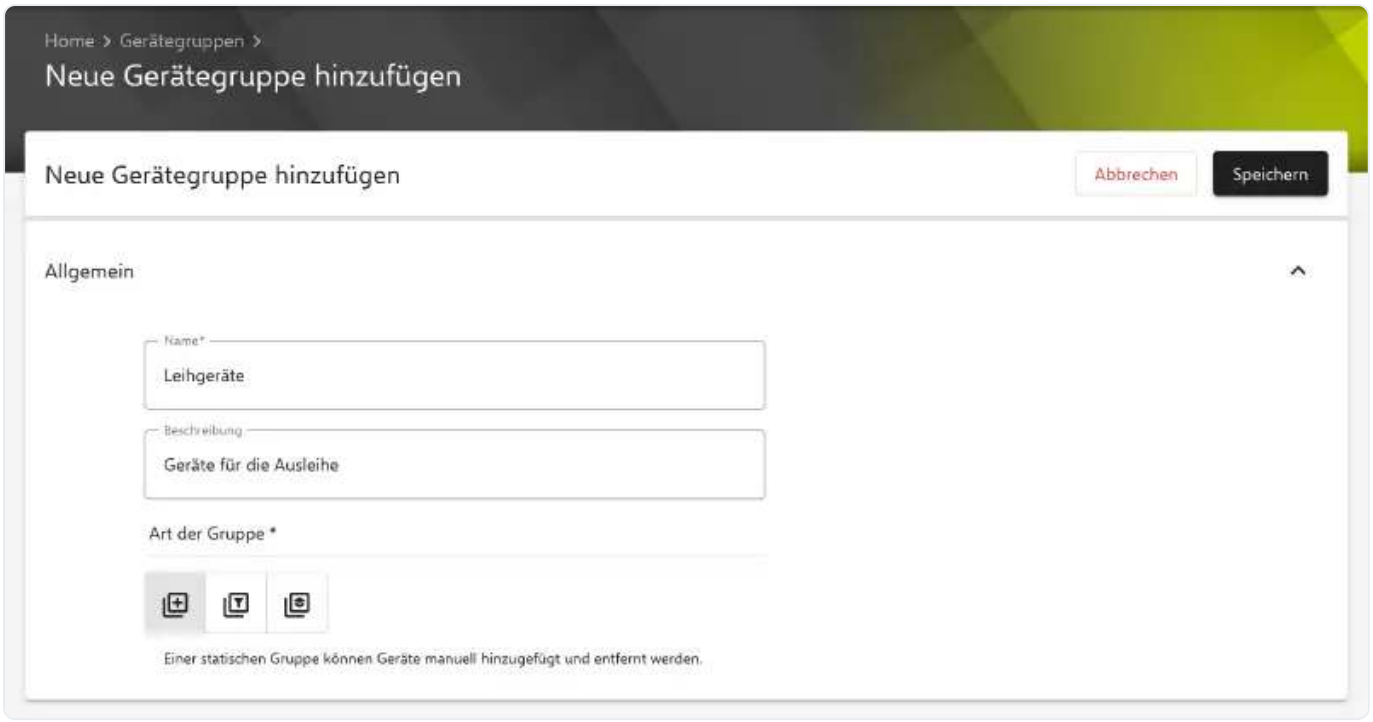
Erstellung neuer Gerätegruppen

Eine neue Gerätegruppe wird über Hinzufügen erstellt. Dabei werden ein Name und (optional) eine Beschreibung für die Gruppe vergeben. Zudem besteht die Wahl der Art der Gruppe. Hier stehen die Optionen Statisch und Dynamisch zur Verfügung, bei einer Education- oder Free-Lizenz zusätzlich Bildung. Voreingestellt ist Dynamisch.

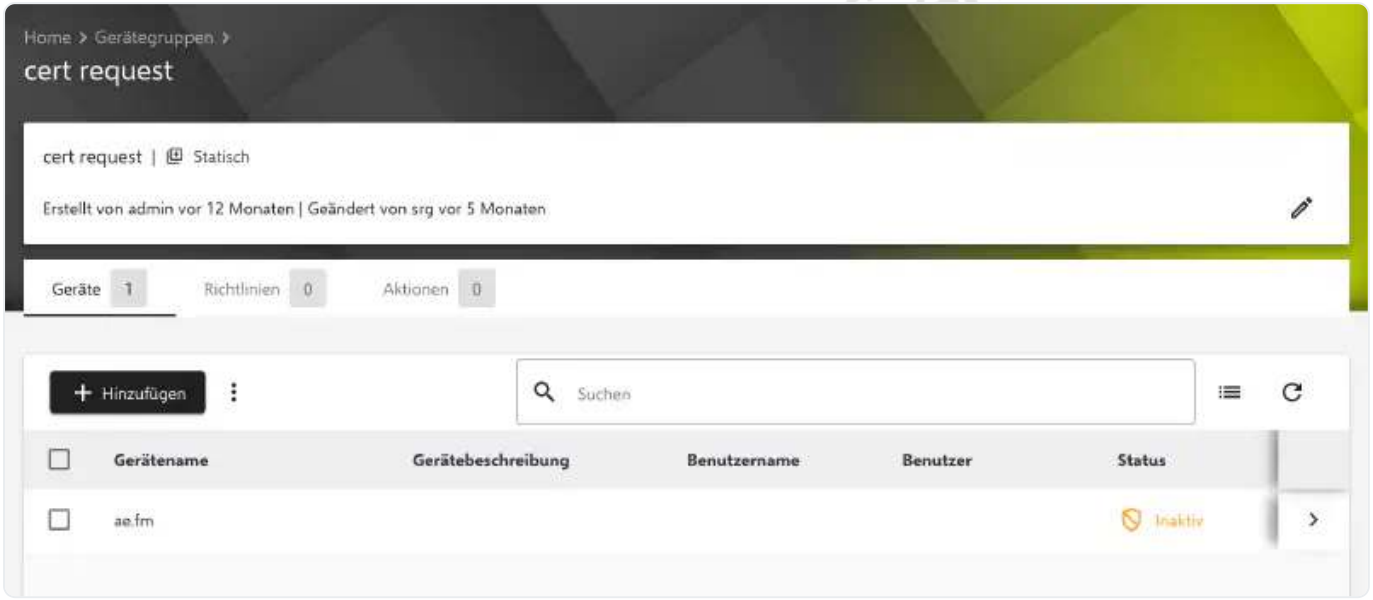
Für Version 26.4.0

Statische Gruppen

Statische Gruppen lassen eine manuelle Verknüpfung zwischen Geräten und Richtlinien zu.

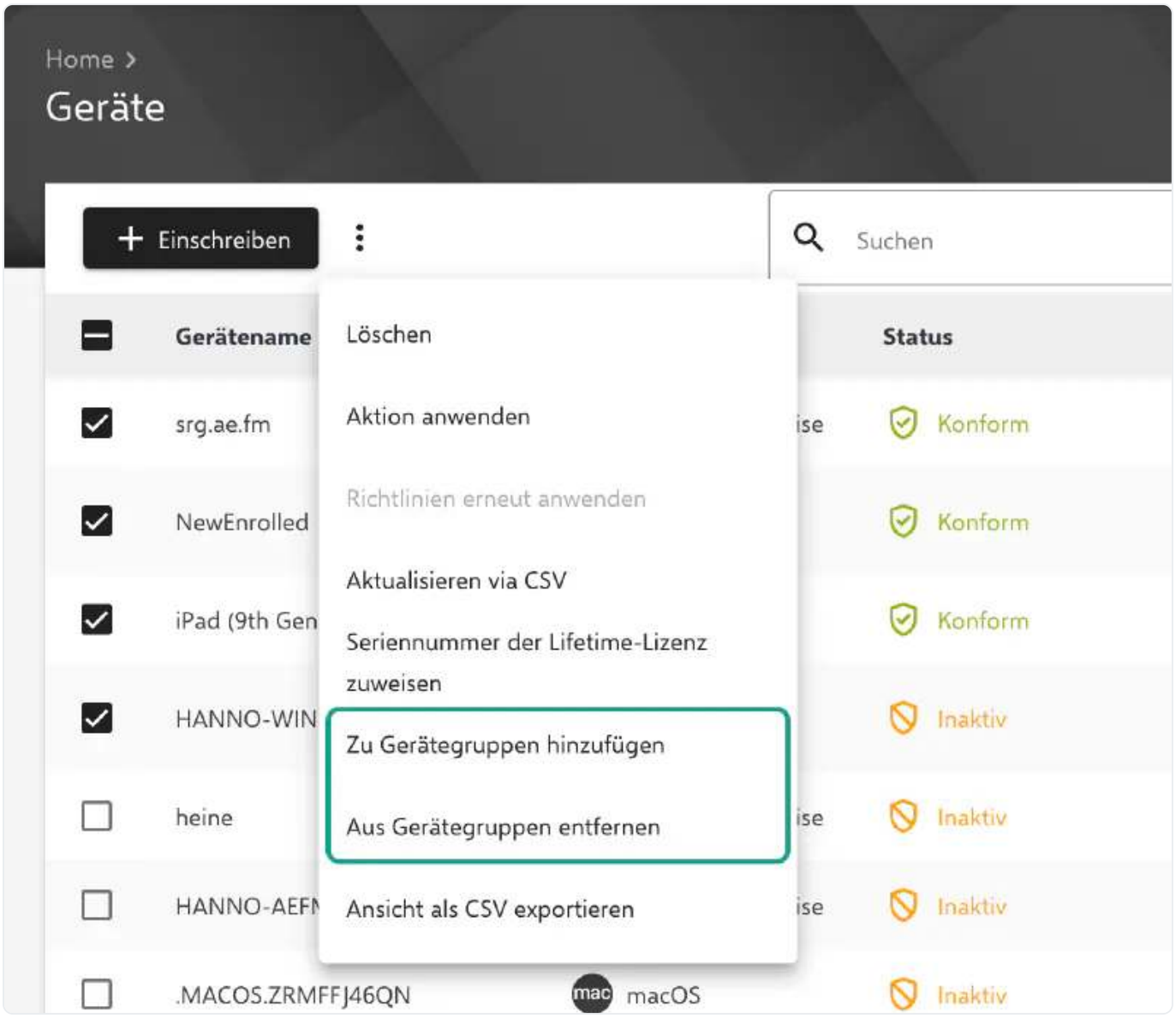


Nachdem die Gruppe erzeugt wurde, lassen sich Geräte und Richtlinien hinzufügen. Es lassen sich nur Richtlinien verknüpfen, die zuvor veröffentlicht wurden.



Massenhinzufügen von Geräten

Mit Relution 26.1.0 ist es möglich, mehrere ausgewählte Geräte im Inventar oder in den Auto-Einschreibungen einer bestehenden statischen Gruppe direkt hinzuzufügen oder sie daraus zu entfernen und damit auch den verbundenen Richtlinien zuzuordnen bzw. zu entziehen. Dafür stehen im 3-Punkte-Menü die Einträge Zu Gerätegruppen hinzufügen und Aus Gerätegruppen entfernen zur Verfügung.

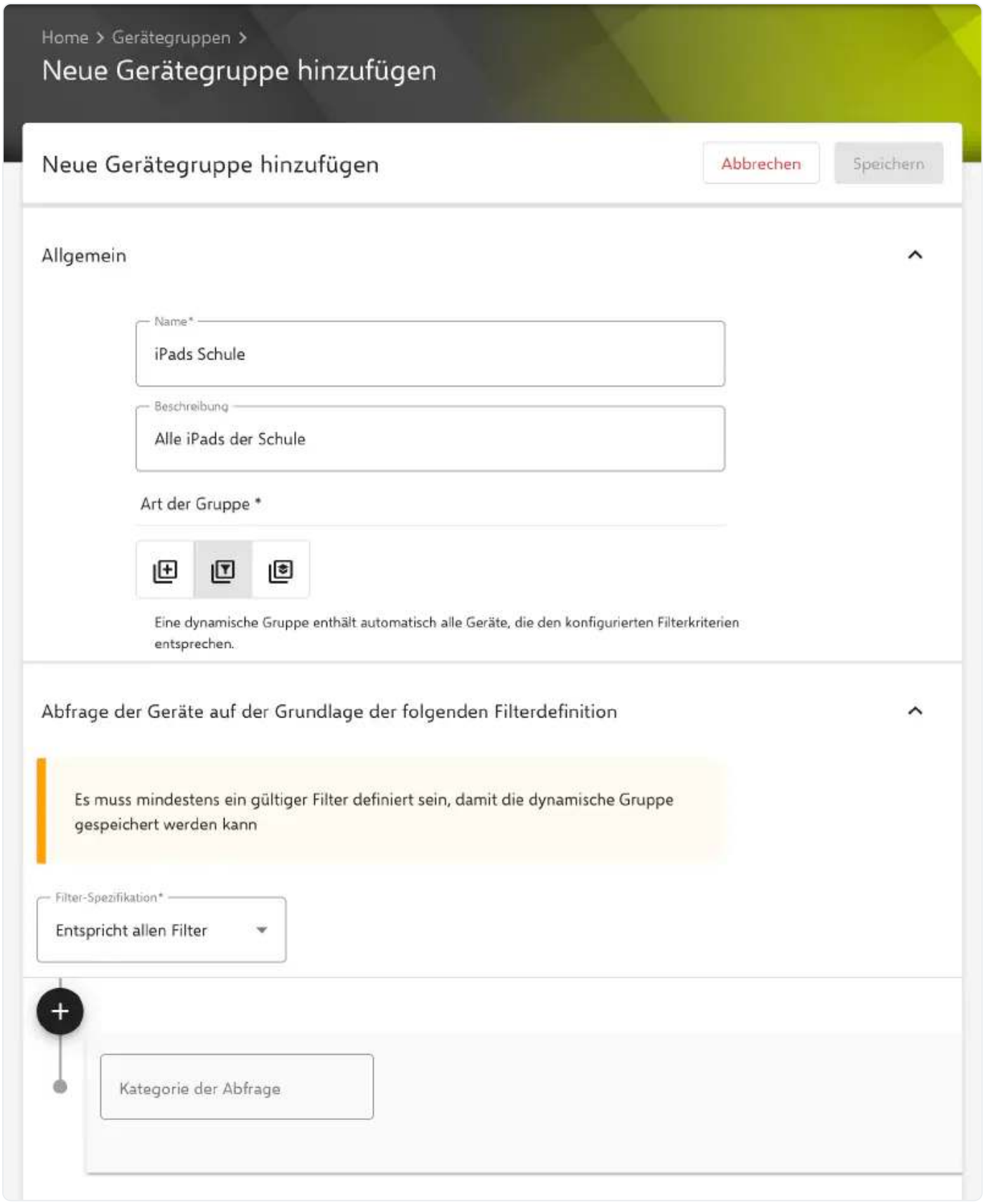


Bereits bei der Einschreibung lassen sich Geräte statischen Gruppen zuordnen: In Einschreibungen und Auto-Einschreibungen steht dafür das Feld Statische Gerätegruppen zur Verfügung.

Dynamische Gruppen

In dynamischen Gruppen müssen Filter definiert werden, anhand derer die Geräte automatisch der Gruppe zugewiesen werden. Dies passiert automatisch im Hintergrund. Bei Filtern auf Benutzergruppen oder Klassen (Kurse) kann es bis zu einer Stunde dauern, bis Änderungen in der Gruppe wirksam werden; zeitnah ausgewertet werden diese Filter nur bei Relution Shared Device-Anmeldungen und -Abmeldungen. Es besteht kein direkter manueller Einfluss auf den Inhalt dieser Gruppen.

Im Abschnitt Gerätevorschau zeigt das Formular nach Klick auf Aktualisieren, wie viele und welche Geräte die Gruppe mit den aktuellen Filtern enthält. Ändert sich beim Speichern einer bestehenden dynamischen Gruppe die Anzahl der Geräte, fragt Relution vor dem Speichern eine Bestätigung ab.



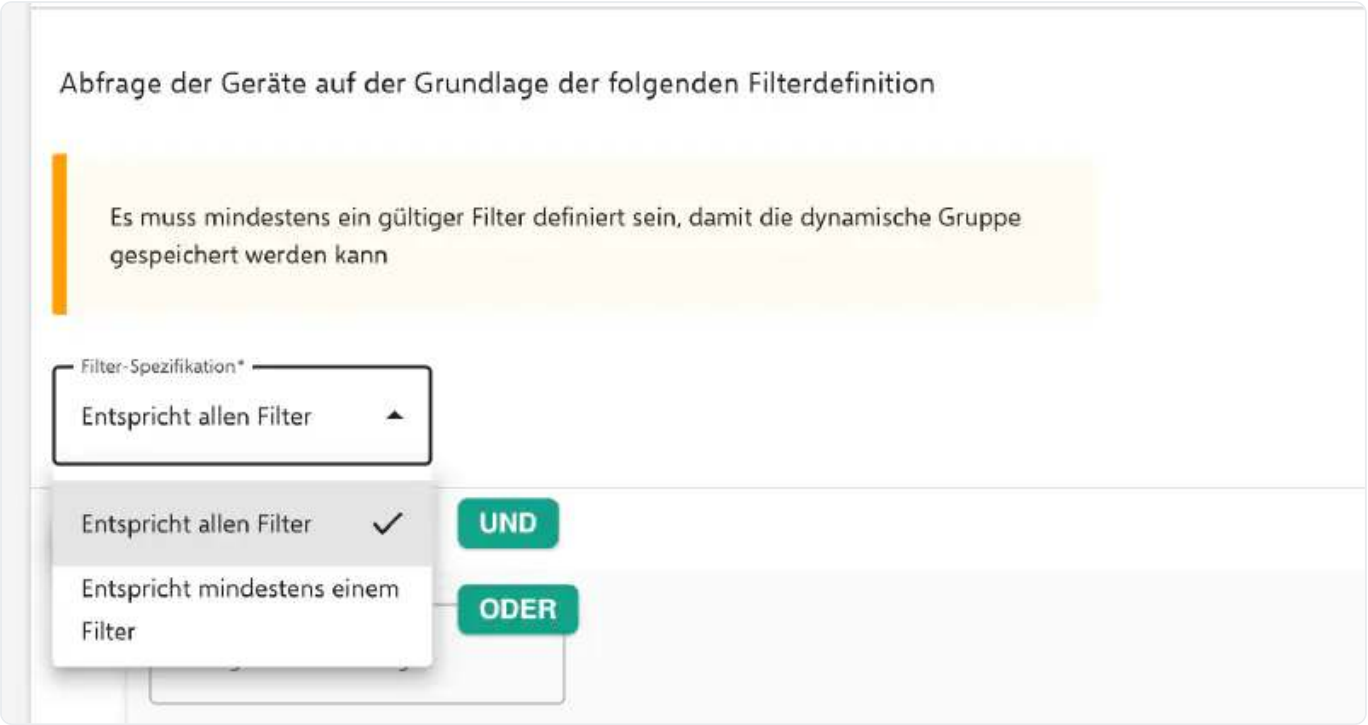
Bei diesem Werkzeug handelt es sich um ein komplexes Tool, dessen Bedienung Konzentration voraussetzt. Unachtsames Handeln kann schnell zu ungewünschten Ergebnissen führen. Bei infrastrukturellen Richtlinien ist bei der Verwendung dynamischer Gruppen besondere Vorsicht geboten. Dabei ist darauf zu achten, dass zum Beispiel keine WLAN-Richtlinie entzogen wird, wenn sich der Gerätestatus ändert.

Achtung: Verliert ein Gerät seine Mitgliedschaft in einer dynamischen Gerätegruppe, werden die über diese Gruppe zugewiesenen Richtlinien entzogen. Ist in einer betroffenen App-Konformität Nicht länger erforderliche Apps automatisch deinstallieren aktiviert, werden die Apps samt ihrer lokalen Daten entfernt. Die Gruppenmitgliedschaft stellt sich automatisch wieder her, sobald die Filterbedingung wieder zutrifft, die App-Daten nicht.

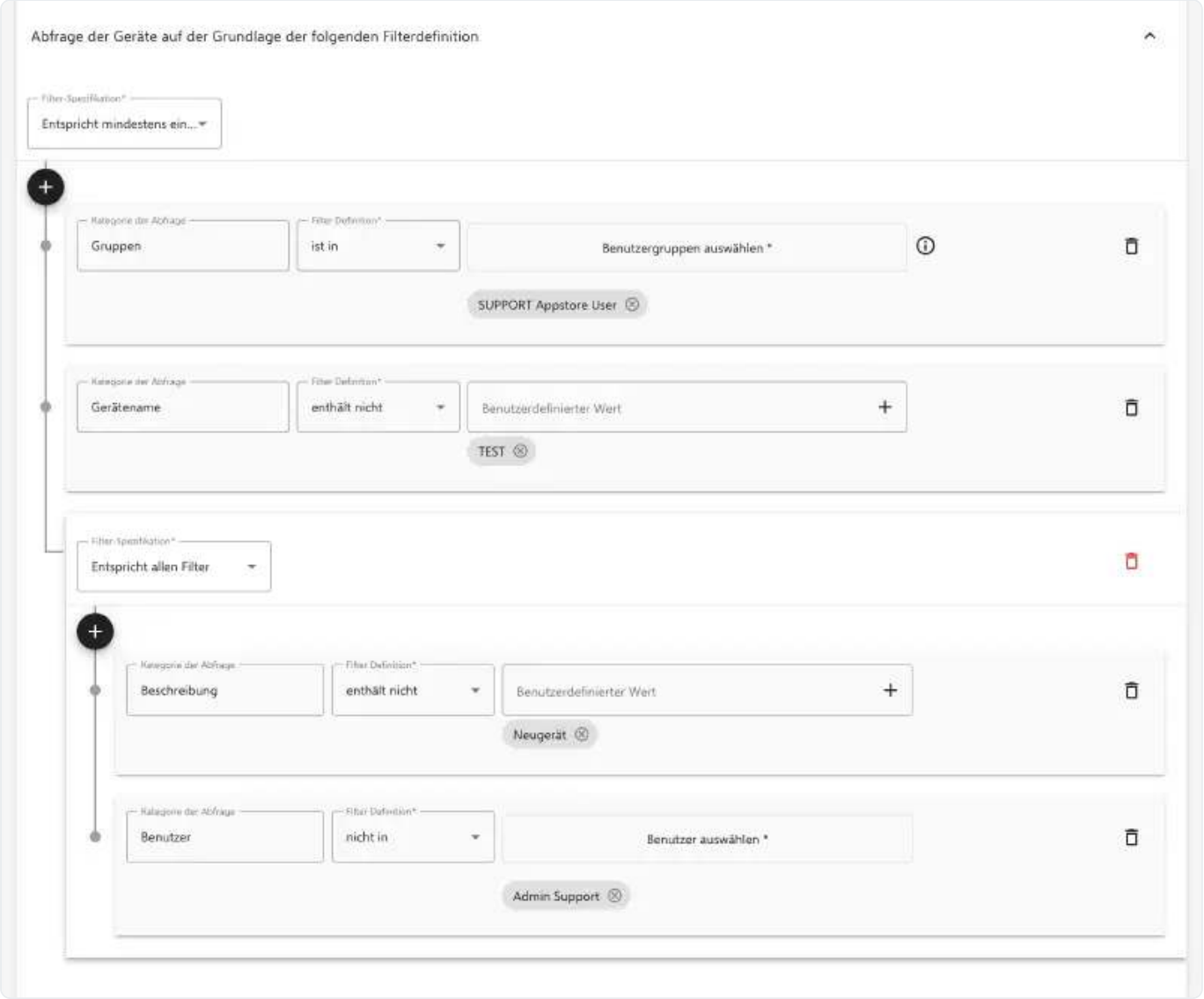
Nahezu alle filterbaren Eigenschaften können sich ohne Zutun eines Administrators ändern: Sie werden vom Gerät gemeldet oder aus Apple, Google, Microsoft oder dem Identitätsanbieter übernommen. Auch die benutzerdefinierten Felder 1–5 sowie Gerätename und Beschreibung werden bei einer erneuten Einschreibung zurückgesetzt.

Für Richtlinien mit automatischer Deinstallation empfiehlt es sich daher, statische Gerätegruppen zu verwenden oder die automatische Deinstallation für Apps mit Nutzerdaten zu deaktivieren.

Im Feld Filter-Spezifikation stehen die Optionen Entspricht allen Filter (UND) und Entspricht mindestens einem Filter (ODER) zur Verfügung. Über das Plus-Symbol werden mit Filter hinzufügen weitere Filter und mit Gruppe hinzufügen verschachtelte Filtergruppen angelegt. Jede Filtergruppe hat eine eigene Filter-Spezifikation; so lassen sich Bedingungen klammern wie im folgenden Beispiel.



Im Beispiel ist ein Filter aus mehreren Eigenschaften und Filter-Spezifikationen definiert worden.



Der Filter integriert folgende Geräte:

- Der verknüpfte Benutzer muss Mitglied der Gruppe `SUPPORT Appstore User` sein.

ODER

- Der Gerätename enthält nicht `TEST`.

ODER

- Die Beschreibung enthält nicht `Neugerät`.

UND

- Der Benutzer ist nicht `Admin Support`.

Alternativ lässt sich der Filter so beschreiben:

```
Gruppen = "SUPPORT Appstore User" ODER Gerätename ENTHÄLT NICHT "TEST"
ODER (Beschreibung ENTHÄLT NICHT "Neugerät" UND Benutzer NICHT "Admin Support")
```

Die Filter-Spezifikationen verhalten sich wie gewöhnliche logische Funktionen.

Um Unfälle zu vermeiden, lässt sich zum Beispiel auch als fester Filterwert die Seriennummer eines einzelnen Geräts hinzufügen, um die Richtlinie wirklich nur auf diesem Gerät anzuwenden und zu prüfen, ob das Ergebnis den Erwartungen entspricht.

Dynamische Gerätegruppen mit Gruppenfilter

Ab Version 5.33 unterstützt Relution die Verwendung von Gerätegruppen als Filter innerhalb dynamischer Gerätegruppen. Damit lassen sich bestehende statische oder dynamische Gruppen als Bedingung in neuen Gruppen einsetzen – sowohl zur Aufnahme als auch zum gezielten Ausschluss von Geräten. Für diesen Filtertyp wird unter Kategorie der Abfrage der Eintrag Geräte Gruppe gewählt und mindestens eine bestehende Gerätegruppe als Bedingung hinzugefügt. Als Filter Definition stehen ist in, nicht in und alle (Gerät ist Mitglied aller ausgewählten Gruppen) zur Verfügung. Die Gruppe, die gerade bearbeitet wird, ist in der Auswahl nicht enthalten.

Vorteile des Gruppenfilters

- Präzisere Zielgruppenbildung, z. B. `alle iPads außer Testgeräte`
- Weniger Pflegeaufwand, da Richtlinien nicht mehr manuell nachgebaut werden müssen
- Klarere Steuerung von Richtlinien, Profilen und Aktionen

Für Version 26.4.0

Durch den neuen Filtertyp lassen sich innerhalb einer dynamischen Gruppe eine oder mehrere andere Gerätegruppen einbeziehen oder explizit ausschließen. Beispielsweise lässt sich eine Testgruppe einfach aus einer dynamischen Produktivgruppe herausfiltern, ohne zusätzliche Kriterien konfigurieren zu müssen.

Die Arbeit mit dynamischen Gerätegruppen erfordert saubere Planung:

- Keine gegenseitigen Abhängigkeiten zwischen Gruppen bilden
- Kritische Grundkonfigurationen z. B. WLAN-Profile nicht versehentlich entfernen
- Richtlinienänderungen immer zuerst mit Pilotgeräten testen

Fehlkonfigurationen können sonst zu unerwünschtem Geräteverlust aus Gruppen oder sogar Endlosschleifen führen.

Bildungsgruppen

Neu in 26.5

Der Gruppentyp Bildung wendet die verknüpften Richtlinien für die Dauer einer Unterrichtsstunde automatisch auf die Geräte der teilnehmenden Schüler an. Die Mitgliedschaft ergibt sich aus den laufenden Unterrichten in Relution Teacher; eine manuelle Zuweisung von Geräten ist nicht möglich. Details unter Bildungsgruppen →.

Gerätegruppen duplizieren

Ab Relution 5.33 können Gerätegruppen dupliziert werden, um eine schnellere und bequemere Verwaltung zu ermöglichen. Dazu können eine oder mehrere gewünschte Gerätegruppen unter `Geräte` → `Gerätegruppen` ausgewählt und über das 3-Punkte-Menü dupliziert werden. Es folgt eine Abfrage, was aus der ursprünglichen Gerätegruppe dupliziert werden soll. Es gibt folgende Möglichkeiten:

- Inklusive Gerätegruppenaktionen (nur mit der Berechtigung zum Anlegen von Gerätegruppenaktionen)
- Einschließlich Geräte (nur bei statischen Gruppen)
- Einschließlich Filter, wenn deaktiviert, wird eine statische Gruppe erstellt (nur bei dynamischen Gruppen; ist die Option deaktiviert, entsteht eine statische Gruppe ohne Geräte)
- Einschließlich Richtlinien

Wird nur eine Gruppe dupliziert, fragt der Dialog zusätzlich den Name des Gerätegruppenduplikats ab. Bei mehreren Gruppen erhalten die Duplikate automatisch den Namen `<Originalname> - Duplikat`.

Gerätegruppen löschen

Nicht mehr benötigte Gerätegruppen können unter `Geräte` → `Gerätegruppen` ausgewählt und über das 3-Punkte-Menü gelöscht werden. Durch das Löschen einer Gruppe bleiben die Geräte eingeschrieben. Richtlinien, die den Geräten nur über diese Gruppe zugewiesen waren, werden jedoch entzogen. Ist in einer betroffenen App-Konformität Nicht länger erforderliche Apps automatisch deinstallieren aktiviert, werden die Apps samt ihrer lokalen Daten entfernt.

Für Version 26.4.0

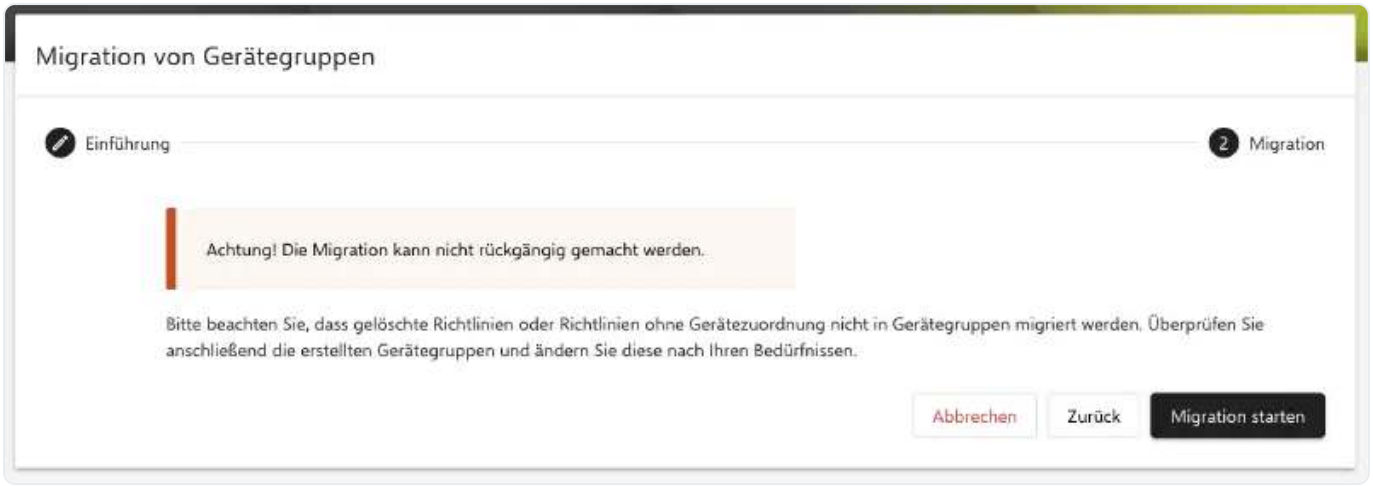
Aktivierung der Gerätegruppen

Veraltet ab Relution 26.0.0 — seither sind Gerätegruppen standardmäßig aktiv.

In älteren Versionen muss die Funktion der Gerätegruppen manuell aktiviert werden. Dies kann über `Einstellungen` → `Geräteverwaltung` → `Migration von Gerätegruppen` passieren. Die damit einhergehende Richtlinienzuweisung auf Gerätegruppen kann nicht rückgängig gemacht werden.

Nach dem Klick auf Migration starten wird ein Hinweistext über die anstehenden Änderungen eingeblendet. Dieser sollte aufmerksam gelesen werden, bevor die Migration mit Weiter fortgesetzt wird.

Im nachfolgenden Dialog lässt sich die Migration final durchführen.



Für Version 26.4.0

Benutzerbezogene Richtlinien

In Relution werden Richtlinien standardmäßig Gerätegruppen zugewiesen. Mit dynamischen Gerätegruppen und benutzerbasierter Filterung lassen sich Richtlinien jedoch auch gezielt an einen einzelnen Benutzer oder eine gesamte Benutzergruppe binden.

Das Prinzip funktioniert wie folgt:

1. Eine dynamische Gerätegruppe wird mit einem Benutzer-Filter konfiguriert.
2. Sobald dem Gerät der entsprechende Benutzer (oder ein Mitglied der Benutzergruppe) als Gerätebenutzer zugewiesen ist, wird das Gerät automatisch in diese Gerätegruppe aufgenommen. Die Zuweisung erfolgt in der Regel bei der Einschreibung oder manuell in den Gerätedetails.
3. Die der Gerätegruppe zugewiesenen Richtlinien werden aktiv und auf das Gerät angewendet.
4. Wird die Zuweisung entfernt oder ein anderer Benutzer zugewiesen, verlässt das Gerät die Gruppe wieder – die Richtlinien werden deaktiviert.

> Eine Anmeldung am Gerät ändert den Gerätebenutzer nur in diesen Fällen: auf Relution Shared Devices (Anmelden und Abmelden) sowie auf Windows-Geräten mit aktiviertem Gerätebenutzerwechsel im Windows Companion. Bei Windows weist die Anmeldung den Benutzer zu; er bleibt bis zur nächsten Anmeldung zugewiesen.

Details dazu stehen in den Artikeln Relution Shared Device → und Benutzerwechsel beim Anmelden →.

Voraussetzungen

Für Version 26.4.0

- Benutzer sind in Relution angelegt und ggf. einer Benutzergruppe zugeordnet
- Geräte sind eingeschrieben und einem Benutzer zuweisbar
- Berechtigungen in der jeweiligen Organisation zum Anlegen von Gerätegruppen, zum Lesen von Benutzern bzw. Gruppen (ohne diese Berechtigung ist die Auswahl im Filter deaktiviert) und zum Zuweisen von Richtlinien

Anwendungsfälle

Szenario	Kategorie der Abfrage	Beschreibung
Einzelner Benutzer erhält spezielle Richtlinie	Benutzer	z. B. Entwickler benötigt gelockerte Restriktionen, privates Exchange-Profil
Abteilung erhält einheitliche Konfiguration	Gruppen	z. B. alle Lehrkräfte erhalten gemeinsam genutztes Exchange-Profil
BYOD-Szenario	Gruppen	Arbeitsprofil-Richtlinien nur für registrierte BYOD-Nutzer

Für einen einzelnen Benutzer

1. Zu `Geräte` → `Gerätegruppen` navigieren.
2. Auf Hinzufügen klicken.
3. Einen aussagekräftigen Namen vergeben, z. B. `DYN – Max Mustermann`.
4. Unter Art der Gruppe die Option Dynamisch wählen (Voreinstellung). Die Optionen werden als Symbole angezeigt; die Bezeichnung erscheint beim Darüberfahren mit der Maus.
5. Im Abschnitt Abfrage der Geräte auf der Grundlage der folgenden Filterdefinition in der vorhandenen Filterzeile folgende Werte wählen:
   - Kategorie der Abfrage: `Benutzer`
   - Filter Definition: `ist in`
   - Über Benutzer auswählen den gewünschten Benutzer im Auswahldialog markieren (Mehrfachauswahl möglich).
6. Die Gerätegruppe speichern.

Für Version 26.4.0

Home > Gerätegruppen >

Neue Gerätegruppe hinzufügen

Neue Gerätegruppe hinzufügen

Abbrechen | Speichern

Allgemein

Name*

DYN – Max Mustermann

Beschreibung

Postfach von Max Mustermann

Art der Gruppe *

Abfrage der Geräte auf der Grundlage der folgenden Filterdefinition

Filter Spezifikation*

Entspricht allen Filter

Kategorie der Abfrage

Benutzer

Filter Definition*

ist in

Benutzer auswählen *

Max Mustermann

Gerätevorschau

Nach der Änderung enthält die Gerätegruppe 1 Geräte.

Aktualisieren

Suchen

Gerätename	Gerätebeschreibung	Benutzername	Benutzer	Status	Aktion
MacBook Pro 13"		MaxMustermann	Max Mustermann	Konform	

Einträge pro Seite: 100

1 - 1 von 1

Sind dem Benutzer mehrere Geräte zugewiesen, werden alle diese Geräte in die Gruppe aufgenommen.

Für eine Benutzergruppe

1. Zu `Geräte` → `Gerätegruppen` navigieren.
2. Auf Hinzufügen klicken.
3. Einen aussagekräftigen Namen vergeben, z. B. `DYN – Lehrkräfte`.
4. Unter Art der Gruppe die Option Dynamisch wählen (Voreinstellung).
5. Im Abschnitt Abfrage der Geräte auf der Grundlage der folgenden Filterdefinition in der vorhandenen Filterzeile folgende Werte wählen:
   - Kategorie der Abfrage: `Gruppen`
   - Filter Definition: `ist in`
   - Über Benutzergruppen auswählen die gewünschte Benutzergruppe wählen (Mehrfachauswahl möglich).
6. Die Gerätegruppe speichern.

Der Filter berücksichtigt auch die Mitglieder verschachtelter Untergruppen der ausgewählten Benutzergruppe.

Benutzergruppen können über LDAP/AD synchronisiert werden. Änderungen an der Gruppenmitgliedschaft werden automatisch in Relution übernommen. Bis dynamische Gerätegruppen mit Filter auf Benutzergruppen neu ausgewertet werden, kann es standardmäßig bis zu einer Stunde dauern (zusätzlich zum LDAP-Synchronisationsintervall). Zeitnah ausgewertet werden nur An- und Abmeldungen an Relution Shared Devices.

Für Version 26.4.0

Weitere Filteroptionen

Neben `ist in` stehen für die Kategorien Benutzer und Gruppen die Filter-Definitionen `nicht in`, `ist leer` und `ist nicht leer` zur Verfügung. Mit `ist leer` lässt sich z. B. eine Gruppe für alle Geräte ohne Gerätebenutzer bilden.

Über + → Filter hinzufügen lassen sich weitere Filter ergänzen, z. B. für das BYOD-Szenario ein Filter mit der Kategorie Eigentümerschaft. Die Filter-Spezifikation legt fest, ob ein Gerät allen Filtern (Entspricht allen Filter) oder mindestens einem Filter (Entspricht mindestens einem Filter) entsprechen muss. Die Gerätevorschau zeigt nach Klick auf Aktualisieren, welche Geräte die Filter aktuell erfüllen. Details zu allen Filtern stehen im Artikel Gerätegruppen →.

Richtlinien der dynamischen Gerätegruppe zuweisen

Nachdem die dynamische Gerätegruppe erstellt wurde, werden ihr die gewünschten Richtlinien zugewiesen:

1. Die neu erstellte Gerätegruppe öffnen.
2. Zum Tab Richtlinien wechseln.
3. Auf Hinzufügen klicken.
4. Im Dialog Richtlinien hinzufügen eine oder mehrere Richtlinien auswählen und mit Bestätigen übernehmen.

Die Richtlinien sind nun mit der dynamischen Gerätegruppe verknüpft und werden automatisch angewendet, sobald ein Gerät die Filterbedingung erfüllt.

Empfehlungen und Best Practices

- Namenskonvention: Ein einheitliches Präfix für dynamische Gerätegruppen, z. B. `DYN –`, unterscheidet sie in der Übersicht klar von statischen Gruppen.
- Richtlinienreihenfolge: Mögliche Konflikte sollten berücksichtigt werden, wenn ein Gerät in mehreren dynamischen Gruppen gleichzeitig Mitglied ist.
- Testen: Neue dynamische Gruppen sollten zunächst mit einem einzelnen Testgerät und Testbenutzer getestet werden, bevor die Konfiguration produktiv eingesetzt wird.
- LDAP-Synchronisation: Bei Nutzung von LDAP-Gruppen sollte geprüft werden, ob die Synchronisationsintervalle für den jeweiligen Anwendungsfall geeignet sind.

Verwandte Artikel

- Richtlinien erklärt →
- Gerätegruppen →
- Benutzerverwaltung →
- Richtlinien per Netzwerk (BYOD) →
- LDAP Konfiguration →

Für Version 26.4.0

Aktionen mit Gerätegruppen

Mit Relution 5.22 ist es möglich, neben Richtlinien auch Aktionen und CRON-Jobs durch die Mitgliedschaft in Gerätegruppen auszulösen. Diese Funktion hat die Regelwerke mit Relution 26.0 vollständig abgelöst. Eine Übernahme alter Regelwerke in die neue Funktionalität findet nicht statt.

> Gerätegruppen funktionieren plattformunabhängig. Aus diesem Grund kann es sein, dass einzelne Aktionen auf bestimmten Geräten nicht angewendet werden können.

Die grundlegende Funktionsweise von Gerätegruppen ist an dieser Stelle erklärt: Gerätegruppen →

Aktionen anlegen

Aktionen gehören jeweils zu einer Gerätegruppe. Sie werden unter `Geräte` → `Gerätegruppen` in der Detailansicht der Gruppe im Reiter Aktionen über Hinzufügen angelegt. Dafür ist die Berechtigung zum Anlegen bzw. Bearbeiten von Gerätegruppenaktionen erforderlich.

Das Formular Aktion hinzufügen besteht aus zwei Bereichen:

- Allgemein: Name, optional Beschreibung sowie Trigger. Im Feld Trigger stehen die Optionen Eventbasiert und CRON-gesteuert zur Auswahl.
- Aktion: Im Feld Aktionstyp wird festgelegt, was auf den Geräten ausgeführt wird (siehe Abschnitt Hauptaktionstypen).

In der Liste der Aktionen lässt sich jede Aktion über den Schalter Aktiviert ein- und ausschalten. Deaktivierte Aktionen werden nicht ausgeführt.

Für Version 26.4.0

Eventbasiert

Eventbasierte Aktionen reagieren auf Änderungen der Gruppenmitgliedschaft:

1. Unter Auslöser der Aktion wird festgelegt, wann die Aktion ausgeführt wird: Kein Auslöser, Wenn ein Gerät der Gruppe beitritt, Wenn ein Gerät die Gruppe verlässt oder Beides.
2. Unter Verzögerung der Ausführung wird zwischen Sofort und Zeitverzögert gewählt. Bei Zeitverzögert wird die Verzögerung in Tage, Stunden und Minuten angegeben; vorbelegt sind 90 Minuten. Ist ein beigetretenes Gerät nach Ablauf der Verzögerung nicht mehr Mitglied der Gruppe bzw. ein ausgetretenes Gerät wieder Mitglied, wird die Aktion nicht ausgeführt. So lassen sich Ausführungen vermeiden, wenn ein Gerät nur kurzzeitig zur Gruppe gehört.

Eventbasierte Aktionen wirken nur auf künftige Beitritte und Austritte. Geräte, die beim Anlegen der Aktion bereits Mitglied der Gruppe sind, lösen die Aktion nicht aus.

CRON-gesteuert

1. Aktionen können zeitgesteuert nach einem CRON-Ausdruck ausgelöst werden WIKI CRON →. Die Aktion wird zu den angegebenen Zeitpunkten für alle Geräte ausgeführt, die dann Mitglied der Gruppe sind.
2. Alle Felder müssen befüllt sein. Komma-Separierung, Bereiche und Schrittwerte werden akzeptiert. Tage des Monats und Wochentage können nicht gleichzeitig konkrete Werte enthalten; eines der beiden Felder wird auf `*` oder `?` gesetzt.
3. Vorbelegt ist eine Ausführung täglich um 06:00 und 21:00 Uhr (Minuten `0`, Stunden `6,21`, Tage des Monats `*`, Monate `*`, Wochentage `?`). Die Zeitpunkte beziehen sich auf die Zeitzone des Relution-Servers.

Feld	Beschreibung	Erlaubte Werte
Minuten	Zeitpunkt innerhalb einer Stunde	0 bis 59
Stunden	Zeitpunkt innerhalb eines Tages	0 bis 23
Tage des Monats	Kalendertag	1 bis 31
Monate	Monat des Jahres	1 bis 12 (oder JAN-DEC)
Wochentage	Tag der Woche	0 bis 6 (0 = Sonntag bis 6 = Samstag, oder SUN-SAT)

Für Version 26.4.

Ergänzende Hinweise zur Syntax

Die Werte werden ohne Leerzeichen eingegeben, da das Portal die Eingabe sonst als ungültig ablehnt.

- Stern (`*`): Steht für “jeden” (z. B. jede Minute, jeden Tag).
- Fragezeichen (`?`): Nur bei Tage des Monats und Wochentage; steht für “keine Angabe”.
- Komma (`,`): Trennt einzelne Werte (z. B. `1,15,30` für die 1., 15. und 30. Minute).
- Bindestrich (`-`): Definiert einen Bereich (z. B. `1-5` für Montag bis Freitag).
- Schrägstrich (`/`): Definiert Intervalle (z. B. `*/5` für alle 5 Einheiten).
- Crontab Guru →

Diese Konfigurationen sind direkt gültig und werden nach dem Speichern angewendet.

Hauptaktionstypen

Im Feld Aktionstyp stehen folgende Typen zur Verfügung:

1. Gerät löschen
2. Geräteaktion
3. Benachrichtigungsaktion
4. Gerätename ändern
5. Geräterichtlinie aktualisieren
6. Webhook

Gerät löschen

Beschreibung:

- Diese Aktion entfernt das Gerät aus der Relution-Verwaltung. Was dabei auf dem Gerät geschieht, hängt von der Einschreibungsart ab:
  - Vollständig verwaltete Android-Enterprise-Geräte werden auf Werkseinstellungen zurückgesetzt.
  - Bei Android-Enterprise-Geräten mit Arbeitsprofil oder mit persönlichem Profil wird nur das Arbeitsprofil entfernt; persönliche Apps und Daten bleiben erhalten.
  - Auf allen anderen Plattformen wird die Verwaltung entfernt (z. B. das MDM-Profil bei Apple-Geräten oder die Registrierung bei Windows), das Gerät wird aber nicht zurückgesetzt.
- Wichtig: Dies kann nicht rückgängig gemacht werden.
- Bei Geräten, die über KME (Knox Mobile Enrollment) eingeschrieben wurden, muss sichergestellt sein, dass im Samsung Knox Enrollment Portal kein Profil zugewiesen ist, da das Gerät sonst nach dem Löschen automatisch neu eingeschrieben wird (nur Android).

Optionen:

- Android:
  - Relution App nicht deinstallieren: ja/nein
- Verwaltetes Gerät (Android Enterprise, vollständig verwaltet):
  - Factory Reset Protection (FRP) aktiviert lassen: ja/nein
  - Den externen Speicher des Geräts ebenfalls löschen (z. B. SD-Karten): ja/nein
  - Nachricht: Text, der Benutzern privater Geräte mit Arbeitsprofil vor dem Entfernen des Arbeitsprofils angezeigt wird. Auf firmeneigenen Geräten hat er keine Wirkung.

Für Version 26.4.0

Geräteaktion

Beschreibung:

- Ermöglicht verschiedene Einzelaktionen auf den Geräten.

Welche Aktionen konkret auf welchem Betriebssystem verfügbar sind, wird nach der Auswahl im Bereich Details als Plattform-Kennzeichnung angezeigt.

Unteraktionen:

1. Lost Mode aktivieren
    - Sperrt das Gerät und ermöglicht seine Ortung. Kann verwendet werden, wenn ein Gerät verloren gegangen ist.
    - Felder: Nachricht, Telefonnummer, Fußnote, E-Mail, Adresse, Organisationsname
2. Lost Mode deaktivieren
    - Hebt den Lost Mode auf.
3. Gerät neu starten
    - Startet das Gerät neu.
    - Feld: Grund für den Neustart (nur Android-Geräte ohne Android Enterprise und interaktive Whiteboards)
    - Optionen: Ausschalten (nur Android-Geräte ohne Android Enterprise und interaktive Whiteboards), Den Benutzer benachrichtigen, um das Gerät neu zu starten (kein erzwungener Neustart), nur macOS ab 11
4. Geräteinformationen aktualisieren
    - Aktualisiert die in Relution gespeicherten Geräteinformationen.
5. Alarm auslösen
    - Lässt einen Alarm auf dem Gerät ertönen.
    - Feld: Dauer (in Sekunden)
6. Bluetooth ein- oder ausschalten
    - Aktiviert oder deaktiviert Bluetooth.
    - Option: Bluetooth einschalten
7. Gerät scannen
    - Startet einen Virenscan mit Microsoft Defender auf Windows-Geräten.
    - Feld: Scan Typ (Schnell Scan oder Vollständiger Scan)
8. Lokale Benutzer löschen
    - Löscht alle lokalen Benutzerkonten und Daten.
    - Option: Kontolöschung erzwingen
9. Persönlichen Hotspot ein- oder ausschalten
    - Aktiviert oder deaktiviert den persönlichen Hotspot.
    - Option: Persönlichen Hotspot einschalten
10. eSIM-Mobilfunktarif
    - Konfiguriert einen eSIM-Mobilfunktarif.
    - Feld: Server-URL
11. Shortcut entfernen
    - Entfernt eine Verknüpfung vom Gerät.
    - Felder: Bezeichnung, URL
12. AirPlay-Wiedergabe starten
    - Startet die AirPlay-Wiedergabe auf einem Apple TV oder einem anderen AirPlay-fähigen Gerät.
    - Felder: Name, MAC-Adresse, Scanzeit (Sekunden), Passwort
13. Return to Service
    - Setzt das Gerät auf die Werkseinstellungen zurück. Danach versucht das Gerät, sich automatisch wieder bei Relution einzuschreiben; dafür muss die Aktivierungssperre deaktiviert sein. Verfügbar für iOS ab 17 und tvOS ab 18.
    - Feld: WLAN-Konfiguration (Pflichtfeld; Auswahl aus den aktivierten WLAN-Konfigurationen veröffentlichter Richtlinien)
    - Option: Bestehenden Datentarif beibehalten (nur iOS)
14. Datei an Gerät senden
    - Sendet eine Datei an das Gerät.
    - Felder: Datei auswählen, Verzeichnis, ZIP-Archive nicht dekomprimieren
15. Gerät auf Werkszustand zurücksetzen
    - Setzt das Gerät auf die Werkseinstellungen zurück.
    - Optionen: Factory Reset Protection (FRP) aktiviert lassen, Den externen Speicher des Geräts ebenfalls löschen, Nachricht, PIN, Bestehenden Datentarif beibehalten, Proximity Setup deaktivieren
16. Prowise-Update installieren
    - Installiert ein Prowise-Update.
    - Feld: Update am
17. Gerät vollständig sperren
    - Sperrt das Gerät mit dem aktuellen Passwort.
    - Felder: Nachricht, Telefonnummer, PIN

Für Version 26.4.0

18. Shortcut hinzufügen
    - Fügt eine Verknüpfung zum Gerät hinzu.
    - Felder: Bezeichnung, URL, Im Vollbildmodus öffnen, Icon
19. Passwort zurücksetzen
    - Setzt das Gerätepasswort zurück.
    - Feld: Neues Passwort
    - Optionen: Sofort sperren, Eingabe vor erneutem Reset erfordern, Beim Booten nicht fragen
20. Passwort zurücksetzen (Windows)
    - Setzt das Passwort eines Windows-Benutzerkontos zurück.
    - Felder: Benutzername, Passwort, Passwort wiederholen
    - Aktion: Beispielkennwort generieren
21. Gerät herunterfahren
    - Fährt das Gerät herunter.
22. AirPlay-Wiedergabe stoppen
    - Beendet die AirPlay-Wiedergabe.
23. Gerät orten
    - Löst die Ortung des Geräts aus.
24. Bildschirmzeit-Code entfernen
    - Entfernt den Bildschirmzeit-Code.
25. Daten-Roaming ein- oder ausschalten
    - Schaltet das Daten-Roaming auf iOS-Geräten ein oder aus. Die Einstellung kann vom Benutzer auf dem Gerät wieder geändert werden.
    - Option: Daten-Roaming aktivieren
26. Im Geräte-Setup-Assistenten fortfahren
    - Setzt das Gerät im Setup-Assistenten fort.
27. Medien installieren
    - Installiert Medien auf dem Gerät.
    - Feld: Token-Auswahl
28. Medien entfernen
    - Entfernt Medien vom Gerät.
    - Feld: Token-Auswahl
29. PowerShell-Skript ausführen
    - Führt ein PowerShell-Skript auf Windows-Geräten aus.
30. Den Benutzer abmelden
    - Meldet den aktuellen Benutzer ab.
31. Shell-Skript ausführen
    - Führt ein Shell-Skript auf macOS- und Linux-Geräten aus. Die Unteraktion steht nur zur Auswahl, wenn der macOS Companion aktiviert ist (`Einstellungen` → `Relution Client Apps`, Schalter macOS Companion aktivieren).
32. Geräteinformationen anfordern
    - Fordert bestimmte Geräteinformationen an (Android Enterprise, Arbeitsprofil auf privatem Gerät, ab Android 13). Der Benutzer wird gebeten, der Weitergabe der Information zuzustimmen.
    - Feld: Typ (eSIM-Kennung (EID))
33. Enterprise Wipe
    - Entfernt das Arbeitsprofil und alle Richtlinien und überlässt das Gerät der persönlichen Nutzung. Apps und Daten des persönlichen Profils bleiben erhalten (Android Enterprise, firmeneigenes Gerät mit persönlichem Profil, ab Android 8).
34. Standard-Apps festlegen
    - Legt die Standard-Apps für Anrufe, Nachrichten und Webbrowser auf iOS-Geräten fest.
    - Felder: Standard-Anruf-App und Standard-Nachrichten-App (ab iOS 26), Standard-Browser-App (ab iOS 18.2)
35. Bildschirmfreigabe aktivieren
    - Aktiviert auf Macs die entfernte Verwaltung über die Apple-Bildschirmfreigabe: Zugriff für alle Benutzer, Empfang entfernter Ereignisse sowie die Optionen Beobachten, Steuern und Anzeigen während Beobachtung. Alle anderen Optionen bleiben unverändert (ab macOS 10.14.4).

Für Version 26.4.0

36. Bildschirmfreigabe deaktivieren
    - Deaktiviert auf Macs die entfernte Verwaltung über die Apple-Bildschirmfreigabe (ab macOS 10.14.4).

Benachrichtigungsaktion

Beschreibung:

- Sendet Benachrichtigungen an Gerätebenutzer oder andere Personen.

Empfänger:

- Gerätebenutzer benachrichtigen
- Andere Benutzer benachrichtigen: Auswahl von Benutzern und Benutzergruppen
- Zusätzliche E-Mail-Empfänger: weitere E-Mail-Adressen

Nachricht:

- Per E-Mail benachrichtigen: Versand einer E-Mail auf Basis einer Vorlage. Über Auf Vorlage zurücksetzen wird der Standardtext wiederhergestellt.
- Per Push-Nachricht benachrichtigen: Die Empfänger erhalten die Push-Nachricht auf allen ihnen zugewiesenen eingeschriebenen Geräten.

In den Texten können Platzhalter verwendet werden; die verfügbaren Platzhalter werden im Formular angezeigt: Erweiterte Platzhalter →

Für Version 26.4.0

Gerätename ändern

Beschreibung:

- Ändert den Namen des Geräts.

Feld: Gerätename. Platzhalter wie `${device.serialnumber}` werden je Gerät aufgelöst. Ergibt sich ein leerer Name, bleibt der bisherige Gerätename erhalten.

Geräterichtlinie aktualisieren

Beschreibung:

- Aktualisiert die auf dem Gerät angewendeten Richtlinien.

Webhook

Beschreibung:

- Sendet eine Anfrage an einen externen Dienst (z. B. ein anderes System).

Felder: URL, Method (GET, POST oder PUT; voreingestellt ist POST), Headers (Request-Header als Liste), Body

Über Prüfen im Bereich Webhook-Parameter testen sendet der Server eine OPTIONS-Anfrage an die angegebene URL und zeigt die Antwort an. So lässt sich prüfen, ob der Zielhost vom Relution-Server aus erreichbar ist.

Geozonen

In diesem Artikel wird beschrieben, wie es möglich ist, Richtlinien automatisch anhand des Gerätestandorts zuzuweisen. Diese Geozonen müssen vorab angelegt und anschließend über dynamische Gerätegruppen zugewiesen werden.

Einschränkungen und Hinweise

Die Funktion der Geozonen setzt eine permanente Internetverbindung, ein GPS-Modul am Gerät und den installierten Relution Agent voraus. Unterstützt werden iOS (iPhone sowie iPad mit Mobilfunkmodul, z. B. Cellular iPad →), Android und Android Enterprise.

- Bei Android-Geräten kann sich die Erkennung je nach Gerätezustand verzögern, in Ausnahmefällen um bis zu 30 Minuten.
- Der Radius einer Geozone ist im Portal fest auf 100 Meter um den gesetzten Standort eingestellt.

Wird die Geozone ohne Internetverbindung und GPS gewechselt, muss auf dem Gerät im Relution Agent ein manueller Sync der Standortdaten ausgelöst werden.

Vorbereitung

Für Version 26.4.0

Damit Geozonen funktionieren, muss der Relution Agent auf dem Gerät installiert und mindestens einmal geöffnet worden sein. Außerdem müssen für den Relution Agent die Berechtigungen für Push-Benachrichtigungen und Standortdienste erteilt sein; der Benutzer darf diese nicht wieder entziehen. Dies gilt für iOS- und Android-Geräte. Unter Android benötigt der Relution Agent die Standortberechtigung dauerhaft, also auch im Hintergrund.

Auf iOS-Geräten kann die Standortberechtigung nicht automatisch über die MDM-Schnittstelle erteilt werden. Deshalb müssen Benutzer diesen Parameter selbst konfigurieren.

Hierzu muss im iOS Gerät unter `Einstellungen` → `Apps` → `Relution Agent` → `Ort` der Wert Zugriff auf Standort erlauben auf Immer gestellt werden.

Ist dies nicht der Fall, kann der Relution Agent den aktuellen Standort nicht an den Server übermitteln und eine automatische Zuweisung der Richtlinien ist nicht möglich.

Sind in der Organisation Zonen oder iBeacons angelegt, erzeugt Relution für Geräte, deren Relution Agent keine Standortberechtigung hat oder deren Ortungsdienste ausgeschaltet sind, einen Konformitätshinweis (Standortgenehmigung bzw. Ortungsdienste). Das Gerät bleibt dabei konform.

Einrichtung einer Geozone

Geozonen werden unter `Einstellungen` → `Dynamische Richtlinienzuweisung` → `Zonen` verwaltet. Über Hinzufügen wird eine neue Geozone angelegt.
Im Abschnitt Allgemein wird ein Name vergeben (Pflichtfeld). Im Abschnitt Adresse wird der Standort festgelegt: über die Suchleiste der Karte (Adresse oder Koordinaten im Format Breitengrad, Längengrad, z. B. `48.7968, 9.2211`), per Rechtsklick oder langes Drücken auf die Karte oder direkt über die Felder Breitengrad und Längengrad. Karte zentrieren richtet die Karte auf die gesetzte Markierung aus.
Mit Speichern wird die Geozone angelegt; die Schaltfläche ist erst aktiv, wenn Name und Koordinaten gesetzt sind. Die angezeigte Adresse ermittelt Relution beim Speichern automatisch aus den Koordinaten.
In der Übersicht der Geozonen sollte nun ein Eintrag hinzugefügt worden sein.

Wird eine Geozone angelegt, geändert oder gelöscht, sendet Relution allen iOS-, Android- und Android-Enterprise-Geräten automatisch die Aktion Zonen neu laden, damit der Relution Agent die aktuellen Zonen lädt. Die Aktion erscheint im Aktionsverlauf des Geräts und lässt sich nicht manuell auslösen.

Für das Anzeigen, Anlegen, Bearbeiten und Löschen von Geozonen sind in der Rolle die Berechtigungen für Zonen im Bereich Dynamische Richtlinienzuweisung erforderlich: Berechtigungen →

Was der Relution Agent dem Benutzer über Zonen und iBeacons in Reichweite anzeigt, legt die Einstellung Anzeige von Informationen über iBeacons und Zonen in Reichweite unter `Einstellungen` → `Geräteverwaltung` im Abschnitt Relution Agent fest: Verstecken (Standard), Vollständige Informationen oder Verschleierte Darstellung.

Gerätegruppe konfigurieren

Für Version 26.4.0

Um die Geozone auf eine dynamische Gerätegruppe anwenden zu können, muss diese mit einem Filter konfiguriert werden.
Unter `Geräte` → `Gerätegruppen` wird eine neue dynamische Gerätegruppe erstellt oder eine bestehende bearbeitet.
Als Kategorie der Abfrage wird Aktive Zonen gewählt, unter Filter Definition beispielsweise ist in; über Zonen auswählen werden die gewünschten Geozonen festgelegt. Geräte, die sich in mindestens einer dieser Zonen befinden, werden daraufhin automatisch Mitglied der Gruppe. Der Gruppe wird anschließend die gewünschte Richtlinie zugewiesen.

Weitere Filterdefinitionen: Mit alle muss sich das Gerät in allen gewählten Zonen befinden, mit nicht in in keiner davon; ist nicht leer bzw. ist leer erfassen Geräte in irgendeiner bzw. in keiner Zone und kommen ohne Zonenauswahl aus.

Gerätegruppen →

In welchen Zonen sich ein Gerät aktuell befindet, zeigen die Spalte und der Filter Aktive Geofence-Zonen in der Geräteliste sowie in den Gerätedetails die Karte Position unter Aktive Zonen.

Neben dem geografischen Standort lassen sich Richtlinien auch anhand von Funksignalen im Raum zuweisen: iBeacons →

iBeacons

Neben Geozonen → lassen sich Richtlinien in Relution auch anhand von iBeacons zuweisen. Ein iBeacon ist ein Bluetooth-Sender, dessen Signal ein Gerät in seiner Nähe empfängt. Befindet sich ein Gerät in Reichweite eines hinterlegten Beacons, kann es über eine dynamische Gerätegruppe automatisch eine andere Richtlinie erhalten.

Beide Verfahren gehören im Portal zum Bereich `Einstellungen` → `Dynamische Richtlinienzuweisung`: Zonen arbeiten mit dem geografischen Standort, iBeacons mit Funksignalen im Raum. iBeacons eignen sich damit auch dort, wo GPS nicht zuverlässig verfügbar ist — etwa innerhalb von Gebäuden.

Einschränkungen und Hinweise

Für die Nutzung der Funktion müssen folgende Anforderungen erfüllt sein:

- Die Relution Agent App muss installiert und mindestens einmal geöffnet worden sein.
- Die Berechtigungen für Push-Benachrichtigungen, Standortdienste und Bluetooth müssen für die Relution Agent App aktiviert sein und dürfen von den Benutzern nicht deaktiviert werden.
- Bei Android-Geräten kann es je nach Gerätezustand zu Verzögerungen bei der Erkennung kommen. In Ausnahmefällen dauert dies bis zu 30 Minuten.

Für Version 26.4.0

Unterstützt werden iOS-, Android- und Android-Enterprise-Geräte. Auf macOS und Windows wertet Relution keine iBeacons aus, auch wenn dort ein Relution Agent installiert ist.

Sind in der Organisation iBeacons oder Zonen angelegt, erzeugt Relution für Geräte, deren Relution Agent keine Standortberechtigung hat oder deren Ortungsdienste ausgeschaltet sind, einen Konformitätshinweis (Standortgenehmigung bzw. Ortungsdienste). Das Gerät bleibt dabei konform.

Die Beacons selbst sind Hardware von Drittanbietern und nicht Bestandteil von Relution. Relution verwaltet lediglich ihre Kennungen und wertet aus, welche davon ein Gerät empfängt.

iBeacon anlegen

Zu `Einstellungen` → `Dynamische Richtlinienzuweisung` → `iBeacons` navigieren und über Hinzufügen einen neuen Eintrag anlegen. Ein iBeacon wird über drei Werte identifiziert, die von der eingesetzten Hardware vorgegeben werden:

- Eindeutige Kennung (UUID) — eine für die Anwendung und den Einsatzzweck spezifische UUID.
- Major ID — spezifiziert einen bestimmten iBeacon und Anwendungsfall, beispielsweise eine Unterregion innerhalb der durch die UUID definierten Region.
- Minor ID — ermöglicht eine weitere Unterteilung der Region oder des Anwendungsfalls.

Dazu kommt ein Name als für Menschen lesbare Bezeichnung, unter der das Beacon später in den Filtern erscheint.

Pflichtfelder sind Name und Eindeutige Kennung (UUID). Major ID und Minor ID sind optional und erlauben Werte von 1 bis 65535.

> Die Kombination aus UUID, Major ID und Minor ID muss eindeutig sein. Existiert bereits ein Eintrag mit denselben drei Werten, wird das Anlegen mit einem Hinweis abgelehnt.

Eine typische Aufteilung ist eine gemeinsame UUID je Liegenschaft, die Major ID je Gebäude oder Etage und die Minor ID je Raum. Damit lassen sich Filter später auf der gewünschten Granularität bilden.

Bestehende Einträge lassen sich in der Liste über Bearbeiten ändern und über Löschen entfernen. Für das Anzeigen, Anlegen, Bearbeiten und Löschen sind in der Rolle die Berechtigungen für iBeacons im Bereich Dynamische Richtlinienzuweisung erforderlich: Berechtigungen →

Wird ein iBeacon angelegt, geändert oder gelöscht, sendet Relution allen iOS-, Android- und Android-Enterprise-Geräten automatisch die Aktion iBeacons neu laden, damit der Relution Agent die aktuellen iBeacon-Definitionen lädt. Die Aktion erscheint im Aktionsverlauf des Geräts und lässt sich nicht manuell auslösen.

---

iBeacons am Gerät nachvollziehen

Welche Beacons ein Gerät aktuell empfängt, ist an zwei Stellen sichtbar:

- In der Inventarübersicht über die Spalte iBeacons in Reichweite. Der gleichnamige Filter grenzt auf einzelne Beacons ein, der Filterwert Keine iBeacons auf Geräte ohne Empfang.
- In den Gerätedetails auf der Karte Position, ebenfalls unter iBeacons in Reichweite. Angezeigt werden die Beacons, die nah genug sind, dass das Gerät ihr Signal empfängt. Die Karte erscheint nur, wenn das Gerät Beacons empfängt, eine Zone betreten hat oder den Status des Ortungsdienstes meldet.

Was der Relution Agent dem Benutzer über iBeacons und Zonen in Reichweite anzeigt, legt die Einstellung Anzeige von Informationen über iBeacons und Zonen in Reichweite unter `Einstellungen` → `Geräteverwaltung` im Abschnitt Relution Agent fest: Verstecken (Standard), Vollständige Informationen oder Verschleierte Darstellung.

Für Version 26.4.0

Gerätegruppe konfigurieren

Damit ein Beacon eine Richtlinie auslöst, wird er in einer dynamischen Gerätegruppe als Filter hinterlegt.

Zu `Geräte` → `Gerätegruppen` navigieren und eine neue dynamische Gerätegruppe erstellen oder eine bestehende bearbeiten. Als Kategorie der Abfrage wird iBeacons in Reichweite gewählt, unter Filter Definition der Operator ist in; über iBeacons auswählen werden die gewünschten Beacons festgelegt. Geräte, die mindestens eines dieser Signale empfangen, werden daraufhin automatisch Mitglied der Gruppe und erhalten die dort zugewiesene Richtlinie.

Weitere Filterdefinitionen: Mit alle müssen alle gewählten Beacons gleichzeitig in Reichweite sein, mit nicht in keiner davon; ist nicht leer bzw. ist leer erfassen Geräte mit irgendeinem bzw. ohne Beacon in Reichweite und kommen ohne Beacon-Auswahl aus.

Gerätegruppen →

Verwandte Themen

- Geozonen → — Richtlinien anhand des geografischen Standorts zuweisen.
- Gerätegruppen → — dynamische Gruppen und ihre Filter.

Richtlinien per Netzwerk (BYOD)

In BYOD-Szenarien werden Geräte sowohl innerhalb als auch außerhalb der Schule verwendet.
Eine rein zeitbasierte Steuerung von Richtlinien ist dabei oft unflexibel und mit hohem Pflegeaufwand verbunden.

Eine bewährte Alternative ist die netzwerkbasierte Richtlinienzuweisung, bei der Richtlinien automatisch angewendet werden, sobald sich ein Gerät im Schulnetzwerk befindet.
Die Erkennung erfolgt über die öffentliche IP-Adresse des Netzwerks.

Dieser Ansatz ist besonders für BYOD geeignet, da Geräte außerhalb der Schule nicht unnötig eingeschränkt werden und gleichzeitig der administrative Aufwand reduziert wird.

Grundprinzip

Der Aufenthaltsort eines BYOD-Geräts wird indirekt über dessen öffentliche IP-Adresse bestimmt.

Der Aufbau besteht aus:

- Einer Richtlinie, die nur im Schulnetz gelten soll
- Einer dynamischen Gerätegruppe, die Geräte anhand der öffentlichen IP-Adresse sammelt

Meldet sich ein Gerät aus dem Schul-WLAN bei Relution, erkennt Relution die öffentliche IP-Adresse des Schulnetzes. Das Gerät wird daraufhin automatisch der dynamischen Gerätegruppe zugewiesen und erhält die entsprechende Richtlinie.

Für Version 26.4.0

Das Gerät muss im Schul-WLAN verbleiben, damit die Konfiguration angewendet und beibehalten wird.

Empfohlene BYOD-Basisgruppe

Unabhängig von der dynamischen Gruppe für das Schulnetz sollten BYOD-Geräte immer einer Basis-Gerätegruppe zugewiesen sein.

Diese enthält Konfigurationen, die dauerhaft gelten, z. B.:

- WLAN-Profile der Schule
- Pflicht-Apps
- Grundlegende Einschränkungen, die auch außerhalb der Schule gelten

So wird sichergestellt, dass Geräte jederzeit funktionsfähig bleiben.

Dynamische Gerätegruppe konfigurieren

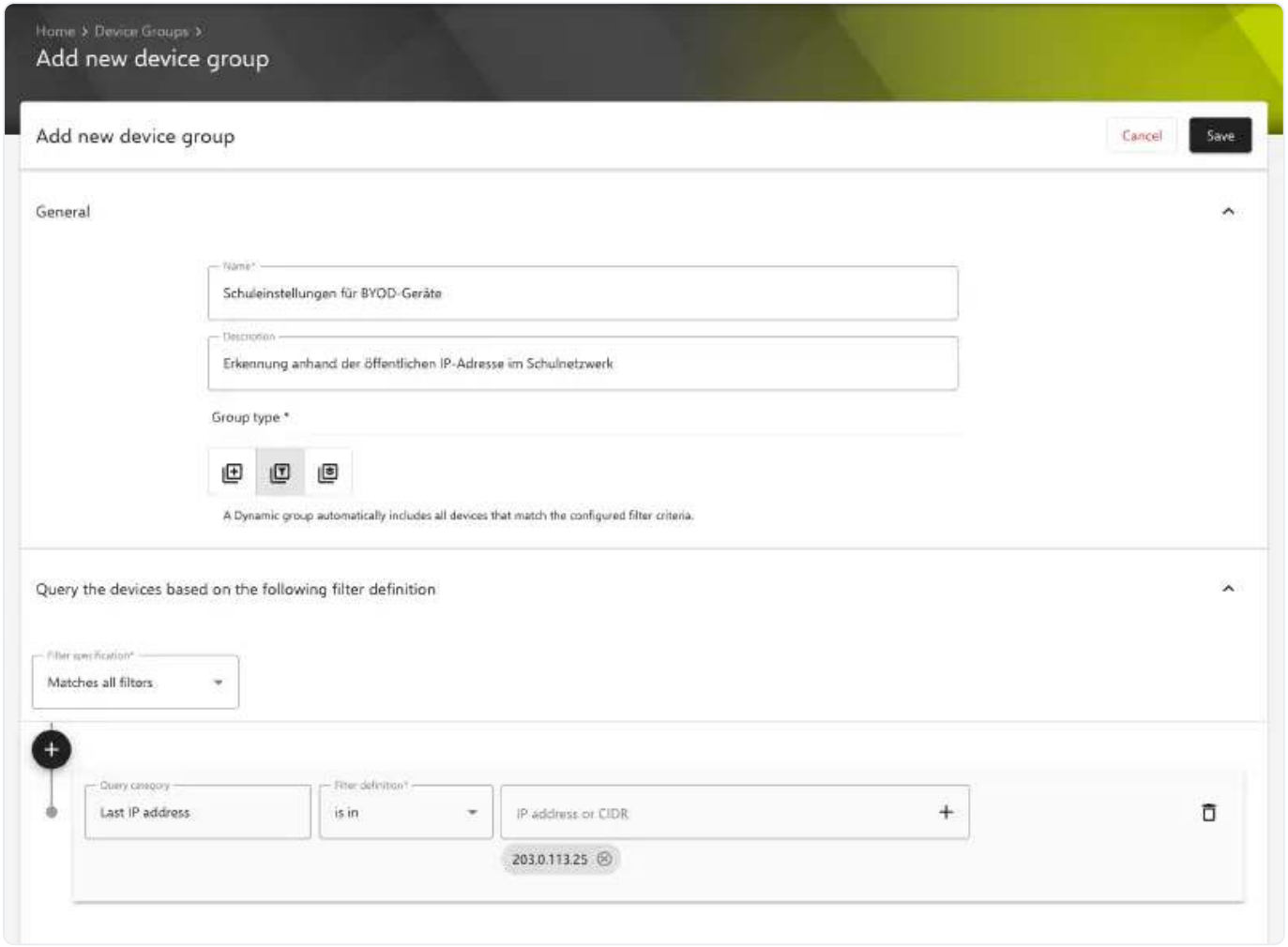
Eine neue dynamische Gruppe wird erstellt. Als Kategorie der Abfrage wird Letzte IP-Adresse gewählt, unter Filter Definition der Operator ist in. Im Feld IP-Adresse oder CIDR wird die öffentliche IPv4-Adresse oder der IPv4-Bereich des Schulnetzwerks eingetragen (z. B. `203.0.113.25` oder `203.0.113.0/24`); mehrere Einträge sind möglich.

Der Filter muss den öffentlichen IP-Bereich des Schulnetzwerks abdecken.
Alle Geräte, deren zuletzt erkannte IP-Adresse in diesem Bereich liegt, werden automatisch der Gruppe hinzugefügt.

Der Filter wertet ausschließlich IPv4-Adressen aus. Erreicht ein Gerät den Relution-Server über IPv6, wird seine letzte IP-Adresse als IPv6-Adresse gespeichert, und das Gerät wird von der Gruppe nicht erfasst.

Welche IP-Adresse Relution zuletzt für ein Gerät erkannt hat, zeigen die Gerätedetails auf der Karte Netzwerk unter Letzte IP-Adresse sowie die gleichnamige Spalte in der Geräteliste. Darüber lässt sich der passende öffentliche Bereich ermitteln.

Gerätegruppen →



Aktualisierung der IP-Adresse

Relution übernimmt die öffentliche IP-Adresse aus der Verbindung, sobald sich das Gerät beim Server meldet. Gezielt auslösen lässt sich das mit der Aktion Geräteinformationen aktualisieren.

Eine Aktualisierung erfolgt insbesondere in folgenden Fällen:

- Beim Ausführen von Richtlinien
- Beim regelmäßigen Ping der Geräteverfügbarkeitsprüfung, sofern Geräteverfügbarkeit überprüfen aktiv ist (standardmäßig einmal täglich, einstellbar über Ping-Intervall in Minuten unter `Einstellungen` → `Geräteverwaltung`; nicht für Android Enterprise)
- Über eine Gerätegruppenaktion mit dem Trigger CRON-gesteuert
- Wenn ein Administrator die Aktion Geräteinformationen aktualisieren für das Gerät im Portal ausführt
- Wenn der Benutzer die Aktualisierung im Self-Service-Portal anstößt (frühestens 5 Minuten nach der letzten Aktualisierung)
- Wenn der Benutzer die Aktion manuell im Relution Agent über den Reiter Einstellungen auslöst

Empfehlung: CRON-gesteuerte Aktion in der Basisgruppe

In den meisten BYOD-Umgebungen empfiehlt sich eine Gerätegruppenaktion vom Aktionstyp Geräteaktion mit Geräteinformationen aktualisieren und dem Trigger CRON-gesteuert. Die Aktion wird in der BYOD-Basisgruppe angelegt, in der sich das Gerät dauerhaft befindet, und nicht in der dynamischen IP-Gruppe. Eine CRON-Aktion wird nur für Geräte ausgeführt, die gerade Mitglied der Gruppe sind. In der dynamischen Gruppe würde sie Geräte außerhalb des Schulnetzes nie erreichen, sodass diese nicht automatisch in die Gruppe aufgenommen würden. Über die Basisgruppe wird sichergestellt, dass Geräte ihre IP-Adresse regelmäßig aktualisieren, ohne dass ein Benutzereingriff erforderlich ist.

Für Version 26.4.0

Hinweise zur Nutzung von CRON-Aktionen

- Keine sehr kurzen Intervalle verwenden
- Keine hohe Wiederholungsfrequenz konfigurieren

Beispielsweise kann ein stündliches Ausführen von Geräteinformationen aktualisieren bei einer großen Anzahl von Geräten zu erheblichen Performance-Problemen führen.

Ein moderates Intervall ist ausreichend und sorgt für einen stabilen Betrieb.
In der folgenden Beispielkonfiguration wird die Aktion an allen Wochentagen um 7:45, 12:45 und 14:45 ausgeführt.

Home > Gerätegruppen > Aktionen >

Aktion hinzufügen

Aktion hinzufügen

Abbrechen | Speichern

Allgemein

Name*
BYOD IP-Adressen aktualisieren

Beschreibung
Wechsel zwischen Schule und Zuhause

Trigger *
CRON-gesteuert

Zeitplan für die Ausführung

Minuten*
45

Stunden*
7,12,14

Tage des Monats*
*

Monate*
*

Wochentage*
1-5

Aktion

Aktionstyp *
Geräteaktion

Aktionstyp *
Geräteinformationen aktualisieren

Vorteile der netzwerkbasierten Zuweisung (BYOD)

- Keine komplexen Zeitpläne notwendig
- Richtlinien gelten nur im Schulnetz
- Weniger Richtlinien im Vergleich zu zeitbasierten Konzepten
- Ideal für privat genutzte Geräte

Einschränkungen und Hinweise

- Geräte müssen mit dem Schulnetz verbunden sein
- Die Methode ist abhängig von stabilen öffentlichen IP-Bereichen
- Nur IPv4 wird unterstützt; Geräte, die Relution über IPv6 erreichen, werden nicht erkannt
- Änderungen greifen ggf. erst nach der nächsten Aktualisierung der Geräteinformationen
- Steht ein Reverse-Proxy vor Relution, muss er die Client-IP im Header `X-Forwarded-For` weitergeben und als vertrauenswürdiger Proxy eingestuft sein (Relution wertet weitergeleitete Header über `server.forward-headers-strategy=native` aus), sonst sieht Relution nur die Adresse des Proxys, siehe IP des Reverse-Proxys als vertrauenswürdig hinterlegen →

Für Version 26.4.0

Zusammenfassung

Die netzwerkbasierte Richtlinienzuweisung über die öffentliche IP-Adresse ist eine wartungsarme und zuverlässige Lösung für BYOD-Umgebungen.

Sie ermöglicht es, schulische Richtlinien gezielt nur dann anzuwenden, wenn sich Geräte tatsächlich im Schulnetz befinden, während sie außerhalb uneingeschränkt nutzbar bleiben.

Inventarübersicht

Die Inventarübersicht in Relution bietet viele Informationen und Anpassungsmöglichkeiten. Es folgt eine Übersicht der möglichen Funktionen. Das Geräteinventar liefert alle relevanten Informationen und Funktionen, die zur Verwaltung der Geräte notwendig sind.

Für Version 26.4.0

Verfügbare Spalten

- Gerätename
- Beschreibung
- Organisation (nur sichtbar mit Leserechten auf Geräte anderer Organisationen)
- Benutzer
- Benutzername
- E-Mail
- Status
- Aktionen (Anzahl offener Aktionen)
- Verfügbare Updates (Windows)
- Verbindungsstatus
- Richtlinien-Status
- Plattform
- Einschreibungsart
- Telefon
- Hersteller
- Modell
- Eigentümerschaft
- Letzte Verbindung
- Datum der letzten Verbindung mit Companion
- Eingeschrieben
- Erstellt am
- Gerätegruppen
- Zu installierende Richtlinien
- Aktive Richtlinien
- Typ für die automatische Einschreibung
- Seriennummer
- OS Version
- OS Edition
- OS Update Status
- WLAN MAC
- Ethernet MAC
- Lost Mode Status
- Wird überwacht (supervised)
- Bootstrap Token
- Shared iPad
- Batteriestand
- IMEI
- ICCID(s)
- Roaming
- Letzte IP-Adresse
- Letzter bekannter Standort (aus der letzten IP-Adresse ermitteltes Land)
- iBeacons in Reichweite
- Aktive Geofence-Zonen
- Ablaufdatum des Identitätszertifikats (in der Spaltenauswahl: Identitätszertifikat ist abgelaufen)
- Abgelaufenen Identitätszertifikaten vertrauen
- FDE
- Sicherheits-Patch-Level
- Deaktivierte Richtlinien
- Verliehen an (nur bei aktiviertem Ausleihsystem, siehe Ausleihe →)
- Verliehen bis (nur bei aktiviertem Ausleihsystem)

Für Version 26.4.0

Zudem stehen fünf benutzerdefinierte Spalten zur Verfügung, die in den Einstellungen aktiviert und benannt werden können, siehe Benutzerdefinierte Geräteeigenschaften →.

Die Reihenfolge und Sichtbarkeit aller Spalten kann durch den Benutzer individuell konfiguriert werden. In der Spaltenauswahl werden die Spalten per Drag-and-drop sortiert. Angepasste Spaltenbreiten werden gespeichert.

Such- und Filtermöglichkeiten

Spalten können auf- und absteigend sortiert werden. Standardmäßig ist die Liste nach Letzte Verbindung absteigend sortiert. Zudem besteht die Möglichkeit mit Suchbegriffen die Liste einzugrenzen und übersichtlicher zu gestalten.

Es stehen folgende Filtermöglichkeiten zur Verfügung:

- Organisation (nur mit Leserechten auf Geräte anderer Organisationen)
- Plattform
- Einschreibungsart
- OS Version
- Sicherheits-Patch-Level
- Hat ein ausstehendes Betriebssystem-Update (ja / nein)
- Gerätemodelle
- Status
- Lost Mode Status
- OS Edition
- Gerätegruppe
- Eigentümerschaft
- Zu installierende Richtlinien
- Aktive Richtlinien
- Verbindungsstatus
- Roaming (ja / nein)
- Letzter bekannter Standort (Auswahl des Landes)
- Hersteller
- Identitätszertifikat ist abgelaufen (ja / nein)
- Abgelaufenen Identitätszertifikaten vertrauen (ja / nein)
- Aktionen (Anzahl offener Aktionen)
- Shared iPad (ja / nein)
- Wird überwacht (ja / nein)
- Bootstrap Token (ja / nein)
- Deaktivierte Richtlinien (ja / nein)
- Typ für die automatische Einschreibung
- iBeacons (nur mit Leserecht für iBeacons)
- Aktive Geofence-Zonen (nur mit Leserecht für Geofence-Zonen)
- KSP Richtlinienname und KSP Rückmeldung (nur bei verfügbarem Android Enterprise und Leserecht für Geräterichtlinien)
- je ein Filter pro aktivierter benutzerdefinierter Spalte (Bezeichnung entspricht dem Spaltennamen)

Der Filter Status ist standardmäßig auf Konform, Inaktiv und Nicht konform gesetzt. Geräte mit dem Status Einschreibung ausstehend… werden daher erst angezeigt, wenn dieser Status im Filter ausgewählt wird.

Für Version 26.4.0

Paging

Die Listen können 50, 100, 250 oder 500 Einträge pro Seite enthalten. Standardmäßig werden 100 Einträge pro Seite angezeigt.

Zusätzliche Funktionen

Aus dem Inventar können Geräte markiert und direkt mit Aktionen versehen werden. Für markierte Geräte stehen unter anderem Löschen, Aktion anwenden, Verschieben (in eine andere Organisation), Richtlinien erneut anwenden, Seriennummer der Lifetime-Lizenz zuweisen, Zu Gerätegruppen hinzufügen und Aus Gerätegruppen entfernen zur Verfügung.

Zudem lassen sich über Aktualisieren via CSV Gerätename, Benutzer (E-Mail-Adresse) und aktivierte benutzerdefinierte Felder aktualisieren. Die Zuordnung der Geräte erfolgt über die Seriennummer.

Über Ansicht als CSV exportieren lässt sich eine CSV mit allen eingeblendeten Spalten exportieren. Bei mehr als 500 Einträgen erscheint ein Dialog mit der Wahl zwischen Seite exportieren (nur die angezeigte Seite) und Alle Daten exportieren.

Gelöschte Geräte werden zunächst in den Papierkorb verschoben (`Geräte` → `Papierkorb`). Dort stehen zusätzlich die Spalten Gelöscht am und Gelöscht von zur Verfügung.

Für Version 26.4.0

Gerät in Organisation verschieben

Eingeschriebene Geräte können von einer Quell-Organisation in eine Ziel-Organisation verschoben werden. In diesem Prozess werden die benutzer- und organisationsspezifischen Gerätedaten der Quell-Organisation angepasst bzw. entfernt.

Voraussetzungen

- Mindestens Relution Version `5.23.0`
- Die Funktionalität steht nur in der Store-Organisation zur Verfügung
- Der ausführende Nutzer benötigt die Berechtigung für das Aktualisieren von Geräten
- Die Ziel-Organisation verfügt über eine gültige Lizenz für Geräte, die nicht überschritten ist. Ausgenommen sind Geräte, deren Seriennummer einer Lifetime-Lizenz → zugeordnet ist.
- Apple-Geräte: Die Ziel-Organisation verwendet dasselbe APNs-Zertifikat, mit dem das Gerät eingeschrieben ist. Das kann auch ein von der übergeordneten Organisation übernommenes Zertifikat sein.
- Unterstützte Plattformen
  - Android Legacy
  - Apple (iOS, iPadOS, macOS, tvOS)
  - Interactive Whiteboards
  - Windows

Ist eine Voraussetzung für ein Gerät nicht erfüllt, wird dieses Gerät nicht verschoben, die übrigen ausgewählten Geräte dagegen schon.

Für Version 26.4.0

Anpassung der Gerätedaten

Benutzer- und organisationsspezifische Daten können nicht in eine andere Organisation verschoben werden. Daher werden entsprechende Daten entweder von dem Gerät gelöscht oder für die Ziel-Organisation angepasst.

Noch nicht abgeschlossene Aktionen des Geräts werden vor dem Verschieben abgebrochen.

Folgende Daten werden immer gelöscht:

- Alle Aktionen des Geräts
- Alle zugewiesenen Regelwerke
- Der zugewiesene Nutzer
- Alle ausgestellten Bildungszertifikate

Folgende Daten werden gelöscht, sofern sie zur Quell-Organisation gehören:

- Ausgestellte Gerätezertifikate
- Informationen bzgl. der Ausleih-Funktionalität
- Zugewiesene Zonen
- Zugewiesene iBeacons

Entsprechende Daten der Store-Organisation bleiben erhalten. Wird ein Gerät aus der Store-Organisation verschoben, bleiben diese Daten daher vollständig erhalten.

Weitere Anpassungen für die Geräte werden in den folgenden Abschnitten beschrieben.

Anpassungen für alle Plattformen

Gerätegruppen

- Das Gerät wird von statischen und dynamischen lokalen Gerätegruppen der Quell-Organisation entfernt.
  - Verlässt das Gerät eine Gerätegruppe, werden die zugewiesenen Richtlinien eliminiert.
- Das Gerät wird zu passenden dynamischen lokalen Gerätegruppen der Ziel-Organisation hinzugefügt.
  - Betritt das Gerät eine Gerätegruppe, werden die darin enthaltenen Richtlinien auf diesem angewendet.
- Das Gerät wird nicht von öffentlichen Gerätegruppen entfernt.

Gerätehistorie

- Die Historie des Geräts wird vollständig gelöscht.
- Zusätzlich wird ein neuer Eintrag für das erfolgreiche Verschieben in die Ziel-Organisation erstellt.

Einschreibung

- Einzel-Einschreibungen werden in die Ziel-Organisation verschoben.
- Für Multi-Einschreibungen wird eine neue, nicht verwendbare Einzel-Einschreibung in der Ziel-Organisation erstellt.
- Zusätzlich werden verknüpfte Benutzer, Regelwerke, Richtlinien und Benachrichtigungen vom Gerät entfernt.
- Eine Zuordnung zu einer automatischen Einschreibung, z. B. über die Automatische Geräteregistrierung (ADE, im Portal: DEP), bleibt nur erhalten, wenn sie aus der Store-Organisation stammt.

Für Version 26.4.0

Anpassungen für Windows

- Die Historie lokaler Skripte der Quell-Organisation wird vom Gerät entfernt. Die Historie öffentlicher Skripte und der Skripte aus der Meta-Organisation bleibt erhalten.

Anpassungen für Apple

- Lizenzen aus Apps und Bücher (im Portal: VPP), die zu einem VPP-Token der Quell-Organisation (lokale VPP-Token) gehören, werden vom Gerät entfernt.
- Lizenzen, die zu einem VPP-Token der Store-Organisation gehören, werden in die Ziel-Organisation verschoben.
- Lizenzen, die zu einem VPP-Token einer Meta-Organisation → gehören, werden in die Ziel-Organisation verschoben, wenn Quell- und Ziel-Organisation derselben Meta-Organisation angehören. Andernfalls werden sie vom Gerät entfernt.
- Managed Media wird nicht vom Gerät entfernt und wird in der Ziel-Organisation zu sehen sein.
  - Mit Ausnahme, wenn die Managed Media über eine Konfiguration angewendet wurde und das Gerät die zugehörige Gerätegruppe verlässt.
  - Managed Media aus der Quell-Organisation kann auch in der Ziel-Organisation vom Gerät entfernt werden.
- Das Supervision-Zertifikat kann nicht in die Ziel-Organisation verschoben werden. Das Zertifikat kann vom verschobenen Gerät nur heruntergeladen werden, wenn die Berechtigung zum Lesen von Geräten sowohl in der Ziel-Organisation als auch in der Organisation besteht, zu der das Zertifikat gehört (in der Regel die Quell-Organisation).

Ablauf

Im Geräteinventar der Store-Organisation können ein oder mehrere Geräte in eine Ziel-Organisation verschoben werden. Zuerst müssen die Geräte selektiert werden, danach kann der Eintrag Verschieben des 3-Punkte-Menüs angeklickt werden. Für ein einzelnes Gerät steht der Eintrag auch im 3-Punkte-Menü der jeweiligen Gerätezeile zur Verfügung. Der Eintrag ist nicht verfügbar, wenn die Auswahl gelöschte Geräte, Geräte mit dem Status `WITHDRAWN` oder Geräte einer nicht unterstützten Plattform enthält.

Im Dialog muss eine Ziel-Organisation ausgewählt werden. Im Allgemeinen können Geräte in alle Organisationen außer in die Store-Organisation, die System-Organisation, Meta-Organisationen und die Quell-Organisation verschoben werden. Meta-Organisationen werden zwar zur Auswahl angezeigt, das Verschieben dorthin wird jedoch abgelehnt und die Geräte verbleiben in ihrer bisherigen Organisation. Wenn nur Geräte aus einer einzigen Organisation selektiert sind, wird diese Organisation nicht in dem Dialog angezeigt. Wenn Geräte aus mehreren Organisationen selektiert sind, so können diese auch ausgewählt werden. Geräte, die bereits zu der Ziel-Organisation gehören, werden nicht berücksichtigt.

Der zweite Dialogschritt enthält eine Informationsbox mit Hinweisen über die möglichen Konsequenzen sowie einen Link auf die Dokumentation.

Nach der Bestätigung werden die ausgewählten Geräte in die Ziel-Organisation verschoben. Jedes Gerät wird dabei einzeln verschoben. Kann ein Gerät nicht verschoben werden, verbleibt es in seiner bisherigen Organisation, z. B. wenn die Ziel-Organisation keine freie Gerätelizenz hat oder bei Apple-Geräten das APNs-Zertifikat der Ziel-Organisation nicht mit dem der Quell-Organisation übereinstimmt. Das Portal zeigt dazu keine Fehlermeldung an. Das Ergebnis sollte daher im Geräteinventar in der Spalte Organisation geprüft werden.

Für Version 26.4.0

Ausleihe

Das Relution-Ausleihsystem unterstützt Schulen bei der effizienten Verwaltung von Leihgeräten. Das System ermöglicht es Administratoren, Ausleihbedingungen festzulegen, Ausleihzeiträume zu verfolgen und den Gerätestatus zu überwachen.

Ziel ist ein transparenter, sicherer und reibungsloser Ablauf der Geräteausgabe und -rücknahme.

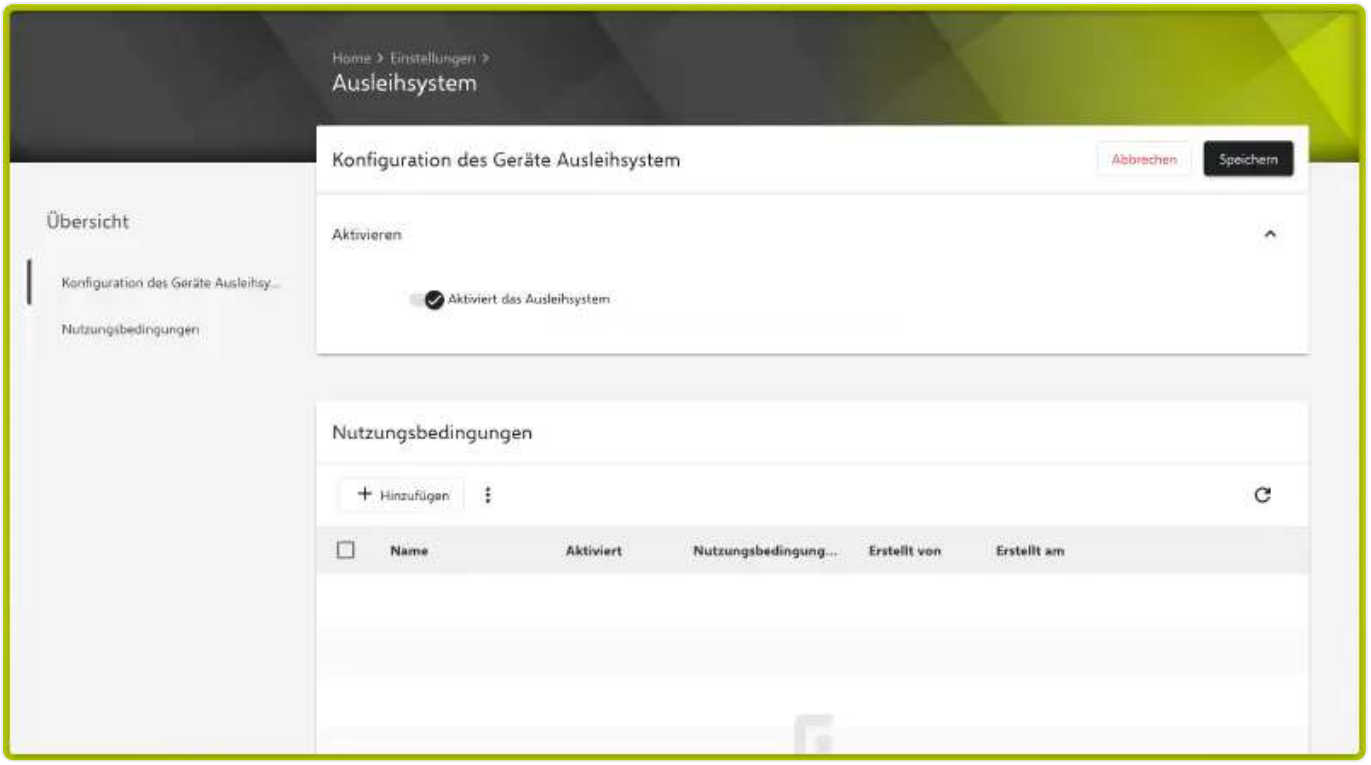
Neu hinzugekommen ist die Möglichkeit der Geräterücknahme mit der Relution Assets App, siehe Assets →.

Ausleihsystem aktivieren

Das Ausleihsystem kann in Relution im gewünschten Mandanten unter folgendem Pfad aktiviert werden:

`Einstellungen` → `Ausleihsystem`

In der globalen Organisation steht das Ausleihsystem nicht zur Verfügung.



Nutzungsbedingungen

Bevor Geräte an Schüler oder Lehrkräfte ausgegeben werden, sollten klare Nutzungsbedingungen definiert sein.

Dazu zählen unter anderem:

- allgemeine Rahmenbedingungen
- Regelungen zur Übergabe und Rückführung von Leihgeräten
- Haftung im Schadens- oder Verlustfall
- initiale Einrichtung und Konfiguration der Geräte
- Einhaltung von Datenschutz- und Jugendschutzbestimmungen

Diese Bedingungen lassen sich in Relution unter `Einstellungen` → `Ausleihsystem` (Bereich Nutzungsbedingungen, Schaltfläche Nutzungsbedingung hinzufügen) hinterlegen und zur besseren Lesbarkeit mit Markdown formatieren.

Es ist möglich, mehrere Nutzungsvarianten zu speichern, die bei der Ausleihe ausgewählt werden können.

Die dokumentierten Nutzungsbedingungen stehen im weiteren Ausleihprozess zur Verfügung und können bei jeder Ausleihe ausgewählt werden. So ist jederzeit nachvollziehbar, unter welchen Voraussetzungen ein Gerät verliehen wurde.

Zur Auswahl stehen nur Nutzungsbedingungen, die mit dem Schalter Aktiviert freigeschaltet sind. Der Text einer Nutzungsbedingung lässt sich nach dem Anlegen nicht mehr ändern, beim Bearbeiten sind nur noch Name und Aktivierung änderbar. Für eine neue Fassung wird eine neue Nutzungsbedingung angelegt und die alte deaktiviert.

Ergänzend kann beim Verleihen ein unterschriebenes Dokument, z. B. ein physischer Leihvertrag, im Feld Unterschrift hochgeladen werden.

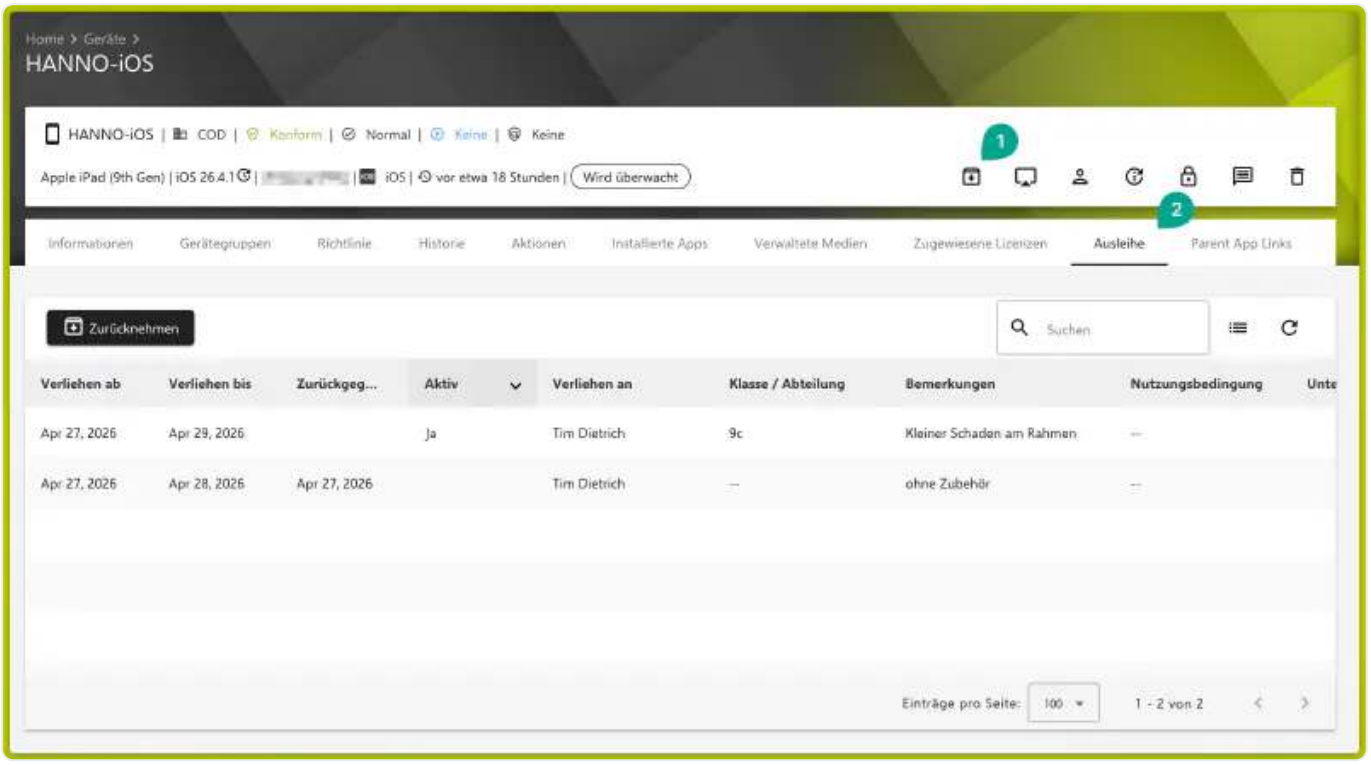
Ausleihe von Geräten

Für Version 26.4.0

Um die Ausleihe in Relution systemisch abzubilden, lassen sich Geräte im Inventar verleihen.

Dazu stehen in den Gerätedetails zwei Einstiege zur Verfügung:

- Schnellzugriff Gerät verleihen in der Infobox (1)
- Reiter Ausleihe mit der Schaltfläche Verleihen (2)



Im anschließenden Dialog wird der Ausleihzeitraum über die Pflichtfelder Verliehen ab (vorbelegt mit dem aktuellen Datum) und Verliehen bis definiert. Die Leihfrist gilt bis zum Ende des unter Verliehen bis gewählten Tages.

Das Gerät wird einem Schüler oder Lehrer zugeordnet. Im Pflichtfeld Verliehen an wird der Name des Ausleihers eingetragen.

Über eine Vorschlagsfunktion lassen sich bereits eingegebene Namen sowie vorhandene Relution Benutzer auswählen.

Optional lässt sich im Feld Klasse / Abteilung die Klasse oder Abteilung des Ausleihers eintragen. Auch hier werden bereits verwendete Einträge vorgeschlagen.

Weitere Angaben bei der Ausleihe

Im Feld Bemerkungen lassen sich Kommentare hinterlegen, beispielsweise:

- Zweck der Ausleihe
- Maßnahme oder Projekt
- Hinweise zum Zustand des Geräts

Wird Zubehör wie ein Netzteil, eine Hülle oder ein Stift ausgegeben, kann dies dokumentiert und bei der Rückgabe geprüft werden.

Zusätzlich lassen sich:

- hinterlegte Nutzungsbedingungen im Feld Nutzungsbedingung auswählen
- im optionalen Feld Unterschrift ein unterschriebenes Dokument (z. B. der Leihvertrag) als PDF, JPG oder PNG hochladen

Im Reiter Ausleihe der Gerätedetails ist eine laufende Ausleihe in der Spalte Aktiv markiert. Das Gerät steht bis zur Rückgabe nicht zur Verfügung und kann erst danach erneut verliehen werden. Der Reiter zeigt außerdem den gesamten Ausleihverlauf des Geräts mit den erfassten Angaben, z. B. Verliehen an, Klasse / Abteilung, Nutzungsbedingung, Unterschrift (zum Herunterladen) und Verliehen von.

Für Version 26.4.0

In der Inventarübersicht erkennt man verliehene Geräte an den Spalten Verliehen an und Verliehen bis. Diese sind standardmäßig ausgeblendet und können über die Spaltenauswahl eingeblendet werden.

Rücknahme von Geräten

Die Rückgabe erfolgt ebenfalls über die Gerätedetailseite:

- Schnellzugriff Gerät zurücknehmen in der Infobox
- Reiter Ausleihe mit der Schaltfläche Zurücknehmen

Im anschließenden Dialog sind die Angaben der Ausleihe gesperrt, nur das Feld Bemerkungen lässt sich noch ändern. Mit Zurückgeben wird die Rücknahme bestätigt, als Rückgabedatum wird der aktuelle Zeitpunkt gespeichert.

Nach erfolgreicher Rückgabe ist die Ausleihe im Reiter Ausleihe nicht mehr als aktiv markiert, in der Spalte Zurückgegeben wird das Rückgabedatum angezeigt.

Das Gerät steht anschließend wieder als Leihgerät zur Verfügung und kann erneut verliehen werden.

Überschrittene Leihfrist

Wird die Leihfrist überschritten und das Gerät nicht rechtzeitig zurückgegeben, erscheint die Datumsangabe Verliehen bis in der Inventarübersicht und im Reiter Ausleihe rot markiert. Zusätzlich zeigt ein Glockensymbol mit dem Tooltip Leihfrist überschritten neben dem Gerätenamen in der Inventarliste die überschrittene Frist an.

Ist die Leihfrist abgelaufen, erhält das Gerät automatisch die Konformitätsverletzung Leihfrist überschritten und gilt als nicht konform. Relution prüft das regelmäßig (standardmäßig stündlich) sowie beim Speichern eines Leihvorgangs. Wird das Gerät zurückgenommen, wird die Verletzung wieder entfernt.

Regeln für überschrittene Leihfristen

Weitere automatische Reaktionen werden über eine dynamische Gerätegruppe mit Aktionen eingerichtet: Die Gruppe filtert auf Konformitätsverletzungen mit dem Wert Leihfrist überschritten (alternativ auf Verliehen bis), und die Gruppenaktionen werden für die Geräte dieser Gruppe ausgeführt, z. B. sobald ein Gerät in die Gruppe aufgenommen wird. Siehe Gerätegruppen → und Aktionen mit Gerätegruppen →.

Über Gruppenaktionen lassen sich folgende Reaktionen an diesen Status knüpfen:

- Über eine Benachrichtigungsaktion mit der Option Andere Benutzer benachrichtigen können Administratoren automatisch informiert werden.
- Über eine Geräteaktion können Leihgeräte gesperrt oder auf den Werkszustand zurückgesetzt werden.

Damit wird eine sichere und kontrollierte Nutzung der Leihgeräte gewährleistet.

Für Version 26.4.0

Zubehör erfassen

Relution bietet die Möglichkeit, unter Benutzerdefinierte Geräteeigenschaften → bis zu fünf zusätzliche Felder individuell zu definieren.

Beispiele:

- Netzteile
- Taschen
- Stifte
- Adapter
- weiteres Zubehör

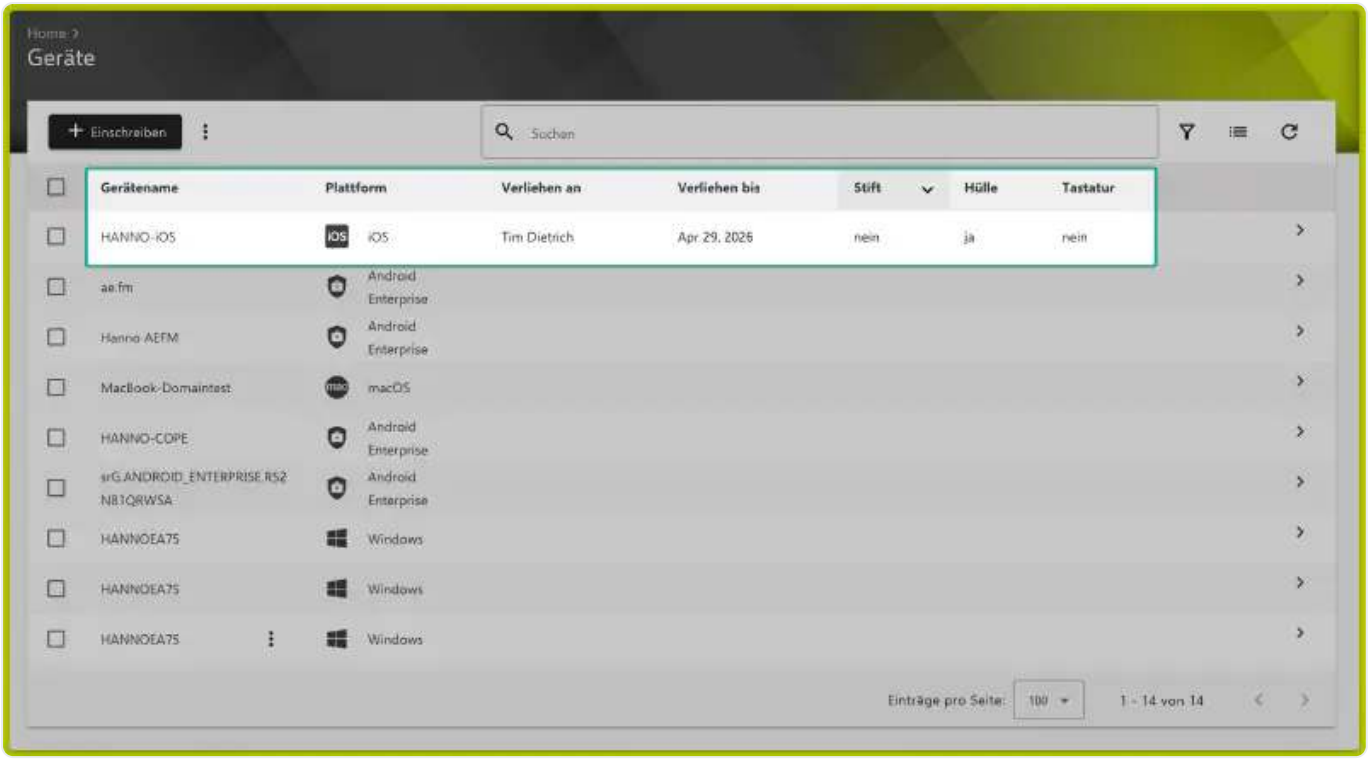
Diese definierten Eigenschaften sind in den Gerätedetails einstellbar und lassen sich bei der Rückgabe gezielt prüfen.

Sobald benutzerdefinierte Geräteeigenschaften aktiviert sind, werden diese in den Gerätedetails unter Informationen am unteren Seitenbereich angezeigt.

Aktivierte benutzerdefinierte Geräteeigenschaften lassen sich außerdem in der Inventarübersicht im Relution Portal einblenden.

So lässt sich komfortabel erfassen, welches Zubehör zu einem Gerät gehört. Bei der Rücknahme kann schnell geprüft werden, ob alle ausgegebenen Gegenstände vollständig zurückgegeben wurden.

Home > Einstellungen >
Benutzerdefinierte Geräteeigenschaften
Benutzerdefinierte Geräteeigenschaften
Allgemein
Folgende Benennungen der Eigenschaften werden lediglich für die Anzeige im Portal verwendet. Das Deaktivieren einzelner Eigenschaften hat zur Folge, dass diese in den anderen Ansichten ausgeblendet werden
Aktiviert
Benutzerdefiniert 1
Hülle
Aktiviert
Benutzerdefiniert 2
Stift
Aktiviert



Für Version 26.4.0

Benutzerdefinierte Geräteeigenschaften

Unter `Einstellungen` → `Benutzerdefinierte Geräteeigenschaften` stehen fünf frei benennbare Freitext-Felder (`Benutzerdefiniert 1` – `5`) zur Verfügung, mit denen sich Geräte um eigene Informationen ergänzen lassen – zum Beispiel Kostenstelle, Standort oder mitgeliefertes Zubehör.

Felder aktivieren und benennen

Jedes der fünf Felder besitzt einen eigenen Ein-/Ausschalter sowie ein editierbares Label. Das Label lässt sich erst eingeben, wenn das Feld aktiviert ist. Ist ein aktiviertes Feld ohne Label gespeichert, erscheint es überall mit dem Standardnamen (z. B. Benutzerdefiniert 1). Die Benennung dient ausschließlich der Anzeige im Portal; das Deaktivieren eines Feldes blendet es in allen Ansichten wieder aus. Die an den Geräten gespeicherten Werte bleiben dabei erhalten.

> Es gibt keine Feldtypen (Zahl, Datum, Auswahlliste etc.) – alle fünf Felder sind reine Freitextfelder.

Verwendung

Für Version 26.4.0

Aktivierte Felder stehen an folgenden Stellen zur Verfügung:

- Geräte-Detailansicht: eigene Karte Benutzerdefinierte Eigenschaften, Werte über das Stiftsymbol direkt editierbar (mit dem Recht zum Bearbeiten von Geräten).
- Einschreibungen und Auto-Einschreibungen: im Formular ein Eingabefeld pro aktiviertem Feld, in der Liste als einblendbare Spalte. Die hinterlegten Werte werden bei der Einschreibung auf das Gerät übernommen.
- Inventarliste: als optional einblendbare Tabellenspalten und als Filter mit Mehrfachauswahl aus den vorhandenen Werten, siehe Inventarübersicht →.
- CSV: Export aus der Geräte- und der Auto-Einschreibungsliste (Spalten `custom1` – `custom5`); Aktualisierung bestehender Geräte und Auto-Einschreibungen über Aktualisieren via CSV (Zuordnung per Seriennummer, Spaltenkopf = vergebenes Label oder `custom1` – `custom5`, leere Zellen ändern nichts).
- Dynamische Gerätegruppen: als Filterkriterium, mit dem hier vergebenen Label als Anzeigename.
- Platzhalter: `${device.custom1}` bis `${device.custom5}`, z. B. in Gerätenamen, siehe Erweiterte Platzhalter →.

Ein Anwendungsbeispiel findet sich unter Ausleihe: Zubehör erfassen →.

Geräte-Logs herunterladen

Debug-Logs für einzelne Geräte lassen sich direkt über das Relution Portal aktivieren und herunterladen.

Für einzelne Geräte lassen sich Debug-Logs direkt über das Relution Portal vom Server herunterladen. Dies erleichtert die Fehleranalyse erheblich, da kein direkter Zugriff auf das Dateisystem des Servers mehr nötig ist.

Voraussetzungen

- Organisation: Die Funktion steht nur in der globalen Organisation zur Verfügung.
- Berechtigungen: System-Administrator oder ein Benutzer, dessen Rolle die Berechtigung Logging im Bereich Geräte enthält (nur für die globale Organisation wählbar).

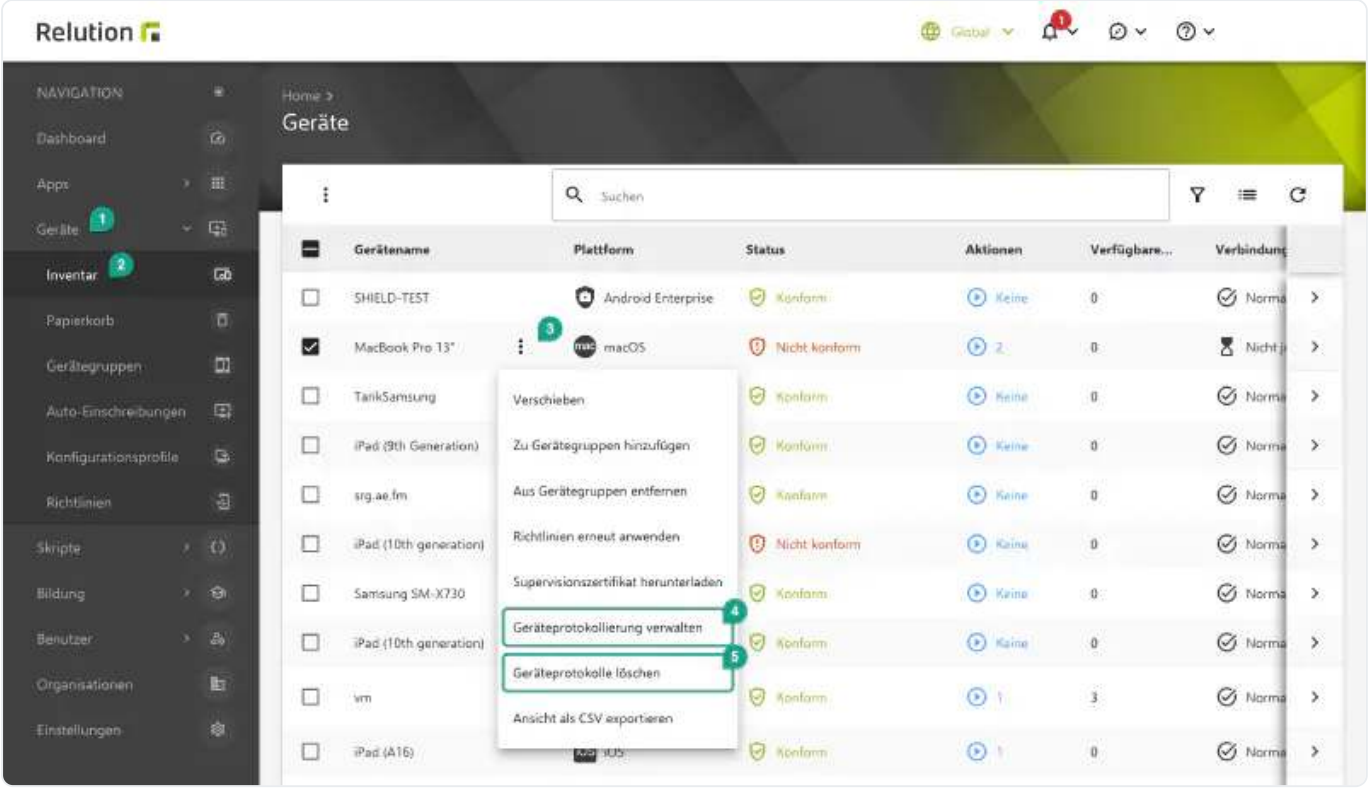
Anleitung

Zum Aktivieren der Protokollierung oder zum Herunterladen vorhandener Logs sind folgende Schritte erforderlich:

1. Anmeldung: Die Anmeldung im Relution Portal erfolgt mit einem Administrator-Konto der globalen Organisation.
2. Geräteauswahl: Unter `Geräte` → `Inventar` wird das entsprechende Endgerät ausgewählt.
3. Kontextmenü öffnen: Das Kontextmenü öffnet sich in der Gerätezeile über das Drei-Punkte-Menü (Aktionen).
4. Protokollierung verwalten: Der Punkt Geräteprotokollierung verwalten öffnet den zugehörigen Dialog.
    - Protokollierung aktivieren: Über den Schalter Gerätebasierte Protokollierung aktivieren wird das Logging eingeschaltet. Im Feld Dauer (in Minuten) wird festgelegt, wie lange das detaillierte Logging aktiv bleibt (Standard: 60 Minuten, Mindestwert: 1). Mit Bestätigen wird die Einstellung übernommen. Bei aktiver Protokollierung zeigt der Dialog Startzeit und Endzeit an. Zum vorzeitigen Beenden wird der Schalter ausgeschaltet und mit Bestätigen übernommen.
    - Download: Im Bereich Geräteprotokolle steht über Download das vom Server für dieses Gerät gesammelte Log-Archiv (ZIP-Datei) bereit. In einer Cluster-Umgebung enthält das Archiv nur dann die Logs aller Instanzen, wenn Spring Boot Admin aktiviert ist; andernfalls werden nur die Logs einer einzelnen Instanz heruntergeladen.
5. Bereinigung: Über den Punkt Geräteprotokolle löschen im Kontextmenü lassen sich die gesammelten Protokolle der ausgewählten Geräte vom Server entfernen.

Die Menüpunkte stehen auch in der Geräteliste einer Gerätegruppe zur Verfügung.

Für Version 26.4.0



Hinweise zur Speicherung

Für Version 26.4.0

- Die Protokolle werden nur im Arbeitsspeicher des Servers gehalten und gehen bei einem Neustart des Servers verloren.
- Pro Gerät wird eine begrenzte Anzahl an Log-Ereignissen gespeichert (standardmäßig 10.000). Bei langer Protokolldauer oder sehr aktiven Geräten werden ältere Meldungen verworfen.
- Einen Tag nach dem Ende der Protokollierung löscht das System die Protokolle automatisch.

DEP konfigurieren

Die Automatische Geräteregistrierung (ADE, im Portal: DEP; früher `Device Enrollment Program`) von Apple bietet Organisationen die Möglichkeit, eigene Apple-Geräte zu registrieren und bereitzustellen. ADE rationalisiert den Prozess der groß angelegten Gerätebereitstellung und -verwaltung, indem es die Vorkonfiguration von Geräten vor deren Verteilung ermöglicht. Die Benutzer erhalten ihre Geräte vollständig konfiguriert und sofort einsatzbereit, während die Daten privat bleiben und das System sicher ist. Alle vorkonfigurierten Einstellungen werden von den Administratoren über die entfernte Verwaltung gesteuert, und die Konformität wird drahtlos aufrechterhalten, so dass nie ein manueller Eingriff vor Ort erforderlich ist.

ADE-kompatible Geräte

Alle iPhones, iPads, Mac-Computer oder Apple TVs, die am oder nach dem 1. März 2011 entweder direkt bei Apple oder bei einem teilnehmenden autorisierten Apple-Händler gekauft wurden, können für ADE angemeldet werden. Auf iPhones und iPads muss iOS/ iPadOS 7 oder neuer laufen, Mac-Computer müssen OS X 10.9 oder neuer verwenden, und Apple TVs müssen tvOS 10.2 oder neuer nutzen. Auch Apple Vision Pro (visionOS) lässt sich über ADE in Relution einschreiben. Apple-Geräte lassen sich mit dem `Apple Configurator` zu ADE hinzufügen, unabhängig davon, wo die Geräte gekauft wurden. Wird ein Apple-Gerät eingerichtet, das manuell registriert wurde, verhält es sich wie jedes andere registrierte Gerät mit obligatorischer Überwachung (Supervision) und MDM-Registrierung (Mobile Device Management). Für Apple-Geräte, die nicht direkt gekauft wurden, haben Benutzer eine 30-tägige Übergangsfrist, um das Gerät aus der MDM-Registrierung und Überwachung zu entfernen.

Für Version 26.4.0

Vorteile von ADE

Der größte Vorteil von ADE ist die Einfachheit des automatischen Registrierungsprozesses. Dieser Prozess stellt sicher, dass alle Apple-Geräte gemäß den Anforderungen der eigenen Organisation konfiguriert sind, und es wird ebenfalls garantiert, dass alle Benutzer dieselben Apps, Einstellungen, Einschränkungen und Berechtigungen auf ihren Geräten haben, bevor diese überhaupt an sie ausgegeben werden.

Weitere Vorteile

- Installation von MDM-Profilen, die Benutzer nicht entfernen können, sodass die Geräte dauerhaft fernverwaltet bleiben. Dazu wird im DEP-Profil die Option Benutzer darf MDM-Einschreibung entfernen deaktiviert (standardmäßig aktiviert).
- Möglichkeit, die Überwachung (Supervision) drahtlos zu aktivieren.
- Vorkonfiguration einer Ersteinrichtung, die zeitaufwändige Probleme für Endanwender vermeidet.
- Stille App-Installation und Push-Funktionen.
- Mehr Kontrolle für die IT-Abteilung.
- Weniger Sicherheitsprobleme.

Überwachte iOS-Geräte, DEP und MDM →

Migration von Geräten über Apple Configurator

`Apple Configurator` ist eine Lösung für kleine Organisationen, die nur wenige Apple-Geräte zu verwalten haben oder nur eine Grundkonfiguration für ihre Geräte benötigen. Da `Apple Configurator` keine drahtlosen Funktionen bietet, müssen die mit `Apple Configurator` verwalteten Geräte physisch mit einem Mac-Computer verbunden werden, um Änderungen vornehmen zu können. Dies kann für Organisationen, die einen praktischen Ansatz benötigen, von Vorteil sein.

Die Migration von `Apple Configurator` zu ADE mit Relution ist die Lösung für Organisationen jeder Größe, die ein benutzerfreundliches System für die Verwaltung einer beliebigen Anzahl von mobilen Apple-Geräten wünschen. Durch die Migration steht eine benutzerfreundliche und drahtlose Lösung mit fortschrittlichen Funktionen zur Verfügung, die an die Bedürfnisse von Organisationen jeder Größe angepasst werden können.

DEP-Geräte mit Apple Configurator 2 hinzufügen →

Restriktionen für die Aufnahme von Geräten in ADE

Apple-Geräte, die am oder nach dem 1. März 2011 gekauft wurden, können nach dem Zurücksetzen auf die Werkseinstellungen bei ADE angemeldet werden. Die einzige weitere Einschränkung ist, dass das Gerät innerhalb von drei Jahren nach dem Kaufdatum in ADE registriert werden muss.

Für Version 26.4.0

Geräte aus ADE entfernen

Geräte lassen sich jederzeit aus ADE entfernen. Beschädigte, verlorene oder gestohlene Geräte können und sollten so schnell wie möglich aus ADE entfernt werden. Sobald ein Gerät aus ADE entfernt wurde, kann es nicht mehr automatisch über den Händler zugeordnet werden; eine erneute Aufnahme ist nur manuell über den `Apple Configurator` möglich.

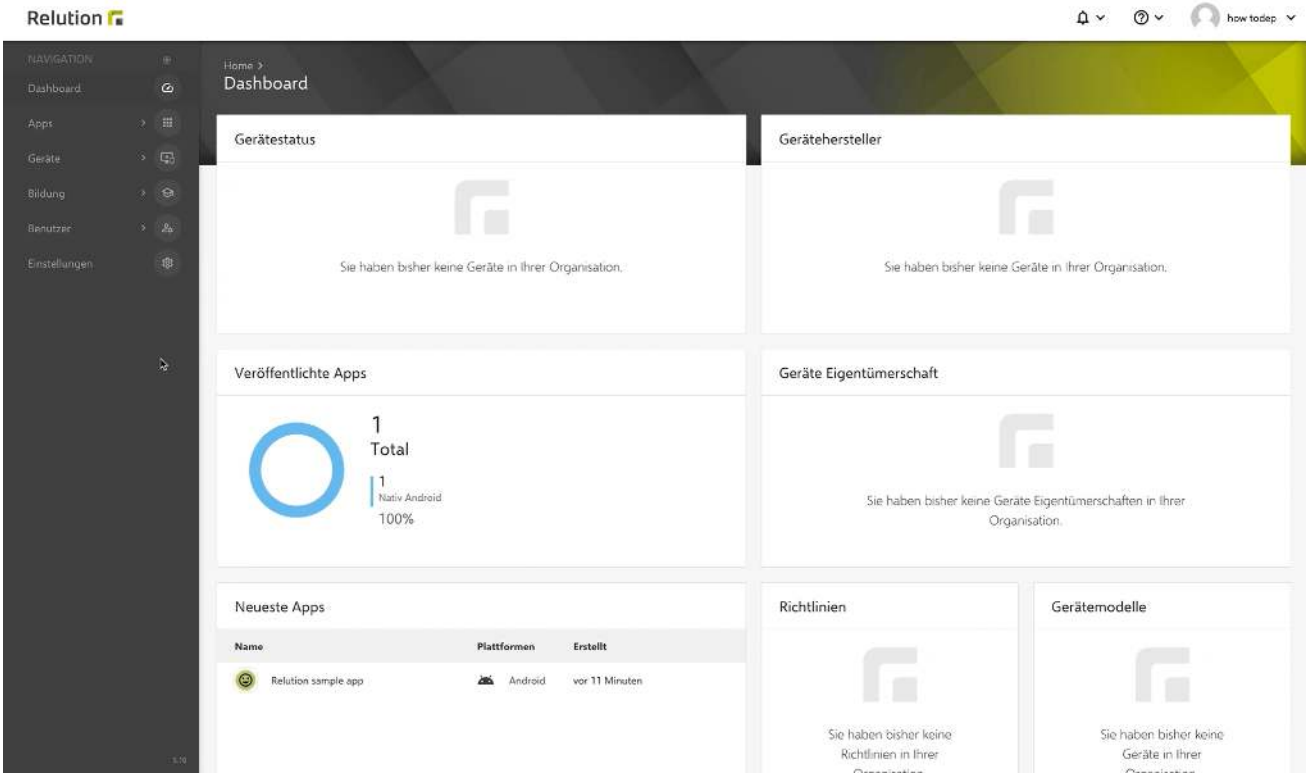
Geräte von autorisierten Händlern zu ADE hinzufügen

ADE funktioniert mit Apple-Geräten, die ADE unterstützen, wenn sie von autorisierten Händlern und Netzbetreibern erworben wurden. Vor dem Kauf eines Apple-Geräts empfiehlt sich eine Rückfrage beim Händler. Für die Registrierung bei Apple für ADE muss eine Apple-Kundennummer oder eine DEP-Händler-ID eingegeben werden. Wenn ein Wiederverkäufer diese Nummer nicht hat, ist kein Zugang zu ADE möglich.

Einrichtung

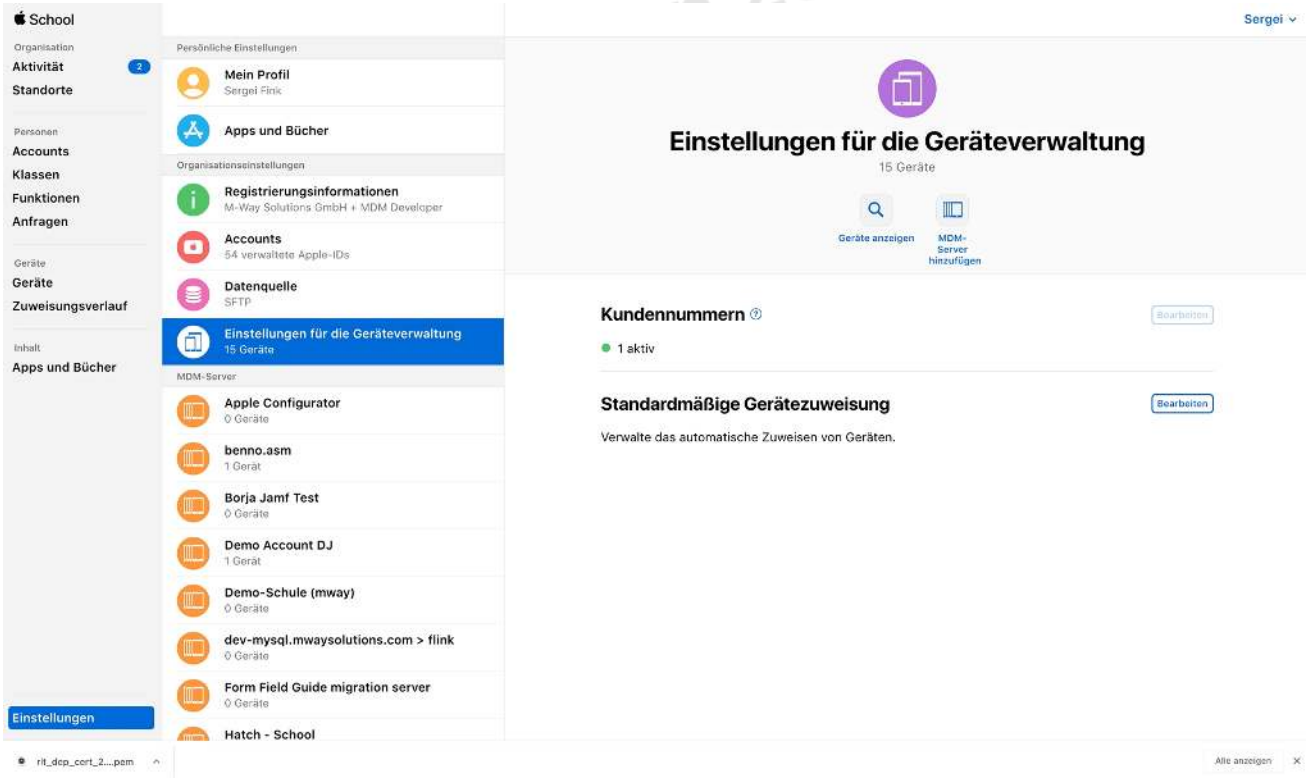
Das DEP-Konto wird in Relution unter `Einstellungen` → `Apple Automated Device Enrollment` (Bereich Geräteplattformspezifisch) eingerichtet.

1. Server-Zertifikat in Relution über Zertifikat herunterladen herunterladen.

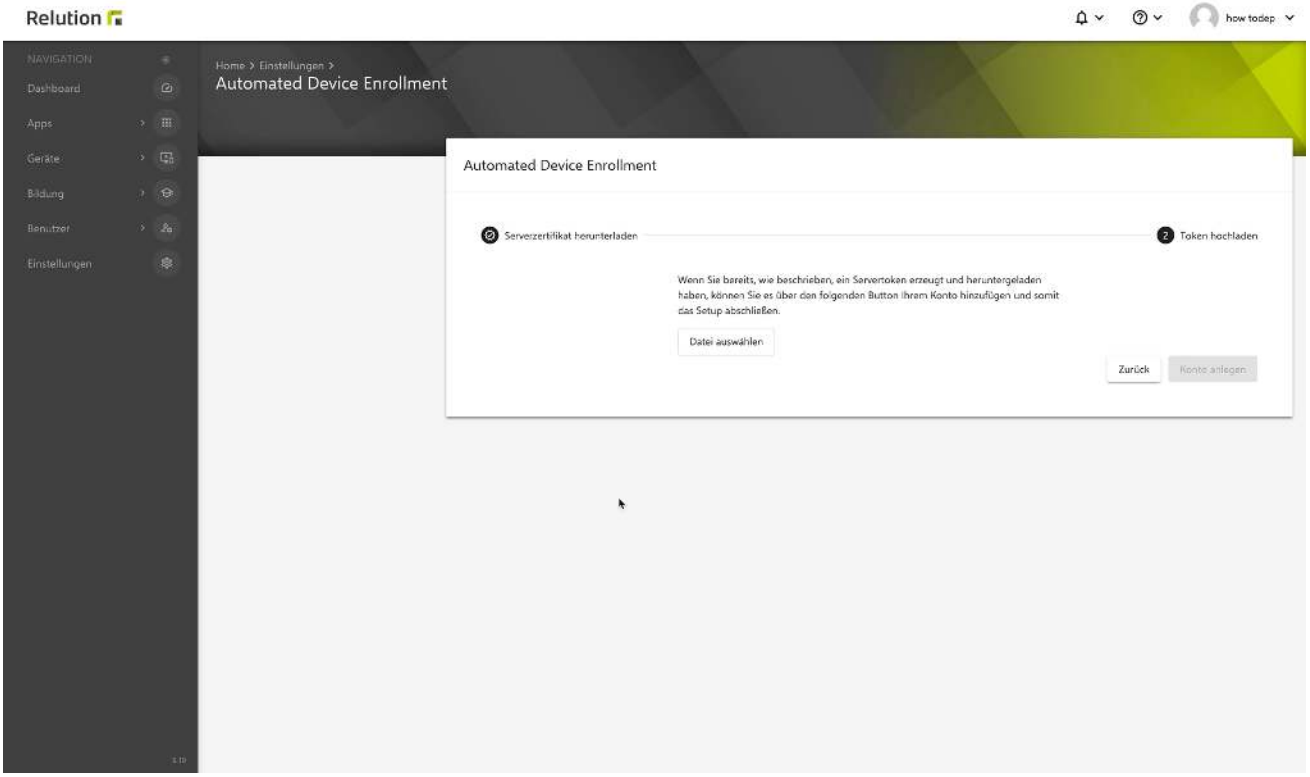


2. MDM Server im Apple School/ Business Manager erstellen.

3. Zertifikat hochladen und Token herunterladen.



4. Token in Relution über Token hochladen hochladen und die Gültigkeit prüfen.



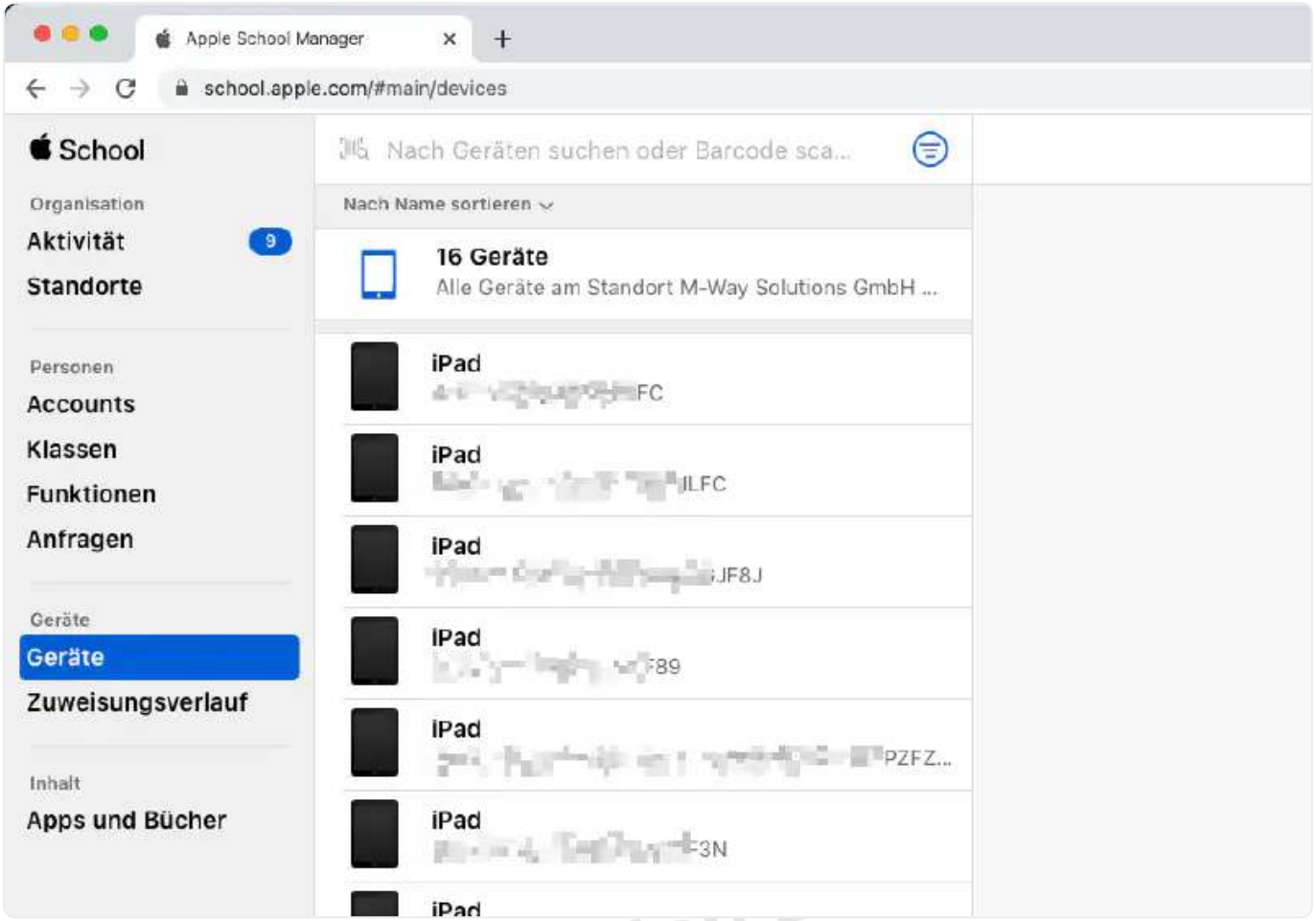
Häufige Fehlerquellen beim Token-Upload, die Dateiendungen im Überblick und Gründe für einen vorzeitigen Gültigkeitsverlust sind unter Wichtige Hinweise zur Fehlervermeidung → zu finden.

Das DEP-Token ist ein Jahr gültig und muss danach erneuert werden. Das Vorgehen ist unter DEP-Token (Server-Token) verlängern → beschrieben.

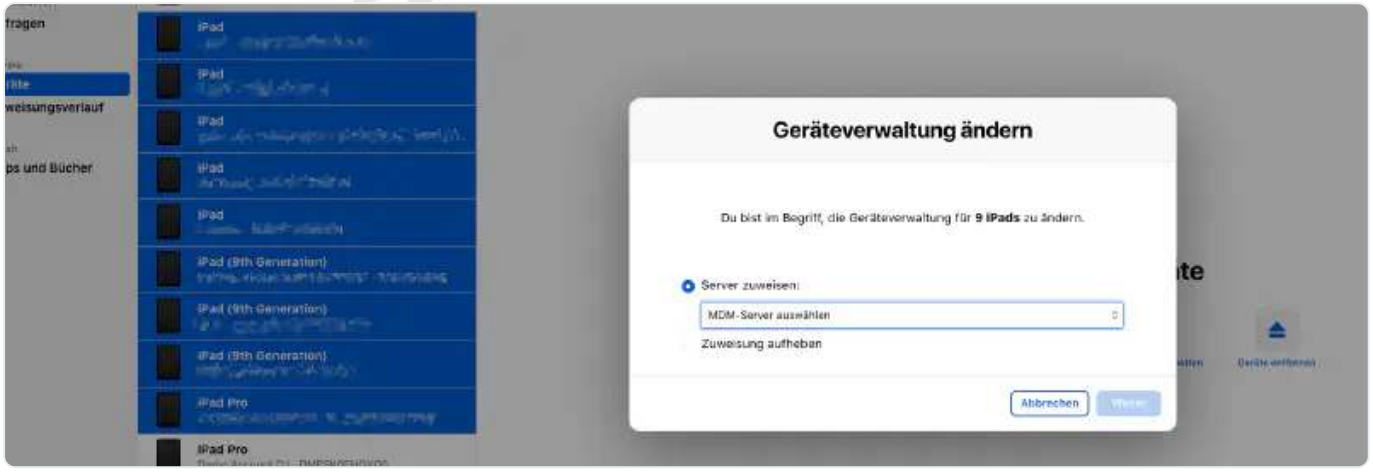
Für Version 26.4.0

Geräte dem MDM-Server zuweisen

Für die Zuweisung von Apple-Geräten zum MDM-Server im Apple School/Business Manager ist ein Zugang mit entsprechenden Berechtigungen notwendig. Im Apple School/ Business Manager wird in den Bereich Geräte gewechselt.



Die gewünschten Geräte werden markiert und dem entsprechenden Server zugewiesen.



Geräte synchronisieren

Im Anschluss werden die Apple-Geräte in Relution unter `Geräte` → `Auto-Einschreibungen` sichtbar. Relution synchronisiert die Geräte standardmäßig einmal täglich automatisch (nachts gegen 3:00 Uhr Serverzeit). Über die Schaltfläche Geräte synchronisieren wird die Synchronisierung sofort angestoßen; dabei werden alle eingerichteten Dienste zur automatischen Einschreibung synchronisiert.

Wurde vorher ein DEP-Profil erstellt und mit Als Standardprofil verwenden markiert, wird es den neuen Geräten bei der Synchronisierung automatisch zugewiesen. Andernfalls wird das DEP-Profil manuell über Profil auswählen zugewiesen – ein DEP-Profil ist zwingend erforderlich. DEP-Profile werden unter `Geräte` → `Konfigurationsprofile` angelegt, siehe Konfigurationsprofil für ADE →.

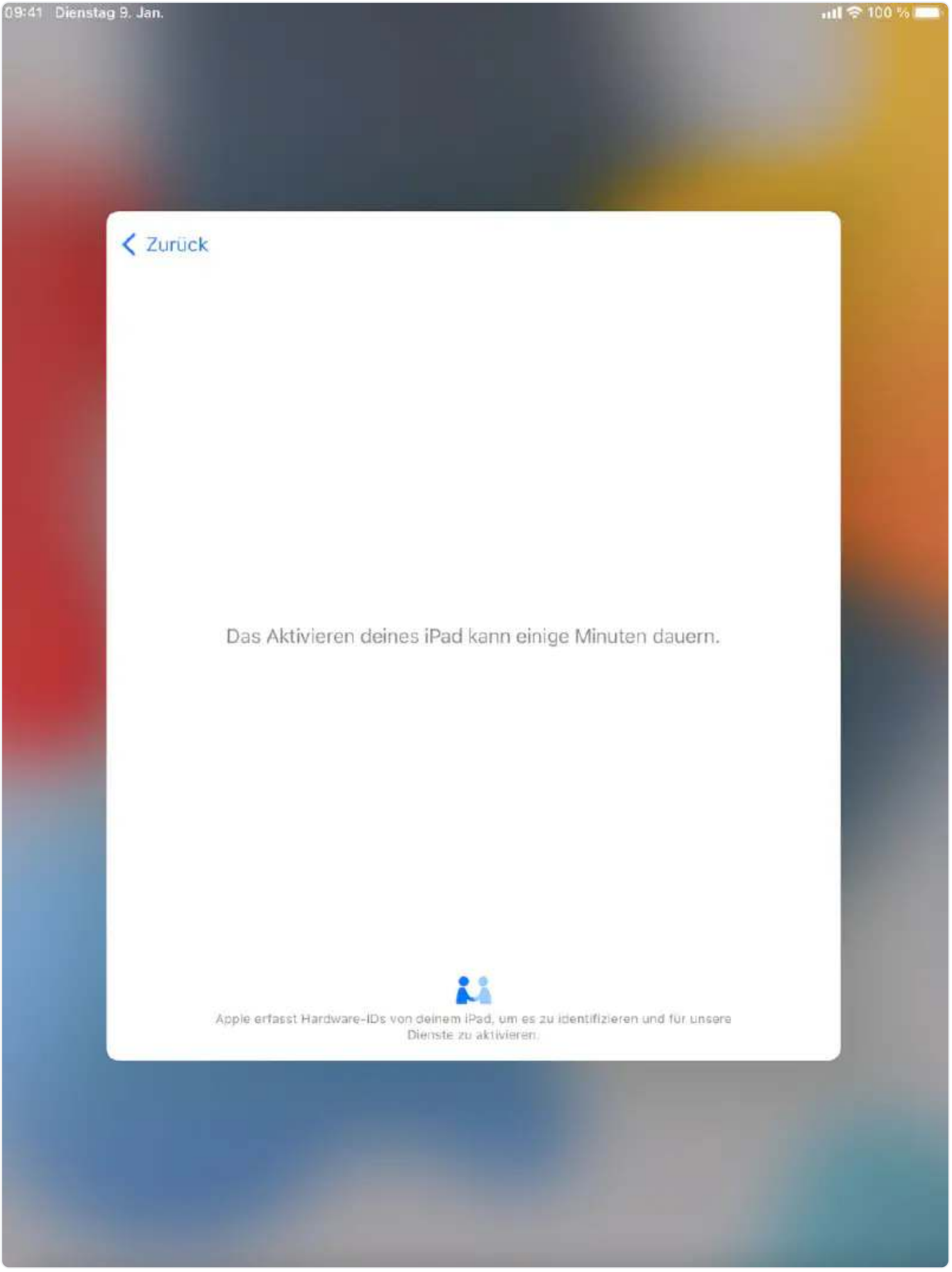
Für markierte Geräte stehen in den Auto-Einschreibungen außerdem folgende Aktionen zur Verfügung:

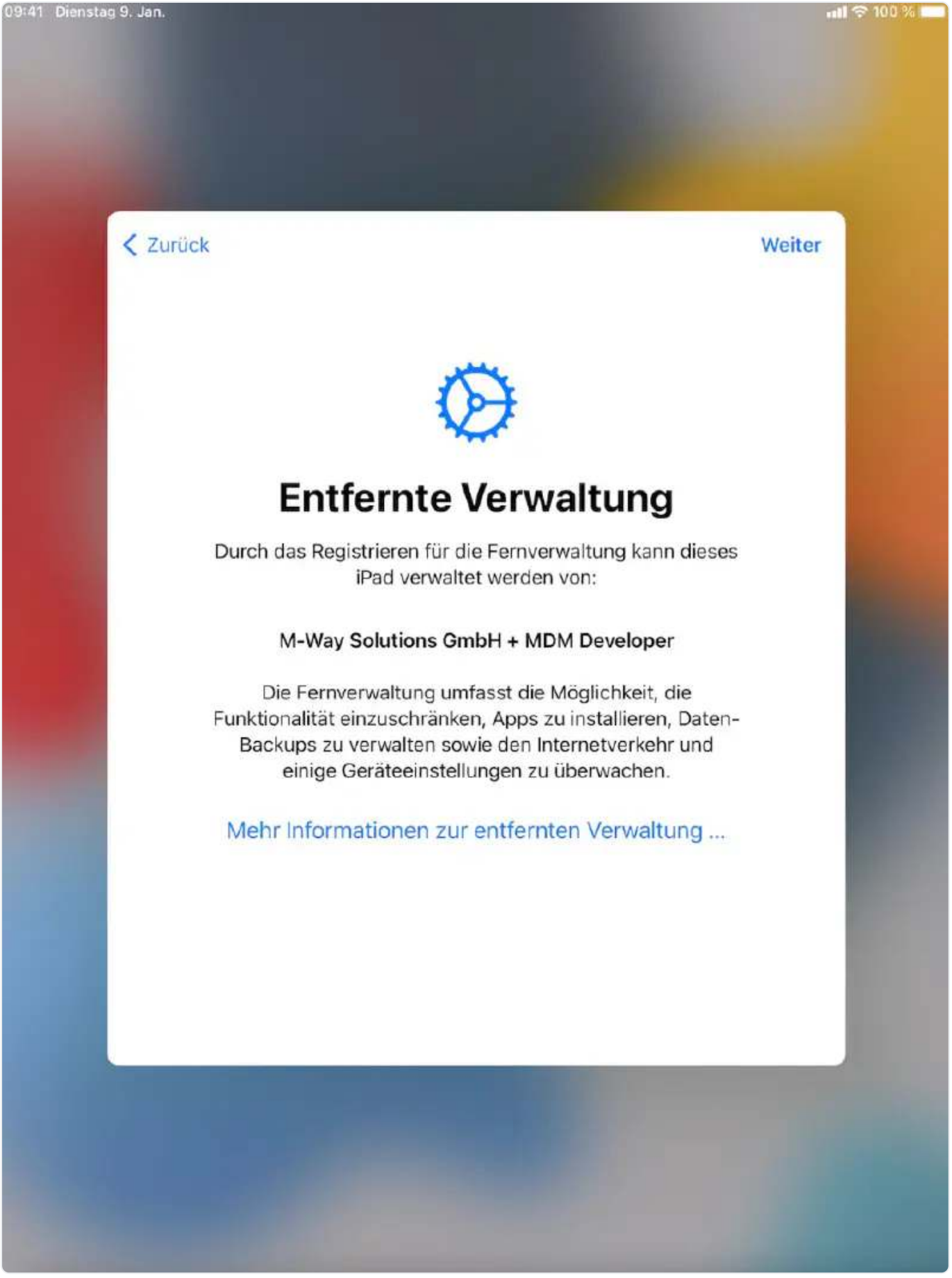
- Benutzer zuweisen und Benutzer entfernen: Ordnet den Geräten einen Benutzer zu bzw. hebt die Zuordnung auf.
- Benutzer als Gerätenamen verwenden: Übernimmt den Namen des zugewiesenen Benutzers als Gerätenamen.
- Zu Gerätegruppen hinzufügen und Aus Gerätegruppen entfernen: Ordnet die Geräte statischen Gerätegruppen zu. Die Richtlinien dieser Gruppen werden bei der Einschreibung automatisch angewendet.

Inbetriebnahme der DEP-Geräte

Wird eines der Geräte in Betrieb genommen oder, falls es schon in Betrieb ist, ein Werksreset durchgeführt, meldet sich das Gerät bei Apple und lädt das DEP-Profil herunter, sofern eine Internetverbindung besteht. Es genügt, den Bildschirm-Anweisungen zu folgen: Am Ende der Anleitung (Wizard) ist das Apple-Gerät eingeschrieben und der `Relution Agent` sollte installiert werden.

Für Version 26.4.0


09:41 Dienstag 9. Jan.
100 %
Zurück
Das Aktivieren deines iPad kann einige Minuten dauern.
Apple erfasst Hardware-IDs von deinem iPad, um es zu identifizieren und für unsere Dienste zu aktivieren.


09:41 Dienstag 9. Jan.
100 %
Zurück
Weiter
Entfernte Verwaltung
Durch das Registrieren für die Fernverwaltung kann dieses iPad verwaltet werden von:
M-Way Solutions GmbH + MDM Developer
Die Fernverwaltung umfasst die Möglichkeit, die Funktionalität einzuschränken, Apps zu installieren, Daten-Backups zu verwalten sowie den Internetverkehr und einige Geräteeinstellungen zu überwachen.
Mehr Informationen zur entfernten Verwaltung ...

Wird die Fehlermeldung `Profil konnte nicht geladen werden` angezeigt, wird geprüft, ob noch ausreichend freie Geräte-Lizenzen vorhanden sind und ob ein DEP-Profil mit dem Gerät verknüpft ist.

Für Version 26.4.0

Konfigurationsprofil für ADE

Sollen Apple-Geräte über die Automatische Geräteregistrierung (ADE, im Portal: DEP) eingeschrieben werden, kommt ein Konfigurationsprofil (früher DEP-Profil) zum Einsatz. Dieses Profil wird von Relution auf den Apple Server übertragen und wird noch vor der eigentlichen Einschreibung auf den Geräten angewendet.

> Es kann immer nur ein Konfigurationsprofil pro Gerät angewendet werden. Zudem wird das Konfigurationsprofil nur bei der Einschreibung einmalig auf die Geräte übertragen. Soll später eine Änderung übermittelt werden, müssen die Geräte auf Werkseinstellungen zurückgesetzt werden, um das aktualisierte Konfigurationsprofil zu empfangen.

Ein Konfigurationsprofil kann nur erstellt werden, wenn ADE (früher DEP) in der Relution-Organisation eingerichtet ist und ein gültiger DEP-Token hinterlegt wurde.

DEP konfigurieren →

Neue Konfigurationsprofile werden unter `Geräte` → `Konfigurationsprofile` über Erstellen angelegt. Sind weitere Arten der automatischen Einschreibung eingerichtet, wird zuerst der Profiltyp abgefragt; dort wird DEP gewählt. Dieser Bereich bietet zudem eine Übersicht über vorhandene Profile.

Über Als Standardprofil verwenden wird ein Konfigurationsprofil zum Standardprofil. Es wird neuen Auto-Einschreibungen automatisch zugewiesen, denen noch kein anderes Konfigurationsprofil zugeordnet ist. Bei Geräten mit laufender MDM-Migration geschieht das nur, wenn im Standardprofil Konfiguration abwarten und Alle installierten Apps beibehalten aktiviert sind. Es empfiehlt sich, ein Standardprofil zu definieren. Der Name des Profils sollte aussagekräftig sein, sodass es leicht identifizierbar ist.

Für Version 26.4.0

Über Vereinbarungen lassen sich Vereinbarungen auswählen, die unter `Einstellungen` → `Allgemein` → `Vereinbarungen` angelegt wurden. Relution stellt deren Texte dem Gerät während der Einschreibung bereit. Die Auswahl erscheint nur für Benutzer mit Leserecht auf Vereinbarungen.

Der Standard Gerätename (höchstens 255 Zeichen) wird auf die Geräte in den Auto-Einschreibungen während der Einschreibung angewendet. Hier können auch Platzhalter genutzt und kombiniert werden, siehe Erweiterte Platzhalter →. Die Felder Support Telefonnummer, Support E-Mail, Abteilungsname (höchstens 125 Zeichen) und Authentifizierungsaufforderung (höchstens 255 Zeichen) enthalten Informationen, die während der Einschreibung angezeigt werden.

MDM-Einschreibung erzwingen

Diese Option sorgt dafür, dass Geräte bei der Inbetriebnahme zwingend eingeschrieben werden müssen. Es gibt keine Option, den Einschreibeprozess zu überspringen oder abzubrechen. Werden Geräte beispielsweise gestohlen, können sie nicht ohne MDM-Einschreibung in Betrieb genommen werden.

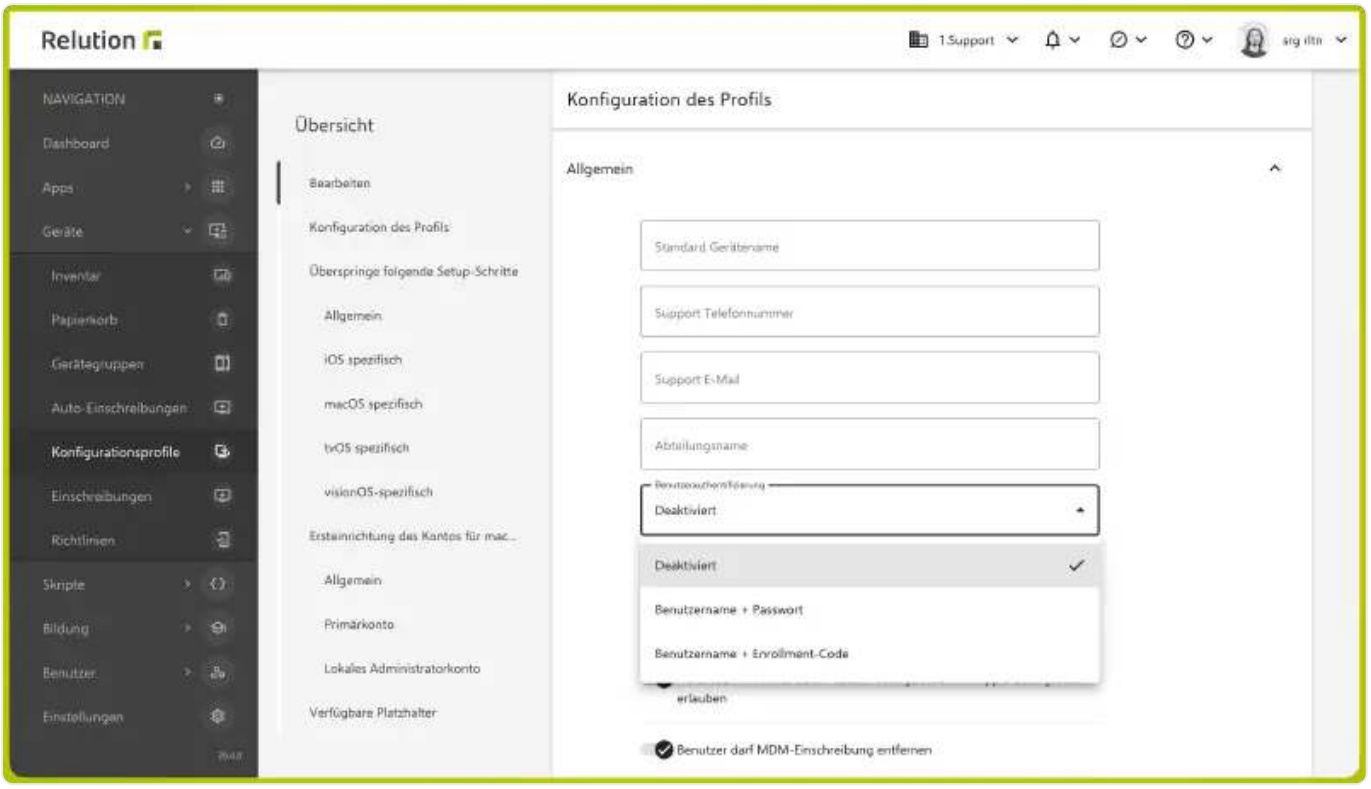
Benutzerauthentifizierung bei der Einschreibung

Neu in 26.4

Über das Feld Benutzerauthentifizierung wird festgelegt, ob und wie sich Benutzer während der Einschreibung authentifizieren müssen. Es stehen drei Optionen zur Auswahl:

- Deaktiviert: Es findet keine Benutzerauthentifizierung statt.
- Benutzername + Passwort: Die Einschreibung muss mit einem Relution-Benutzerkonto authentifiziert werden. Ein Apple Account ist dafür nicht notwendig und wird hier nicht unterstützt.
- Benutzername + Enrollment-Code (ab Version 26.4): Anstelle eines Passworts wird ein einmaliger, von Relution generierter Enrollment-Code abgefragt.

Werden Geräten in der Liste der Auto-Einschreibungen einzelnen Benutzer zugeordnet, können nur diese sich authentifizieren und die entsprechenden Geräte in Betrieb nehmen.



> Für Benutzername + Enrollment-Code muss dem Gerät in der Auto-Einschreibung ein Benutzerkonto mit hinterlegter E-Mail-Adresse zugeordnet sein. Der Code wird bei der Einschreibung generiert und ausschließlich per E-Mail an diese Adresse versendet. Damit dies funktioniert, muss der Mailversand auf dem Server eingerichtet sein und funktionieren.
> Mail Versand einrichten →

Bei Benutzername + Enrollment-Code wird anstelle des Benutzernamens auch die E-Mail-Adresse des zugeordneten Benutzers akzeptiert. Der achtstellige Code ist nur einmal gültig und verfällt nach mehr als fünf Fehlversuchen. Wird die Anmeldeseite erneut geöffnet, erzeugt Relution einen neuen Code und versendet ihn.

Verbinden mit Macs oder PCs und Konfigurieren mit Apple Configurator erlauben

Die Option ist standardmäßig aktiviert; wird sie deaktiviert, zeigt das Portal einen Warnhinweis. Ist diese Option deaktiviert, kann später keine Verbindung mit einem PC oder Mac hergestellt werden, um z.B. Fotos zu kopieren oder ein Backup der Geräte zu erstellen. Es ist empfehlenswert, diese Option zu aktivieren und in den Restriktionen die Verbindung mit Computern zu verbieten, falls dies gewünscht ist. Der Vorteil ist, dass Restriktionen in den Richtlinien jederzeit änderbar sind. Das Konfigurationsprofil hingegen nicht. Die Geräte müssten in diesem Fall zwingend zurückgesetzt werden, um die Option zu ändern.

Benutzer darf MDM-Einschreibung entfernen

Wird die Option aktiviert, können Benutzer auf Geräten das MDM-Profil und damit die Verwaltbarkeit durch Relution entfernen.

Die Option ist bei neuen Konfigurationsprofilen standardmäßig aktiviert. Soll das Entfernen des MDM-Profils verhindert werden, muss die Option vor der Einschreibung der Geräte deaktiviert werden; nachträglich lässt sie sich nur durch Zurücksetzen der Geräte ändern.

Aktiviere Geteiltes iPad

Dies ist die einzige Möglichkeit, den Mehrbenutzermodus von Apple – Geteiltes iPad – zu aktivieren. Ist diese Option eingeschaltet, sind alle Häkchen, die weiter unten für die zu überspringenden Setup-Schritte gesetzt werden, überflüssig, da diese automatisch übersprungen werden.

Für Version 26.4.0

Kein Profil aus dem Backup verwenden

Die Option betrifft Geräte ab iOS/iPadOS 26 bzw. visionOS 26. Ist sie aktiviert, verwendet das Gerät beim Wiederherstellen eines Backups nicht das im Backup enthaltene Profil. Details zum Umzug per Backup: Backup →

Automatische Voreinstellung für macOS und tvOS

Ist die Option aktiviert, wechselt der Einrichtungsassistent auf macOS- und tvOS-Geräten automatisch zwischen seinen Bildschirmen. Das Gerät benötigt dafür eine Ethernet-Verbindung. Solange die Option aktiviert ist, lassen sich die zu überspringenden Setup-Schritte nicht auswählen.

Konfiguration abwarten

Ist Konfiguration abwarten aktiviert, verbleibt das Gerät im Setup-Assistenten, bis alle Apps und Konfigurationen installiert wurden. Über die Geräteaktion Im Geräte-Setup-Assistenten fortfahren wird dem Gerät mitgeteilt, dass die Vorkonfiguration abgeschlossen ist und es im Setup-Assistenten fortfahren kann.

Die Option Alle installierten Apps beibehalten ist nur zusammen mit Konfiguration abwarten verfügbar und standardmäßig aktiviert. Sie ist erforderlich, damit verwaltete Apps und ihre Daten bei der Migration verwalteter Geräte zwischen MDM-Servern erhalten bleiben.

Mindest-Betriebssystemversion

Neu in 26.5

Über die Option Mindest-Betriebssystemversion wird festgelegt, dass Geräte während des Einrichtungsassistenten zunächst auf eine bestimmte Betriebssystemversion aktualisiert werden müssen, bevor sie eingeschrieben werden können. Für jede Plattform kann unabhängig eine Mindestversion hinterlegt werden:

- Mindestversion iOS/iPadOS
- Mindestversion macOS
- Mindestversion visionOS

Bleibt ein Feld leer, wird für die entsprechende Plattform keine Mindestversion erzwungen. tvOS wird von dieser Funktion nicht unterstützt.

Für Version 26.4.0

Erfüllt ein Gerät die konfigurierte Mindestversion bereits, ändert sich am Einschreibevorgang nichts. Meldet ein Gerät während der Einschreibung dagegen eine Version unterhalb der konfigurierten Mindestversion, wird es im Einrichtungsassistenten zunächst zur Aktualisierung aufgefordert. Erst nach erfolgreichem Update und einem erneuten Durchlauf des Einrichtungsassistenten wird die Einschreibung fortgesetzt. Relution fordert dabei automatisch die niedrigste von Apple aktuell angebotene Version an, welche die Mindestanforderung erfüllt – nicht zwangsläufig die neueste verfügbare Version. Diese Erzwingung setzt zudem voraus, dass das Gerät während der Einrichtung überhaupt zu einem Update aufgefordert werden kann; dies wird von Apple ab iOS/iPadOS 17, macOS 14 beziehungsweise visionOS 26 unterstützt.

> Bietet Apple aktuell keine Version an, welche die konfigurierte Mindestversion erfüllt, wird die Einschreibung des Geräts abgelehnt, anstatt es auf eine nicht verfügbare Version zu verweisen. Dies verhindert, dass Geräte im Einrichtungsassistenten hängen bleiben.

Über die Option Geräte blockieren, die die Erzwingung nicht unterstützen (standardmäßig aktiviert) wird festgelegt, wie mit Geräten umgegangen wird, die während der Einrichtung nicht zu einem Update aufgefordert werden können, etwa weil sie eine zu alte Betriebssystemversion besitzen. Ist die Option aktiviert, werden solche Geräte von der Einschreibung ausgeschlossen. Ist sie deaktiviert, werden sie ohne Anwendung der Mindest-Betriebssystemversion eingeschrieben.

Setup-Schritte überspringen

Für Version 26.4.0

Alle Optionen, die aktiviert sind, werden beim initialen Geräte-Setup übersprungen.

Einrichtungsschritte, die nach der Ersteinrichtung erneut angezeigt werden, z. B. nach einem Softwareupdate, werden davon nicht erfasst. Sie lassen sich über die Konfiguration Setup-Assistent in einer Richtlinie ausblenden, siehe Setup-Assistent (iOS) → und Setup-Assistent (macOS) →.

Ist Ortungsdienste nicht aktiviert, wird der Schritt während der Einrichtung angezeigt. Dort kann die Geräteortung zugelassen werden, damit die Geräte automatisch die richtige Zeitzone einstellen. Die Option wirkt sich nur auf den Einrichtungsassistenten aus und hat keinen Einfluss auf die spätere Standortbestimmung der Geräte.

Ersteinrichtung des Kontos für macOS

In diesem Abschnitt lassen sich Benutzer- und Administrator-Konten zu macOS-Geräten hinzufügen, die automatisch bei der Inbetriebnahme erstellt werden. Es sind hier auch Platzhalter verfügbar, siehe Erweiterte Platzhalter →.

Geräte zum DEP hinzufügen

Ursprünglich konnten nur Apple-Geräte, die direkt bei Apple oder bei vertrauenswürdigen Händlern gekauft wurden, zum Apple School/ Business Manager hinzugefügt werden. Wurden Geräte über andere Quellen beschafft, konnten diese nicht automatisch über die Automatische Geräteregistrierung (ADE, im Portal: DEP) in Relution eingeschrieben werden.

iOS / tvOS Geräte via Apple Configurator 2

Mittlerweile ermöglicht Apple, iOS- und tvOS-Geräte mit dem `Apple Configurator` manuell zum Apple School/Business Manager hinzuzufügen. So lassen sich alle Vorteile der automatischen Einschreibung über ADE nutzen, unabhängig davon, wo die Geräte gekauft wurden. Apple-Geräte nachträglich zu DEP hinzufügen →

macOS Geräte via Apple Configurator (mobile)

Apple hat mit dem Apple Configurator für Mobilgeräte (iOS/iPadOS) eine einfache Möglichkeit bereitgestellt, um macOS Geräte in den Apple School/ Business Manager aufzunehmen. Apple Configurator Manual →
Apple Configurator App →

Für Version 26.4.0

Anleitung

1. Apple Configurator auf einem iOS/ iPadOS Gerät mit mind. iOS 16 installieren
2. Auf dem Gerät mit einem gültigen Apple School/Business Manager-Konto im Apple Configurator anmelden
3. macOS Gerät starten und im Systemassistenten anhalten, wenn der Bereich für Land oder Region angezeigt wird
4. Das iOS/ iPadOS Gerät nah an den Mac halten, am Mac auf manuell koppeln links unten im Systemassistenten klicken
5. Die 6-stellige Zahlenkombination am iOS/ iPadOS Gerät eingeben
6. Sobald das macOS Gerät mit dem Prozess fertig ist, werden ein Neustart oder das Ausschalten angeboten
7. Im Apple School/Business Manager einem Standort zuweisen
8. In Relution unter `Geräte` → `Auto-Einschreibungen` die Synchronisierung über Geräte synchronisieren anstoßen (ohne manuellen Anstoß erfolgt sie automatisch einmal täglich). Ist ein DEP-Profil mit Als Standardprofil verwenden markiert, wird es dabei Geräten ohne Profil automatisch zugewiesen; andernfalls das Gerät markieren und über Profil auswählen ein DEP-Profil zuweisen
9. Am Gerät die Apple übliche Willkommenseinrichtung abschließen

DEP-Profile werden unter `Geräte` → `Konfigurationsprofile` angelegt, siehe Konfigurationsprofil für ADE →.

Hinweis zum Status in den Auto-Einschreibungen

- Blau - Profil wurde zugewiesen - Dem Gerät wurde ein DEP-Profil zugewiesen, das noch nicht angewendet wurde
  - Das kann bei Änderungen des Profils für bereits eingeschriebene Geräte auftreten oder bei Geräten, die die Einrichtung noch nicht beendet haben
- Grün - Profil wurde gepushed - Das Profil wurde angewendet und vom Gerät als ausgeführt zurückgemeldet
- Rot - Profil wurde entfernt - Das Profil wurde vom Gerät entfernt
- Grau - Kein Profil vorhanden - Dem Gerät ist kein DEP-Profil zugewiesen oder ein zugewiesenes Profil wurde gelöscht
- Grau - Profil ist unbekannt - Apple hat einen Profilstatus gemeldet, den Relution nicht zuordnen kann

Geräte entfernen

Häufig gibt es Geräte, die sich im Besitz von Endnutzern befinden und beispielsweise für schulische Zwecke in ADE aufgenommen wurden, später jedoch wieder in die private Nutzung übergehen sollen. In diesem Fall müssen die Geräte ordnungsgemäß aus dem MDM und aus ADE entfernt werden, um eine problemfreie weitere Nutzung zu gewährleisten.

Dabei ist folgende Reihenfolge einzuhalten:

1. Daten sichern.
2. Gerät im Apple School/Business Manager aus der Organisation freigeben oder vom Relution-MDM-Server lösen.
3. Erst danach das Gerät zurücksetzen, entweder durch den Benutzer oder in Relution über die Aktion Gerät auf Werkszustand zurücksetzen.

Wird das Gerät vor Schritt 2 zurückgesetzt, bleibt die ADE-Zuordnung bestehen und das Gerät schreibt sich im Systemassistenten erneut in Relution ein.

Sicherung der Daten

Die einfachste Möglichkeit, Benutzerdaten zwischen dem Zurücksetzen und der Neueinrichtung zu sichern, ist die Verwendung der Apple iCloud mit einem privaten Apple Account. Dazu muss sichergestellt sein, dass in Relution in der Konfiguration Restriktionen die Option Account-Modifikationen erlauben aktiviert ist und auf das Gerät angewendet wurde. Die Option ist standardmäßig aktiviert; Handlungsbedarf besteht nur, wenn eine zugewiesene Restriktion sie deaktiviert. Dadurch kann sich der Benutzer mit einem privaten Apple Account am Gerät anmelden und die gewünschte Datensicherung durchführen.

Für Version 26.4.0

Entfernen aus dem Apple School / Business Manager

Die Freigabe bzw. Trennung kann problemlos im Apple ASM/ABM Portal vorgenommen werden, ohne dass sie unmittelbare Auswirkungen auf das Gerät hat. Erst beim nächsten vollständigen Zurücksetzen auf Werkseinstellungen erhält das Gerät von Apple die aktuelle Zuordnung und wird nicht mehr automatisch eingeschrieben. In Relution wird die Auto-Einschreibung bei der nächsten Synchronisierung entfernt, sobald Apple das Gerät als entfernt meldet. Die Synchronisierung erfolgt automatisch einmal täglich oder sofort über Geräte synchronisieren unter `Geräte` → `Auto-Einschreibungen`.

Entfernen aus dem MDM

In Relution sollte in der Konfiguration Restriktionen die Option ‘Alle Inhalte & Einstellungen löschen’ erlauben aktiviert sein (standardmäßig aktiviert). Dadurch kann der Benutzer sein Gerät nach der Datensicherung selbst zurücksetzen. Eine Rückmeldung an den Relution-Administrator ist sinnvoll, da ein zuvor getrenntes WLAN am Gerät möglicherweise die Kommunikation mit dem MDM verhindert und somit keine Informationen über den Status des Gerätes vorliegen. Alternativ kann in Relution die Aktion Gerät auf Werkszustand zurücksetzen ausgelöst werden, wodurch das Gerät in den Papierkorb verschoben wird und die Geräteinformationen entsprechend aktualisiert werden.

Änderungen an der ADE-Zuordnung und am DEP-Profil werden erst nach einem Werksreset wirksam.

VPP konfigurieren

Bei der Anschaffung und Verteilung von Apps an Benutzer bestehen für den Administrator eines MDM-Systems gewisse Herausforderungen. Wenn Benutzer eine App aus dem Apple App Store beziehen, egal, ob dies von einem schul-/ bzw. firmeneigenen oder privaten Gerät erfolgt, muss die App unter Nutzung einer persönlichen Apple-ID einzeln heruntergeladen werden. Die App-Lizenz gehört dann nicht der Schule oder dem Unternehmen, sondern ist der privaten Apple-ID zugeordnet.

Dies ist vor allem bei kostenpflichtigen Apps ein Problem, wenn die beschaffte App-Lizenz in Form von Kostenerstattung oder gekauften Coupons an die Benutzer erstattet werden, da Benutzer über die persönliche Apple-ID immer Eigentümer der App-Lizenz bleiben. Wird die Schule gewechselt oder das Unternehmen verlassen, geht damit auch die App-Lizenz mit den Schülern bzw. Mitarbeitern unwiderruflich verloren. Soll eine App nun an eine Vielzahl von Geräten verteilt werden, entsteht unter der Nutzung persönlicher Apple-IDs zusätzlich schnell eine unübersichtliche und schwer zu kontrollierende Situation für den Administrator.

Wozu gibt es Apps und Bücher (VPP)?

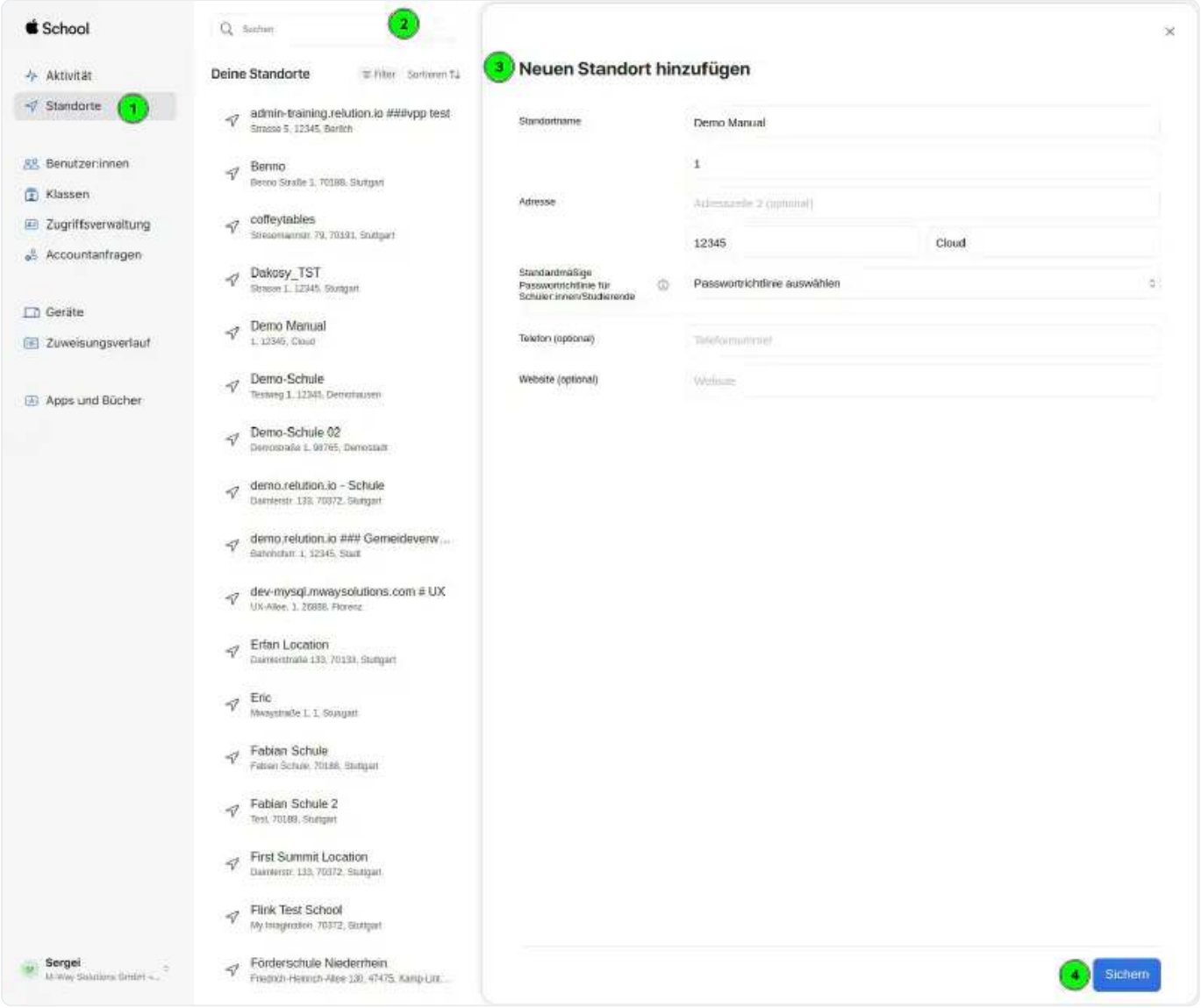
Um die beschriebenen Herausforderungen zu lösen und Apps aus dem Apple App Store über Relution verteilen zu können, ohne eine Apple-ID auf dem Mobilgerät zu benötigen, gibt es das Apple-Programm Apps und Bücher (im Portal: VPP), früher Apple Volume Purchase Program. Hierbei lassen sich Apps in großen Mengen zentral kaufen und benutzerunabhängig verteilen, ohne dass eine Apple-ID auf den Geräten erforderlich ist. Die App-Lizenzen aus Apps und Bücher, im Portal VPP-Lizenzen genannt, werden so zentral verwaltet, ohne jemals die Eigentümerschaft zu wechseln, und können jederzeit durch den Administrator zurückgezogen werden.

Apps und Bücher wird über den Apple Business Manager bzw. Apple School Manager abgebildet und konfiguriert. Hier werden auch die App-Lizenzen zentral unter Verwendung einer Apple-ID der Schule oder des Unternehmens beschafft. Dies gilt sowohl für kostenlose als auch für kostenpflichtige Apps.

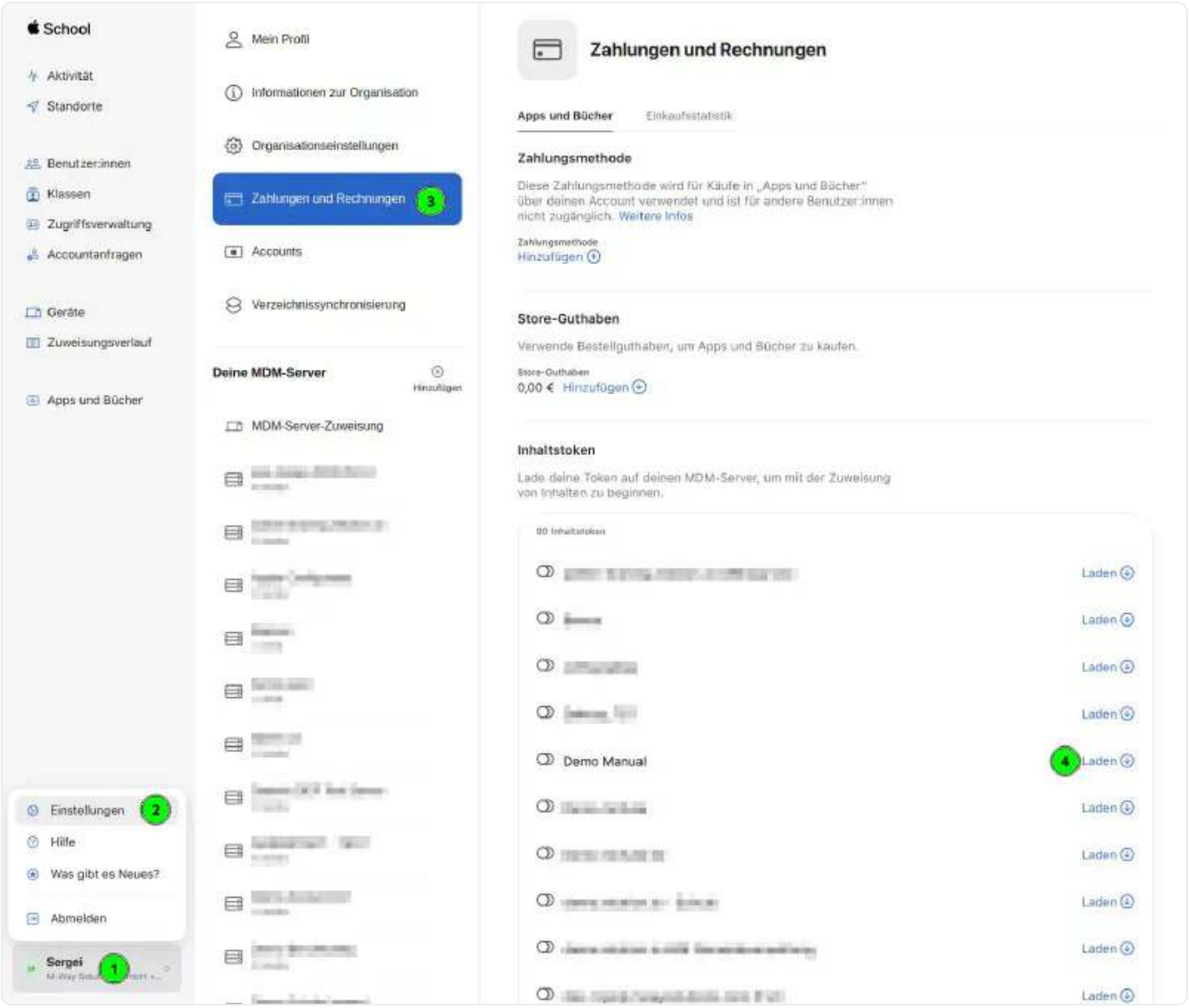
Für Version 26.4.0

Wie wird VPP mit Relution verknüpft?

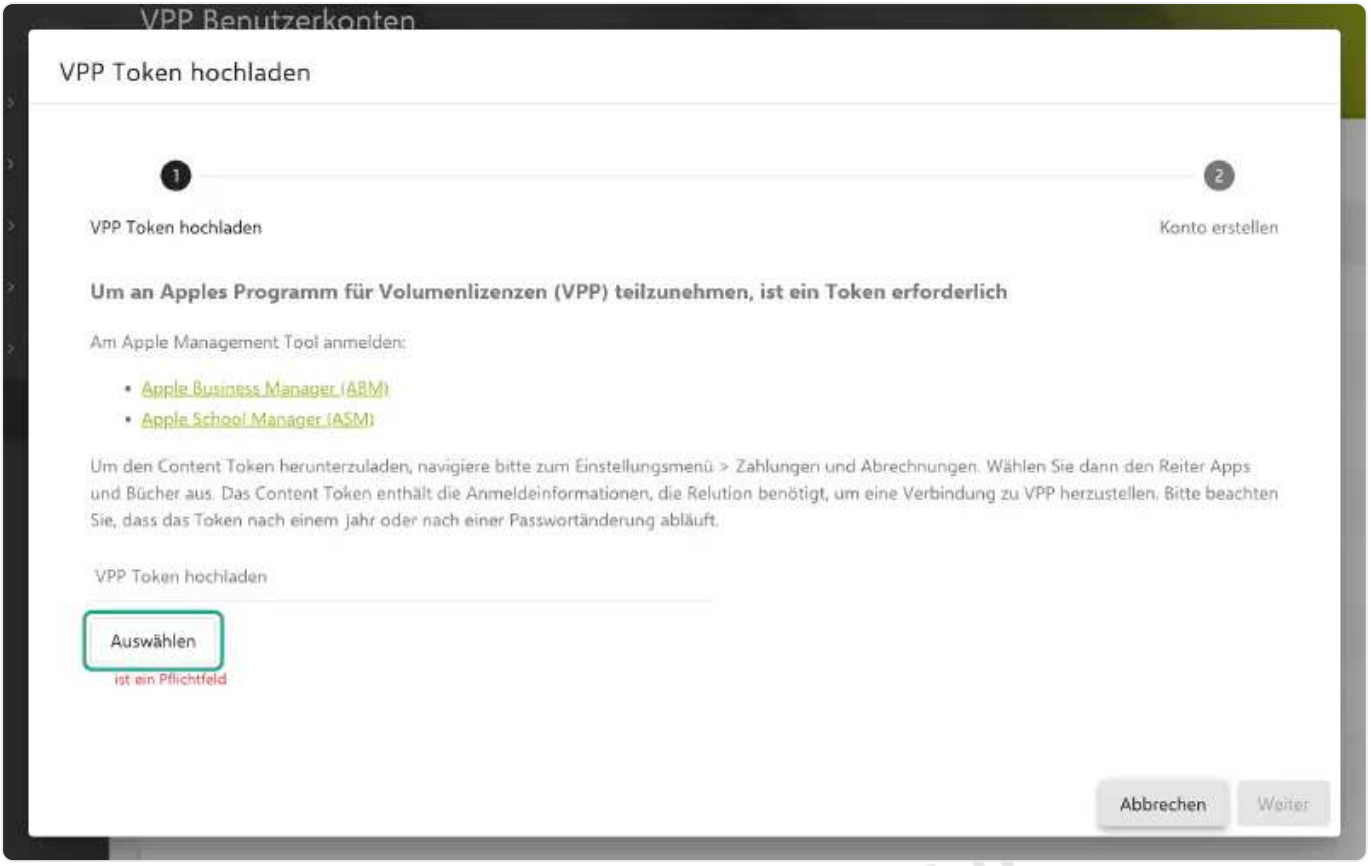
Um beschaffte VPP-Lizenzen über Relution verteilen zu können, müssen die beiden Systeme gekoppelt werden. Im Apple Business Manager bzw. Apple School Manager wird unter Standorte zunächst ein neuer Standort angelegt.



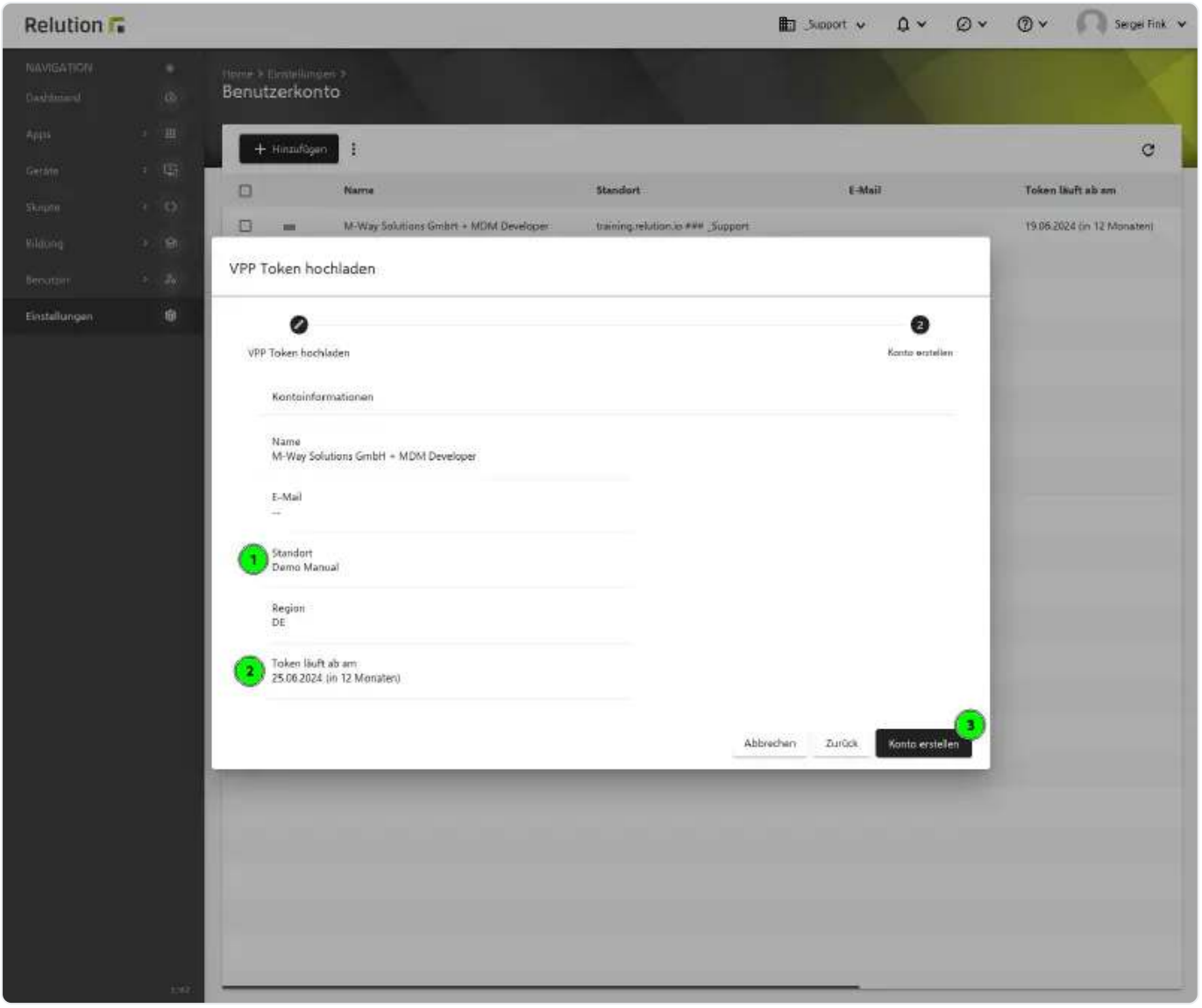
Um diesen Standort mit einem MDM-Server zu verbinden, muss unter `Einstellungen` → `Apps und Bücher` ein VPP-Token für den jeweiligen Standort generiert werden.



Sobald der VPP-Token in Relution unter `Einstellungen` → `Volume Purchase Program (VPP)` → `Benutzerkonto` hochgeladen ist, sind die beiden Systeme miteinander verknüpft.



Für Version 26.4.0



Wird der Token bereits von einem anderen MDM-Server verwaltet, weist der Dialog beim Anlegen des Kontos darauf hin. Mit dem Anlegen des Kontos übernimmt Relution die Verwaltung des Tokens. Die Spalte Abonnement-Status der Kontenliste zeigt, ob Relution für Benachrichtigungen von Apple zu diesem Konto registriert ist. Dafür muss der Relution-Server für die Apple-Server erreichbar sein.

Jeder VPP-Token ist für ein Jahr gültig und muss anschließend im Apple Business Manager bzw. Apple School Manager für den jeweiligen Standort neu geladen werden. Der neue Token wird in Relution am bestehenden Konto über das Drei-Punkte-Menü → Token aktualisieren eingespielt (siehe VPP-Token (Inhaltstoken) verlängern →). Ein Löschen des Kontos entfernt alle VPP-Daten, und ein zweites Konto für denselben Standort lässt sich in derselben Organisation nicht anlegen. Das Relution Notification Center weist rechtzeitig darauf hin, sofern ein VPP-Token abläuft.

E-Mail-Benachrichtigungen über ablaufende und abgelaufene VPP- und DEP-Token sind standardmäßig aktiviert. Unter `Einstellungen` → `Benachrichtigungen` lassen sie sich über die Optionen VPP-Token läuft bald ab, VPP-Token ist abgelaufen, DEP-Token läuft bald ab und DEP-Token ist abgelaufen anpassen. Die erste Erinnerung kommt 30 Tage vor Ablauf, ab 15 Tagen vor Ablauf dann täglich. Die E-Mails gehen an die Benutzer, die berechtigt sind, die VPP- bzw. DEP-Einstellungen zu verwalten.

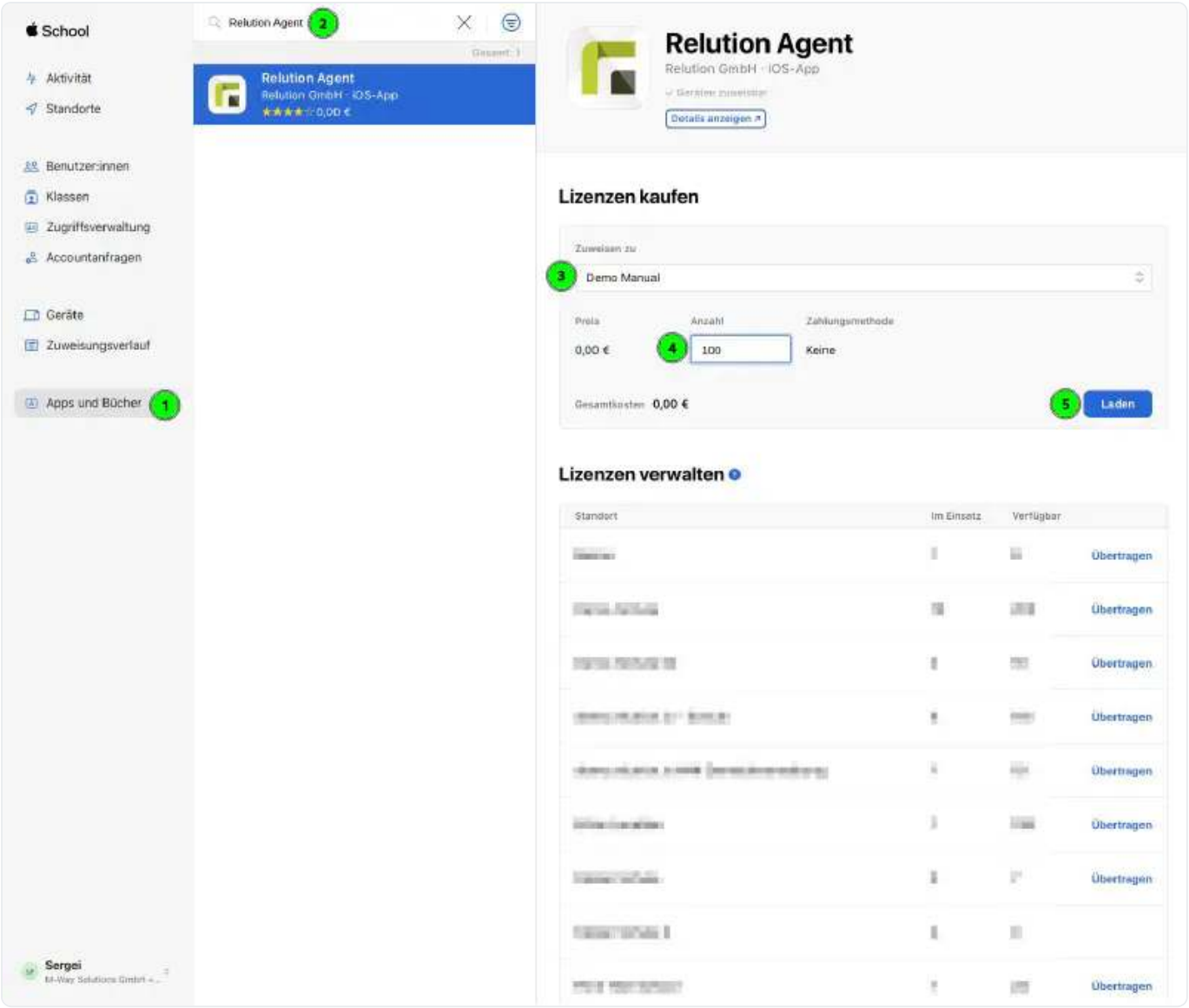
Die Nutzung von mehreren VPP-Tokens in einer Relution Organisation ist in einem separaten Abschnitt beschrieben.

Nach der Kopplung erscheinen in Relution unter Apps die Menüpunkte Gekaufte Apps und Medien. In Gekaufte Apps werden alle über Apps und Bücher beschafften Apps und die dazugehörigen VPP-Lizenzen (Anzahl) aufgelistet, Medien enthält die beschafften Bücher. Die VPP-Lizenzen werden automatisch in regelmäßigen Abständen synchronisiert. Zudem lassen sich die VPP-Lizenzen für die Organisation über Synchronisieren auch manuell aktualisieren. Den Verlauf der Synchronisierungen einschließlich fehlgeschlagener Vorgänge zeigt `Einstellungen` → `Volume Purchase Program (VPP)` → `Synchronisierungshistorie`.

Wie werden App-Lizenzen in VPP beschafft?

Für Version 26.4.0

Im Apple Business Manager bzw. Apple School Manager können nun unter Apps und Bücher App-Lizenzen bezogen werden. Dabei werden die App-Lizenzen einem konfigurierten Standort zugewiesen.

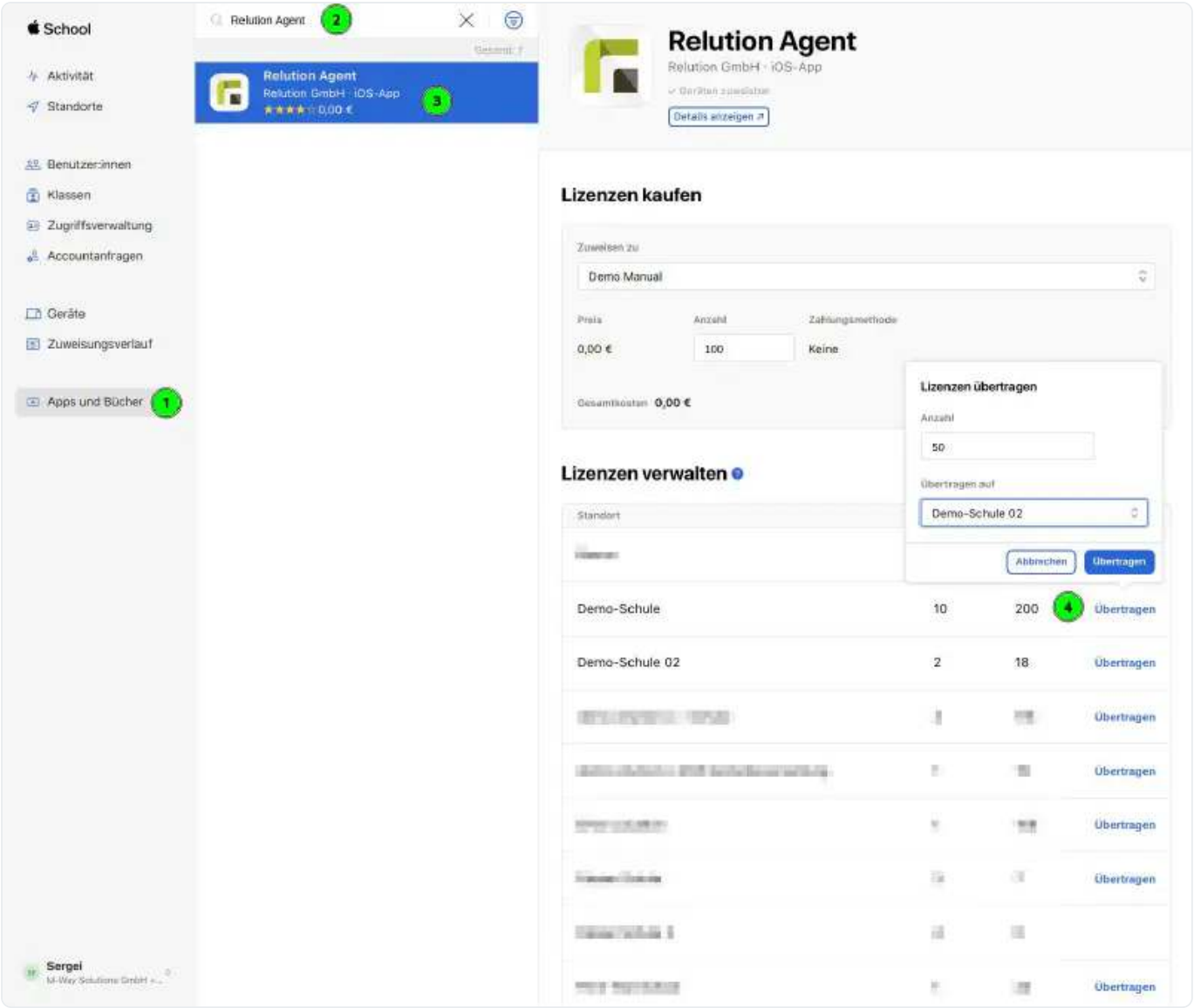


Sobald diese geladen sind, stehen sie im Apple Business Manager bzw. Apple School Manager zur Verfügung. Zudem können die App-Lizenzen in der entsprechenden Organisation in Relution, die mit dem ausgewählten Standort über einen VPP-Token verknüpft ist, auf Geräte verteilt werden.

Lassen sich mit VPP auch App-Lizenzen für unterschiedliche Organisationen bzw. Standorte verwalten?

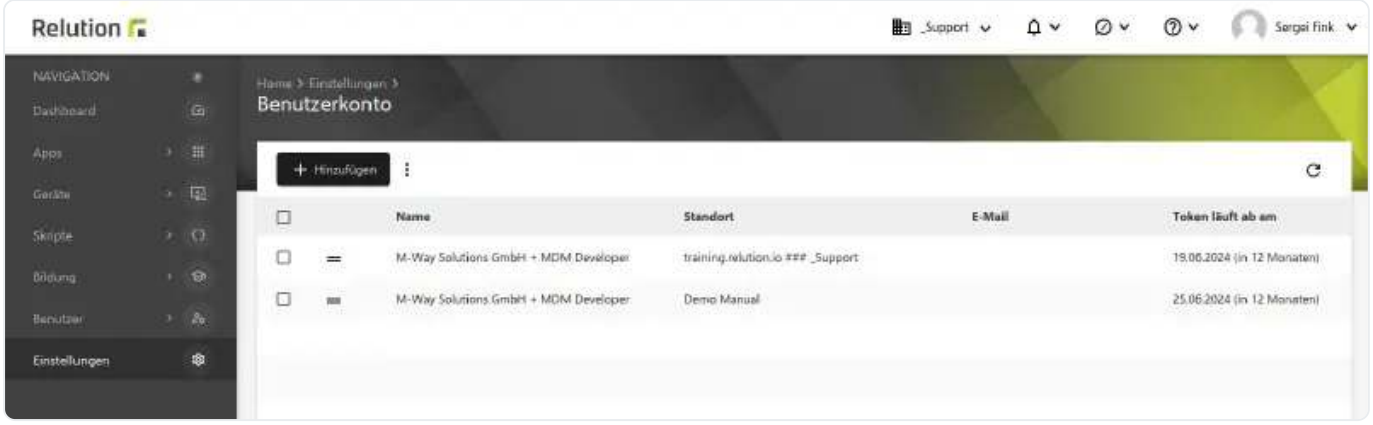
Werden in Relution über die Mandantenfähigkeit mehrere Organisationen verwaltet, wie dies z.B. bei einem Schulträger mit mehreren Schulen der Fall ist, so können mit einer Apple-ID des Schulträgers zentral App-Lizenzen beschafft und auf die jeweiligen Schulen verteilt werden. Hierfür muss im Apple School Manager für jede Schule ein Standort angelegt und der VPP-Token in die entsprechende Relution-Organisation einer jeden Schule hinterlegt werden. Dies gilt analog für den Apple Business Manager im Unternehmenskontext.

Angeschaffte VPP-Lizenzen lassen sich im Apple Business Manager bzw. Apple School Manager verwalten und auf andere Standorte übertragen. Dadurch ist es möglich, App-Lizenzen einmalig für einen führenden Standort zentral zu beschaffen und anschließend paketweise auf andere Standorte zu verteilen.

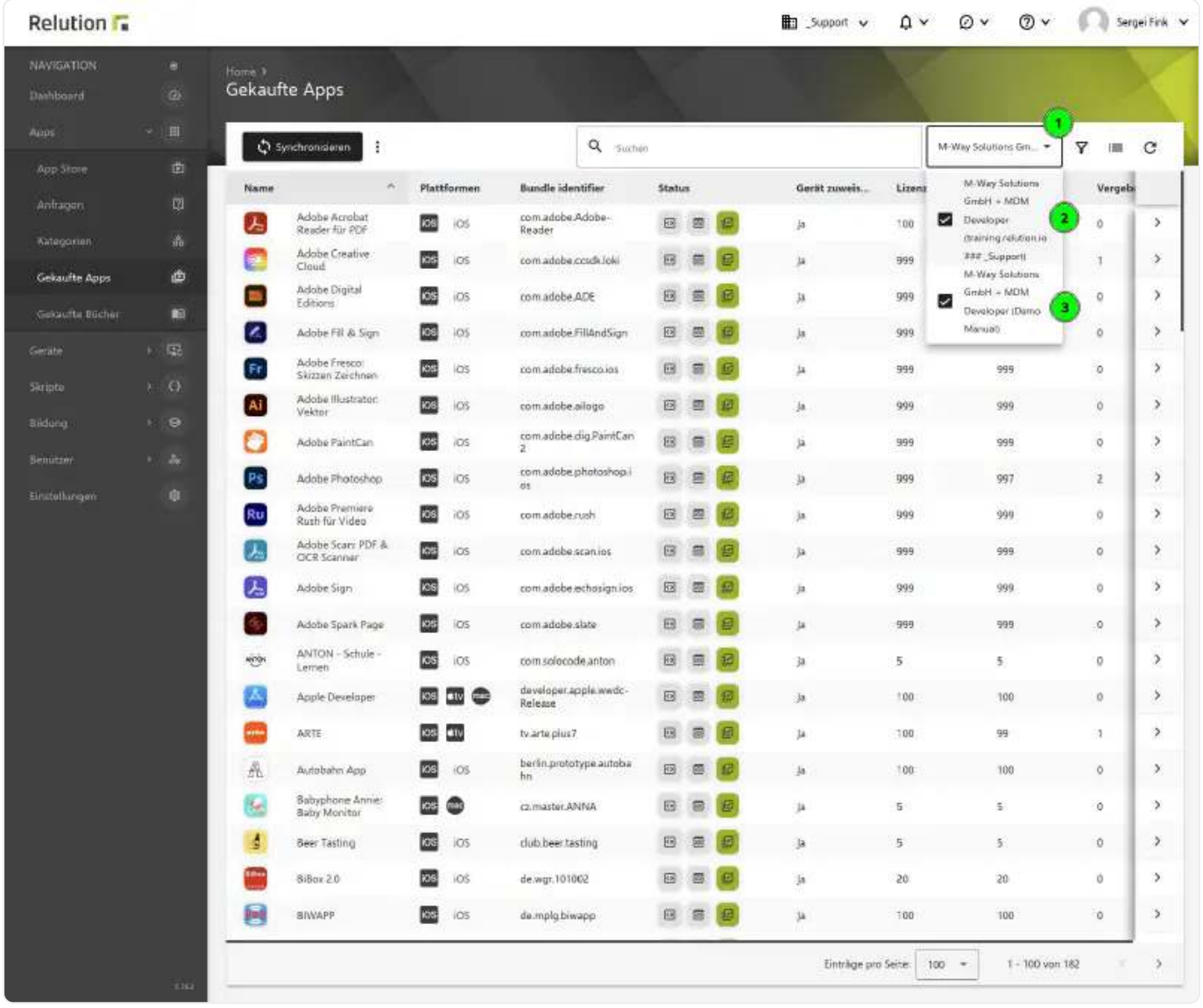


Ist es möglich, innerhalb einer Relution Organisation mehrere VPP-Token zu verwenden?

Innerhalb von Relution besteht die Möglichkeit, unter `Einstellungen` → `Volume Purchase Program (VPP)` → `Benutzerkonto` mehrere VPP-Tokens zu hinterlegen. Dies verfolgt den Zweck, unterschiedliche Apple School Manager Konten zu verknüpfen, wenn z.B. eine Schule von einem Schulträger mit VPP-Apps ausgestattet wird, gleichzeitig aber ebenfalls eigene VPP-Lizenzen besitzt und einsetzt. Analog funktioniert dies ebenso mit dem Apple Business Manager.



Die Summe aller App-Lizenzen aus mehreren VPP-Tokens für eine Organisation wird in der Ansicht Gekaufte Apps aggregiert dargestellt. Über eine Auswahlliste lassen sich die VPP-Lizenzen nach den jeweiligen Standorten aus dem Apple School Manager filtern.



VPP-Lizenzen werden unter `Apps` → `Gekaufte Apps` zugewiesen: Nach Auswahl einer App öffnet Lizenz zuordnen einen Dialog, in dem Geräte, Benutzer oder Gruppen ausgewählt werden. Existiert die App-Lizenz in mehr als einem hinterlegten VPP-Token, wird zuerst ausgewählt, von welchem Token die App-Lizenz genutzt werden soll. Über Lizenz entziehen wird eine Zuweisung wieder aufgehoben.

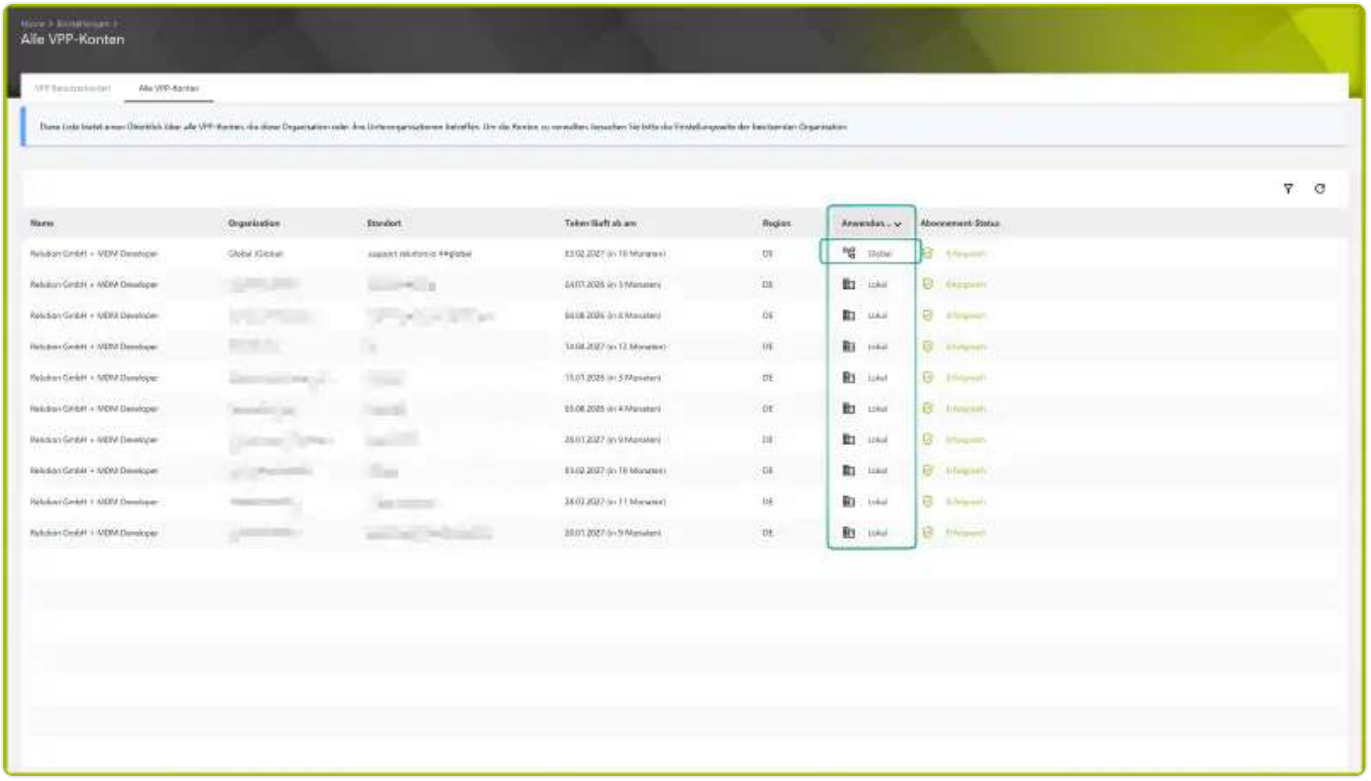
Global VPP

Mit Relution ist es möglich, in der globalen Organisation VPP-Token einzubinden. Dadurch können zentral beschaffte Apps an Mandanten nach unten verteilt werden.

Ein VPP-Token in der globalen Organisation steht automatisch in allen Organisationen zur Verfügung, ein VPP-Token in einer Meta-Organisation in deren Unterorganisationen. Apps aus VPP-Konten der globalen Organisation ersetzen automatisch bestehende Apps in den anderen Organisationen; das lässt sich nicht rückgängig machen. In der untergeordneten Organisation ist der übernommene Token nicht bearbeitbar (auch nicht die Einstellungen zu App-Updates), nur seine Reihenfolge lässt sich ändern. In Gekaufte Apps und Medien beziehen sich die angezeigten Zuweisungen auf die aktuelle Organisation; die Gesamtzahl der Lizenzen gilt über alle Organisationen hinweg.

Somit entfällt ein mehrfaches Einrichten im Apple School Manager / Apple Business Manager sowie das wiederholte Aktualisieren mehrerer Token. Im besten Fall muss nur noch einmal pro Jahr ein einzelner Token erneuert werden.

Für Version 26.4.0



Wichtiger Hinweis zur Lizenzierung

Es ist essenziell, dass ausreichend VPP-Lizenzen für alle Geräte und Mandanten bezogen werden.

Beispiel:

- Organisation 1: 250 Geräte
- Organisation 2: 100 Geräte
- Organisation 3: 1000 Geräte

In diesem Fall sollten mindestens 1350 VPP-Lizenzen global bezogen werden.

Mandantenspezifische VPP-Token

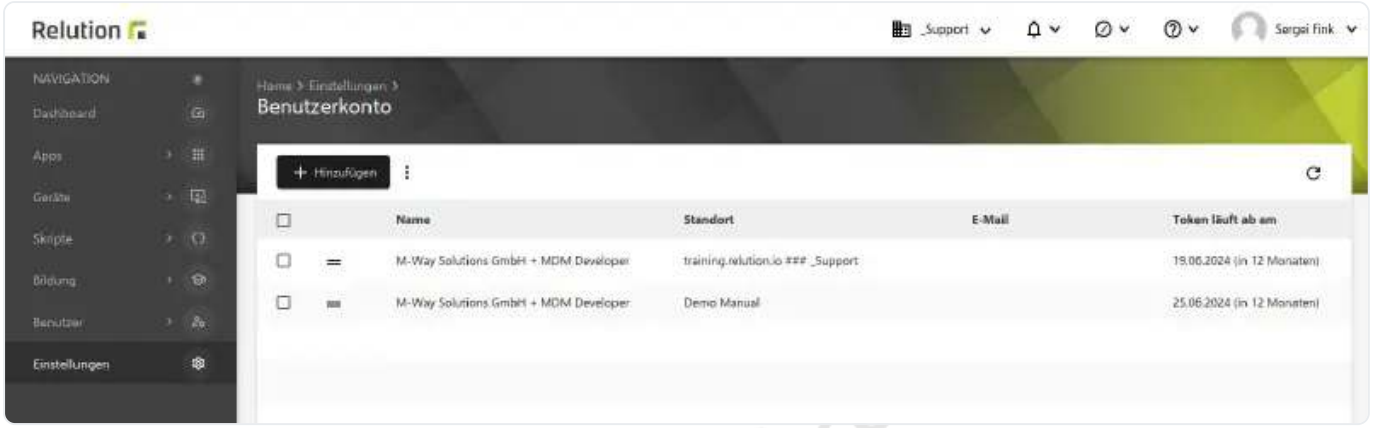
Sollte ein Standort kostenpflichtige Apps nutzen oder einen zusätzlichen eigenen VPP-Token mit individuellen Apps benötigen, kann dieser direkt im jeweiligen Mandanten eingebunden werden.

So lässt sich eine klare Kosten- und Lizenztrennung zwischen globaler und lokaler Verwaltung realisieren.

Für Version 26.4.0

Können VPP-Lizenzen in Relution auch automatisch auf Geräte zugewiesen werden?

Werden Apps über Auto-Deployments oder eine Richtlinie (App-Konformität) automatisch auf Geräte installiert, prüft Relution, ob eine VPP-Lizenz für diese App hinterlegt ist. Ist dies der Fall, wird die VPP-Lizenz automatisch an das Gerät zugewiesen. Bei App-Store-Apps, die nur macOS oder nur tvOS unterstützen, sind VPP-Lizenzen Voraussetzung für ein Auto-Deployment: Ohne verfügbare VPP-Lizenzen in der Organisation lässt sich für diese Apps kein Auto-Deployment konfigurieren. Bei iOS-Apps ist die VPP-Lizenz optional. Sind mehrere VPP-Tokens für die Organisation hinterlegt und in allen ist die App-Lizenz vorhanden, wird die VPP-Lizenz vom ersten VPP-Token in der Liste verwendet. Unter `Einstellungen` → `Volume Purchase Program (VPP)` → `Benutzerkonto` kann die Reihenfolge der VPP-Tokens geändert werden, um zu bestimmen, von welchem Token die VPP-Lizenz bei einer automatischen Zuweisung über Auto-Deployments verwendet werden soll.



Ob Relution verfügbare Updates von Apps aus Apps und Bücher auf den Geräten installiert, wird unter `Einstellungen` → `Volume Purchase Program (VPP)` → `App-Updates` mit App-Updates ausführen festgelegt: Nie, Sofort, nachdem es erkannt wurde oder Nach Zeitplan. Beim Zeitplan werden die Wochentage unter Wiederholt sich am und die Startzeit angegeben.

Häufige Fehlerquellen beim Token-Upload, die Dateiendungen im Überblick und Gründe für einen vorzeitigen Gültigkeitsverlust sind unter Wichtige Hinweise zur Fehlervermeidung → zu finden.

DEP / VPP Token verlängern

Token für die Automatische Geräteregistrierung (ADE, im Portal: DEP) und für Apps und Bücher (im Portal: VPP) besitzen eine maximale Gültigkeit von 1 Jahr und müssen regelmäßig erneuert werden, um eine unterbrechungsfreie Geräteverwaltung und App-Zuweisung zu gewährleisten. Diese Anleitung beschreibt, wie sich diese Token unkompliziert verlängern lassen.

Die Token für ADE und für Apps und Bücher sind voneinander unabhängig: Jedes Token läuft ein Jahr nach seiner eigenen Erstellung ab. Verlängert wird daher nur das Token, dessen Ablauf bevorsteht. Relution erinnert per E-Mail an ablaufende und abgelaufene Token, erstmals 30 Tage vor Ablauf und ab 15 Tagen vor Ablauf täglich (siehe VPP konfigurieren →). In der Liste der DEP-Konten markiert die Spalte Token läuft ab am ein Token ab 60 Tagen vor Ablauf mit einem Warnsymbol und ein abgelaufenes Token mit einem roten Symbol.

> Apple hat den Apple Business Manager (ABM) im April 2026 in Apple Business umbenannt.

Zudem bietet Relution ab Version 5.33 die Möglichkeit, alle verbundenen DEP- und VPP-Token in einer zentralen Übersicht anzuzeigen. Administratoren der `Global`-Organisation oder einer Meta-Organisation können dadurch auf einen Blick erkennen:

- Welche DEP- und VPP-Token gültig oder abgelaufen sind
- Wann die jeweiligen Token ablaufen

Token im Relution Portal

Für Version 26.4.0

Beide Token-Typen werden im Portal an unterschiedlichen Stellen geführt.

DEP-Konten aufrufen

Die zentrale Übersicht der DEP-Konten ist über folgende Schritte erreichbar:

1. In der `Global`-Organisation oder einer Meta-Organisation anmelden.
2. Die Einstellungen in der linken Seitenleiste öffnen.
3. Zum Bereich Geräteplattformspezifisch navigieren.
4. Apple Automated Device Enrollment auswählen.
5. Den Tab Alle DEP-Konten öffnen (verfügbar ab Version 5.33.0).

VPP-Konten aufrufen

Die Übersicht der VPP-Konten ist über folgende Schritte erreichbar:

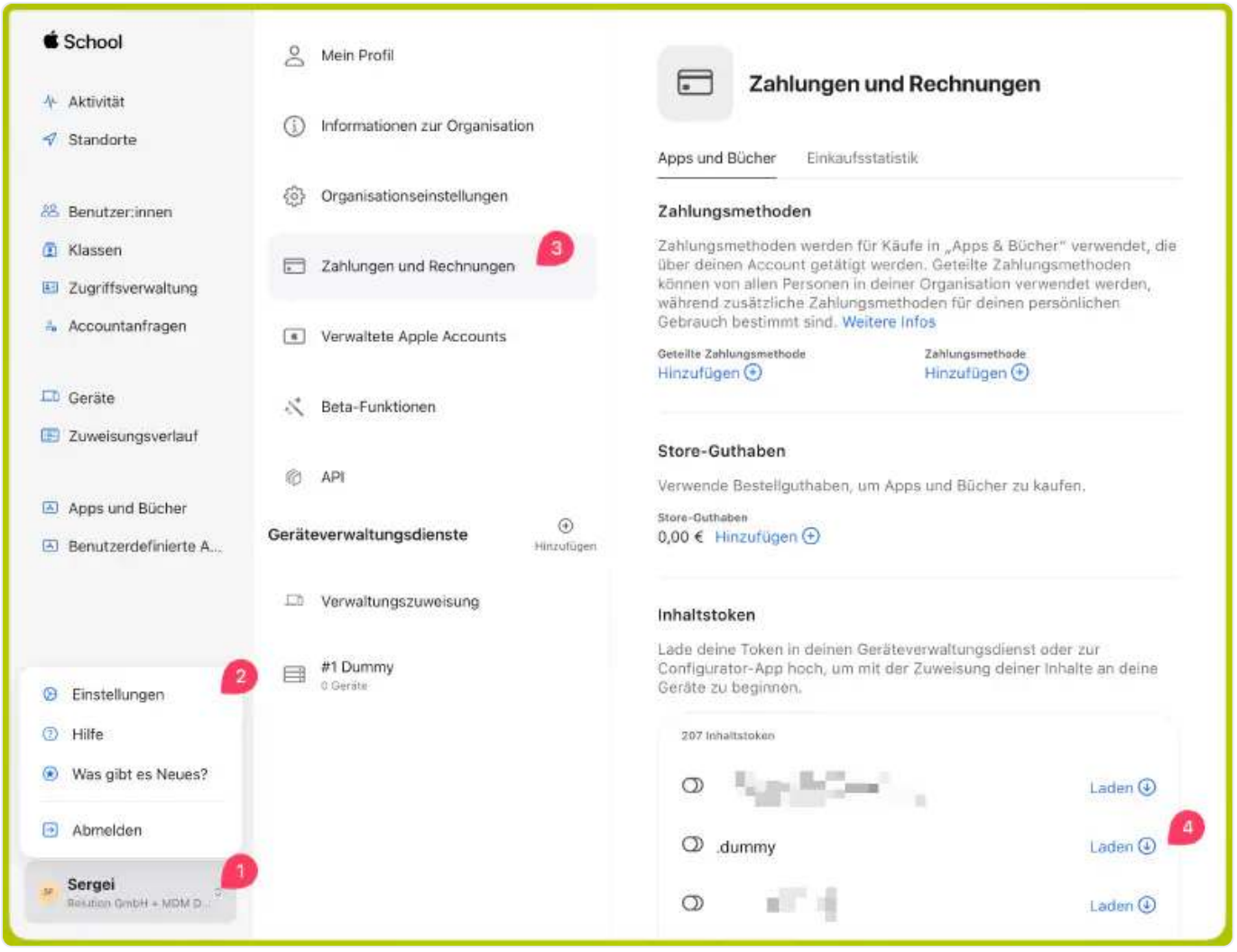
1. In der `Global`-Organisation oder einer Meta-Organisation anmelden.
2. Die Einstellungen in der linken Seitenleiste öffnen.
3. Zum Bereich Volume Purchase Program (VPP) navigieren.
4. Benutzerkonto auswählen.
5. Den Tab Alle VPP-Konten öffnen (verfügbar ab Version 5.33.0).

VPP-Token (Inhaltstoken) verlängern

Das VPP-Token wird zunächst bei Apple heruntergeladen und anschließend in Relution eingespielt.

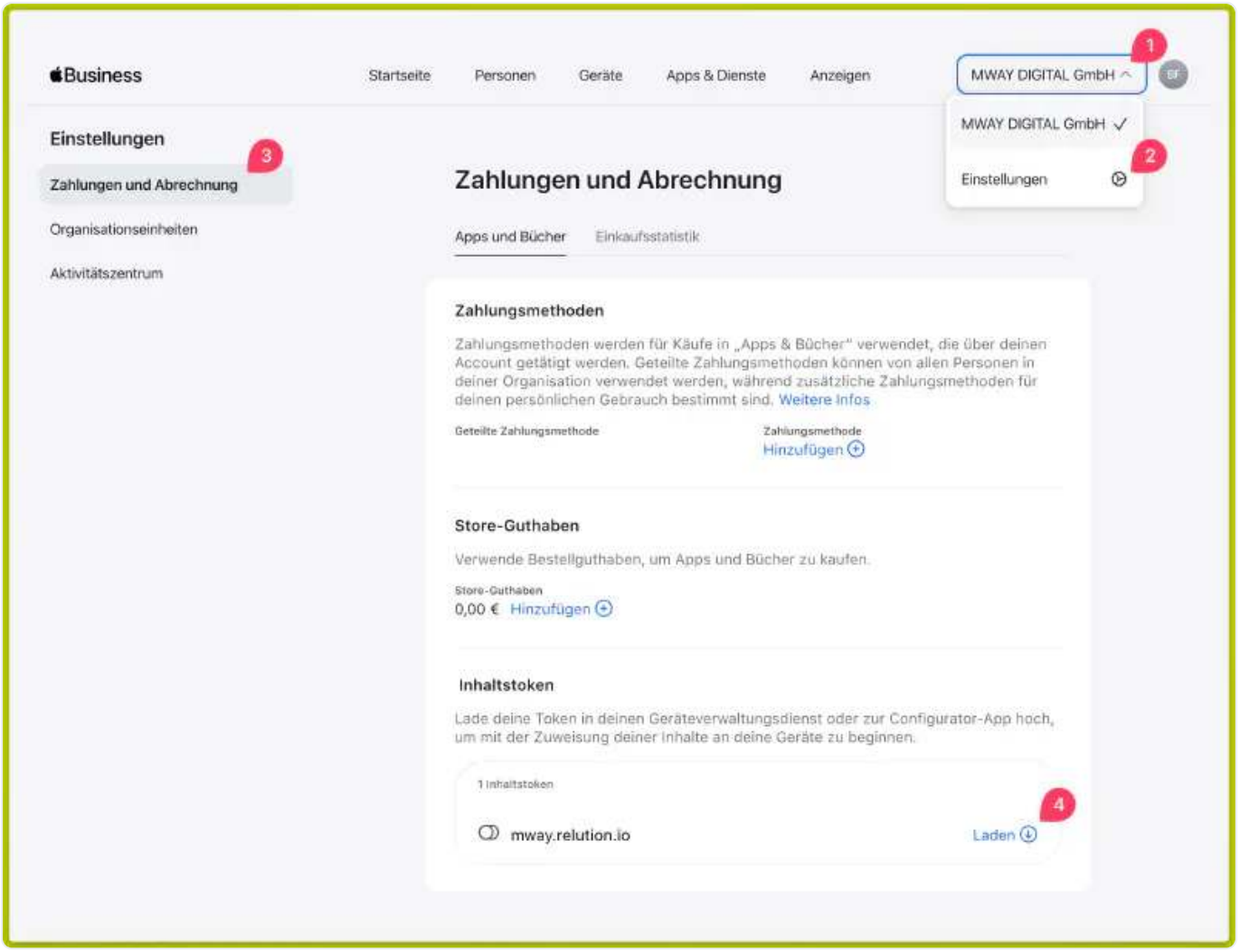
Download im Apple School Manager (ASM)

1. Im Apple School Manager → anmelden.
2. Unten links auf den angemeldeten Benutzernamen klicken.
3. Die Einstellungen öffnen.
4. Zahlungen und Rechnungen auswählen.
5. Unter Inhaltstoken beim gewünschten Token auf Laden klicken.
    - *Dateiformat:* `sToken_for_ [Standort].vpptoken`



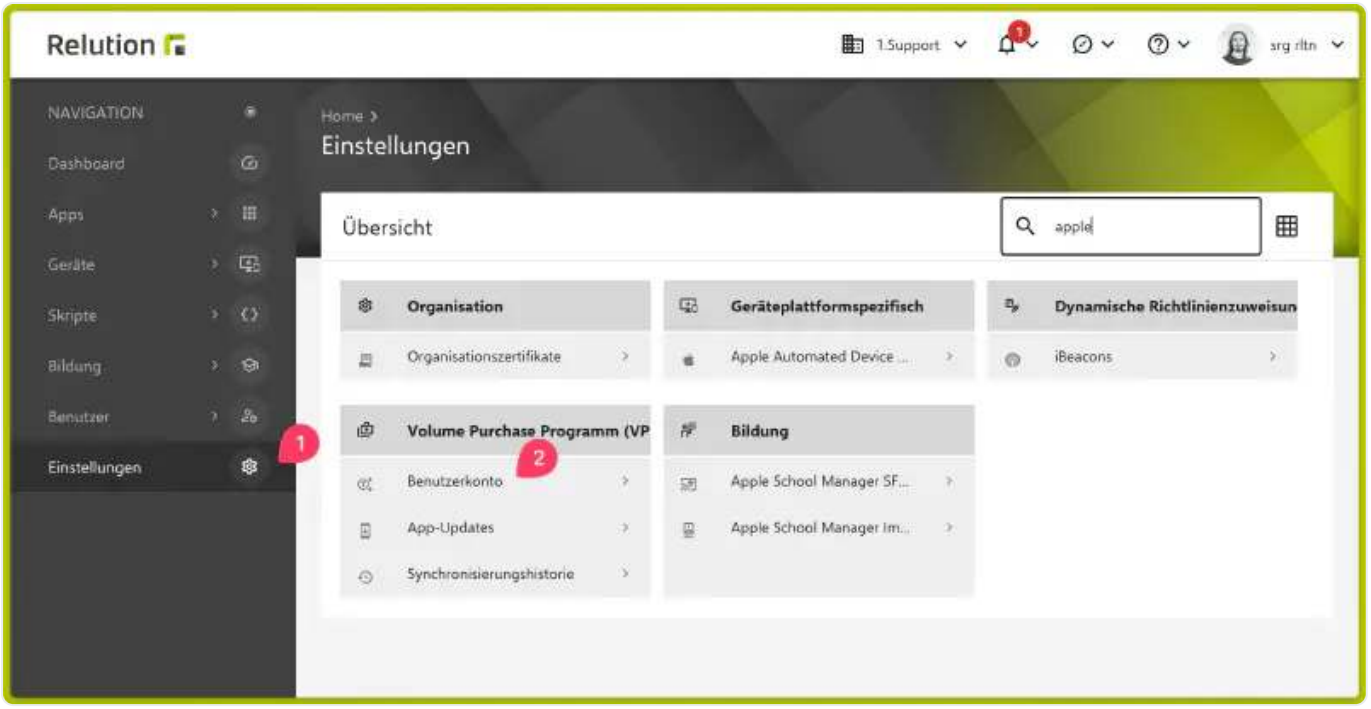
Download in Apple Business (ehemals ABM)

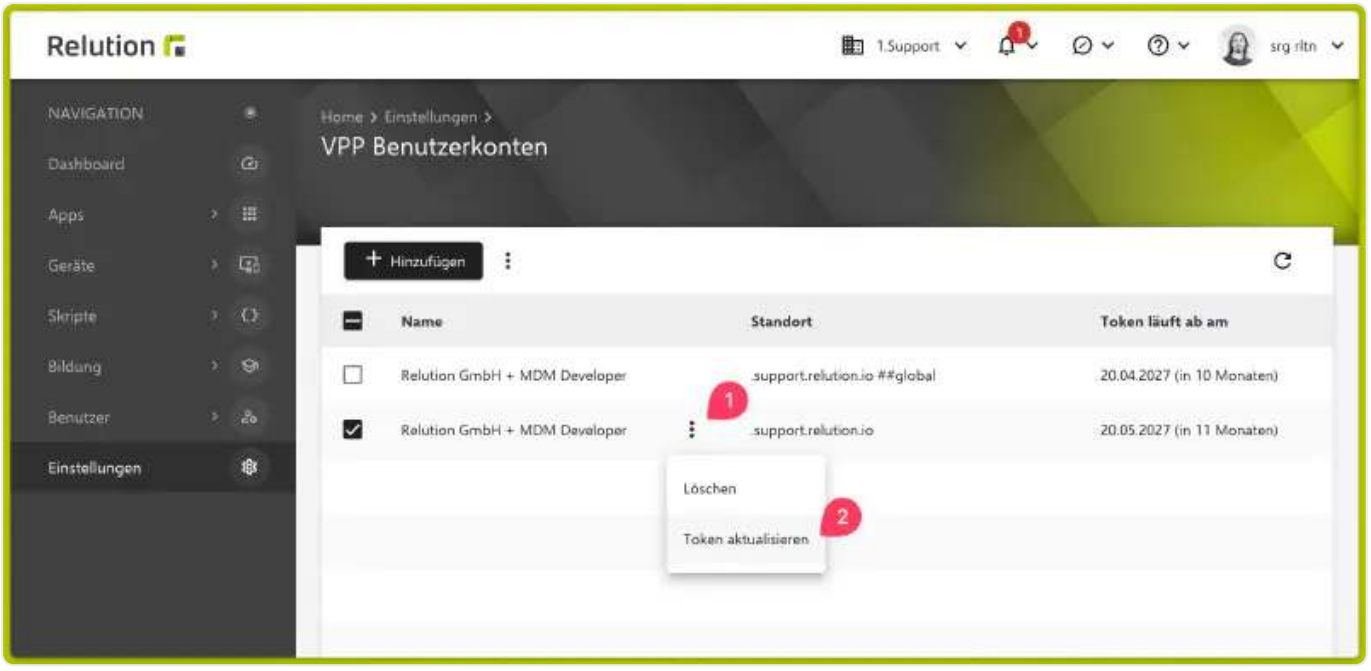
1. In Apple Business → anmelden.
2. Oben rechts auf den Namen der Organisation klicken.
3. Die Einstellungen öffnen.
4. Zahlungen und Abrechnung auswählen.
5. Unter Inhaltstoken beim gewünschten Token auf Laden klicken.
    - *Dateiformat:* `sToken_for_ [Standort].vpptoken`



Einspielen in Relution

1. Im Relution Portal anmelden und in die entsprechende Organisation wechseln.
2. Die Einstellungen öffnen.
3. Zu Volume Purchase Program (VPP) → Benutzerkonto navigieren.
4. Das zu verlängernde Token über das Drei-Punkte-Menü auswählen.
5. Auf Token aktualisieren klicken.
6. Die zuvor heruntergeladene Datei (`*.vpptoken`) hochladen.
7. Den Vorgang mit einem Klick auf Token aktualisieren abschließen.





In der `Global`-Organisation weist der Dialog darauf hin, dass Apps aus globalen VPP-Konten bestehende Apps in anderen Organisationen ersetzen. Wird das Konto bereits von einem anderen MDM-Server verwaltet, erscheint ebenfalls ein Hinweis; mit dem Aktualisieren übernimmt Relution die Verwaltung.

DEP-Token (Server-Token) verlängern

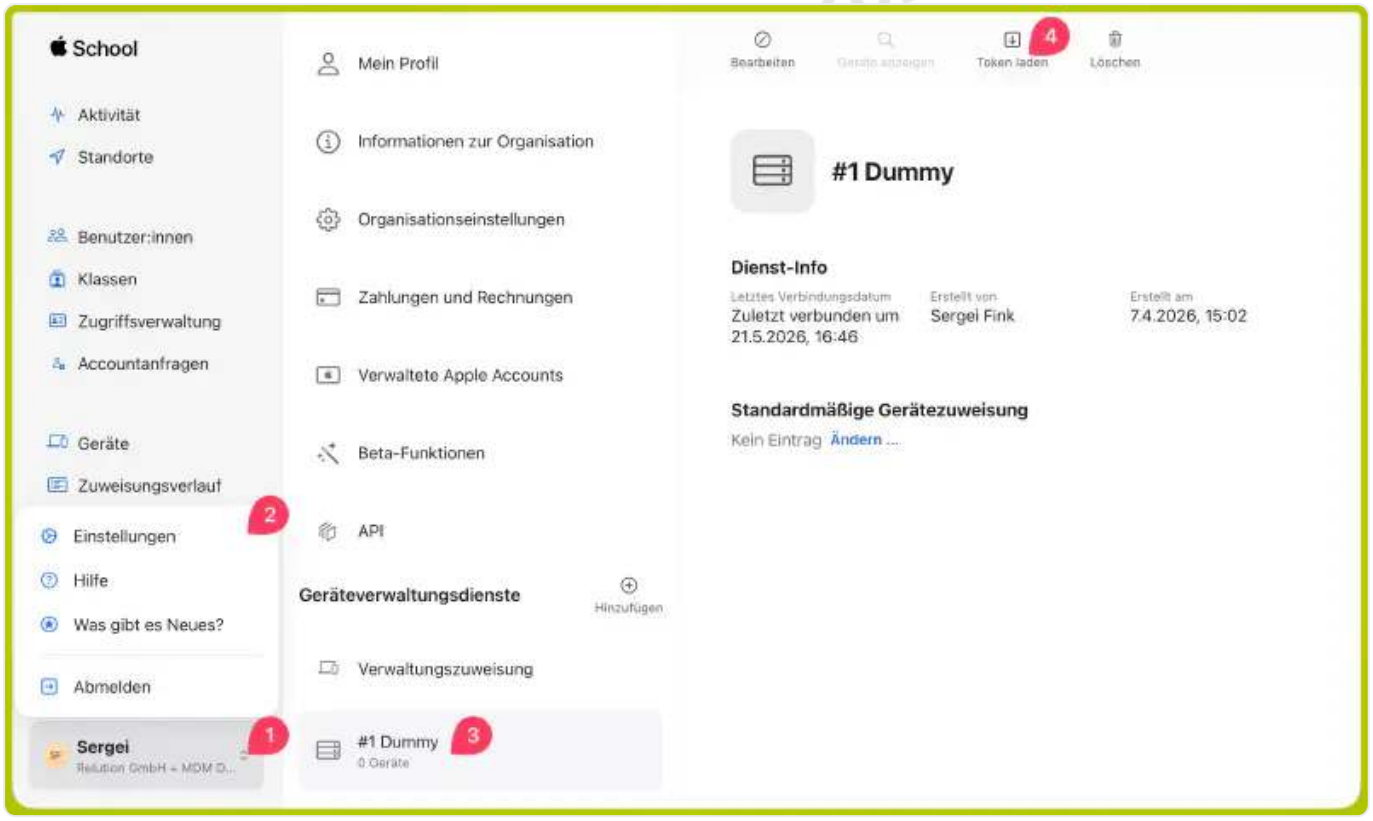
Apple verschlüsselt das neue Token mit dem Public Key, der bei der Ersteinrichtung im ABM/ASM hinterlegt wurde. Relution speichert das zugehörige Zertifikat je DEP-Konto, daher muss der Public Key bei der Verlängerung nicht erneut hochgeladen werden. Wird das Zertifikat trotzdem benötigt, lässt es sich im Dialog Token hochladen (über Token aktualisieren geöffnet) mit Zertifikat herunterladen speichern.

Download im Apple School Manager (ASM)

1. Im Apple School Manager → anmelden.
2. Unten links auf den angemeldeten Benutzernamen klicken.
3. Die Einstellungen öffnen.
4. Unter Geräteverwaltungsdienste den Geräteverwaltungsdienst auswählen, der mit Relution verbunden ist.
5. Auf Token laden klicken.

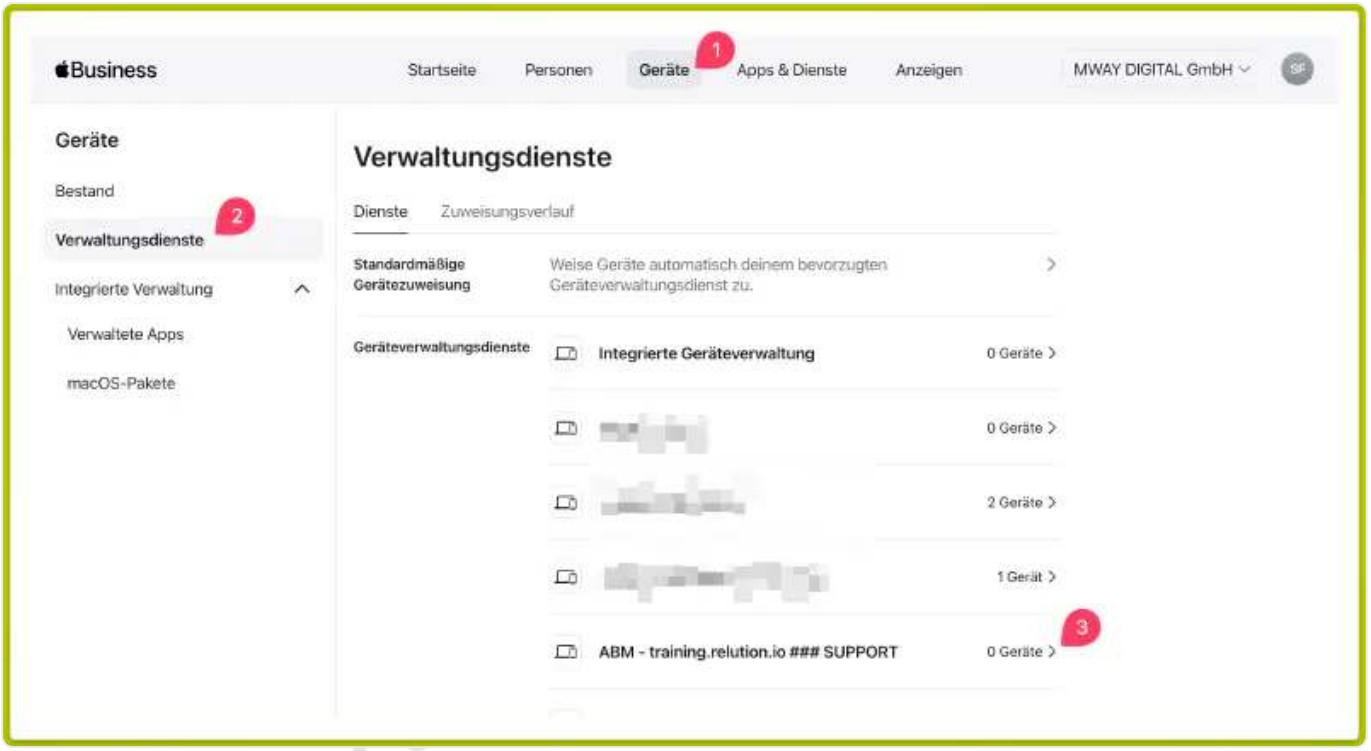
> Mit dem Laden eines neuen Tokens wird der bestehende Token zurückgesetzt.

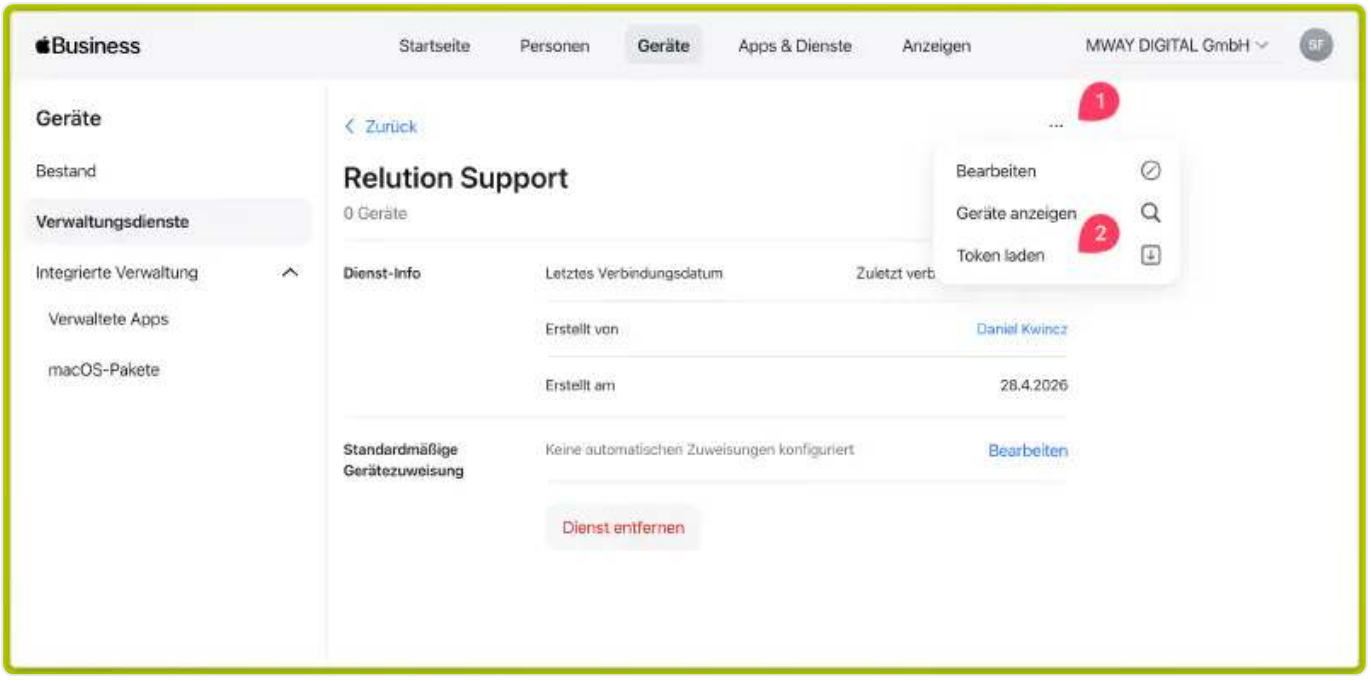
- *Dateiformat:* `*_smime.p7m`



Download in Apple Business (ehemals ABM)

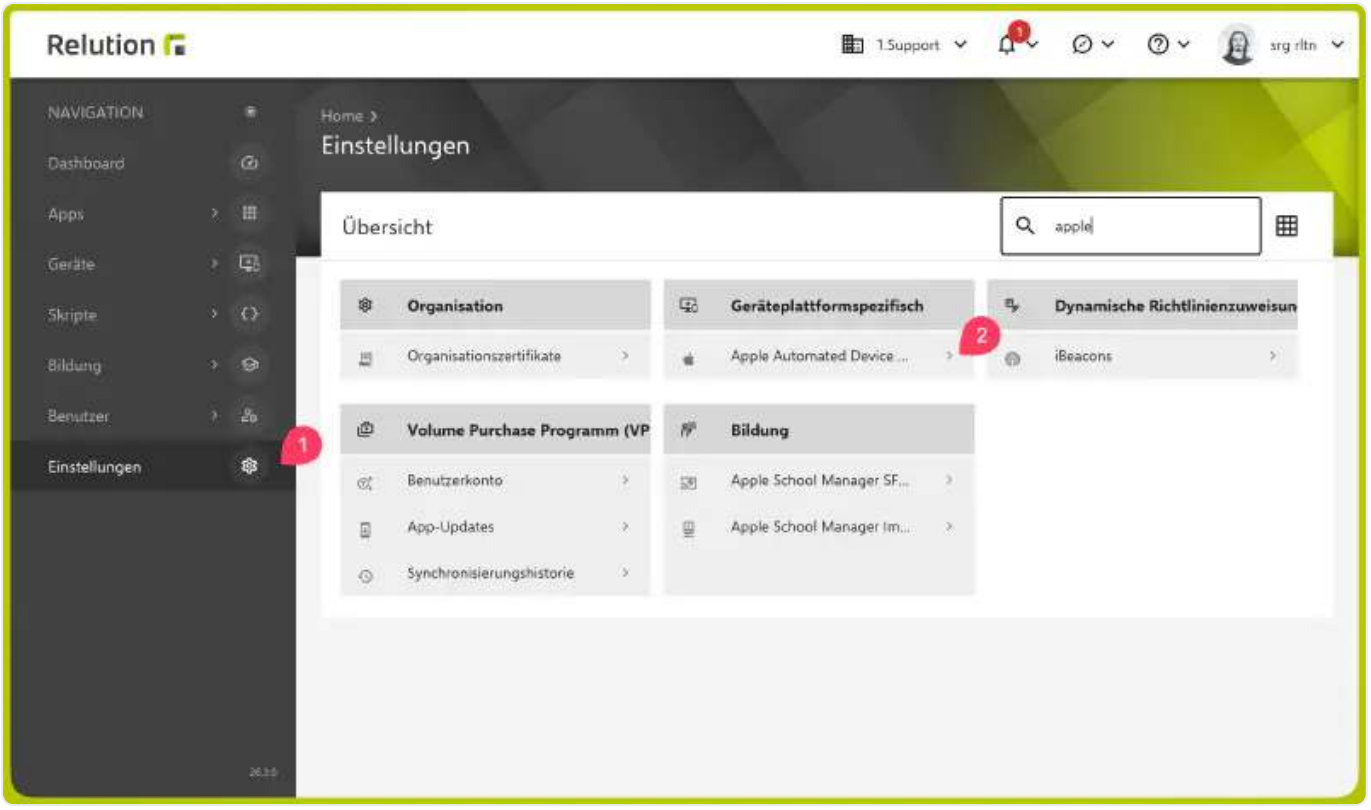
1. In Apple Business → anmelden.
2. In der oberen Mitte auf Geräte klicken.
3. In der linken Navigation den Punkt Verwaltungsdienste auswählen.
4. Unter Geräteverwaltungsdienste den gewünschten Dienst auswählen.
5. Oben rechts das Drei-Punkte-Menü (⋯) öffnen und auf Token laden klicken.
    - *Dateiformat:* `*_smime.p7m`

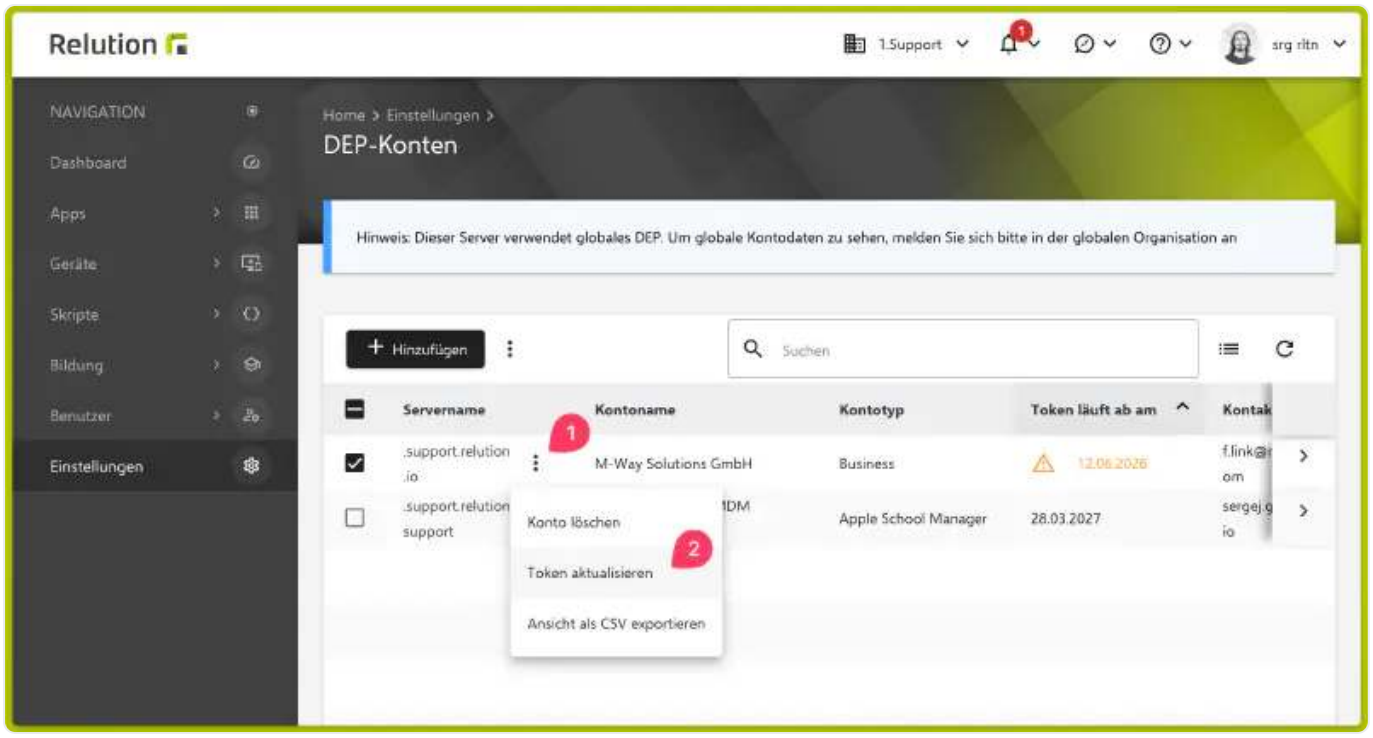




Einspielen in Relution

1. Im Relution Portal anmelden und in die entsprechende Organisation wechseln.
2. Die Einstellungen öffnen.
3. Zu Geräteplattformspezifisch → Apple Automated Device Enrollment navigieren.
4. Das gewünschte Token über das Drei-Punkte-Menü auswählen.
5. Auf Token aktualisieren klicken.
6. Die Datei (`*_smime.p7m`) über Auswählen hochladen.
7. Den Vorgang mit Speichern abschließen.





Wichtige Hinweise zur Fehlervermeidung

Die folgenden Punkte führen erfahrungsgemäß am häufigsten zu fehlgeschlagenen Token-Erneuerungen.

Für Version 26.4.0

Häufige Fehlerquellen

Es kommt in der Praxis häufig vor, dass VPP-Token (`.vpptoken`) und DEP-Token (`.p7m`) miteinander verwechselt und im falschen Menü hochgeladen werden. Wird ein VPP-Token im DEP-Menü hochgeladen, meldet Relution Übertragene Daten nicht gültig. Im VPP-Menü lässt sich ein DEP-Token nicht auswählen: Die Datei wird ohne Meldung verworfen und das Upload-Feld bleibt leer. Ist eine `.p7m`-Datei kein gültiges DEP-Token, erscheint Die Ressource wird nicht unterstützt oder ist korrupt.

Gehört ein DEP-Token zu einem anderen Geräteverwaltungsdienst als dem, der mit dem DEP-Konto verknüpft ist, lehnt Relution es mit Das hochgeladene Token gehört nicht zu dem MDM-Server, der mit diesem DEP-Konto verknüpft ist ab. In diesem Fall wird das Token beim richtigen Geräteverwaltungsdienst im ABM/ASM geladen.

Kommt es beim Hochladen des DEP-Tokens zur Fehlermeldung Unbekannter Fehler oder Das Token ist nicht valid. Bitte das Token in den Einstellungen updaten, hat Apple die Anfrage abgelehnt. Eine mögliche Ursache ist eine nicht synchrone Serverzeit; sie wird zuerst geprüft und korrigiert. Bleibt der Fehler bestehen, ist das Token ungültig (z. B. weil im Apple Business Manager bzw. Apple School Manager inzwischen ein neues Token für den MDM-Server erzeugt wurde). In diesem Fall wird ein neues Token heruntergeladen und hochgeladen.

Dateiendungen der Token-Typen

Token-Typ	Verwendungszweck	Dateiendung
DEP-Token	Automatische Geräteregistrierung (Automated Device Enrollment, ADE)	`*_smime.p7m`
VPP-Token →	App- und Buchlizenzen (Volume Purchase Program)	`*.vpptoken`
Public Key	Verschlüsselungszertifikat von Relution für ABM/ASM	`*.pem` *(Nur bei der Ersteinrichtung erforderlich)*

Vorzeitiger Gültigkeitsverlust

Ein Token kann auch vor Ablauf der regulären 1-Jahres-Frist ungültig werden. Häufige Ursachen hierfür sind:

- Passwortänderung: Das Passwort des zugrunde liegenden verwalteten Apple Accounts (im Portal: Managed Apple ID) im ABM/ASM wurde geändert.
- Account-Status: Der verwendete Administrator-Account wurde gelöscht, deaktiviert oder in seinen Rechten eingeschränkt.
- Neue Apple-AGB: Apple hat neue Geschäftsbedingungen im ABM/ASM-Portal veröffentlicht. Die Token-Kommunikation wird in diesem Fall so lange blockiert, bis ein Hauptadministrator den neuen Bedingungen im Portal zugestimmt hat.

Für Version 26.4.0

Nachträglich zum DEP hinzufügen

Diese Anleitung beschreibt, wie iOS-, iPadOS- und tvOS-Geräte mit dem Apple Configurator 2 nachträglich in den Apple Business Manager (ABM) oder Apple School Manager (ASM) aufgenommen werden, um sie über das Device Enrollment Program (DEP) mit Relution zu verwalten.

Wofür wird der Apple Configurator 2 verwendet?

Der Apple Configurator 2 ist eine kostenlose Mac-App zur manuellen Konfiguration von Apple-Geräten via USB. Er ermöglicht:

- Das Erstellen und Aufspielen von Konfigurationsprofilen.
- Das nachträgliche Hinzufügen von Geräten zum DEP, die nicht bereits von einem autorisierten Wiederverkäufer zugewiesen wurden.

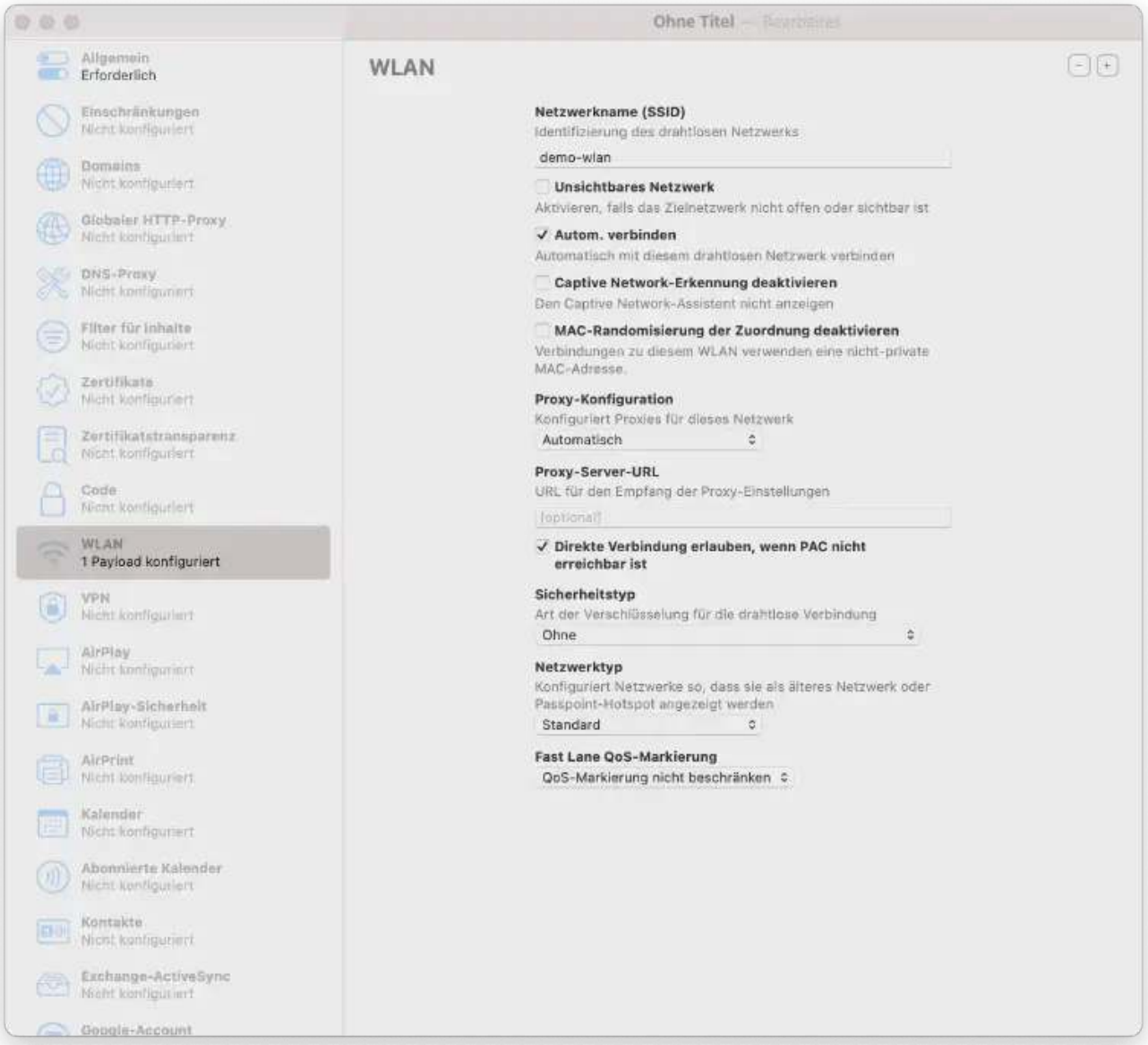
Vorbereitungen

Um eine automatische Registrierung zu gewährleisten, sollte im Vorfeld ein WLAN-Profil angelegt werden:

1. Im Apple Configurator: Menü `Ablage` → `Neues Profil` → `WLAN`.
2. Die Zugangsdaten des eigenen Netzwerks eingeben.
3. Das Profil als Datei auf dem Mac speichern.

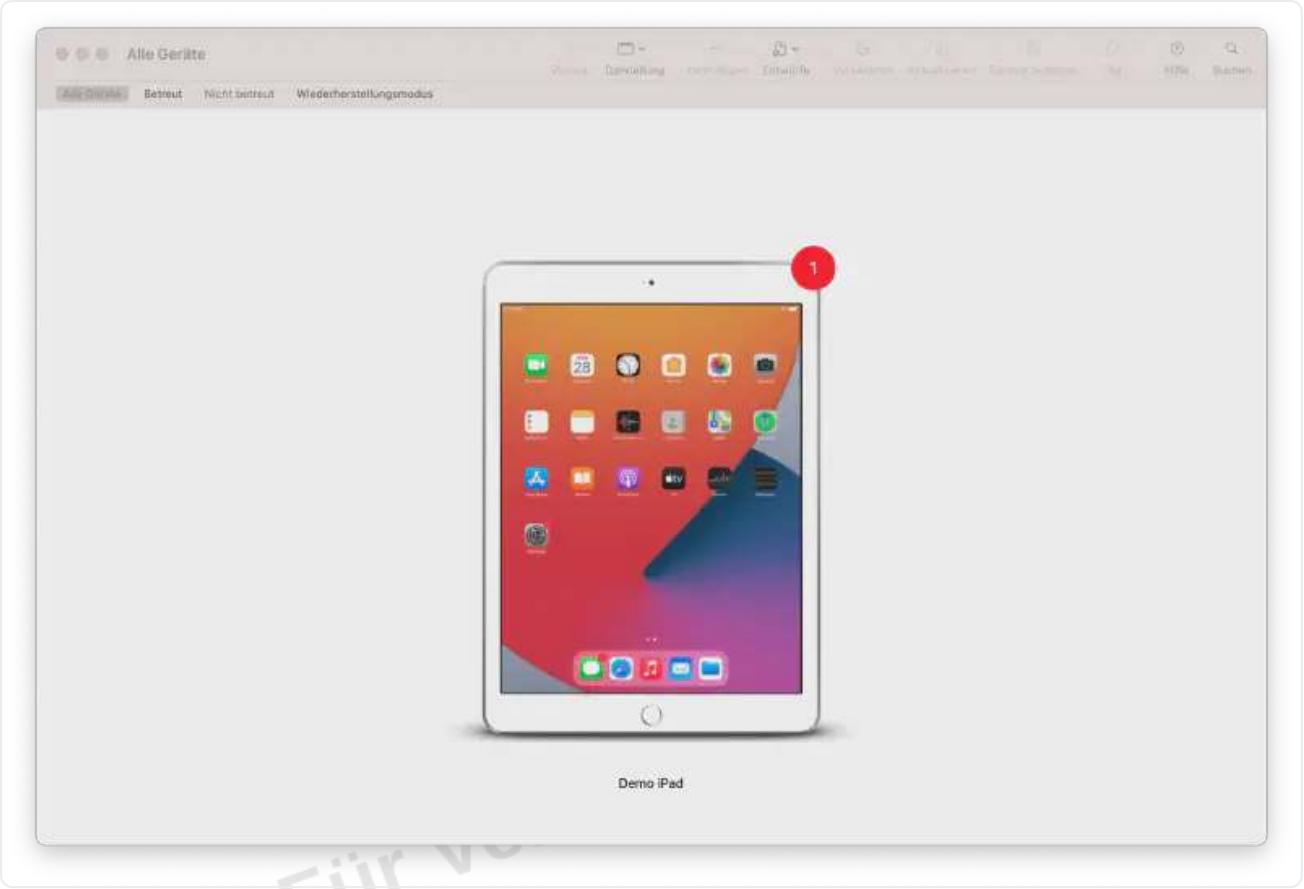
Sicherstellen, dass die eingegebenen Werte funktionieren.

Für Version 26.4.0


Ohne Titel
Allgemein
Erforderlich
Einschränkungen
Nicht konfiguriert
Domains
Nicht konfiguriert
Globaler HTTP-Proxy
Nicht konfiguriert
DNS-Proxy
Nicht konfiguriert
Filter für Inhalte
Nicht konfiguriert
Zertifikate
Nicht konfiguriert
Zertifikatstransparenz
Nicht konfiguriert
Code
Nicht konfiguriert
WLAN
1 Payload konfiguriert
VPN
Nicht konfiguriert
AirPlay
Nicht konfiguriert
AirPlay-Sicherheit
Nicht konfiguriert
AirPrint
Nicht konfiguriert
Kalender
Nicht konfiguriert
Abonnierte Kalender
Nicht konfiguriert
Kontakte
Nicht konfiguriert
Exchange-ActiveSync
Nicht konfiguriert
Google-Account
WLAN
Netzwerkname (SSID)
Identifizierung des drahtlosen Netzwerks
demo-wlan
Unsichtbares Netzwerk
Aktivieren, falls das Zielnetzwerk nicht offen oder sichtbar ist
Autom. verbinden
Automatisch mit diesem drahtlosen Netzwerk verbinden
Captive Network-Erkennung deaktivieren
Den Captive Network-Assistent nicht anzeigen
MAC-Randomisierung der Zuordnung deaktivieren
Verbindungen zu diesem WLAN verwenden eine nicht-private MAC-Adresse.
Proxy-Konfiguration
Konfiguriert Proxies für dieses Netzwerk
Automatisch
Proxy-Server-URL
URL für den Empfang der Proxy-Einstellungen
[optional]
Direkte Verbindung erlauben, wenn PAC nicht erreichbar ist
Sicherheitstyp
Art der Verschlüsselung für die drahtlose Verbindung
Ohne
Netzwerktyp
Konfiguriert Netzwerke so, dass sie als älteres Netzwerk oder Passpoint-Hotspot angezeigt werden
Standard
Fast Lane QoS-Markierung
QoS-Markierung nicht beschränken

Durchführung: Geräte zum DEP hinzufügen

1. Gerät verbinden: Das Apple-Gerät per USB an den Mac anschließen und den Apple Configurator 2 starten.

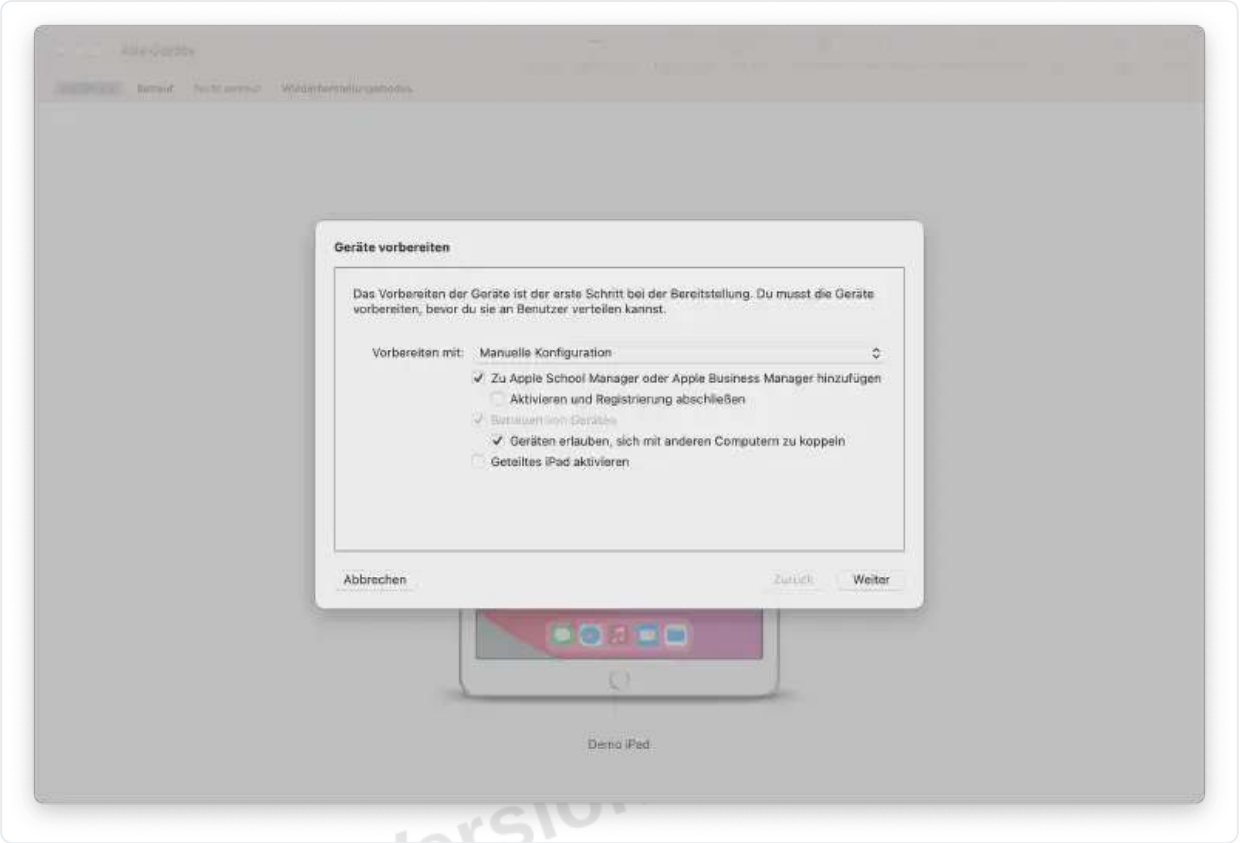


2. Factory Reset: Das Gerät mit der rechten Maustaste auswählen und auf `Erweitert` → `Alle Inhalte und Einstellungen löschen` klicken.

3. Vorbereiten: Das Gerät mit der rechten Maustaste auswählen und auf Vorbereiten… klicken.

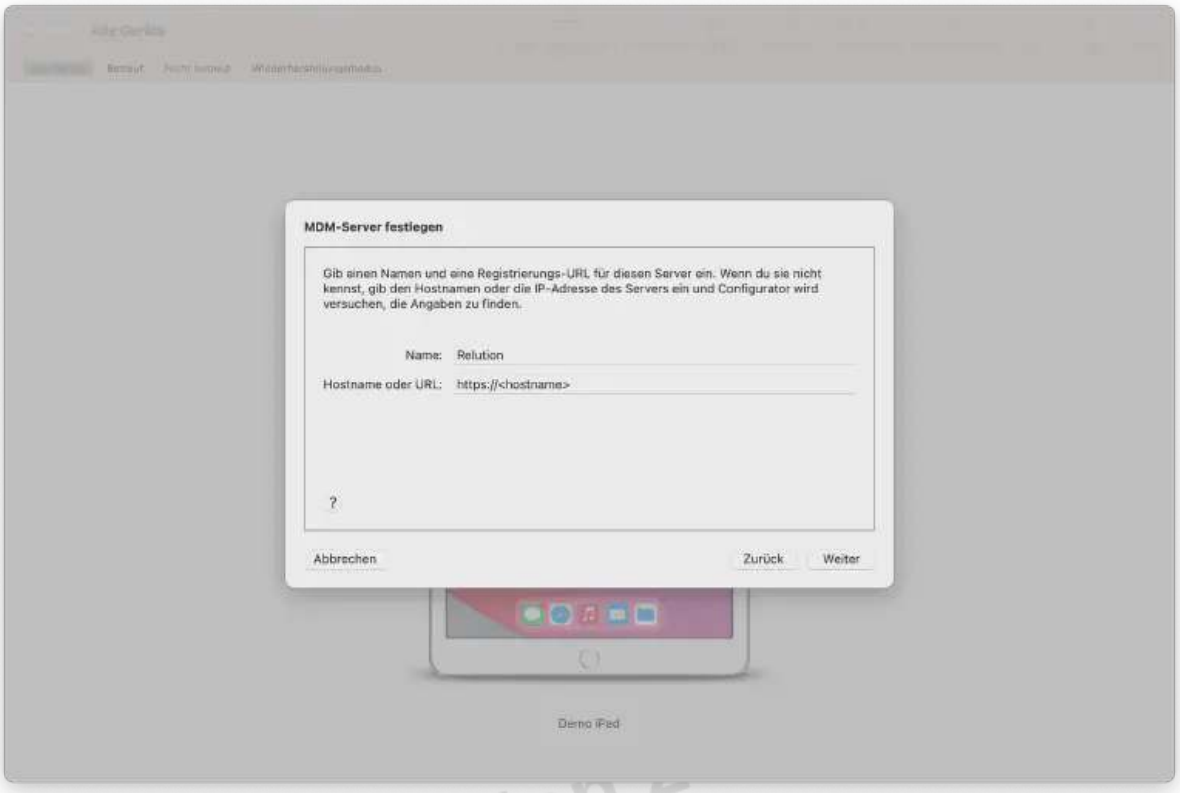
4. Optionen wählen:

    - Zu Apple Business Manager oder Apple School Manager hinzufügen.
    - Geräten erlauben, sich mit anderen Computern zu koppeln (aktivieren).
    - Wichtig: Die Option Aktivieren und Registrierung abschließen darf NICHT angewählt werden.



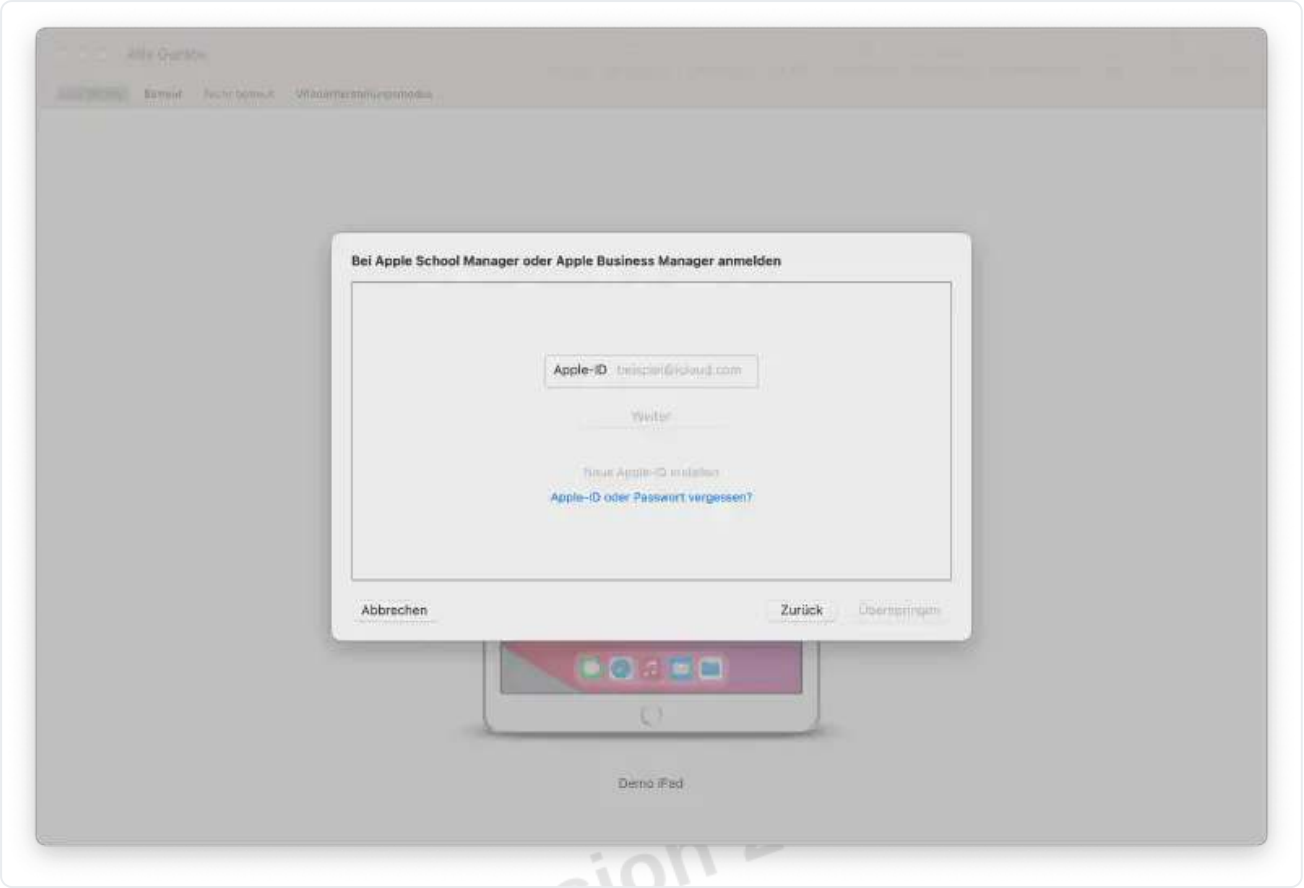
Für Version

5. Server-Konfiguration: Neuer Server wählen und die Relution-URL angeben:
   - Standard (iOS/iPadOS): `https://live.relution.io/`
   - Für tvOS: `https://live.relution.io/api/enrollment/v1/appleMdm/depenroll`



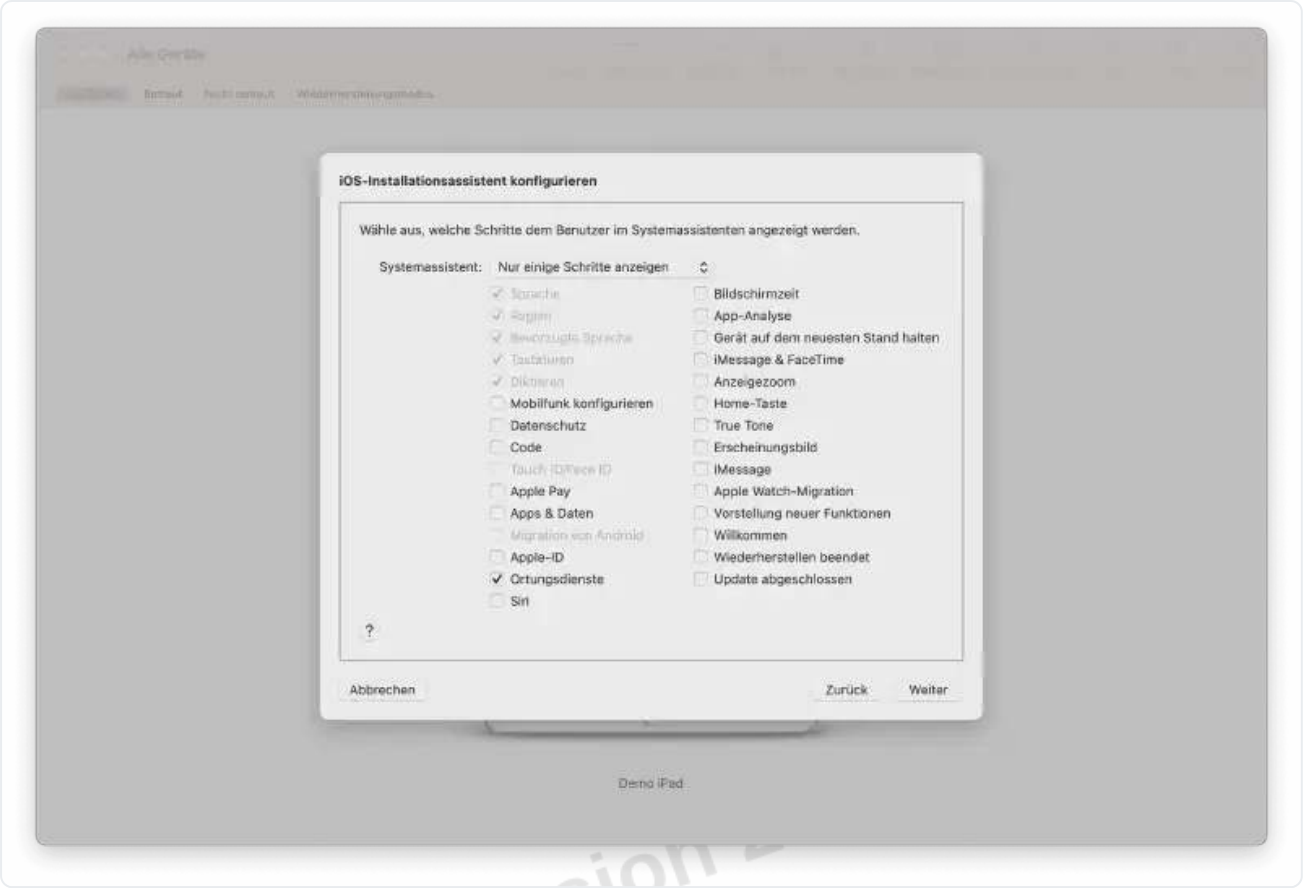
Für Version 2

6. Organisation: Neue Organisation wählen und sich mit der Apple-ID des ABM/ASM-Accounts anmelden (2-Faktor-Authentifizierung erforderlich).



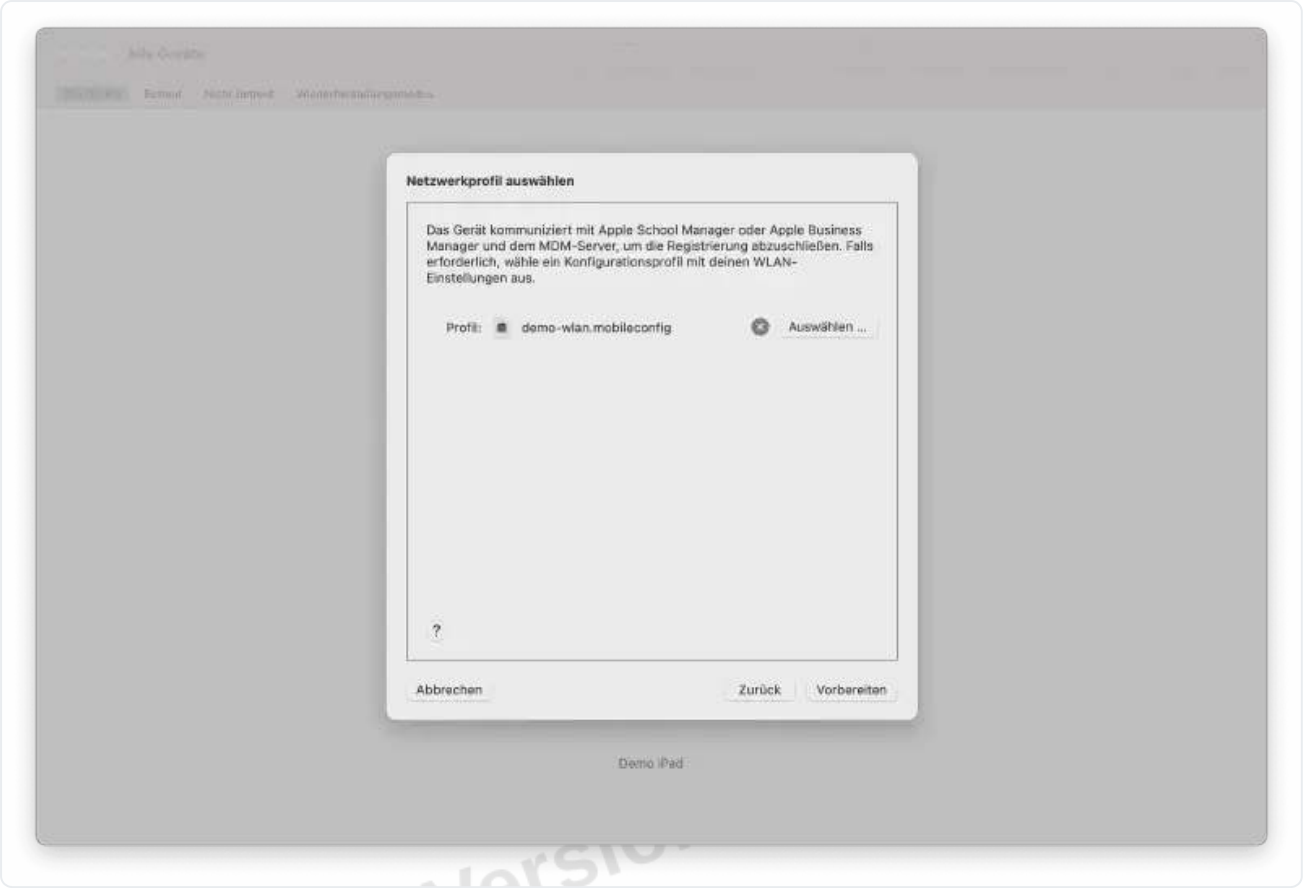
Für Version

7. Setup-Schritte: Die Schritte auswählen, die am Gerät nicht übersprungen werden sollen (Empfehlung: Ortungsdienste für korrekte Zeitzonen).



Für Version

8. Netzwerk-Zuweisung: Das zuvor erstellte WLAN-Konfigurationsprofil auswählen. Dies ermöglicht dem Gerät, die DEP-Registrierung nach dem Neustart an die Apple-Server zu übertragen.



Für Version

9. Abschluss: Auf Vorbereiten klicken. Das Gerät wird neu gestartet und im ABM/ASM hinterlegt.

Einschreibung abschließen

1. Zuweisung im Portal: Im Apple Business/School Manager einloggen. Die neuen Geräte dem Relution MDM-Server zuweisen.
2. Synchronisation: In Relution unter `Geräte` → `Auto-Einschreibungen` die Liste aktualisieren.
3. Profil-Zuweisung: Sicherstellen, dass den Geräten in Relution ein DEP-Profil zugewiesen und synchronisiert ist.
4. Aktivierung: Das Gerät neu starten und den Setup-Assistenten bis zur automatischen Konfiguration durchlaufen.

> Hinweis zur Karenzzeit: Bei nachträglich hinzugefügten Geräten besteht eine 30-tägige Frist. In dieser Zeit kann die MDM-Verwaltung vom Nutzer manuell in den Einstellungen entfernt werden. Erst nach Ablauf dieser Zeit wird die Sperre permanent.

Fehlerbehebung: Unexpected Error 33007

Sollte während des Vorgangs die Fehlermeldung „Provisional Enrollment failed. Network communication error [MCCloudConfigErrorDomain – 0x80EF (33007)]“ erscheinen, liegt dies meist an einer der folgenden Ursachen:

1. Das Gerät wird noch von einem anderen MDM verwaltet

Ein Gerät kann nicht in ein neues DEP-System (ABM/ASM) aufgenommen werden, solange es noch in einer anderen MDM-Instanz registriert oder gesperrt ist.

- Lösung: Das Gerät vollständig aus dem vorherigen MDM-System entfernen und es gegebenenfalls auf Werkseinstellungen zurücksetzen, bevor der Vorgang im Apple Configurator erneut gestartet wird.

2. Fehlende Internetverbindung während der Vorbereitung

Das Gerät benötigt während des “Provisional Enrollment” zwingend Zugriff auf die Apple-Server.

- Lösung: Sicherstellen, dass dem Gerät während des Vorbereitungsschritts ein WLAN-Profil zugewiesen wird, damit es sofort nach dem Neustart online gehen kann. Ohne aktive Internetverbindung schlägt die Kommunikation mit der Cloud Config Domain fehl.

Für Version 26.4.0

Einschreibungsarten

Um iOS-Geräte in Relution verwalten zu können, müssen diese zuerst eingeschrieben werden. Dieser Einschreibungsprozess kann auf drei unterschiedliche Arten erfolgen. Die Einschreibungsarten unterscheiden sich und wirken sich nachhaltig auf die späteren Funktionen aus.

Manuelle Einschreibung

Die Einschreibung wird durch ein manuell auf die Geräte heruntergeladenes und installiertes MDM-Profil vorgenommen. Hierzu muss entweder ein QR-Code auf den Geräten gescannt oder die entsprechende URL manuell aufgerufen werden. Im Anschluss muss das MDM-Profil auf den Geräten installiert werden.

Vorteile

- Die Einschreibung kann vorgenommen werden, ohne die Geräte auf Werkseinstellungen zurücksetzen zu müssen.

Nachteile

- Die Einschreibung kann jederzeit in den Einstellungen auf den Geräten entfernt werden (MDM-Profil).
- Nur bedingt für BYOD-Geräte geeignet, da Administratoren sehen können, welche Apps installiert sind.
- Nicht alle Aktionen und Richtlinien-Konfigurationen sind möglich.
- Geräte sind häufig nicht überwacht (Supervised Mode).

Für Version 26.4.0

Zur manuellen Einschreibung →
Supervision →

Automatisch über Apple DEP

Die iOS-Geräte bauen bei Inbetriebnahme eine Verbindung zum Apple Server auf und werden, sofern es sich um Geräte handelt, welche im DEP hinterlegt wurden, automatisch zum MDM Server umgeleitet und eingeschrieben. Der Vorgang kann erzwungen werden, sodass Benutzer diesen nicht überspringen können. Ebenso lässt sich die Funktion des Apple geteilten iPads aktivieren und das MDM-Profil auf den Geräten vor einer Löschung schützen. Hierzu ist ein Zugang mit entsprechenden Berechtigungen für den Apple School/Business Manager notwendig.

Vorteile

- Die Einschreibung findet weitgehend automatisch statt.
- Geräte werden vor Diebstahl geschützt.
- Die Einschreibung (MDM-Profil auf dem Gerät) kann nicht entfernt werden.
- Die Geräte befinden sich im überwachten Modus (Supervised Mode).
- Apple geteiltes iPad (Shared iPad) kann aktiviert werden.

Nachteile

- Die Geräte müssen zuvor auf Werkseinstellungen zurückgesetzt werden.

Zur automatischen Einschreibung →
Konfigurationsprofil für ADE →

Einschreibung über die Apple-Benutzer-Einschreibung (User Enrollment)

Hierbei handelt es sich um die typische Einschreibung für Bring Your Own Device-Geräte (BYOD). Die Benutzer können die Einschreibung selbst durchführen und die iOS-Geräte müssen nicht auf Werkseinstellungen zurückgesetzt werden.

Vorteile

- Administratoren können privat installierte Apps nicht einsehen.
- Geräte bleiben unter Kontrolle der Benutzer.

Nachteile

- Nicht alle Aktionen und Richtlinien-Konfigurationen sind möglich.
- Managed Apple IDs sind notwendig.

Zur Apple-Benutzer-Einschreibung für iOS →

Für Version 26.4.0

Benutzer Einschreibung

Mit der Benutzer-Einschreibung, auch `User Enrollment` genannt, lassen sich private iOS- und macOS-Geräte einschreiben, ohne dass Besitzer die gesamte Kontrolle über die Geräte abgeben müssen. So lassen sich basierend auf dem `Bring Your Own Device`-Ansatz (BYOD) private Geräte von Schüler oder Mitarbeiter im Schul- bzw. Unternehmenskontext unter Einhaltung des Schutzes privater Daten einbinden und nutzen.

Geräte dürfen sich für eine Apple-Benutzer-Einschreibung nicht im Überwachten Modus/Supervised Mode → befinden.

Es gibt zwei Varianten für die Benutzer-Einschreibung: Kontobasiert und profilbasiert (klassische manuelle Einschreibung).

Die profilbasierte Einschreibung steht ab iOS 18 nicht mehr zur Verfügung.

Vorteile

- Administratoren können privat installierte Apps nicht einsehen.
- Geräte bleiben unter Kontrolle der Benutzer.

Für Version 26.4.0

Nachteile

- Nicht alle Aktionen und Richtlinien-Konfigurationen sind möglich.
- Managed Apple IDs sind notwendig.

Einschreibung in Relution vorbereiten

Ausgehend von der Relution-Organisation kann klassisch eine manuelle Einschreibung für iOS- bzw. macOS-Geräte angelegt und der Einschreibungslink an die gewünschten Schüler oder Mitarbeiter gesendet werden.

Grundvoraussetzung für die Erstellung einer Benutzer-Einschreibung ist die Zuordnung von Benutzer. Für diese muss entweder eine `Managed Apple ID` oder `E-Mail-Adresse` in den Benutzer-Details hinterlegt werden. Anschließend können die entsprechenden Benutzer hinzugefügt und die Einschreibung abgeschlossen werden. Geräten zugewiesene Benutzer lassen sich bei eingeschriebenen Geräten via Benutzer-Einschreibung nicht mehr ändern bzw. entfernen.

Profilbasierte Benutzer-Einschreibung (bis iOS 17)

Über den empfangenen Einschreibungslink wird die Geräte-Einschreibung auf dem iOS- bzw. macOS-Gerät unter Verwendung der Managed Apple IDs der Benutzer durchgeführt und das Gerät erscheint automatisch im Geräte-Inventar der entsprechenden Relution-Organisation.

Kontogesteuerte Benutzer-Einschreibung

Relution unterstützt die kontobasierte Benutzer-Registrierung von iOS- und macOS-Geräten, die sich nicht im `Überwachter Modus` → (Supervised Mode) befinden.

Um die kontobasierte Benutzerregistrierung nutzen zu können, wird Folgendes benötigt:

- Service Discovery Well-Known Hosts

Eine Service Discovery muss konfiguriert werden, damit Apple die Geräte an den richtigen MDM Server übertragen kann. Dazu muss eine HTTP well-known Ressourcen-Datei an der Domain hinterlegt werden, mit der sich die Benutzer anmelden werden. Apple muss diese Datei über einen HTTP GET unter folgender URL abrufen können:

```
https://yourdomain.com/.well-known/com.apple.remotemanagement
```

Unter dem Punkt `yourdomain.com` muss die Domain hinterlegt werden, die auch für die Apple IDs genutzt wird. Die anzulegende Datei muss auf einer Domain hinterlegt werden, die mit HTTP GET Anfragen umgehen kann.

Die Datei im JSON-Format mit dem Inhaltstyp application/json anlegen. Um die richtigen Informationen in die Datei einzutragen, lassen sich die benötigten Informationen direkt aus dem Relution-Portal kopieren. Hierzu öffnen:

1. Einstellungen
2. Geräteverwaltung
3. Kontobasierte Apple Benutzerregistrierung
4. Den Schieberegler auf an setzen
5. Den Text in den geschweiften Klammern kopieren und in die eigene Datei einfügen.

Für Version 26.4.0

> Wichtig, damit die Datei richtig funktioniert darf die Datei keine Dateiendung haben.

Beispiel: maxmustermann@musterhausen.de

In diesem Beispiel wäre die Domain der ID `Musterhausen.de` Die Service Discovery muss also dort hinterlegt werden.

Mit der kontobasierten Benutzerregistrierung wird die Registrierung von persönlichen Geräten in Relution erheblich erleichtert. Sobald sich Relution-Benutzer über die Option `Bei Arbeits- oder Schulaccount anmelden...` in `VPN & Geräteverwaltung` der allgemeinen Einstellungen auf privaten Geräten registrieren, werden in Relution automatisch Benutzer-Einschreibungen erzeugt.

Über die Managed Apple ID der jeweiligen Benutzer wird die Registrierungs-URL der jeweiligen MDM-Lösung automatisch identifiziert. Nach Anmeldung mit den Login-Daten der Benutzer aus Relution tauchen die Geräte nach erfolgreicher Authentifizierung automatisch im Geräte-Inventar der entsprechenden Relution-Organisation auf.

Verwandte Themen

- Apple DEP und VPP Übersicht → — Übersicht zu Apple-Registrierungsprogrammen.
- Geräte nachträglich zu Apple DEP hinzufügen → — Anleitung zum Hinzufügen unsupervised Geräte.

Für Version 26.4.0

Manuelle Einschreibung

Die Einschreibung wird durch ein manuell auf die iOS-Geräte heruntergeladenes und installiertes MDM-Profil vorgenommen. Hierzu muss entweder ein QR-Code auf den Geräten gescannt oder die entsprechende URL manuell aufgerufen werden. Im Anschluss muss das MDM-Profil auf den Geräten installiert werden.

Vorteile

- Die Einschreibung kann vorgenommen werden, ohne die Geräte auf Werkseinstellungen zurücksetzen zu müssen.

Nachteile

- Die Einschreibung kann jederzeit in den Einstellungen auf den Geräten entfernt werden (MDM-Profil).
- Nur bedingt für BYOD-Geräte geeignet, da Administratoren sehen können, welche Apps installiert sind.
- Nicht alle Aktionen und Richtlinien-Konfigurationen sind möglich.
- Geräte sind häufig nicht überwacht (Supervised Mode).

Für Version 26.4.0

Um eine manuelle Einschreibung durchzuführen, muss diese in Relution zuerst angelegt werden. Hierzu im Menü auf `Geräte` → `Einschreibungen` wechseln und anschließend auf `Hinzufügen` klicken.

Einschreibungen sind abhängig vom Betriebssystem. Daher entweder `iOS, macOS oder tvOS` als `Plattform` und die `Geräteeinschreibung` als `Typ` wählen. Die `Eigentümerschaft` lässt sich entsprechend dieser wählen.

Um einen `Benutzer` mit dem einzuschreibenden Gerät zu verknüpfen, diesen auswählen. Benutzer sollten hierfür die Rolle Device User haben.

Jede Einschreibung ist nur einmalig nutzbar. Es sei denn, der Schalter für die `Mehrfach-Einschreibung` wird aktiviert. Ist dies der Fall, können über den Einschreibungslink solange neue Geräte eingeschrieben werden, bis entweder das Gültigkeitsdatum überschritten wurde oder keine Geräte-Lizenzen mehr in Relution verfügbar sind.

Unter `Richtlinien` und `Regelwerke` lassen sich ebensolche mit der Einschreibung verknüpfen. Wird das Gerät eingeschrieben, kommen diese direkt zur Anwendung.

Nach dem Speichern und Anlegen der Einschreibung besteht im Anschluss die Möglichkeit, den erstellten QR-Code auf dem iOS-Gerät zu scannen oder die URL manuell im Browser einzugeben. Das MDM-Profil wird über die Schaltfläche Einschreibung heruntergeladen und muss im nächsten Schritt auf dem Gerät in den `Einstellungen` unter `VPN und Geräteverwaltung` installiert werden.

Schritt-für-Schritt-Anleitung

1. Die Einschreibung starten, indem auf `Einschreibung` gedrückt wird.
2. Dann auf `Zulassen` drücken.
3. Das nächste Fenster mit `Schließen` schließen.
4. In die `Einstellungen` wechseln.
5. Dort in den Bereich `Allgemein`.
6. Ganz unten auf `VPN und Geräteverwaltung` drücken.
7. Das geladene MDM-Profil auswählen.
8. Das MDM-Profil prüfen, auf `Installieren` drücken und den Dialog erneut durch Drücken auf `Installieren` bestätigen.
9. Es wird eine Sicherheitsmeldung eingeblendet. Auch hier auf `Installieren` drücken.
10. Der entfernten Verwaltung mit `Vertrauen` zustimmen.
11. Mit der Bestätigung auf `Fertig` ist das MDM-Profil installiert.

Damit ist die Einschreibung abgeschlossen.
Nun wird der Relution Agent auf dem Gerät installiert und im Geräte-Inventar des Relution-Portals sollte ein neuer Eintrag erscheinen.

Für Version 26.4.0

Apple-Geräte migrieren

Mit dem Release von iOS 26 bietet Apple nun die Migration von verwalteten Apple-Geräten von einer Mobile Device Management-Lösung (MDM) wie beispielsweise Jamf oder iServ zu Relution an. Ziel ist, die Geräte vollständig zu übernehmen, ohne sie zurückzusetzen, ohne manuelle Neuregistrierung und ohne Verlust bestehender Konfigurationen, Apps oder Managed Apple IDs.

Gerätevoraussetzungen

- Ein iPhone, iPad oder Mac, der verwaltet wird (MDM–Profil aktiv) via DEP über den Apple Business Manager (ABM) oder Apple School Manager (ASM).
- Gerät befindet sich im Modus „Supervised“ (voll betreut).
- Betriebssystemversion iOS/iPadOS 26+ oder macOS 26+.
- Das iPad darf nicht im Modus „Geteiltes iPad” (Shared iPad) betrieben werden – für Shared iPads steht die Migration nicht zur Verfügung; diese Geräte müssen zurückgesetzt und neu eingeschrieben werden.
- Das Gerät darf sich nicht im Single App Mode (Kiosk-Modus) befinden – dieser muss vor der Migration deaktiviert werden, andernfalls kann die Migration nicht durchgeführt werden.

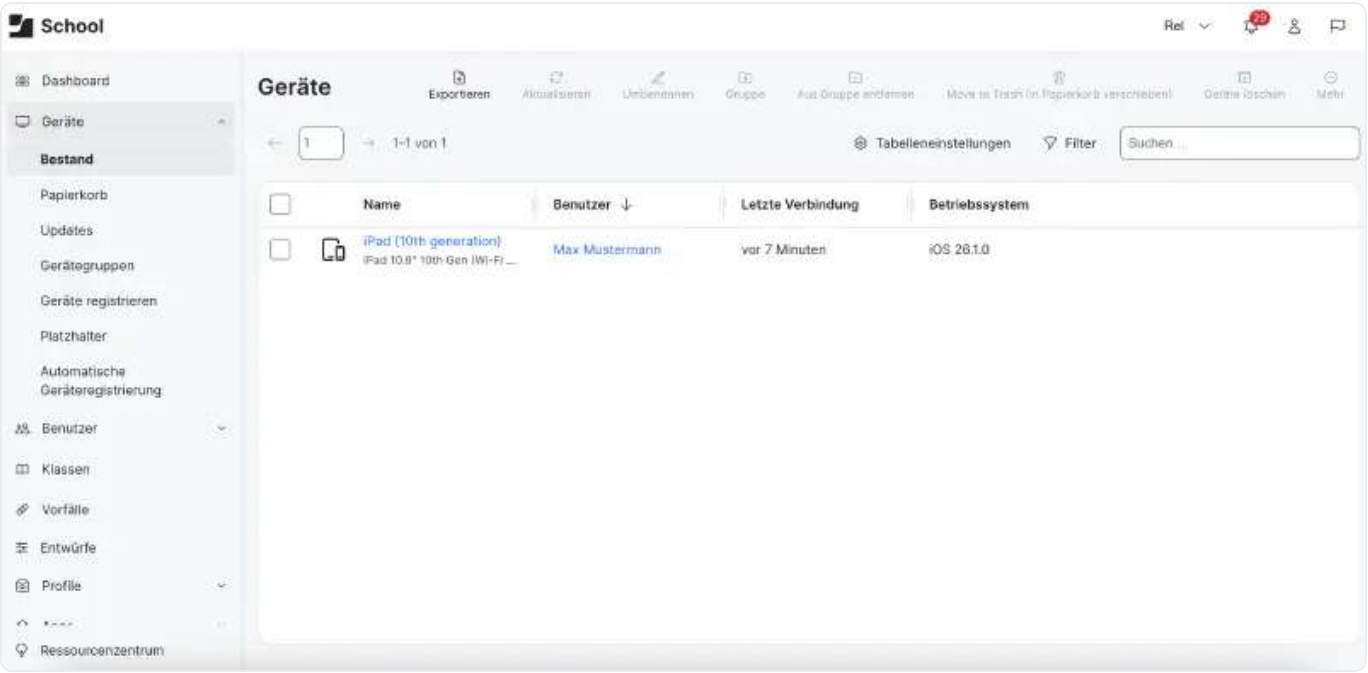
MDM-Voraussetzungen

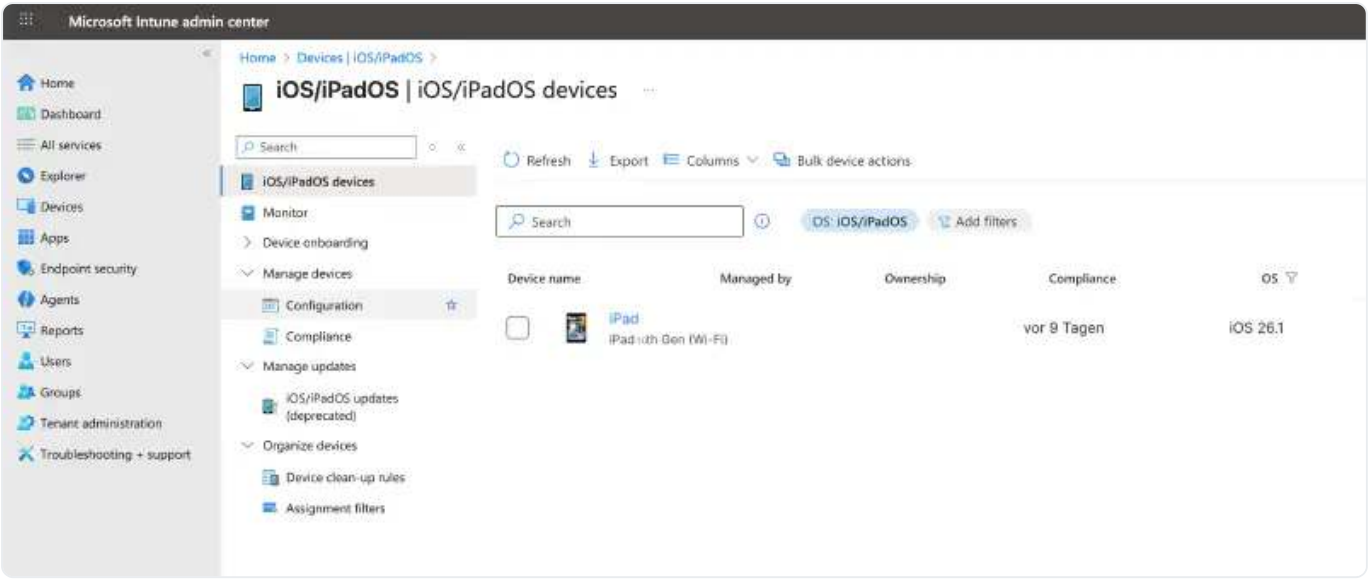
- Bestehendes Drittanbieter MDM-System erlaubt Gerätezuweisung bzw. Übertragung via ABM/ASM. In Relution wird dieses Feature seit Version `5.34` unterstützt.
- Relution ist im ABM/ASM als MDM-Server registriert und betriebsbereit.

Für Version 26.4.0

Überprüfen der Geräte in Drittanbieter MDM

- Die Geräte, die zu Relution migriert werden sollen, müssen im Drittanbieter MDM sichtbar sein – wie in den folgenden Beispielen dargestellt.
- Weitere Konfigurationen im alten MDM sind für die Migration der Geräte zu Relution nicht erforderlich.



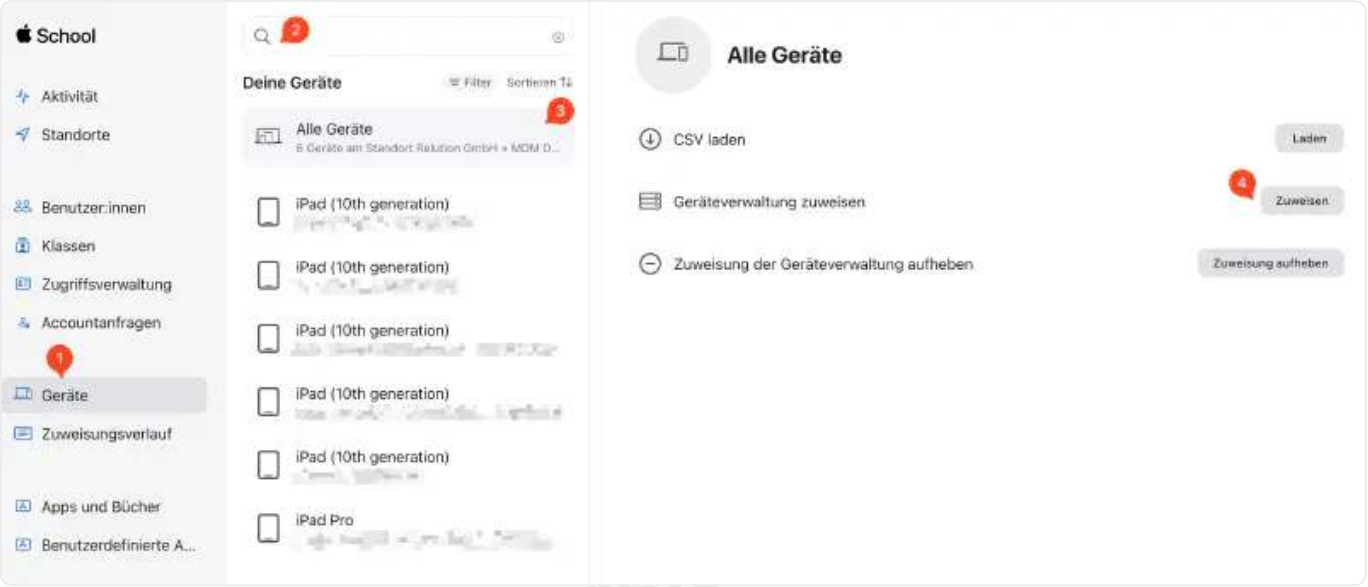


Vorbereitung in Relution

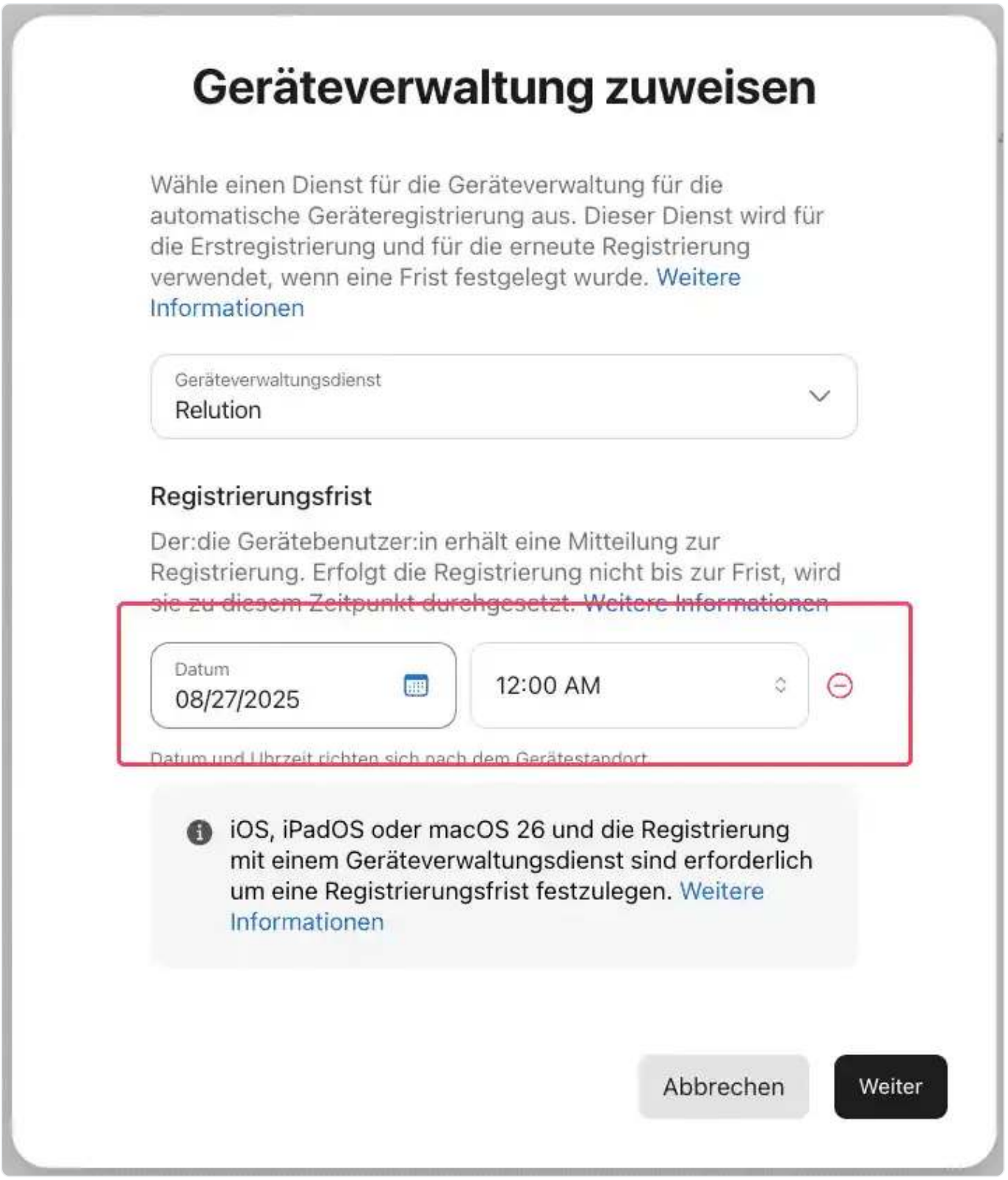
- In Relution prüfen, ob der DEP → und der VPP → Token verfügbar und gültig sind.
- Eine Gerätegruppe erstellen oder identifizieren, die die zu migrierenden Geräte enthalten soll.
- Alle benötigten Konfigurationen (Profile, Zertifikate, Apps) in Relution anlegen.
- Um Fehlkonfigurationen zu vermeiden, empfiehlt es sich, die Migration zunächst mit Testgeräten durchzuführen.
- Im DEP-Profil die Einstellung „Apps installieren und konfigurieren, bevor mit dem Setup-Assistenten fortgefahren wird“ anpassen. Andernfalls wird dem Gerät bei der Einschreibung kein Profil automatisch zugewiesen.

Zuweisung im ABM/ASM

- Beim Apple Business Manager oder Apple School Manager anmelden.
- Zu `Geräte` → `Alle Geräte` navigieren und nach Seriennummern der zu migrierenden Geräte filtern.
- Die Geräte auswählen → Geräteverwaltung zuweisen.
- Im Dialogfeld: Relution als neuen Server auswählen.
- Es sollte eine Migrationsfrist festgelegt werden; Der Benutzer hat somit Zeit bis zu der Frist die Migration abzuschließen, danach muss der Benutzer die Migration durchführen um das Gerät weiterverwenden zu können.
- Die Änderung bestätigen – Apple markiert die Geräte nun für Relution.

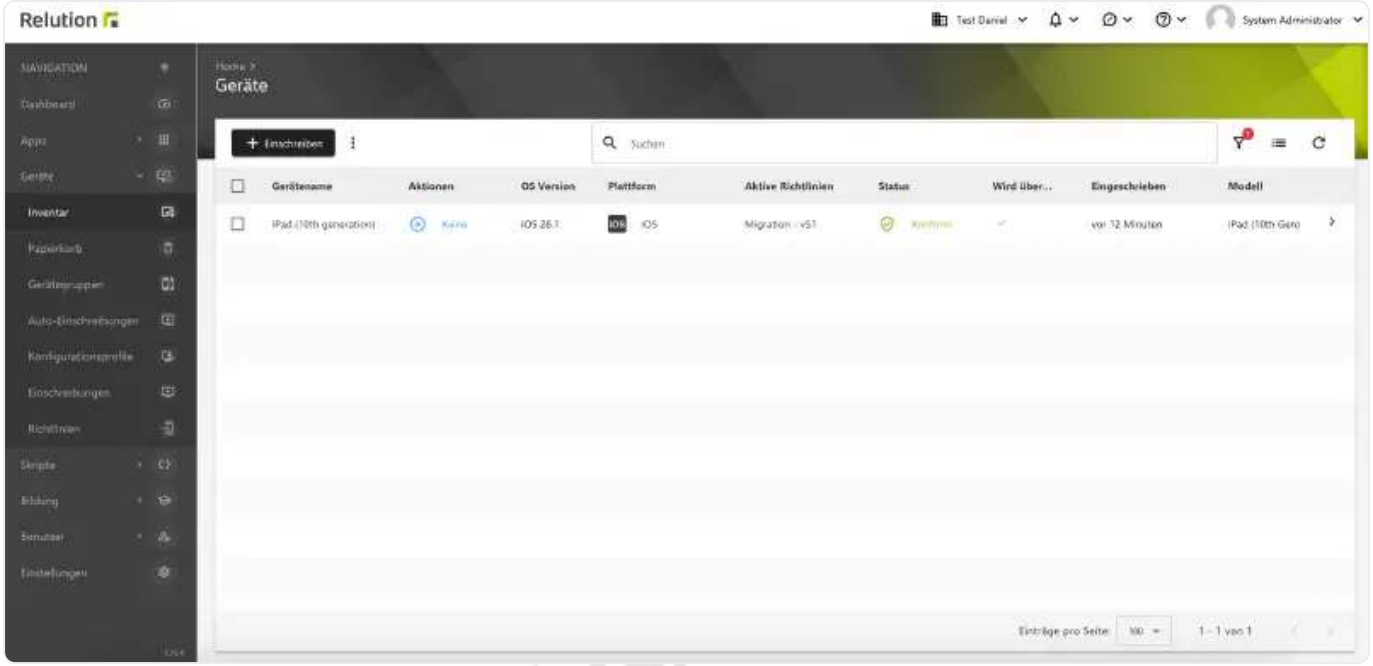


Für Versi

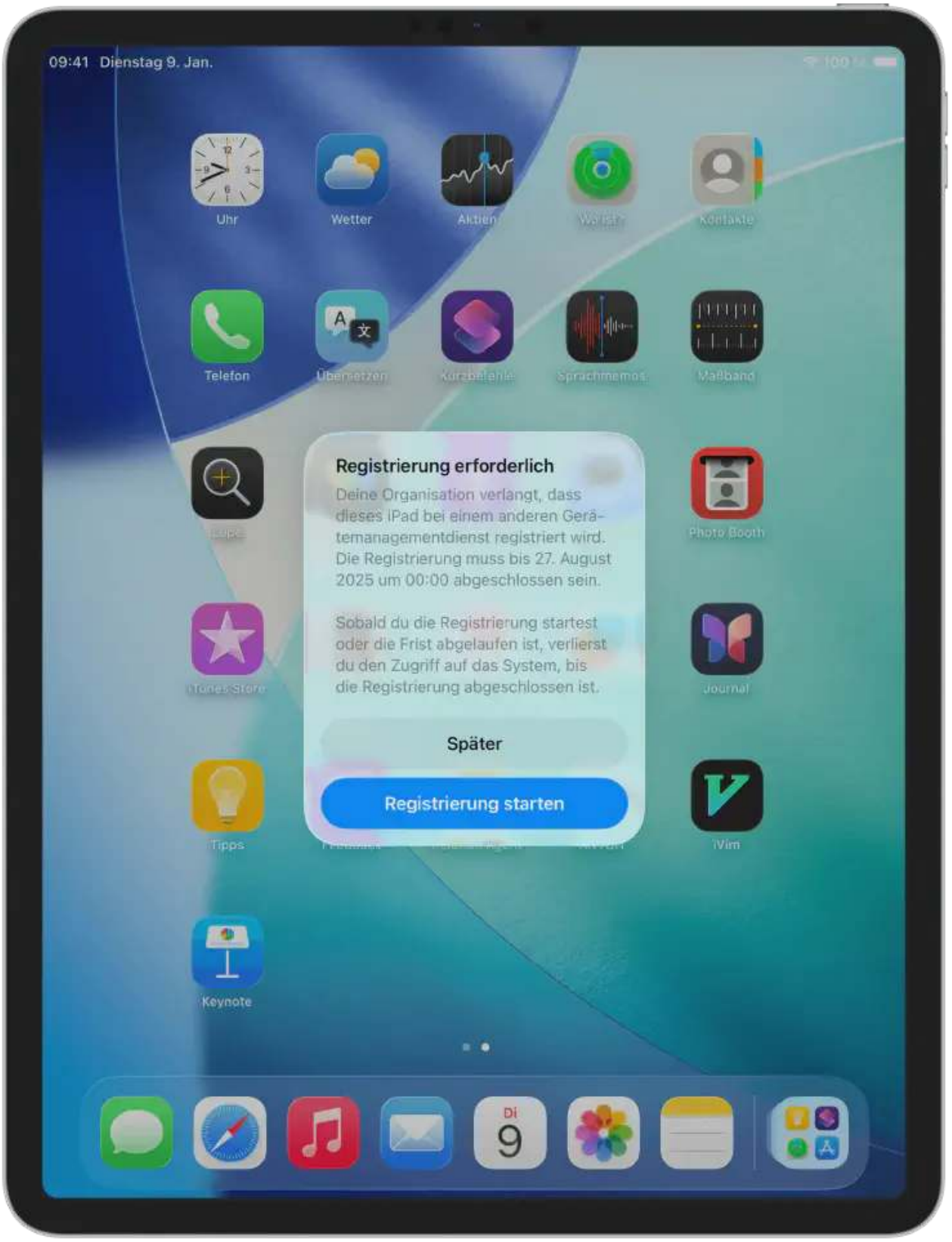

Geräteverwaltung zuweisen
Wählen einen Dienst für die Geräteverwaltung für die automatische Geräteregistrierung aus. Dieser Dienst wird für die Erstregistrierung und für die erneute Registrierung verwendet, wenn eine Frist festgelegt wurde. Weitere Informationen
Geräteverwaltungsdienst
Relution
Registrierungsfrist
Der:die Gerätebenutzer:in erhält eine Mitteilung zur Registrierung. Erfolgt die Registrierung nicht bis zur Frist, wird sie zu diesem Zeitpunkt durchgesetzt. Weitere Informationen
Datum
08/27/2025
12:00 AM
Datum und Uhrzeit richten sich nach dem Gerätestandort.
iOS, iPadOS oder macOS 26 und die Registrierung mit einem Geräteverwaltungsdienst sind erforderlich um eine Registrierungsfrist festzulegen. Weitere Informationen
Abbrechen
Weiter

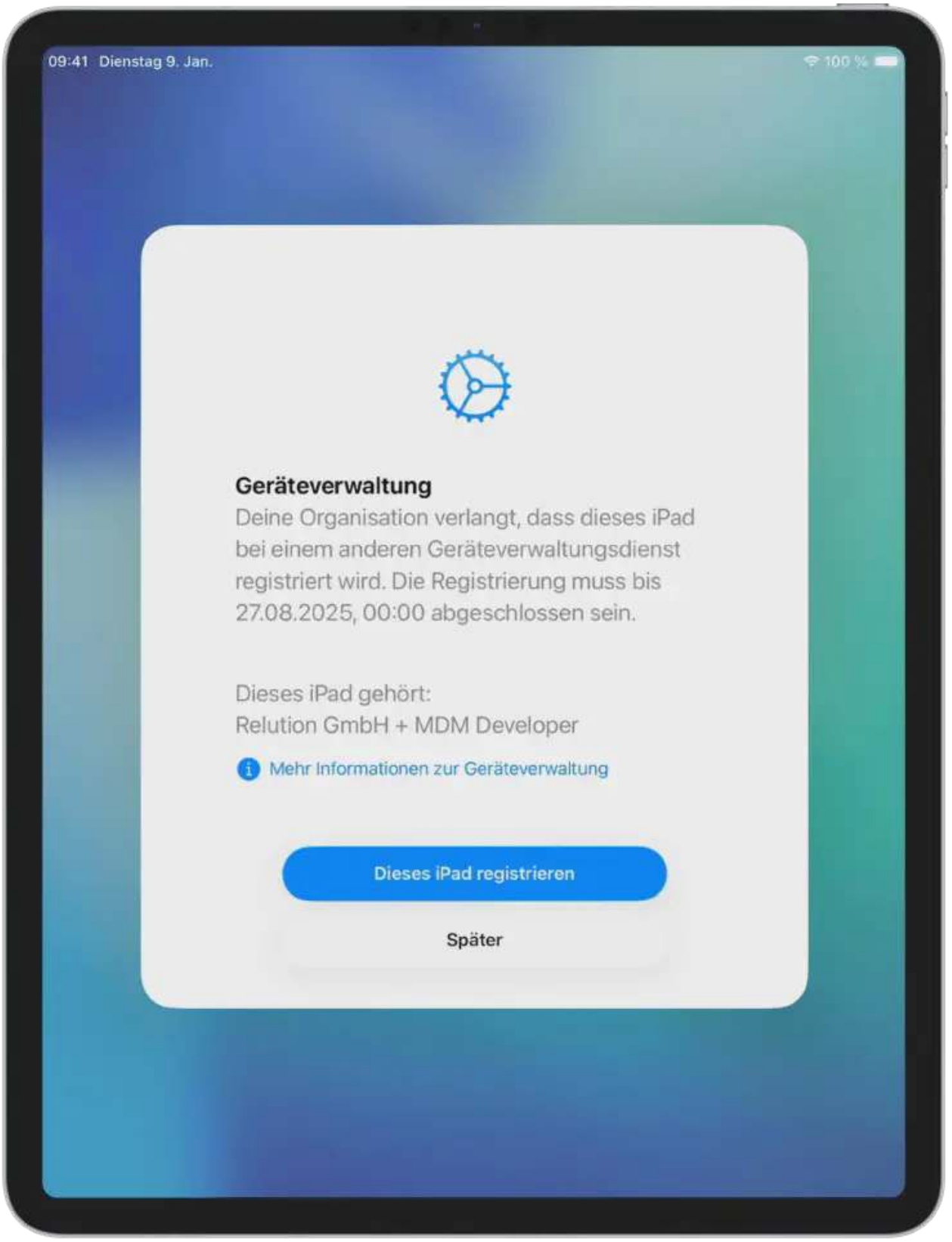
Migration auf dem Gerät

- Für eine direkte Migration kann auf dem Gerät `Einstellungen` → `Allgemein` → `VPN & Geräteverwaltung` die Migration gestartet werden mit Klick auf Registrierung starten.
- Wenn der Vorgang gestartet wird, wird das Gerät beim alten MDM entfernt und zu Relution hinzugefügt, ohne Zurücksetzung auf Werkseinstellung.
- Nach Abschluss erscheint das Gerät in Relution als verwaltet.



Für Vers


09:41 Dienstag 9. Jan.
Uhr
Wetter
Aktien
Kontakte
Telefon
Übersetzen
Kurzbefehle
Sprachmemos
Maßband
Photo Booth
Journal
Tipps
iVim
Keynote
Registrierung erforderlich
Deine Organisation verlangt, dass dieses iPad bei einem anderen Gerätemanagementdienst registriert wird. Die Registrierung muss bis 27. August 2025 um 00:00 abgeschlossen sein.
Sobald du die Registrierung startest oder die Frist abgelaufen ist, verlierst du den Zugriff auf das System, bis die Registrierung abgeschlossen ist.
Später
Registrierung starten
Di
9


09:41 Dienstag 9. Jan.
100 %
Geräteverwaltung
Deine Organisation verlangt, dass dieses iPad bei einem anderen Geräteverwaltungsdienst registriert wird. Die Registrierung muss bis 27.08.2025, 00:00 abgeschlossen sein.
Dieses iPad gehört:
Relution GmbH + MDM Developer
Mehr Informationen zur Geräteverwaltung
Dieses iPad registrieren
Später

Grenzen & Hinweise

- Geräte, die nicht über DEP betreut werden und nicht im ABM/ASM geführt werden, müssen neu eingeschrieben werden.
- Damit die Migration unter iOS 26 funktioniert, muss im ASM/ABM eine Frist gesetzt werden. Ist die Option ausgegraut, steht die Migration nicht zur Verfügung.
- Die Migrationsoption im ASM/ABM kann erst bis zu zwei Tage nach dem Update auf iOS 26 erscheinen.

Für Version 26.4.0

Nicht überwachtes Gerät supervised registrieren

Ein nicht überwachtes (unsupervised) iOS-Gerät kann nachträglich bei Apple DEP registriert werden, ohne dass Nutzer ihre Daten und Inhalte verlieren. Laut Apple-Dokumentation übernimmt eine Wiederherstellung jedoch den Geräteverwaltung-Status aus dem Backup, wenn dabei auf demselben Gerät wiederhergestellt wird - ein nicht überwachtes Gerät lässt sich also nicht direkt aus seinem eigenen Backup in den supervised DEP-Zustand überführen. Der folgende Workaround leitet das Backup deshalb über ein zweites, temporäres Gerät um: Da die Wiederherstellung damit als Wiederherstellung auf einem anderen Gerät zählt, übernimmt Apple den Verwaltungsstatus stattdessen von Apple School/ Business Manager.

Apple beschreibt dieses Verhalten so:

- Bei der Wiederherstellung von einem Backup auf dasselbe iPhone oder iPad wird der Geräteverwaltung-Status aus dem Backup wiederhergestellt.
- Bei der Wiederherstellung von einem Backup auf einem anderen iPhone oder iPad stammt der Geräteverwaltung-Status von Apple School/ Business Manager.

Beispiel

Ist ein Gerät so konfiguriert, dass es supervised und automatisch im MDM-System registriert wird, anschließend aber aus einem Backup wiederhergestellt wird, das erstellt wurde, als dasselbe Gerät nicht überwacht war, wird das Gerät nicht überwacht. Ein nicht überwachtes Gerät lässt sich also nicht direkt aus seinem eigenen Backup wiederherstellen, wenn dabei `Überwachter Modus` aktiviert und das Gerät bei Apple DEP registriert werden soll - genau deshalb ist der Umweg über ein zweites Gerät nötig.

Für Version 26.4.0

DEP-Recovery-Profil vorbereiten

In Relution ein eigenes, temporäres DEP-Profil für diesen Workaround anlegen mit folgenden Einstellungen:

- Aktivieren von `Verbinden mit Macs oder PCs und Konfigurieren mit Apple Configurator erlauben`.
- Setup-Schritt `Geräteortung zulassen` nicht überspringen.
- Setup-Schritt `Backup einspielen` nicht überspringen.
- Setup-Schritt `Mit Apple ID anmelden` nicht überspringen.

Mehr zur Konfiguration eines DEP-Profils in Relution: Konfigurationsprofil für ADE →

Ablauf

Für Gerät-01 und Gerät-02 muss dieselbe Betriebssystemversion installiert sein. Außerdem ist sicherzustellen, dass `Mein iPhone suchen` auf beiden Geräten deaktiviert ist, da eine aktive Gerätesuche die Sicherung oder Wiederherstellung eines Backups verhindern kann.

1. Sicherung

Ein Backup am nicht überwachten Gerät-01 über iCloud oder lokal auf einem Mac oder PC erstellen. Dieses Backup auf ein zweites Gerät, Gerät-02, einspielen. Anschließend von Gerät-02 erneut ein Backup über iCloud oder lokal erstellen - dieses zweite Backup wird später auf Gerät-01 zurückgespielt und gilt dabei als Backup „eines anderen Geräts“.

2. Vorbereitung

Gerät-01 auf Werkseinstellungen zurücksetzen. Gerät-01 über den Apple Configurator 2 zum Apple School/ Business Manager hinzufügen. Mehr dazu unter Apple-Geräte nachträglich zum DEP hinzufügen →. Gerät-01 außerdem das zuvor erstellte DEP-Recovery-Profil zuweisen.

3. Einbindung in Relution

Gerät-01 per Apple School/ Business Manager dem entsprechenden Relution Server mit dem zuvor erstellten DEP-Recovery-Profil zuweisen. Das Gerät einrichten, indem der Einrichtungsassistent auf dem Gerät durchlaufen wird.

4. Backup wiederherstellen

Am Gerät-01 im Einrichtungsassistenten den Punkt `Wiederherstellung von Apps und Daten` auswählen und das zuvor erstellte Backup von Gerät-02 wählen. Bei einem iCloud-Backup muss dieselbe Apple ID für die Wiederherstellung verwendet werden, die bei der Sicherung verwendet wurde.

Weil das Backup technisch von Gerät-02 stammt, zählt die Wiederherstellung als Wiederherstellung auf einem anderen Gerät: Die Einstellungen zur Geräteverwaltung werden nicht aus dem Backup übernommen, sondern aus dem in Relution konfigurierten DEP-Profil - Gerät-01 wird dadurch supervised und DEP-registriert.

Nach erfolgreicher Wiederherstellung wieder auf das ursprüngliche Standard-DEP-Profil zurückwechseln. Der Setup-Schritt zum Wiederherstellen des Backups auf dem Gerät wird dann nicht mehr angezeigt.

Für Version 26.4.0

Einschreibung aufheben

Mit dem Aufheben der Einschreibung endet die Verwaltung eines Geräts durch Relution. Die Einschreibung wird aufgehoben, indem das Gerät gelöscht wird: Die Aktion Löschen steht im Geräteinventar sowie in den Gerätedetails zur Verfügung. Nach Bestätigung des Löschdialogs wird das MDM-Profil — einschließlich aller über Relution verteilten Konfigurationen, Zertifikate und verwalteten Apps — vom Gerät entfernt und das Gerät wird aus dem Inventar gelöscht. Das Gerät selbst wird nicht zurückgesetzt; persönliche Daten bleiben auf dem Gerät erhalten.

Der Vorgang wird im Audit-Protokoll aufgezeichnet; eine erneute Einschreibung des Geräts ist jederzeit möglich. Dies gilt für Geräte, die über die Manuelle Einschreibung → oder die Benutzer Einschreibung → eingeschrieben wurden.

Über Automated Device Enrollment (DEP) eingeschriebene Geräte

Durch das Löschen eines Geräts in Relution wird es nicht aus dem Apple School Manager oder Apple Business Manager entfernt. Soll ein Gerät die Organisation dauerhaft verlassen — etwa für eine anschließende private Nutzung —, muss es zusätzlich aus dem Apple DEP entfernt werden. Die vollständige Vorgehensweise ist unter Geräte entfernen → beschrieben.

Papierkorb

Gelöschte Geräte werden zunächst in den Papierkorb des Geräteinventars verschoben. Erst durch erneutes Löschen im Papierkorb wird ein Gerät endgültig aus Relution entfernt.

Für Version 26.4.0

Überwachter Modus / Supervision

`Überwachter Modus`, auch `Supervision` genannt, ist eine von Apple eingeführte Bereitstellungsstrategie zur Verwaltung von iOS-, macOS- und tvOS-Geräte durch Organisationen. Seit der Einführung mit iOS 5 steht Organisationen `Supervision` als effektive Methode zur Verwaltung von Apple-Geräten zur Verfügung. `Supervision` bedeutet, dass eine Organisation Eigentümer der Geräte ist und die vollständige Kontrolle über sie hat. Endanwender können auf überwachte Geräte zugreifen und sie nutzen; die Organisation hat jedoch die vollumfängliche administrative Kontrolle. So kann der Eigentümer entscheiden, welche Funktionen auf den Geräten verwendet werden dürfen, indem es erweiterte Einschränkungen durchsetzt oder die Geräteeinstellungen per MDM-System anpasst.

Relution unterstützt die Einschreibungsart über Apple DEP, um Geräte in `Überwachter Modus` zu bringen.

Automatische Einschreibung →

Geräte in Überwachter Modus / Supervised Mode versetzen

Um über ein MDM-System auf alle Funktionen von Apple-Geräten zugreifen zu können, müssen diese überwacht bzw. supervised sein. Dieser Zustand wird über die Aufnahme der Geräte in das Apple `Device Enrollment Program` (DEP) erreicht. Hierzu ist es notwendig, die Geräte in den Apple School/Business Manager hinzuzufügen. Sind Geräte bereits hinterlegt, kann im folgenden Bereich weitergelesen werden.

Automatische Einschreibung →

Für Version 26.4.0

iOS- und tvOS-Geräte zum Apple School / Business Manager hinzufügen

> Benötigt werden ein Mac und die Software Apple Configurator 2.

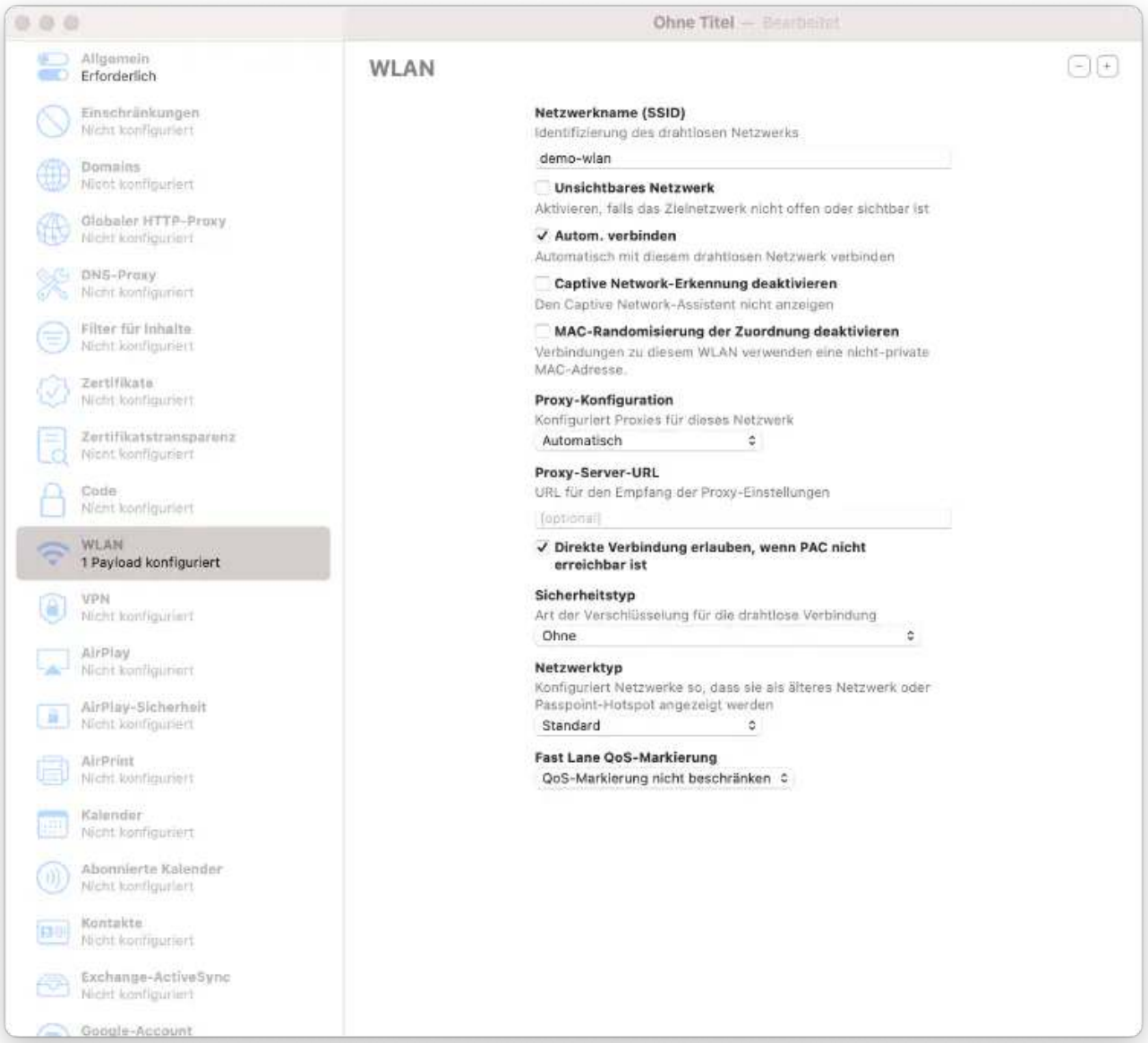
`Apple Configurator 2` ist eine kostenlose App, die im Mac App Store verfügbar ist. Mit der Anwendung lassen sich über USB verbundene Apple-Geräte manuell mit einem Mac Computer konfigurieren, bevor die Geräte an Benutzer ausgehändigt werden. Hierzu können sogenannte Profile erstellt und auf die Geräte angewendet werden. Zudem ermöglicht es der `Apple Configurator 2` Apple-Geräte, die nicht bereits von einem autorisierten Wiederverkäufer zum DEP hinzugefügt wurden, nachträglich ins DEP aufzunehmen. Diese Option steht ausschließlich für iPhones, iPads und Apple TVs zur Verfügung. macOS-Geräte müssen zwingend von einem autorisierten Wiederverkäufer gekauft werden, um von den Vorzügen der automatischen Einschreibung über Apple DEP zu profitieren. Insgesamt empfiehlt es sich, direkt DEP-Geräte zu beschaffen, da ein nachträgliches Hinzufügen mit manuellen Aufwänden verbunden ist.

Apple-Geräte, die nachträglich über `Apple Configurator 2` im Apple School/Business Manager registriert sind, funktionieren in den ersten 30 Tagen nach der Bereitstellung nicht wie direkt im DEP registrierte Geräte beim Kauf über einen autorisierten Wiederverkäufer. Selbst wenn die manuelle Entfernung der MDM-Verwaltung auf den Geräten über das zugehörige DEP-Profil im MDM-System blockiert wurde, können Benutzer die MDM-Verwaltung unter `Einstellungen` → `Allgemein` → `Profile` entfernen.

Mit Ablauf der 30-Tage-Frist ab Registrierung werden Benutzer daran gehindert, die MDM-Verwaltung auf den Geräten zu entfernen.

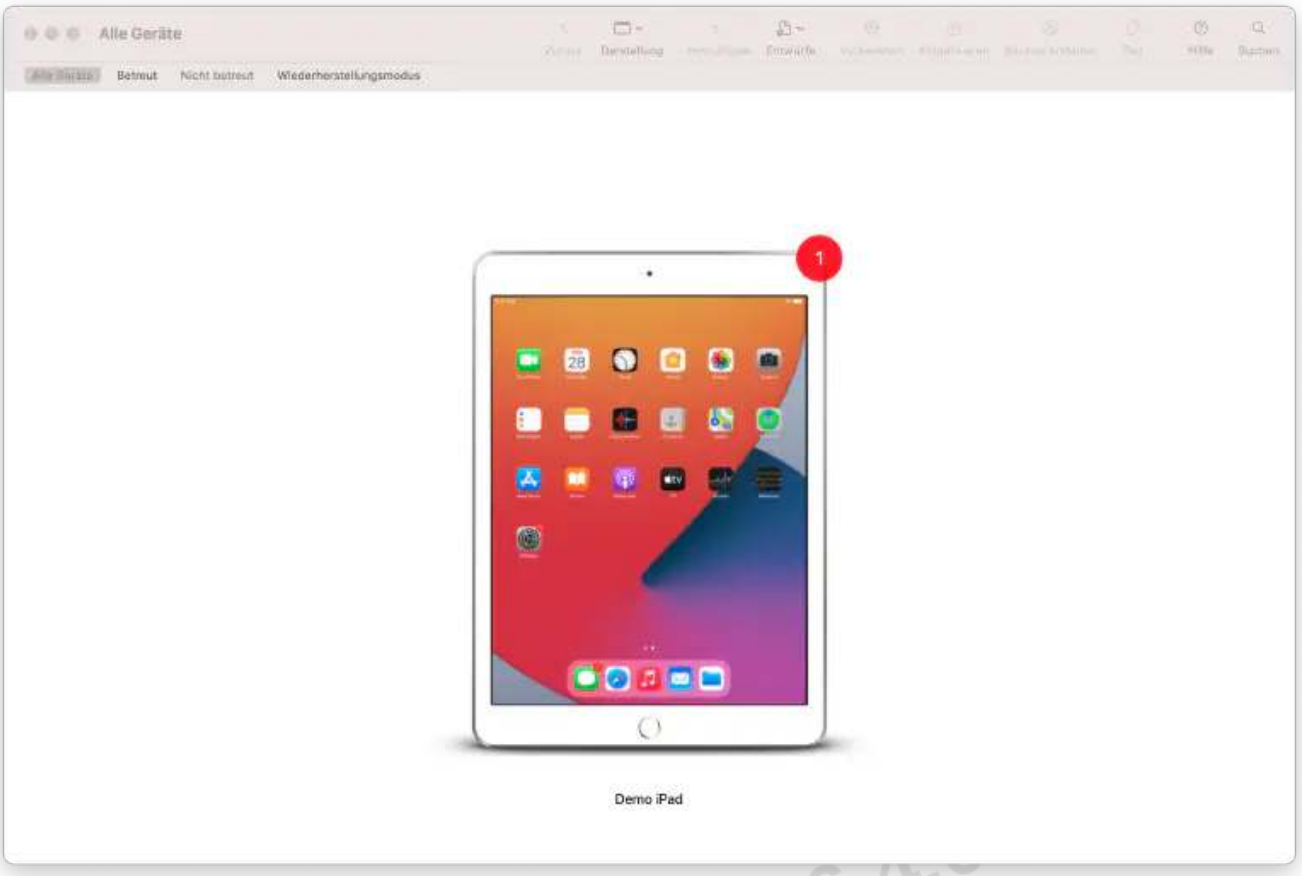
Vorbereitung

Damit Apple-Geräte automatisch eine Internetverbindung herstellen können und die nachträgliche Registrierung zu DEP möglichst komfortabel durchgeführt werden kann, empfiehlt es sich im Vorfeld, ein `WLAN-Profil` anzulegen. Dies kann auf einem Mac über den Menüpunkt `Ablage` → `Neues Profil` → `WLAN` erstellt und anschließend als Datei gespeichert werden.



Geräte zu DEP hinzufügen

Die Apple-Geräte müssen über ein USB-Kabel mit einem Mac Computer verbunden werden, auf dem anschließend der `Apple Configurator 2` gestartet wird. Es erscheint folgender Dialog:

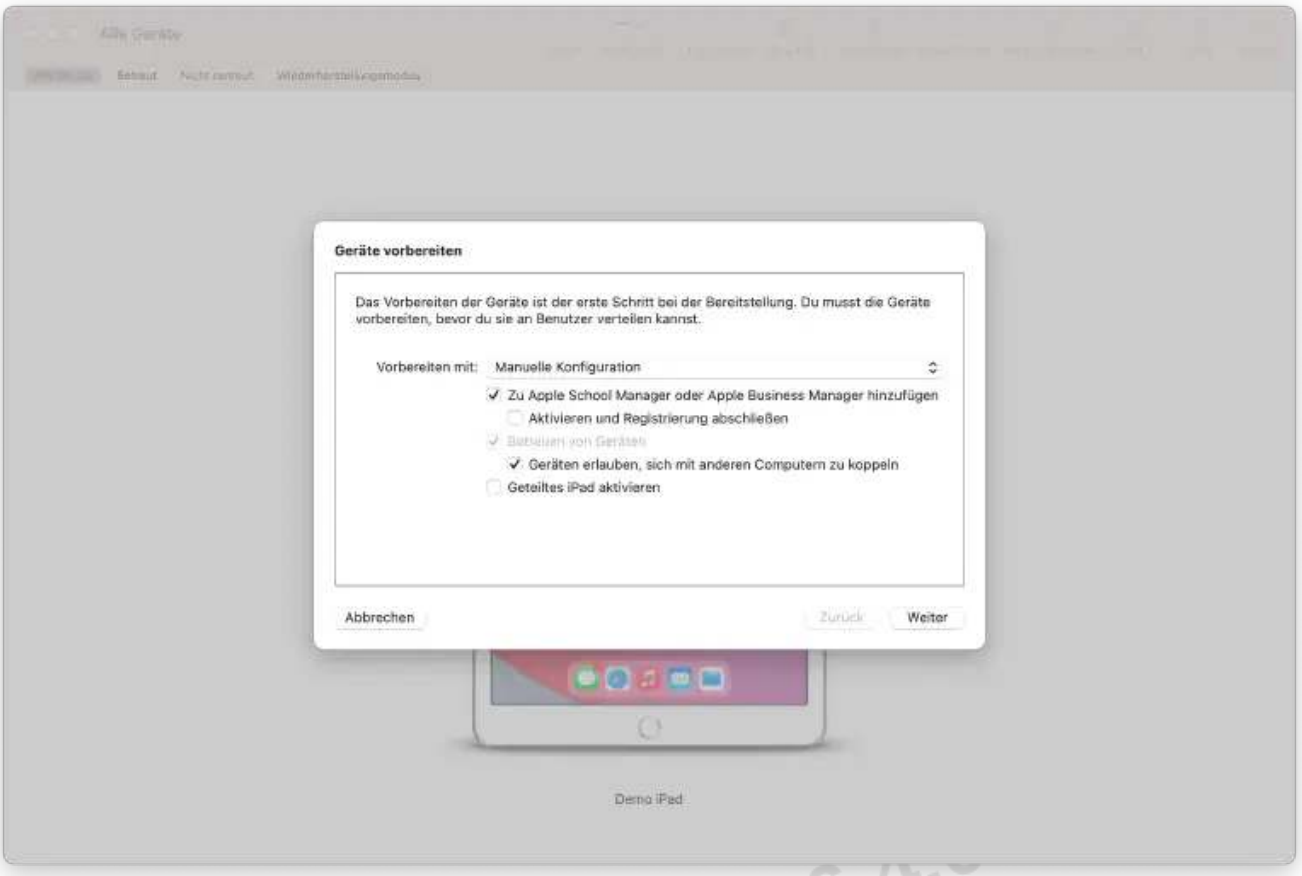


Das dargestellte Gerät mit der rechten Maustaste auswählen und `Vorbereiten...` klicken. Im nächsten Schritt müssen folgende Optionen gewählt werden:

- Zu Apple School Manager oder Apple Business Manager hinzufügen (Bildungseinrichtungen/ Firmenkunden).
- Geräten erlauben, sich mit anderen Computern zu koppeln.

> Die Option Aktivieren und Registrierung abschließen darf nicht angewählt werden, da das Gerät sonst direkt versucht, eine Einschreibung durchzuführen. Hierzu sind nach dem Hinzufügen zu DEP jedoch noch weitere Konfigurationen im Apple School/Business Manager und in Relution notwendig.

Für Version 26.4.0



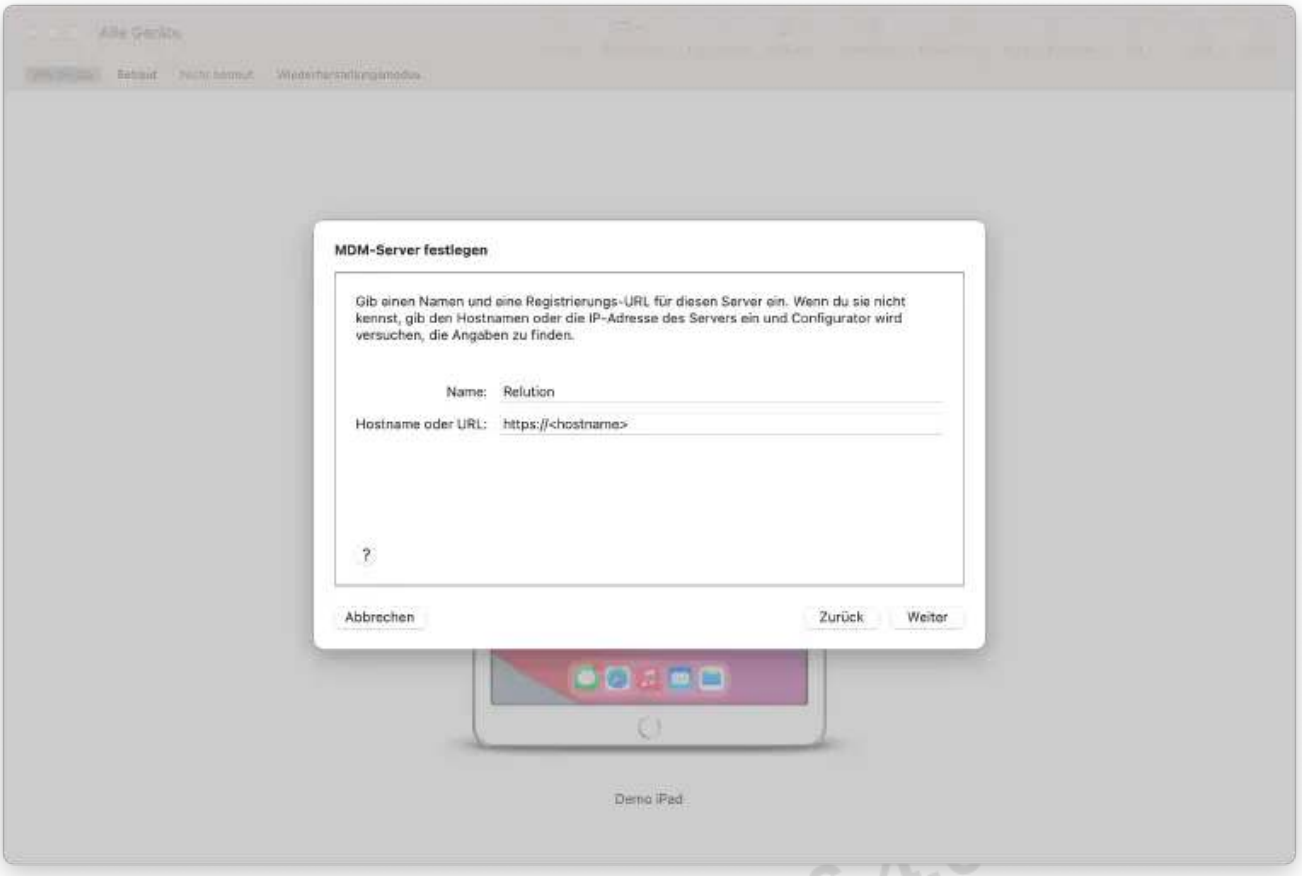
Für Version 26.4.0

Im nächsten Schritt `Neuer Server...` auswählen und `Weiter` klicken.

Nun wird der Name und die URL des entsprechenden Relution Servers angegeben. Der Name kann beliebig gewählt werden. Die URL beginnt mit `https://` und lautet z.B. für das Relution-Livesystem:

- für iOS-Geräte `https://live.relution.io/`
- für tvOS-Geräte `https://live.relution.io/api/enrollment/v1/appleMdm/depenroll`.

> Die URLs gelten für das Relution-Livesystem. Bei einer eigenen Relution-Instanz wird `live.relution.io` durch den Hostnamen des eigenen Servers ersetzt.



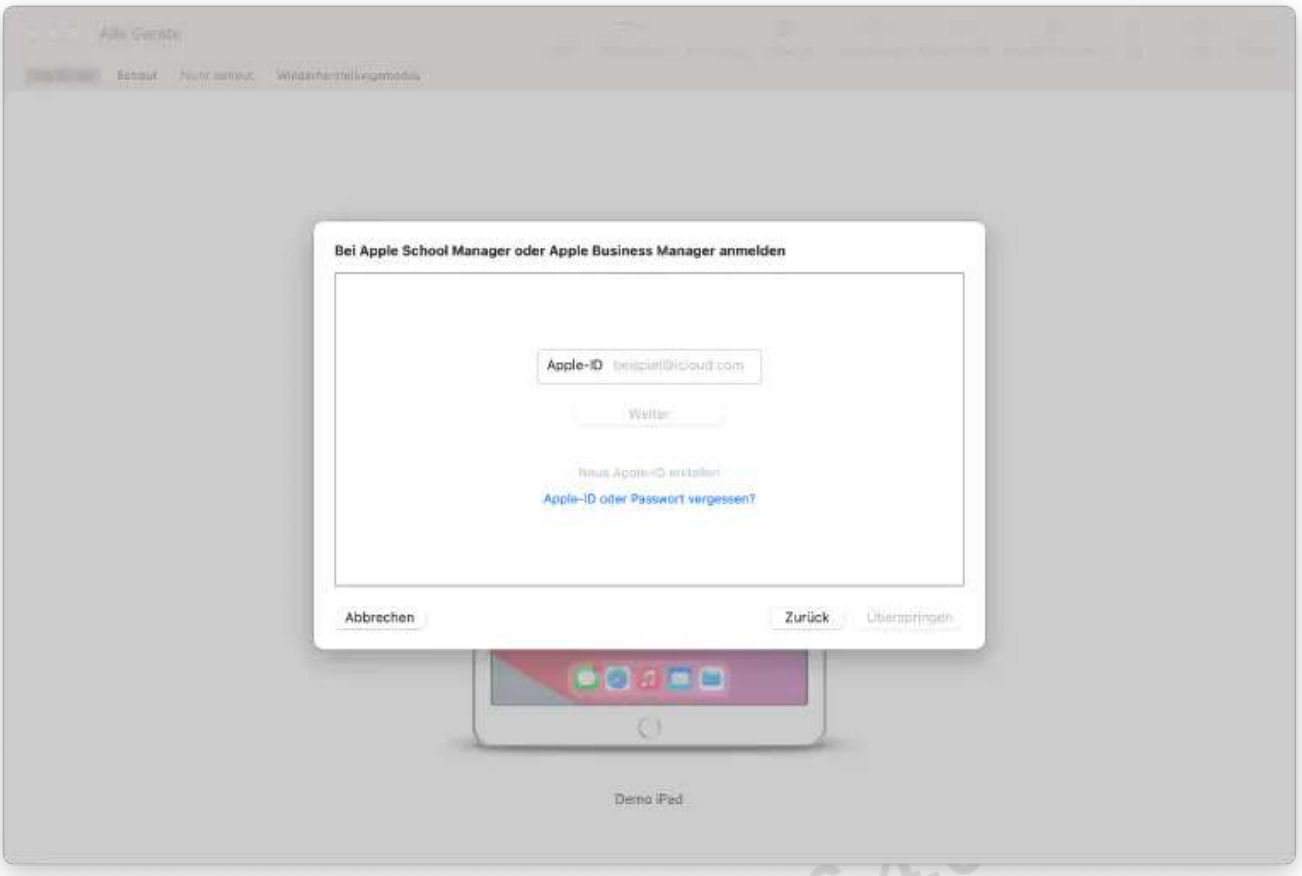
Für Version 26.4.0

Anschließend wird im nächsten Schritt das angezeigte Zertifikat ausgewählt. Bei mehreren Zertifikaten wird das erste gewählt.

Damit ist der Server festgelegt und wird im `Apple Configurator 2` gespeichert. Die Angaben stehen für die Aufnahme weiterer Geräte in das `Device Enrollment Program` zu einem späteren Zeitpunkt erneut zur Verfügung.

Nun wird im nachfolgenden Dialog `Neue Organisation...` gewählt und mit `Weiter` bestätigt.

Als nächstes erfolgt die Verbindung mit dem Apple DEP Server. Hierzu wird die Apple-ID und das Passwort des jeweiligen Apple School/ Business Manager Accounts angegeben.

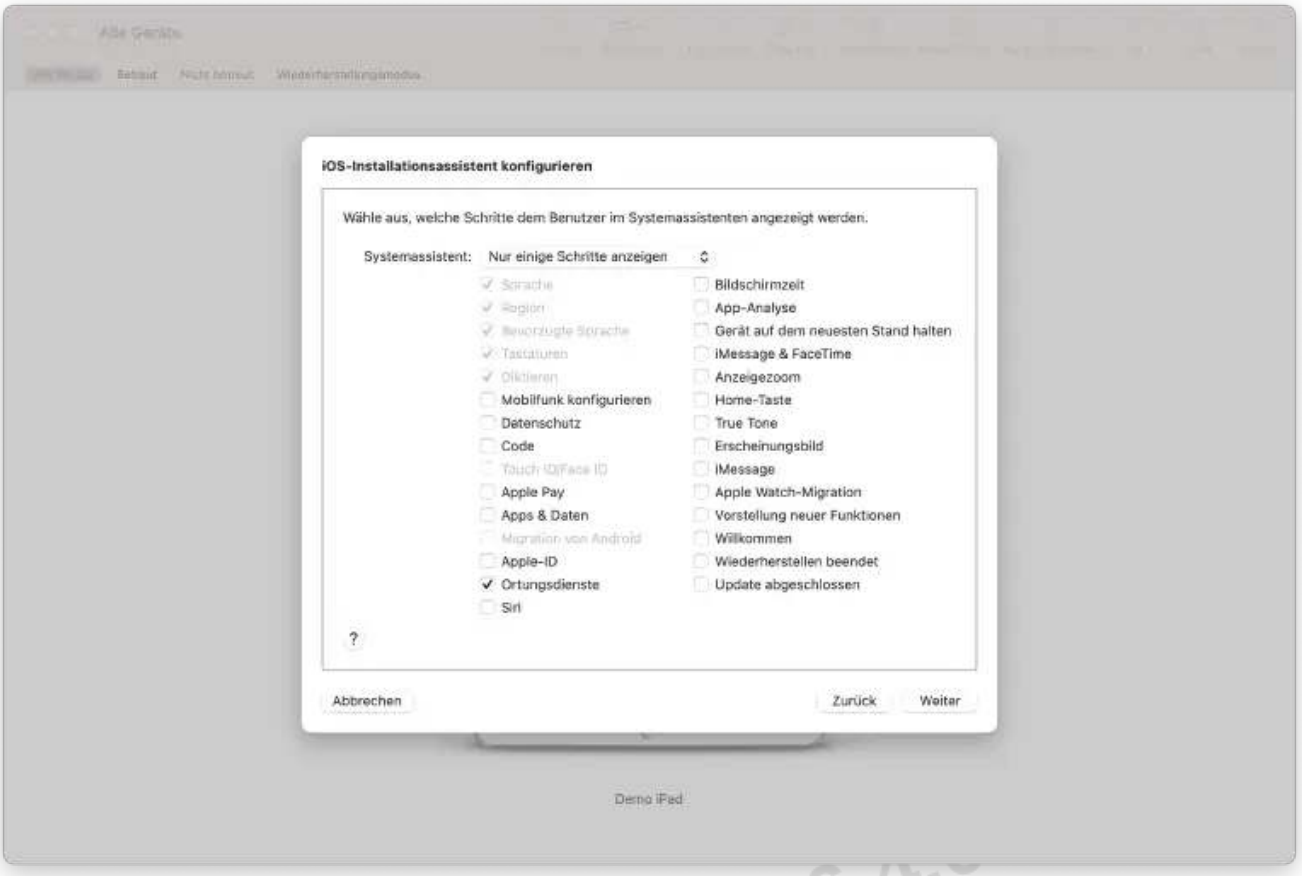


Für Version 26.4.0

Gegebenenfalls muss diese Anmeldung per 2-Faktor-Authentifizierung bestätigt werden (Eingabe eines 4-stelligen Codes, der per SMS versendet wird).

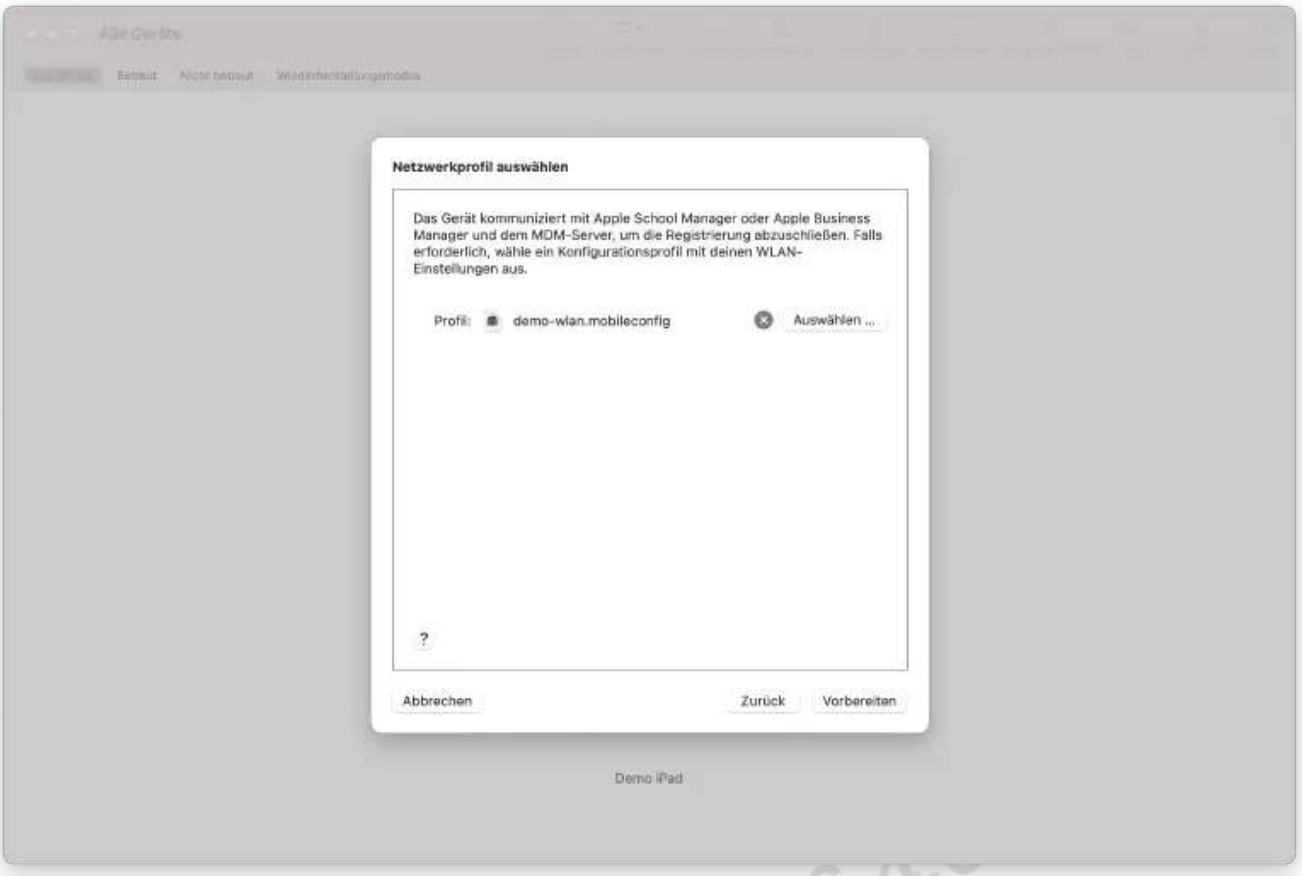
Jetzt `Neue Betreuungsidentität erstellen` wählen und mit `Weiter` bestätigen. Die Organisationsdaten werden ebenfalls vom `Apple Configurator 2` gespeichert, sodass sie später wiederverwendet werden können und keine neue Organisation mehr angelegt werden muss.

Anschließend werden im nächsten Dialog die Setup-Schritte ausgewählt, die bei der Einrichtung der Geräte nicht übersprungen werden sollen. Dabei sollte die Option `Ortungsdienste` gewählt werden, da sonst das Apple-Gerät nicht der richtigen Zeitzone zugeordnet wird.



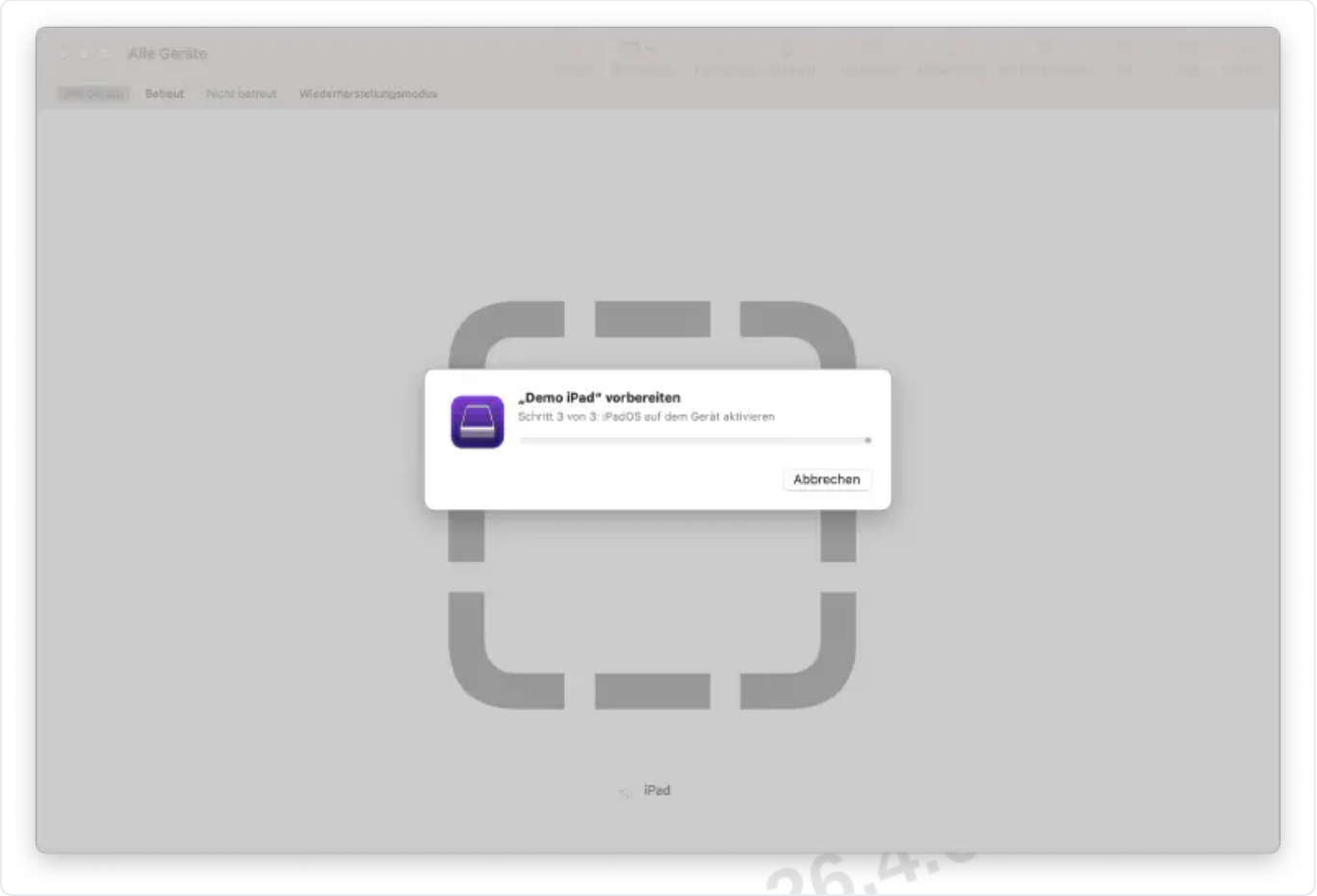
Für Version 26.4.0

Als nächstes sollte ein vorher im `Apple Configurator 2` über `Ablage` → `Neues Profil` angelegtes WLAN-Konfigurationsprofil ausgewählt werden, welches nach dem Neustart vom Gerät automatisch übernommen wird und direkt eine Internetverbindung herstellt.



Dadurch kann das Apple-Gerät die nachträgliche Registrierung für DEP an die Apple Server übertragen. Alternativ zum WLAN-Profil lässt sich auch die Internet-Verbindung vom Mac Computer mit dem angeschlossenen Gerät über die USB-Verbindung teilen. Wenn kein Profil ausgewählt wird, werden die WLAN-Einstellungen beim Neustart der Geräte von Hand eingegeben. Mit Klick auf Vorbereiten wird das Gerät neu gestartet. Es wird automatisch ins DEP eingeschrieben und anschließend im Apple School/Business Manager manuell dem entsprechenden MDM Server von Relution zuordnet.

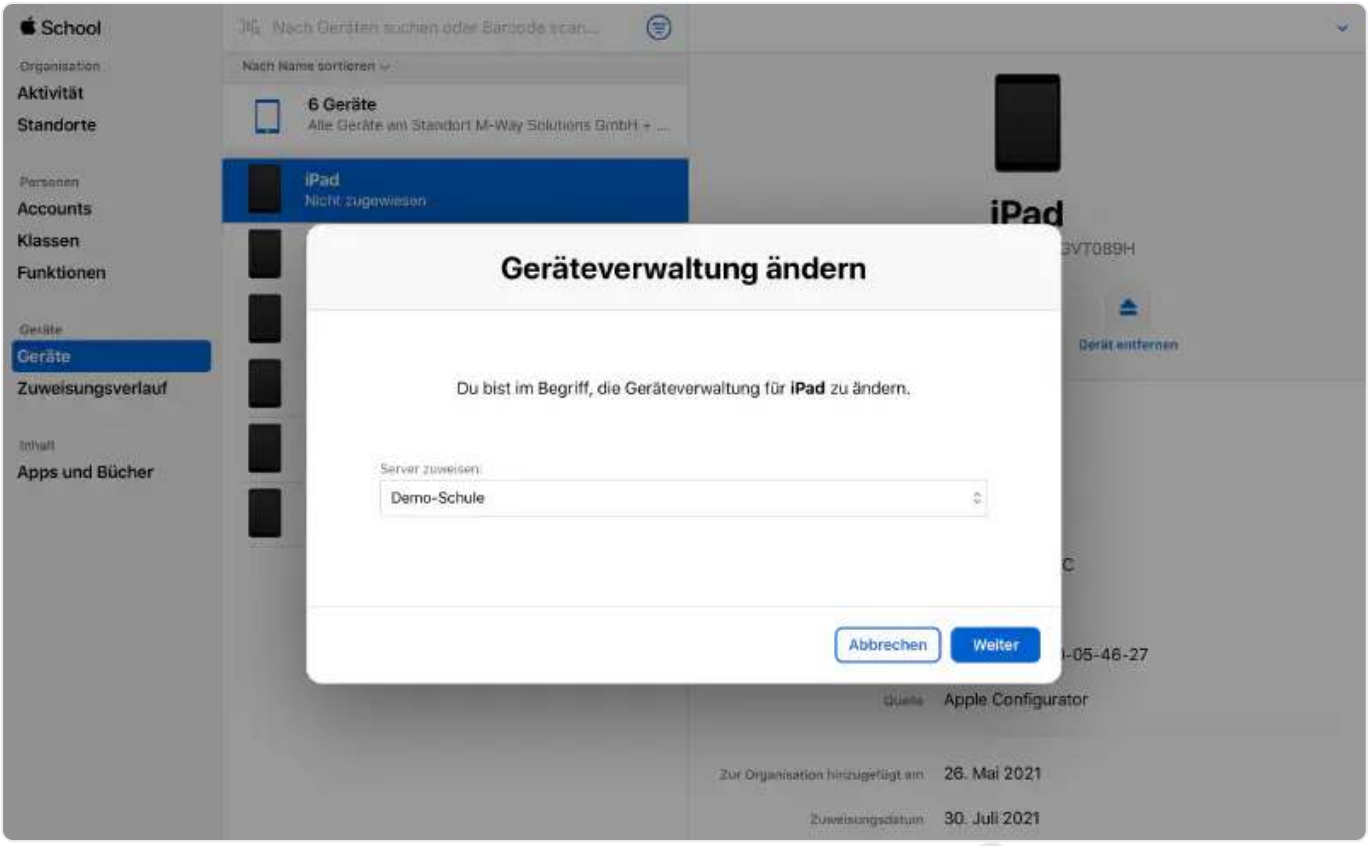
Standardmäßig werden Geräte über diesen Weg dem Apple Configurator 2 zugewiesen.



Für Version 26.4.0

Einstellungen im Apple School und Business Manager

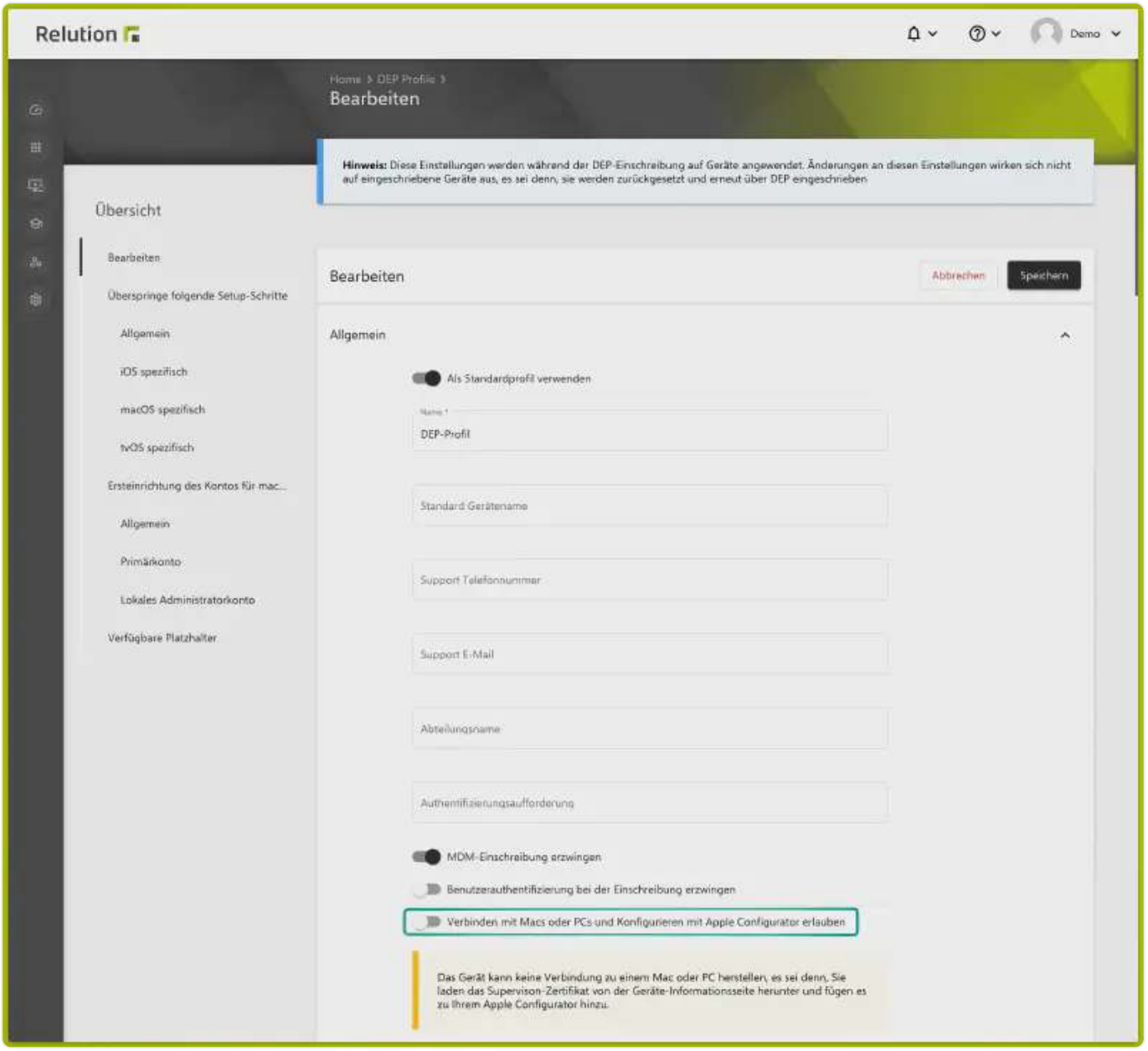
Nach dem manuellen Hinzufügen von Apple-Geräten in DEP müssen diese im Apple School / Business Manager dem gewünschten MDM Server zugewiesen werden. Alternativ kann im Apple School / Business Manager eine Einstellung konfiguriert werden, wodurch neue Geräte automatisch einem definierten MDM Server zugeordnet werden. Alle Konfigurationsoptionen sind in der Online-Dokumentation von Apple beschrieben.



Für Version 26.4.0

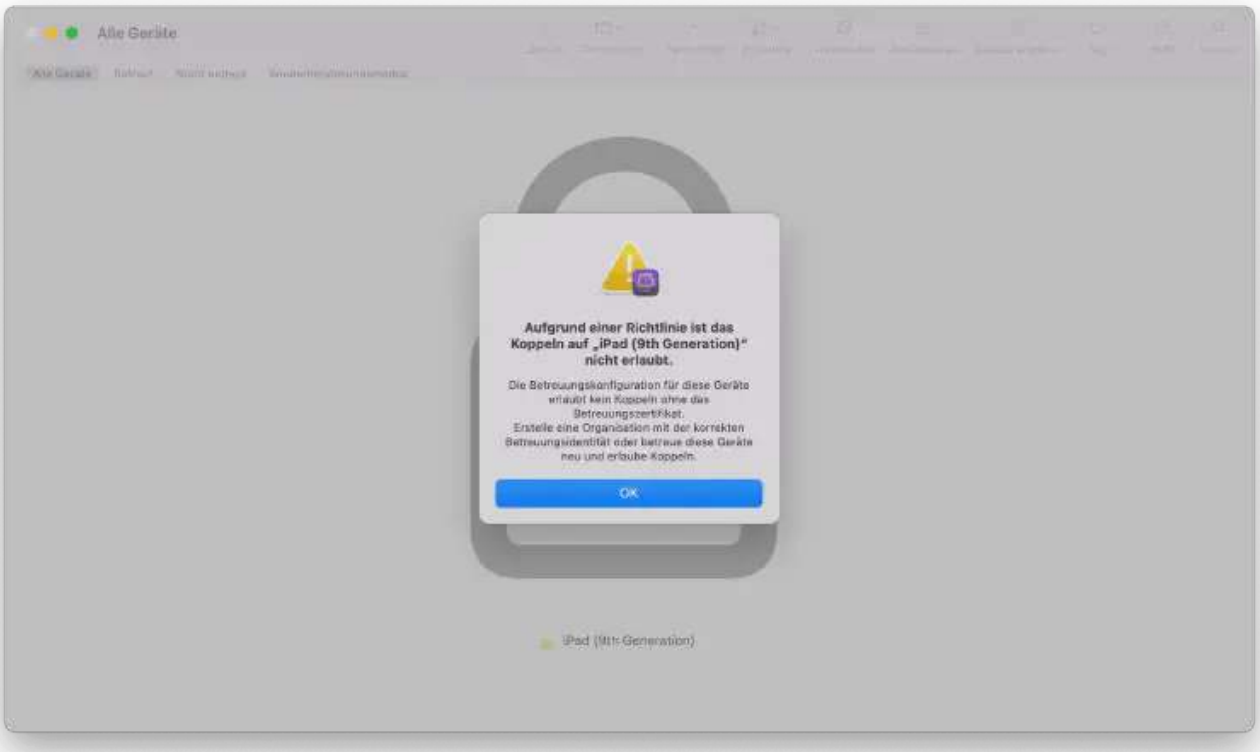
Supervisionszertifikat

Um DEP-Geräte zu schützen und unerlaubte Zugriffe auf die Geräte zu unterbinden, ermöglicht Relution im DEP-Profil die Deaktivierung der Einstellung `Verbinden mit Macs oder PCs und Konfigurieren mit Apple Configurator erlauben`. Damit besteht keine Möglichkeit, mit dem Apple-Gerät eine Verbindung zu einem Mac oder PC herzustellen und eine nachträgliche Konfiguration über den Apple Configurator durchzuführen. So wird beispielsweise verhindert, dass Benutzer das MDM-Profil entfernen können. Diese Konfiguration kann nicht nachträglich geändert werden, ohne dass das Gerät zurückgesetzt wird.



Worauf sollte geachtet werden, wenn diese Einstellung verwendet wird?

Unter Umständen kann ein gesperrter Zugriff über einen Mac oder PC dazu führen, dass dem Administrator die Möglichkeit genommen wird, ein Gerät manuell über einen Computer zurückzusetzen. Dies kann beispielsweise eintreten, wenn die WLAN-Einstellungen falsch konfiguriert sind oder der MDM-Server kaputt geht. Das Gerät ist dann über Relution nicht mehr erreichbar und kann nicht verwaltet oder zurückgesetzt werden. Man spricht auch von einem Lock-in-Effekt.



Für Version 26.4.0

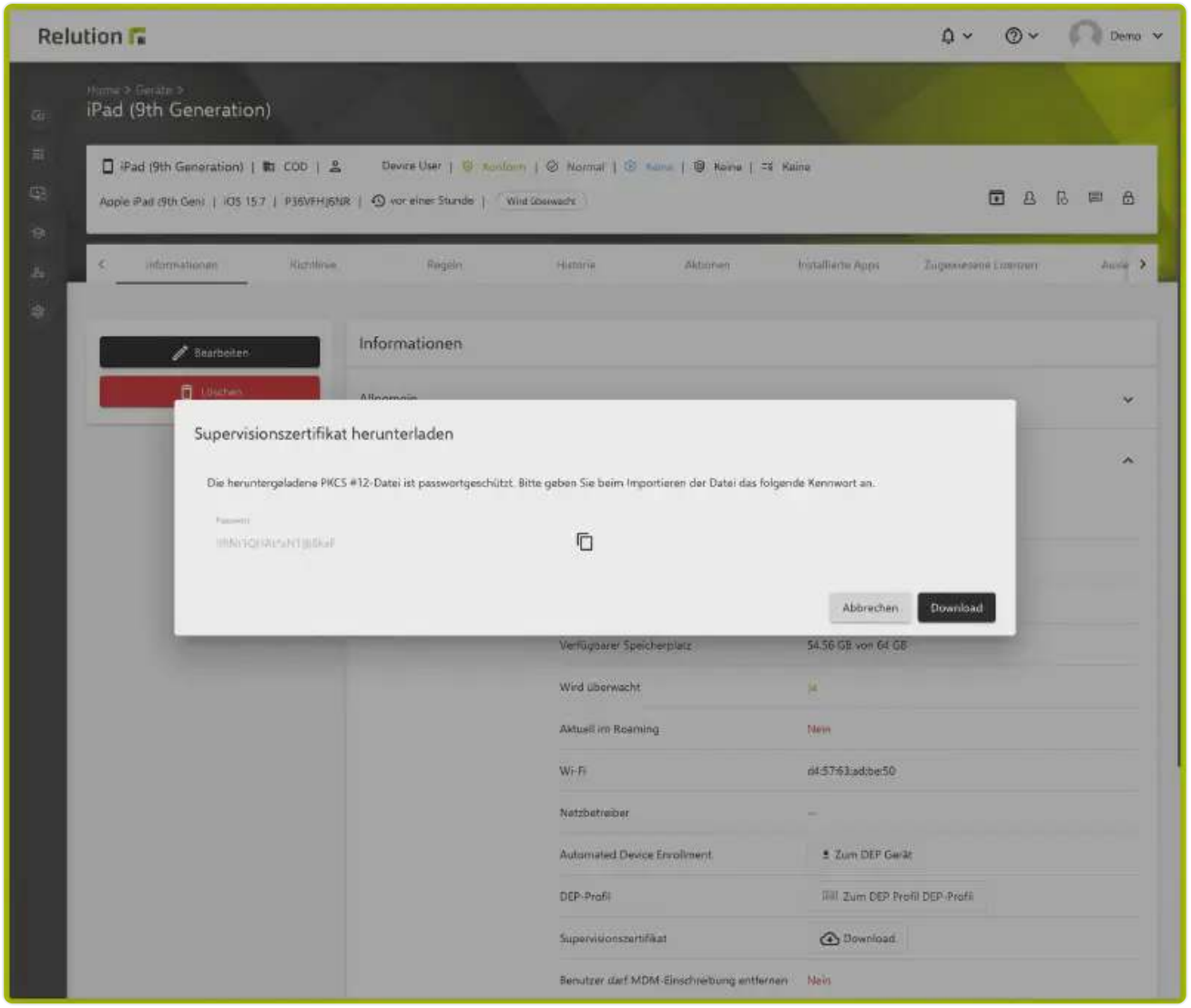
Wie können erlaubte Zugriffe mit Relution sichergestellt werden?

Mit der Server Version 5.13 ermöglicht Relution die Verbindung mit Macs oder PCs, auch wenn dies über das DEP-Profil untersagt wird. Bei der Einschreibung von DEP-Geräten in Relution wird automatisch ein Supervisionszertifikat erzeugt. Mittels dieses Zertifikats kann der Administrator das Gerät trotz Restriktion mit einem Mac oder PC verbinden. Hierzu wird das Zertifikat von Relution heruntergeladen und bei der Verbindung mit dem Apple Configurator initial einmalig angegeben. Das Zertifikat steht in den Gerätedetails zum Download bereit. Anschließend kann wieder auf das Gerät zugegriffen werden.

Was muss beim Entsperren des Gerätes beachtet werden?

Nachfolgend wird der Prozess bei der Entsperrung über den Apple Configurator beschrieben:

1. Herunterladen des Supervisionszertifikats und Zwischenkopieren des Passworts

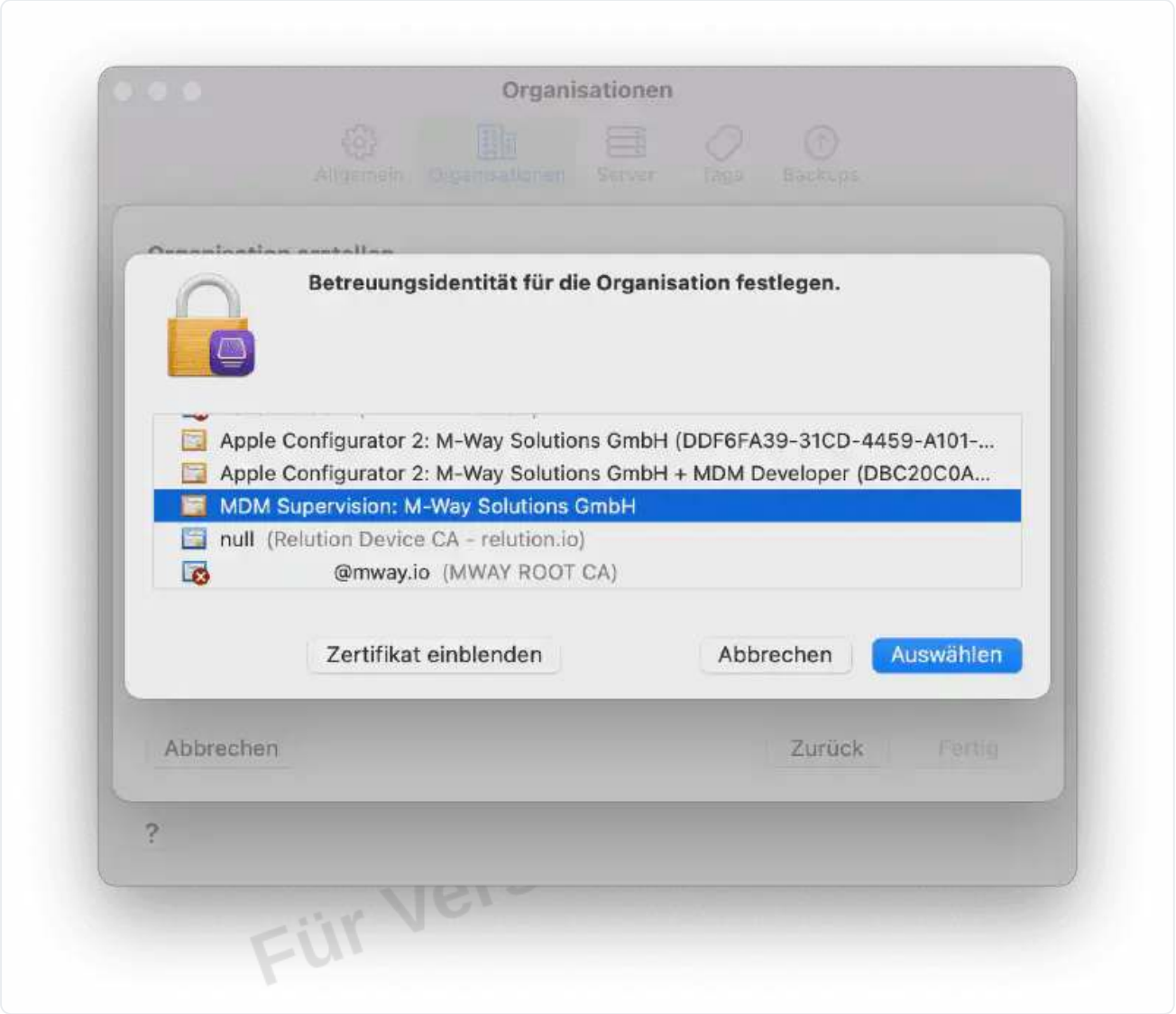


2. Über die Apple Configurator Einstellungen eine neue Organisation erstellen und die Apple-ID sowie den Verifizierungscode eingeben

3. Bestehende Betreuungsidentität auswählen und weiter klicken

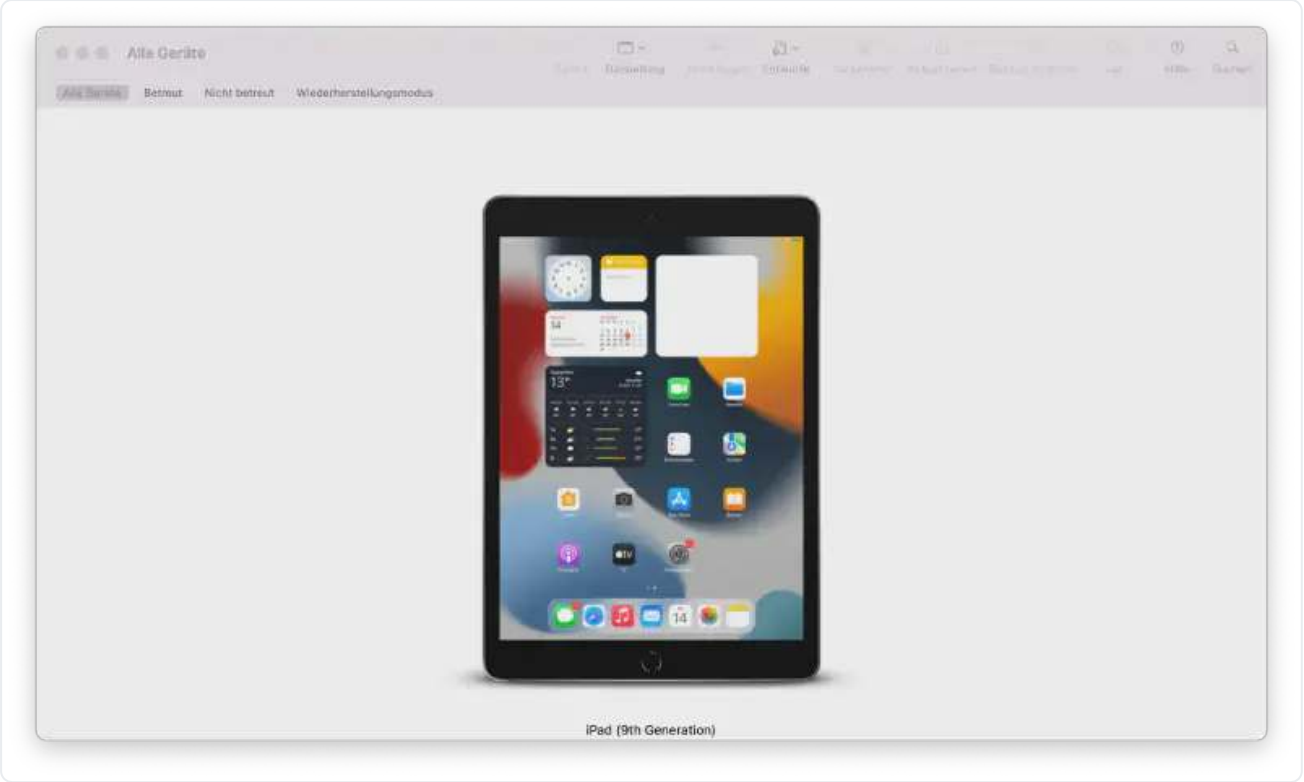
4. Anschließend das heruntergeladene Supervisionszertifikat auf dem Computer mit dem Passwort aus Relution öffnen. Die Keychain mit dem Zertifikat öffnet sich

5. Anschließend taucht das Zertifikat im Apple Configurator Dialog unter Betreuungsidentitäten zur Auswahl auf



6. Organisation erstellen

7. Nun ist das Gerät wieder freigeschaltet und kann über den Apple Configurator verwaltet werden



Was ist bei der Verwendung des Supervisionszertifikates zu beachten?

Das Zertifikat wird nur erzeugt, wenn DEP-Geräte neu eingeschrieben werden. Während der DEP-Einschreibung wird das Zertifikat automatisch erstellt und auf das Gerät gespielt. Die Funktionalität findet nicht bei bereits eingeschriebenen Geräten Anwendung und für Bestandsgeräte wird kein Zertifikat erzeugt.

Für Version 26.4.0

Überwachter Modus entfernen

Hin und wieder kann es notwendig sein Apple-Geräte, welche im `Überwachter Modus` (Supervised Mode) betrieben werden, diesen Modus zu entziehen.

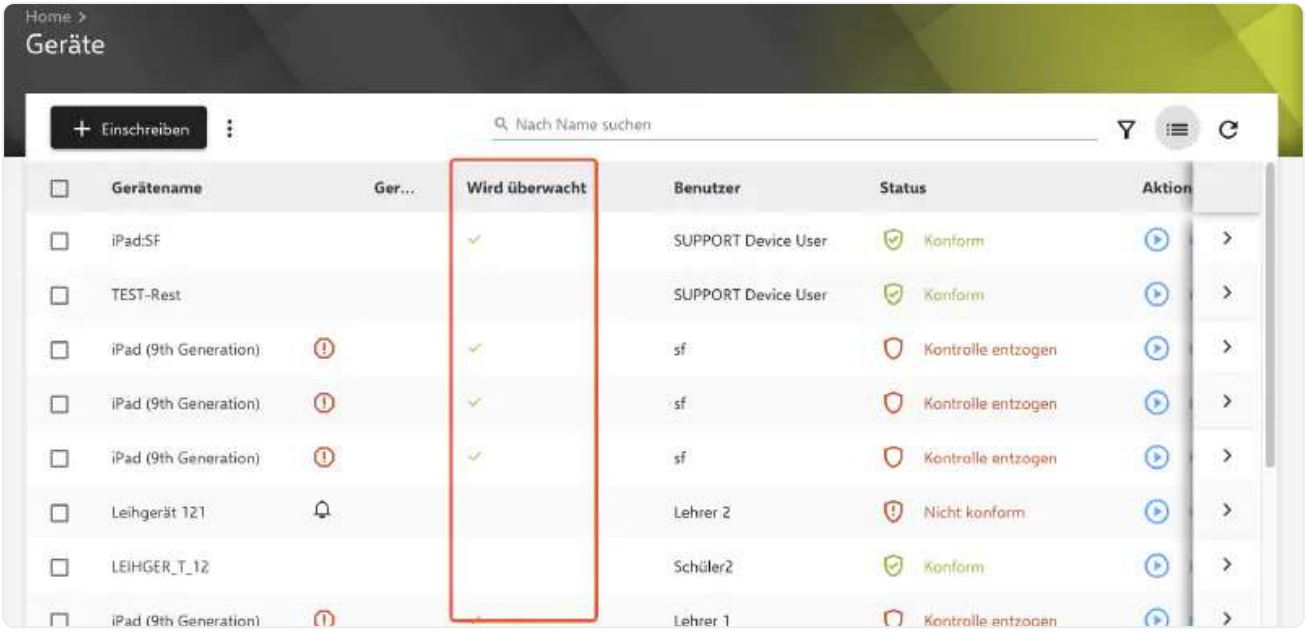
> Für iOS- und tvOS-Geräte kann dieser Zustand rückgängig gemacht werden. macOS-Geräte hingegen können ab Version 11 nur noch im `Überwachter Modus` betrieben werden.

Überwachte Geräte identifizieren

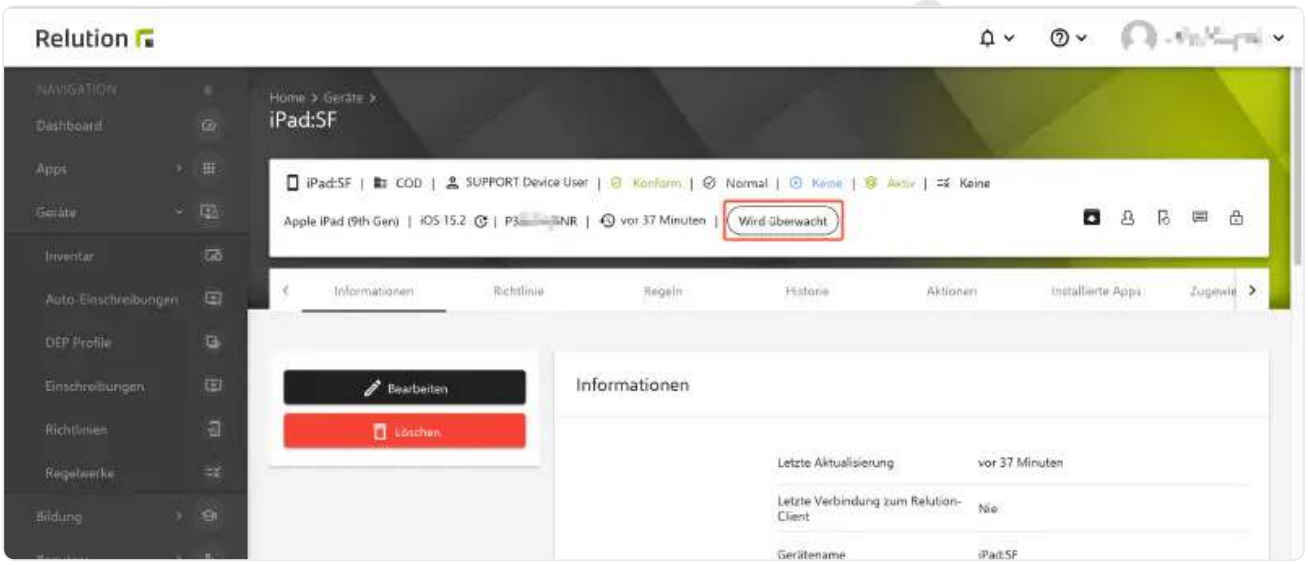
Überwachte Geräte lassen sich wie folgt ausfindig machen:

Für Version 26.4.0

1. Im Inventar die Spalte `Wird überwacht` einblenden. Die entsprechenden Geräte sind mit einem Haken markiert.



2. In den Gerätedetails lässt sich der Status über die entsprechende Badge `Wird überwacht` in der Infobox ablesen.



Über den Apple Configurator eingeschriebene Geräte

Durch diesen Vorgang wird auch das MDM-Profil von den Geräten entfernt, sodass sie im Anschluss nicht mehr verwaltet werden können, ohne erneut eingeschrieben zu werden. Zudem werden alle Apps und Daten von den Geräten entfernt.

Die Geräte mit einer der folgenden Möglichkeiten zurücksetzen:

1. Eine Gerät auf Werkszustand zurücksetzen-Aktion an die Geräte schicken.
2. In die Geräteeinstellungen unter `Allgemein` → `iPad übertragen/zurücksetzen` → `Alle Inhalte & Einstellungen löschen` gehen.
3. Geräte an einen Mac Computer anschließen und die Anwendung `Apple Configurator 2` öffnen. Einen Rechtsklick auf die Geräte machen und `Erweitert` und dort `Alle Inhalte & Einstellungen löschen` wählen.

> Es ist möglich, dass Endanwender keinen `Factory Reset` auf den Geräten durchführen dürfen, da dies in den Restriktionen verboten wurde.

Über Apple School/ Business Manager eingeschriebene DEP-Geräte über autorisierten Händler

Sind Geräte über den Apple School/Business Manager zum MDM-System hinzugefügt worden, muss die Verknüpfung dort rückgängig werden, da sich die Geräte sonst nach einem `Factory Reset` immer wieder automatisch bei dem MDM-System melden und den `Überwachter Modus` erhalten.

1. Im Apple School/Business Manager einloggen und auf `Geräte` klicken
2. Das entsprechende Gerät auswählen und auf der rechten Seite auf `Gerätezuweisung bearbeiten` klicken.
3. Auf `Zuweisung aufheben` klicken.
4. Das Gerät auf Werkseinstellungen zurücksetzen.

Für Version 26.4.0

DEP-Geräte, die nachträglich über den Apple Configurator hinzugefügt wurden

Das Entfernen von `Überwachter Modus` bei Geräten, die über den `Apple Configurator` zum Apple School/Business Manager hinzugefügt wurden, funktioniert analog der eingeschriebenen DEP-Geräte über einen autorisierten Händler.

> Jedoch können Endanwender innerhalb der ersten 30 Tage nach Hinzufügen der Geräte zum DEP das MDM-Profil auf den Geräten manuell entfernen. Dadurch geht die MDM-Einschreibung sowie auch der Überwachter Modus verloren.

Verfügbare Aktionen

Übersicht der Aktionen, mit denen sich iOS-Geräte in Relution verwalten lassen.

Relution bietet eine Vielzahl von Aktionen, die auf iOS-Geräten ausgeführt werden können, um die Geräteverwaltung zu optimieren. Diese Aktionen ermöglichen es, Geräte effizient zu steuern, die Sicherheit zu erhöhen und den Arbeitsablauf zu verbessern. Die folgende Übersicht beschreibt die verfügbaren Aktionen und liefert Anwendungsbeispiele, um deren Nutzen zu verdeutlichen.

Für Version 26.4.0

Verfügbare Aktionen für iOS-Geräte

Aktion	Beschreibung
AirPlay-Wiedergabe starten	Ermöglicht die kabellose Bildschirmübertragung auf kompatible Anzeigegeräte.
AirPlay-Wiedergabe stoppen	Beendet die laufende AirPlay-Übertragung.
Alarm auslösen	Gibt einen akustischen Alarm auf dem Gerät aus, auch im Lautlosmodus.
App entfernen	Deinstalliert eine ausgewählte App vom Gerät.
App vom Apple App Store installieren →	Installiert Apps direkt aus dem Apple App Store.
Bildschirmzeit-Code entfernen	Löscht den Bildschirmzeit-Code und zugehörige Beschränkungen.
Bluetooth ein-/ausschalten	Aktiviert oder deaktiviert die Bluetooth-Funktion.
Benutzer abmelden	Erzwingt die Abmeldung des aktuellen Benutzers.
eSIM-Mobilfunktarif aktualisieren	Aktualisiert den Mobilfunktarif der eSIM.
Gerät auf Werkszustand zurücksetzen	Löscht alle Daten und setzt das Gerät zurück.
Gerät herunterfahren	Fährt das iOS-Gerät herunter.
Gerät neustarten	Startet das iOS-Gerät neu.
Gerät orten	Ermittelt den aktuellen Standort des Geräts.
Gerät vollständig sperren	Sperrt das Gerät mit dem aktuellen Passwort.
Geräteinformationen aktualisieren	Synchronisiert die Geräteinformationen mit Relution.
Im Geräte-Setup-Assistenten fortfahren	Setzt den Setup-Assistenten fort.
Lokale Benutzer löschen	Entfernt lokale Benutzerkonten.
Lost Mode aktivieren →	Aktiviert den “Verloren-Modus” mit Sperrbildschirm und Ortung.
Lost Mode deaktivieren	Beendet den Verloren-Modus auf dem Gerät.
MDM-Profil aktualisieren	Aktualisiert das MDM-Profil auf dem Gerät.
Medien entfernen →	Entfernt bereitgestellte Medien (PDF, ePub).
Medien installieren →	Installiert Medien auf dem Gerät.
Nachricht senden	Zeigt eine Textnachricht auf dem Gerät an.

Aktion	Beschreibung
Passwort zurücksetzen	Setzt das Benutzerpasswort zurück.
Persönlichen Hotspot ein- oder ausschalten	Aktiviert den Hotspot auf dem Gerät.
Relution Store App bereitstellen →	Installiert eine App aus dem Relution App Store.
Return to Service →	Setzt das Gerät auf Werkseinstellungen zurück und nimmt es automatisch wieder in Betrieb.
Shortcut entfernen →	Entfernt einen Shortcut vom Homescreen des Geräts.
Shortcut hinzufügen →	Fügt einen Shortcut zu einer Webseite hinzu.
Standard-Apps festlegen	Legt die Standard-Apps für Anrufe, Nachrichten und Surfen im Internet fest.
Update installieren	Installiert ein OS-Update, sofern verfügbar.
Bedingter Zugriff →	Erfordert die Einrichtung von Bedingtem Zugriff über den Relution Agent, um geschützte Ressourcen nutzen zu können.
Daten Roaming →	Aktiviert oder deaktiviert Daten-Roaming.

Für Version 26.4.0

App Installation

Relution bietet, abhängig von der verwalteten Plattform, mehrere Möglichkeiten Apps auf Geräten zu installieren.

1. Installation per `Aktion`.
2. Installation über eine Richtlinien-Konfiguration.
3. Installation über `Auto-Deployments`.

Jede dieser Möglichkeiten hat Eigenschaften, die in bestimmten Anwendungsfällen nützlich sein können.

Installation per Aktion

Auf in Relution verwalteten Geräten können Apps per `Aktion` installiert werden. Dazu in den Geräte-Details auf den Tab-Reiter `Aktionen` wechseln und dort auf die Schaltfläche Aktion anwenden klicken. Je nach Betriebssystem die Option `App aus dem Play Store installieren` (`Android Enterprise`) oder `App installieren` (alle anderen Plattformen) wählen.

Im Anschluss die gewünschte App wählen und auf `Weiter` klicken.

In der Aktions-Übersicht wird eine neue `Aktion` angelegt und die Installation wird gestartet, sobald diese an das entsprechende Gerät ausgeliefert wurde.

Für Version 26.4.0

Installation per Richtlinien-Konfiguration

Apps per Richtlinien-Konfiguration zu installieren, ist bei einer größeren Anzahl von Apps und Geräten eine sinnvollere Vorgehensweise, als dies per Aktionen einzeln durchzuführen.

Wie dies funktioniert, ist den einzelnen Kapiteln der Plattform-Richtlinien zu entnehmen.

App-Konformität iOS →
App-Konformität tvOS →
Apps verwalten Android Enterprise →.

Installation über Auto-Deployment

`Auto-Deployments` sind benutzerspezifische App-Installationen, die in Abhängigkeit von den Benutzerkonten und Gruppen, die mit den Geräten verbunden sind, stehen. So können bestimmte Apps auf Geräten installiert werden, sobald sich die entsprechenden Benutzer auf diesen anmelden.

> Auto-Deployments können mit einer App-Konformität kollidieren. Wird in einer App-Konformität die Benutzung einer bestimmten App untersagt, welche aber in einem Auto-Deployment auf Benutzer- oder Gruppenebene hinterlegt ist, wird diese den entsprechenden Benutzer nicht zur Verfügung stehen.

Die Einstellungen für `Auto-Deployments` finden sich jeweils an folgenden Stellen im Relution-Portal:

Benutzer- oder Gruppen-Details

Am unteren Ende einer Detailseite einer Benutzer oder einer Gruppe können entsprechende Apps benutzer- oder gruppenspezifisch hinterlegt werden.

App-Details

Am unteren Ende einer App-Detailseite können entsprechende Benutzer oder Gruppen hinterlegt werden.

Daten Roaming

Steuerung des Daten-Roamings auf iOS-Geräten direkt über Relution.

Mit Relution 26.2 haben Administratoren die Möglichkeit, Daten Roaming auf iOS-Geräten ein- oder auszuschalten. Diese Funktion kann auch als direkte Aktion auf dem Gerät ausgeführt werden.

> Diese Einstellung kann vom Benutzer auf dem Gerät deaktiviert werden.

Für Version 26.4.0

Return to Service

Mit iOS 17+ und Relution Server Version 5.20 ist es möglich, auf iOS-Geräten eine `Return to Service` Aktion auszulösen. Diese Aktion setzt das Gerät auf die Werkseinstellungen zurück. Das Gerät versucht, sich nach dem Löschen automatisch wieder anzumelden. Somit entfallen die sich sonst wiederholenden Schritte wie die WLAN-Eingabe und Einrichtungsschritte, welche im DEP-Profil als nicht übersprungen aktiviert sind.

Der Benutzer muss alle Aktivierungssperren deaktivieren, damit diese Funktion korrekt funktioniert.

Voraussetzung

1. Das Zielgerät muss ein in Relution eingeschriebenes iOS 17+ Gerät mit einem DEP Profil sein.
2. Der Relution Server muss mindestens die Version 5.20+ haben.
3. Es muss eine Richtlinie mit einer WLAN-Konfiguration angegeben werden.

Aktion Return to Service ausführen

Für Version 26.4.0

Hierzu muss der Menüpunkt `Aktion anwenden` bei dem gewünschten Gerät im Inventar ausgewählt werden.

Über die Suche kann die Aktion gefunden und ausgewählt werden.

Im nächsten Schritt wird die Richtlinie mit der WLAN-Konfiguration ausgewählt. Hier gibt es für eSIM die Option `Bestehenden Datentarif behalten`.

Zum Abschluss erfolgt noch eine letzte Rückmeldung zum Ausführen der Aktion.

Lost Mode und Geräteortung

Mit dem `Verloren / Lost Mode` kann ein iPhone oder iPad gesperrt werden, um sicherzustellen, dass niemand auf persönliche Daten zugreifen kann. Der Modus ermöglicht es, eine Nachricht für das Gerät zu konfigurieren, die besagt, dass das Gerät verloren gegangen ist, und dabei Angaben zu den Kontaktdaten für eine Rückmeldung zu machen. Darüber hinaus kann der aktuelle Standort des Geräts auf einer Karte angezeigt werden. Dies bietet eine zusätzliche Möglichkeit, das Gerät wiederzufinden, falls es verloren geht.

Der Lost Mode und die Standortortung erfordern eine Internetverbindung am Gerät.

Einmalige Anwendung

Um ein Gerät zu sperren oder zu orten, muss es im `Geräteinventar` in Relution ausgewählt werden. Im Reiter `Aktionen` muss dann die Option `Lost Mode` ausgewählt werden. Hier können Angaben zum Kontakt hinterlegt werden, die auf dem Lockscreen angezeigt werden.

Zusätzlich kann das Gerät geortet werden. Dazu muss eine weitere Aktion `Gerät orten` ausgelöst werden. Nachdem die Aktion durchgeführt wurde, muss die Relution-Webseite neu geladen werden, indem die Tastenkombination `STRG+R` (Windows) bzw. `CMD+R` (Mac) gedrückt wird. Dadurch wird der Reiter `Standort` neben den `Aktionen` eingeblendet und der Standort auf einer Karte dargestellt.

Für Version 26.4.0

Dauerhafte Anwendung

Es ist auch möglich, den Lost Mode dauerhaft für DEP-Geräte zu aktivieren, insbesondere bei Diebstahl des Geräts. Der Vorteil besteht darin, dass Geräte, die zurückgesetzt und in Betrieb genommen werden, automatisch in den Lost Mode versetzt werden, sobald sie mit dem Internet verbunden werden. Dies kann über das Relution-Portal unter `Geräte` → `Auto-Einschreibungen` → `betroffenes Gerät` → `Lost Mode aktivieren` → `speichern` dauerhaft für das Gerät aktiviert werden.

Hinweise

- Um möglichen Missbrauch einzuschränken, bietet Relution ab Version 5.31.0 die Möglichkeit, eine Berechtigung zur Ortung anzupassen.

MDM-Profil sperren

Die automatische Geräte-Anmeldung über Apple DEP ermöglicht es Organisationen, Apple-Geräte automatisch in einer MDM-Lösung anzumelden. Das Konfigurationsprofil, das während der DEP-Registrierung mit den Geräten verknüpft wird, ermöglicht die Bereitstellung von Konfigurationen direkt bei der Inbetriebnahme. Eine kontinuierliche Geräteverwaltung ist daher nur möglich, solange das MDM-Profil auf den Geräten gesperrt bleibt. Wenn Benutzer das MDM-Profil manuell von Geräten entfernen, können Administratoren diese Geräte nicht mehr verwalten. Deshalb lässt sich das MDM-Profil auf den Geräten sperren, sodass Endbenutzer dieses auf den Geräten nicht entfernen können.

DEP-Profil konfigurieren

DEP-Profil im Relution-Portal bearbeiten oder erstellen unter `Home` → `Geräte` → `DEP-Profile` → `erstellen / bearbeiten`

Hier kann die Option `Benutzer darf MDM-Einschreibung entfernen` deaktiviert werden.

DEP-Profil als Standard festlegen

DEP-Profile können als Standard für alle zukünftigen Geräte festlegt werden. Bei neuen Einschreibungen wird dann automatisch das gewählte DEP-Profil zugewiesen.

Für Version 26.4.0

Bereits eingeschriebenen Geräten ein DEP-Profil zuweisen

Für bereits bestehende Geräte kann ein DEP-Profil nachträglich zugewiesen und synchronisiert werden.

> Änderungen am DEP-Profil wirken sich nicht automatisch auf bereits eingeschriebene Geräte aus. Hierzu müssen die betroffenen Geräte zurückgesetzt und neu eingeschrieben werden.

SFTP-Upload

Relution kann genutzt werden, um Managed Apple ID's in großer Stückzahl anzulegen.
Dies ist über das Relution Portal in den Einstellungen möglich und erleichtert Schulen und Schulbehörden die automatisierte Konfiguration von diesen ID's um diese für Schüler und Lehrer bereitstellen zu können.
Über diesen Prozess werden auch automatisch die Klassen, die in Relution angelegt wurden zu Klassen im Apple School Manager migriert.

Voraussetzungen

- Port 22 Ausgehend zu den Apple Servern zulassen vor allem für die URL: `upload.appleschoolcontent.com`
- Einen Apple School Manager
- Eine Education Lizenz in Relution
- Mindestens eine bestätigte Domain im Apple School Manager (Reserve Adressen von Apple sind nicht möglich)
- Eine Klasse in Relution mit mindestens einem Lehrer und einem Schüler Benutzer
- Die Lehrer müssen teil der Systemgruppe `Teacher` und die Schüler Teil der Systemgruppe `Student`

Konfiguration

Für Version 26.4.0

- Relution Portal und Apple School Manager öffnen.
- Zum folgenden Punkt in Relution navigieren: `Einstellungen` → `Bildung` → `Apple School Manager SFTP-Upload`
- Im Setup-Assistenten weiter bis zur Eingabe von Server-URL, Benutzer und Passwort.
- Im School Manager zu folgendem Punkt navigieren: links unten in der Ecke auf den eigenen `Benutzer` → `Einstellungen` → `verwaltete Apple Accounts` → `Starten Sie die ersten Schritte der Verknüpfung der Verzeichnissynchronisierung`.
- Klick auf Neue Accounts erstellen
- Klick auf CSV-Datei im Apple Format verwenden
- Bei Punkt 1. `SFTP Einrichten`
- Die Werte kopieren und in Relution in die Felder eintragen, dann `Weiter` klicken.
- Die bestätigte Domain aus dem Apple School Manager eintragen und weiter navigieren.
- Klick auf Daten Synchronisieren
- Klick auf Weiter im Apple School Manager und auf den Import warten.

Die ID's werden jetzt angezeigt und können hier auf Fehler überprüft werden. Im nächsten Schritt kann der Aufbau der Apple ID's bestimmt werden.

z.B.:

- Schüler: `(Vorname + Nachname)@relution.io`
- Lehrer: `(Erster Buchstabe Vorname + Nachname)@relution.io`

Standort

Der SFTP-Upload erstellt für jede Relution Organisation, die den SFTP-Upload nutzt einen neuen Standort im Apple School Manager. Der Name dieses Standortes wird genauso benannt, wie der eindeutige Name der Organisation der jeweiligen Relution Organisation.

Als Beispiel:

- Organisationsname: `User-Import-Test`
- Eindeutiger Name der Organisation: `UIT`
- Neuer Standort im ASM: `UIT`

Wenn der Standort im Apple School Manager, der für den Einkauf von Apps genutzt wird und schon existiert genauso heißt, kann es zu Problemen führen.
Dies vorher mit dem jeweiligen Betreiber des eigenen Servers oder dem eigenen Partner absprechen.

Trennen der Verbindung

Niemals die Verbindung des SFTP-Uploads trennen, wenn die ID's noch aktiv genutzt werden und in Zukunft auch weitere ID's erstellt werden sollen. Wird die Verbindung aufgetrennt, werden alle ID's, die über den SFTP-Upload angelegt wurden, auf die Quelle Manuell von SFTP geändert.
Wird jetzt erneut eine Verbindung hergestellt, kann es zu einer Vervielfältigung von Apple ID's kommen. Da mit der Relution Version 5.26 auch der Import von Benutzern dazu gekommen ist, kann dadurch ein Kreislauf entstehen.

Für Version 26.4.0

Verfügbare Konfigurationen

Eine Richtlinie ist eine Sammlung einer oder mehrerer Konfigurationen. Jede Richtlinie kann auf einem oder mehreren Geräten gleichzeitig angewendet werden. Zudem können mit jedem Gerät eine oder mehrere Richtlinien verknüpft sein.

Für Version 26.4.0

Konfigurationen im Überblick

Konfiguration	Beschreibung
Administrierte Domänen →	Administrierte E-Mail- oder Web-Domänen definieren
AirPlay	Verwaltung der kabellosen Übertragung von Inhalten auf AirPlay-fähige Empfängergeräte
AirPrint →	Verwaltung von Airprint Druckereinstellungen
App Konformität →	Verwaltung appspezifischer Einschränkungen
App zu VPN Zuordnung →	Konfiguration des verwendeten VPN einzelner Apps
Apple Configurator 2 Konfiguration →	Ein Konfigurationsprofil (mobileconfig), welches mittels Apple Configurator 2 erstellt wurde, auf Geräte anwenden
Audio-Zubehör-Einstellungen →	Temporäres Pairing von Audiozubehör zentral konfigurieren und steuern
Bedingter Zugriff →	Einrichtung vom Bedingten Zugriff auf dem Gerät über den Relution Agent erfordern, um geschützte Ressourcen nutzen zu können
Benachrichtigungen →	Benachrichtigungseinstellungen für Apps konfigurieren
DNS Proxy	DNS Proxy Konfiguration
DNS-Verschlüsselungs-Einstellungen	Konfigurieren der DNS-Verschlüsselungs-Einstellungen
E-Mail	E-Mail Konfigurationen für mehrere Benutzer hinzufügen
Einschreibungen für die Apple Watch →	Aktiviert die Einschreibung gekoppelter Apple Watches über ein verwaltetes iPhone
Einstellungen geteiltes iPad	Einstellungen für gemeinsam genutzte iPad Geräte konfigurieren
Einzel-App-Modus →	Geräte auf eine einzige App begrenzen
Erweiterbares Single Sign On →	App-Erweiterung konfigurieren, die Single Sign On durchführt
Exchange →	Verwaltung von Exchange-Konten
Externe Intelligenz-Einstellungen →	Externe, cloudbasierte KI-Integrationen über Siri und Apple Intelligence steuern
Filter für Inhalte →	Spezifizierte URLs erlauben oder verbieten
Geräte Sperrzeit →	Einrichtung einer zeitlich begrenzten Gerätesperrung
Geräteeinstellungen	Allgemeine Geräteeinstellungen konfigurieren

Konfiguration	Beschreibung
Gerätename →	Konfigurieren des Gerätenamens
Globaler HTTP Proxy	Globale Proxy-Einstellungen konfigurieren
Google Account	Verwaltung von Google-Konten
Hintergrundbild →	Hintergrundbild verwalten
Homescreen Layout →	Apps auf dem Homescreen nach Kategorie gruppieren
Intelligence-Einstellungen →	Apple-Intelligence-Funktionen wie Genmoji, Image Playground und Schreibwerkzeuge zentral steuern
Relution Decon →	Konfiguration für die Relution Decon App
Kalender →	Verwaltung von CalDAV-Kalendern
Kalender-Abonnements	Kalender-Abonnements verwalten
Kontakt	Verwaltung von CardDAV-Konten
Managed App →	App Konfigurationen für gemanagte Apps pushen
Mathematische Einstellungen →	Funktionen und Modi der Apple Taschenrechner App zentral konfigurieren
Mobilfunknetz	Konfiguriert Einstellungen für das Mobilfunknetz
Nachricht auf Sperrbildschirm	Beliebigen Text auf dem Sperrbildschirm konfigurieren
Passwort →	Passwortrichtlinie für Apple-Geräte
Relution Dateifreigaben →	Konfiguration von Dateifreigaben für die Relution-Client-App
Relution Shared Device →	Geräte in den Shared Device Modus bringen
Restriktionen →	Verwaltung von Geräterestriktionen
Safari-Einstellungen →	Verhalten des Safari-Browsers zentral steuern (Cookies, JavaScript, Startseite u. a.)
Safari-Erweiterungen →	Einzelne Safari-Erweiterungen zulassen und auf bestimmte Domains beschränken
SCEP	Verwaltung der SCEP-Einstellungen
Schriftart →	Schriftarten auf dem Gerät hinzufügen
Setup-Assistent →	Einrichtungsschritte ausblenden, die nach der Ersteinrichtung angezeigt werden (nur betreute Geräte)
Siri-Einstellungen →	Verhalten von Siri zentral steuern, u. a. Obszönitätsfilter und Zugriff im gesperrten Zustand
Softwareupdates →	Aktualisierungen von Apple-Geräten verwalten (iOS/tvOS)

Konfiguration	Beschreibung
Verwaltete Softwareupdates →	Betriebssystemupdates erzwingen und eine Zielversion bis zu einer Frist vorgeben (Nachfolger von System-Updates)
Tastatur-Einstellungen →	Tastaturfunktionen wie Autokorrektur, Diktat und Rechtschreibprüfung zentral steuern
VPN	Verwaltung von VPN Einstellungen
Verwaltete Medien →	Schiebt selbst erstellte PDF- oder ePUB-Dateien auf das Gerät
Weblink →	Weblink auf Geräte hinzufügen
WLAN	Verwaltung der WLAN Einstellungen
Zeitzone	Konfiguration der Zeitzone
Zertifikat	Zertifikat wählen, das standardmäßig auf dem Gerät installiert werden soll

Für Version 26.4.0

Passwort

Die Apple Passwort-Policy definiert Sicherheitsvorgaben für Gerätepasswörter (Codes) auf iOS-Geräten. Bei der Benutzerregistrierung unter iOS greift eine systemseitige Einschränkung: Wenn eine Passcode-Richtlinie konfiguriert ist, erzwingt iOS automatisch einen komplexen Code mit mindestens sechs Zeichen – unabhängig von weiteren Einstellungen. Dadurch werden bestimmte Konfigurationswerte ignoriert.

Trotzdem bietet die Richtlinie eine Vielzahl an Optionen, um Anforderungen an die Passwortsicherheit weiter anzupassen. Dazu zählen unter anderem Vorgaben zur Komplexität, Länge, Gültigkeitsdauer und Anzahl zulässiger Fehlversuche.

Konfigurationsmöglichkeiten

- Einfache Passwörter erlauben
- Zahlen und Buchstaben erzwingen
- Minimale Passwortlänge
- Benötigte Anzahl von Sonderzeichen
- Maximales Passwortalter (in Tagen)
- Inaktivität (in Minuten): Verfügbarer Maximalwert für den Endbenutzer zur Auswahl.
- Passwortverlauf
- Maximale Zeitgrenze für Gerätesperrung (in Minuten)
    - Sofort
    - 1 Minute
    - 5 Minuten
    - 15 Minuten
    - 60 Minuten
    - 4 Stunden
- Maximale Anzahl von Fehlversuchen

> Wird die Anzahl überschritten, wird eine Wipe-Aktion ausgelöst.

Für Version 26.4.0

Shared iPad: Betriebsmodi und Passcode-Verhalten

Apple bietet für das Shared iPad zwei Betriebsmodi an:

Verwendung mit verwalteten Apple IDs (Managed Apple Accounts) In diesem Modus wird das Gerät mit Benutzerkonten verwalteter Apple IDs konfiguriert. Die Passcode-Vergabe und -Verwaltung erfolgt zentral über diese Accounts. Eine individuelle Anpassung der automatischen Sperrzeit durch den Benutzer ist in diesem Modus nach aktuellem Stand nicht vorgesehen.

Verwendung im Gastmodus In dieser Variante melden sich Benutzer als „Gast“ an. Es wird kein individuelles Benutzerkonto und kein Passcode verwendet. Diese Option eignet sich insbesondere für Szenarien mit häufig wechselnden Nutzern, in denen keine personalisierte Datenhaltung erforderlich ist.

Hinweis: Bei Wunsch nach einer flexiblen Nutzung ohne Passcode ist der Gastmodus in der Regel die geeignete Wahl.

Gerätename

Mit Relution ist es möglich, bei iOS, iPadOS und macOS den Gerätenamen zu setzen. Hierfür kann eine Richtlinie mit der Konfiguration `Gerätename` erstellt und an Gerätegruppen verteilt werden.

Der Gerätename kann statisch vergeben werden, z. B. `Koffer iPad`. Somit erhalten alle Geräte in der Gerätegruppe denselben Namen.

Für mehrere Geräte in einer Gruppe kann es jedoch sinnvoller sein, Platzhalter in der Konfiguration zu verwenden.

Ein Beispiel: Der Gerätename wird wie folgt zusammengesetzt: `Koffer ${device.model} ${user.name}` Dies führt zu einer Darstellung wie: `Koffer iPad12,1 Max.Mustermann` Dies erleichtert die Übersicht im Inventar erheblich.

Weitere Funktionen wie Teilzeichenfolgen, Standardwerte für leere Felder oder das Ersetzen von Umlauten sind im Artikel Erweiterte Platzhalter → beschrieben.

Für Version 26.4.0

App Konformität

In der Richtlinien-Konfiguration `App-Konformität` wird festgelegt, welche App auf einem iOS-Gerät verfügbar sein soll und welche nicht. In Relution ist es möglich, die `App-Konformität` auf zwei unterschiedliche Arten zu konfigurieren.

Alle Apps in der folgenden Liste sind nicht erlaubt

Hierbei handelt es sich um eine klassische `Sperrliste (Blocklist)`. Alle Apps, die auf dieser Liste hinterlegt sind, werden im Anschluss auf iOS-Geräten ausgeblendet und Benutzer können diese nicht mehr aufrufen. Die Apps werden nicht deinstalliert. Hier können zum Beispiel einzelne System-Apps oder auch Apps aus dem öffentlichen App Store hinterlegt werden, die nicht auf den Geräten genutzt werden dürfen.

> Diese Listenart ist nicht mit Relution Shared Device kompatibel. In Kombination mit Relution Shared Device immer die Positivliste (Allowliste) verwenden.

Alle Apps in der folgenden Liste erlaubt

Für Version 26.4.0

Dies ist die klassische `Positivliste (Allowlist)`. Alle Apps, die hier hinterlegt sind, können auf iOS-Geräten installiert werden, sind im Anschluss für Benutzer sichtbar und können genutzt werden.

Es gibt noch drei weitere Optionen, die konfiguriert werden können:

Alle erforderlichen Apps hinzufügen

Alle Apps, die auf der Liste `Erforderliche Apps` hinterlegt sind, werden automatisch auf die `Positivliste` gesetzt. Dies erspart Aufwand und vermeidet Fehler.

Alle Auto-Deployments hinzufügen

Alle Apps, die bei entsprechenden Benutzerkonten oder Gruppen in den `Auto-Deployments` hinterlegt sind, werden automatisch auf die `Positivliste` gesetzt. Dies erspart Aufwand und vermeidet Fehler.

Weblinks

- Weblinks blockieren
  Alle Weblinks werden blockiert - egal, ob sie über eine Richtlinie oder eine Aktion auf die iOS-Geräte gebracht wurden.

- Weblinks im Vollbildmodus erlauben
  Es werden nur Weblinks angezeigt, die für den Vollbildmodus konfiguriert wurden.

- Alle Weblinks erlauben
  Alle Weblinks werden erlaubt. Hier wird automatisch der Safari Browser freigeschaltet.

Erforderliche Apps

Alle Apps auf dieser Liste werden automatisch installiert und Benutzer können sie nicht von den iOS-Geräten entfernen. Ist eine App dieser Liste nicht installiert worden, wird das entsprechende Gerät als `nicht konform` im Geräte-Inventar angezeigt. Der `Relution Agent` kann nicht auf diese Liste aufgenommen werden. Er wird automatisch bei der Einschreibung auf den Geräten installiert.

Zudem sollten System-Apps ebenfalls nicht auf die Liste Erforderliche Apps aufgenommen werden. Diese brauchen nicht installiert werden, da sie sich bereits auf den Geräten befinden. Es reicht aus, wenn sie auf der Positivliste hinterlegt werden.

Für Version 26.4.0

SSO Login für iOS konfigurieren

Die Single Sign-On (SSO)-Technologie ermöglicht es Nutzern, sich einmal anzumelden und nahtlos auf verschiedene Anwendungen zuzugreifen. Insbesondere für iOS-Geräte bietet die Integration von Microsoft SSO eine effiziente Lösung, um Nutzerfreundlichkeit und Sicherheit zu vereinen. Sie erleichtert nicht nur den Arbeitsalltag durch vereinfachte Anmeldungen, sondern reduziert auch Sicherheitsrisiken und IT-Aufwand. Diese Anleitung dient als Basis für eine SSO-Konfiguration mit iOS und Microsoft SSO.

Voraussetzungen

In Relution werden hierfür 2 Konfigurationen und eine App benötigt.

- `App Konformität`
- `Erweiterbares Single Sign On`
- `VPP App Microsoft Authenticator`

App Konformität Konfiguration

Hier muss die Microsoft Authenticator App → zur Liste der erforderlichen Apps hinzugefügt werden. Diese beinhaltet die für Microsoft SSO notwendige Erweiterung `com.microsoft.azureauthenticator.ssoextension`

Erweiterbares Singe Sign On Konfiguration

Für Version 26.4.0

Die folgenden zu konfigurierenden Punkte können als minimal funktionierende Vorlage für Microsft SSO verwendet werden. Nicht erwähnte Punkte können im Standard belassen werden. Die endgültige Konfiguration muss entsprechend an die eigene Umgebung angepasst werden.

- Kennung der Erweiterung
  - `com.microsoft.azureauthenticator.ssoextension`
- Typ
  - `Umleitung`
- URLs
  - `https://login.microsoftonline.us`
  - `https://login.microsoftonline.com`
  - `https://login-us.microsoftonline.com`
  - `https://login.microsoft.com`
  - `https://login.partner.microsoftonline.cn`
  - `https://sts.windows.net`

Benutzerinteraktion

Fertig konfiguriert und den Geräten zugewiesen können sich die Benutzer nun an einem Microsoft Service im Browser z.B. Outlook oder einer Microsoft App z.B. Teams anmelden und werden dadurch automatisch in allen weiteren kompatiblen Apps angemeldet.

App zu VPN Zuordnung

Bei der Einrichtung eines geräteübergreifenden VPNs werden alle Daten der Geräte durch das private Netzwerk geleitet. Manchmal möchte ein Unternehmen ein VPN nur für seine Unternehmensanwendungen einrichten. Apple ermöglicht die Einrichtung von VPN-Verbindungen für iPhones, iPads und MacBooks auf App-Basis. Hier können Administratoren genau steuern, welche Daten durch das VPN fließen. Die Richtlinien-Konfiguration einer App-zu-VPN-Zuordnung hilft Unternehmen, den Datenverkehr auf App-Ebene auseinander zu halten und ermöglicht so die Trennung von persönlichen und unternehmensbezogenen Daten.

Voraussetzung

Eine App-zu-VPN-Zuordnung kann direkt über Relution eingerichtet werden. Dies funktioniert nur für Apps, die vom MDM auf den Geräten installiert und verwaltet werden. Darüber hinaus können Administratoren VPN-Verbindungen auch so konfigurieren, dass automatisch VPN-Verbindungen für bestimmte Domänen aufgebaut werden, wenn eine entsprechende App eine Netzwerkverbindung anfordert.

Relution unterstützt die folgenden Verbindungstypen für den Aufbau einer VPN-Verbindung auf iOS- und macOS-Geräten:

- IPSec
- JuniperSSL
- SonicWALL
- AnyConnect Legacy
- AnyConnect
- IKEv2
- Benutzerdefiniertes SSL.

Für Version 26.4.0

Wie man per App-zu-VPN für iOS- und macOS-Geräte konfiguriert

1. Für die Einrichtung verwendeter VPN für einzelne Apps werden zwei Richtlinien-Konfigurationen benötigt:
    - VPN
    - App-zu-VPN-Zuordnung.
2. Innerhalb der VPN-Konfiguration muss die Option `VPN-Verbindung für Apps und Konten` aktiviert und je nach VPN-Typ alle notwendigen Felder ausgefüllt werden.
3. Innerhalb der Konfiguration `App-zu-VPN-Zuordnung` können Apps für hinterlegte VPN-Verbindung festgelegt werden.
4. Zusätzlich sind in der VPN-Konfiguration unter `Per-Account-VPN`-Einstellungen für Domäne und E-Mail möglich.

Schriftarten

Mit Relution ist es möglich, Schriftarten an iOS- und macOS-Geräte über eine Richtlinie zu verteilen.
Diese Schriftart steht dann in unterstützten Apps wie z.B. `Keynote` zur Auswahl.
Die Schrift kann nicht als Systemschrift gesetzt werden und ist nur in Apps auswählbar.

Voraussetzung

- Eine Schriftart im Format `otf` oder `ttf` (andere Formate wie `ttc` oder `woff` werden nicht unterstützt)
- Eine Richtlinie mit der Schriftart Konfiguration
- Apps die die Auswahl einer installierten Schriftart ermöglichen z.B. `Keynote`

Schriftarten verwalten

Schriftarten werden zentral unter `Einstellungen` → `Schriftarten` verwaltet, bevor sie einer Richtlinie zugewiesen werden können.

Für Version 26.4.0

Schriftart hochladen

Über Hinzufügen lässt sich eine neue Schriftart hochladen. Erforderlich sind ein Name (max. 255 Zeichen) sowie die Schriftdatei im Format `otf` oder `ttf`.

Sichtbarkeit (Scope)

Die Sichtbarkeit einer Schriftart richtet sich automatisch danach, in welcher Organisation sie angelegt wird — eine manuelle Auswahl ist nicht möglich:

- Global: Angelegt in der globalen Organisation → in allen Organisationen verfügbar.
- Lokal: Angelegt in einer regulären Organisation → nur dort verfügbar.

Die Übersichtsliste zeigt neben dem Scope auch Erstellungs-/Änderungsdatum und den jeweiligen Bearbeiter und lässt sich per CSV exportieren.

> Heruntergeladen werden können nur Schriftarten der eigenen Organisation — global geerbte Schriftarten anderer Organisationen lassen sich nicht herunterladen.

Löschen

Schriftarten lassen sich einzeln oder per Mehrfachauswahl löschen; eine nachträgliche Bearbeitung ist nicht möglich.

Beim Löschen wird nicht geprüft, ob die Schriftart noch in einer Richtlinie verwendet wird. Wird eine verwendete Schriftart gelöscht, führt dies bei der nächsten Konfigurationsübertragung zu einer Compliance-Verletzung auf den betroffenen Geräten.

Anwendung

Die gewünschte Schriftart kann in Relution unter `Home` → `Einstellungen` → `Schriftarten` → `Hinzufügen` hochgeladen werden.
Zudem muss ein Name für die Schriftart vergeben werden.
Anschließend muss diese in einer iOS- oder macOS-Richtlinie in der Konfiguration `Schriftart` hinzugefügt werden.

Für Version 26.4.0

Homescreen Layout

Mit dem Homescreen Layout kann die Anordnung von Apps und Ordnern auf iOS- und iPadOS-Geräten durch Administratoren gesteuert werden. Hierfür gibt es zwei Layout-Typen:

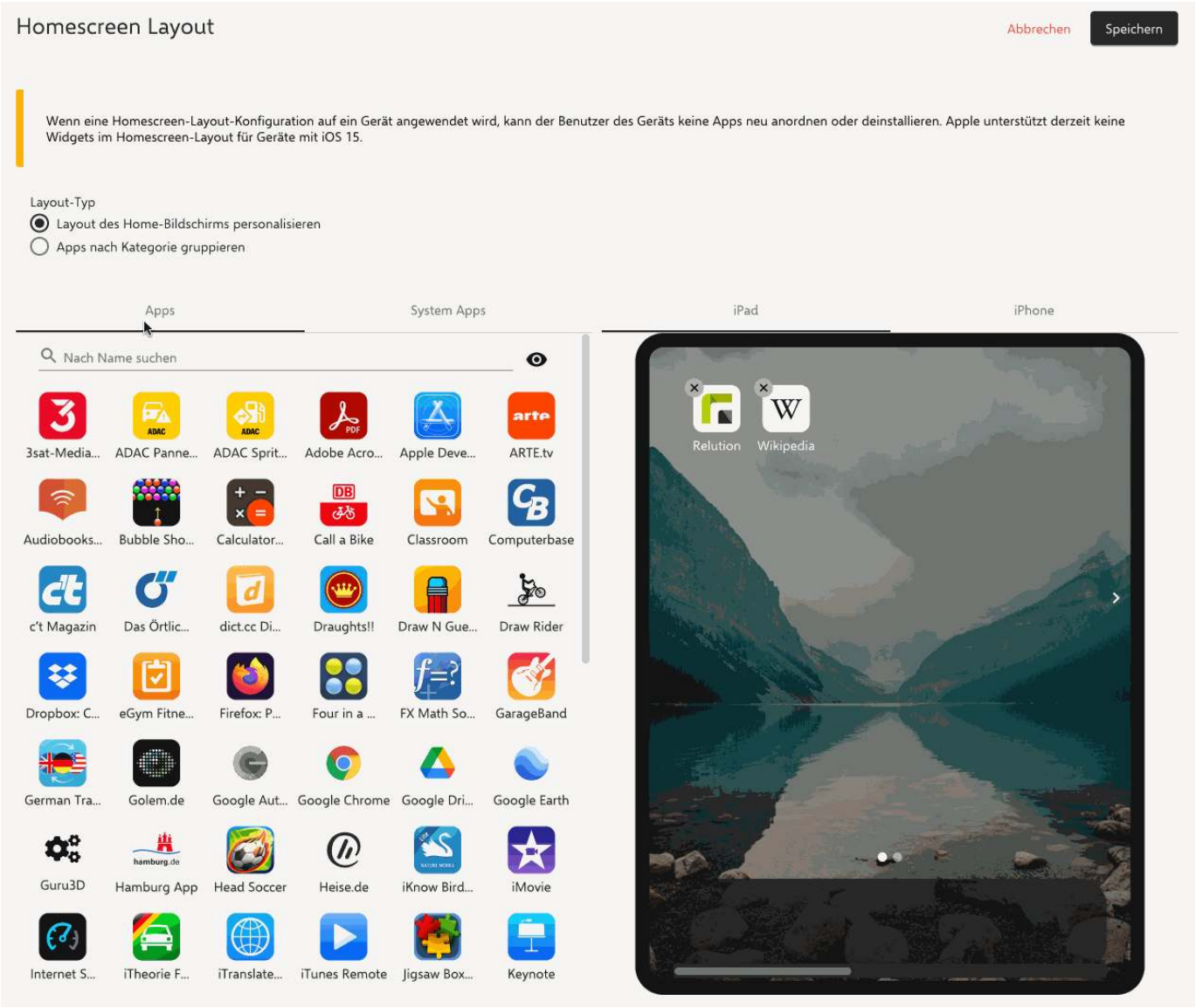
1. Layout des Home-Bildschirms personalisieren.
2. Apps nach Kategorie gruppieren.

> Wenn eine Homescreen Layout-Konfiguration auf Geräten angewendet wird, können Benutzer keine Apps manuell auf den Geräten neu anordnen oder deinstallieren. Apple unterstützt derzeit keine Widgets im Homescreen Layout für Geräte mit iOS 15.

Home-Bildschirm personalisieren

Das Layout lässt sich durch eine individuelle Anordnung der Apps personalisieren. Ordner können für eine Kategorisierung von Apps erstellt werden.

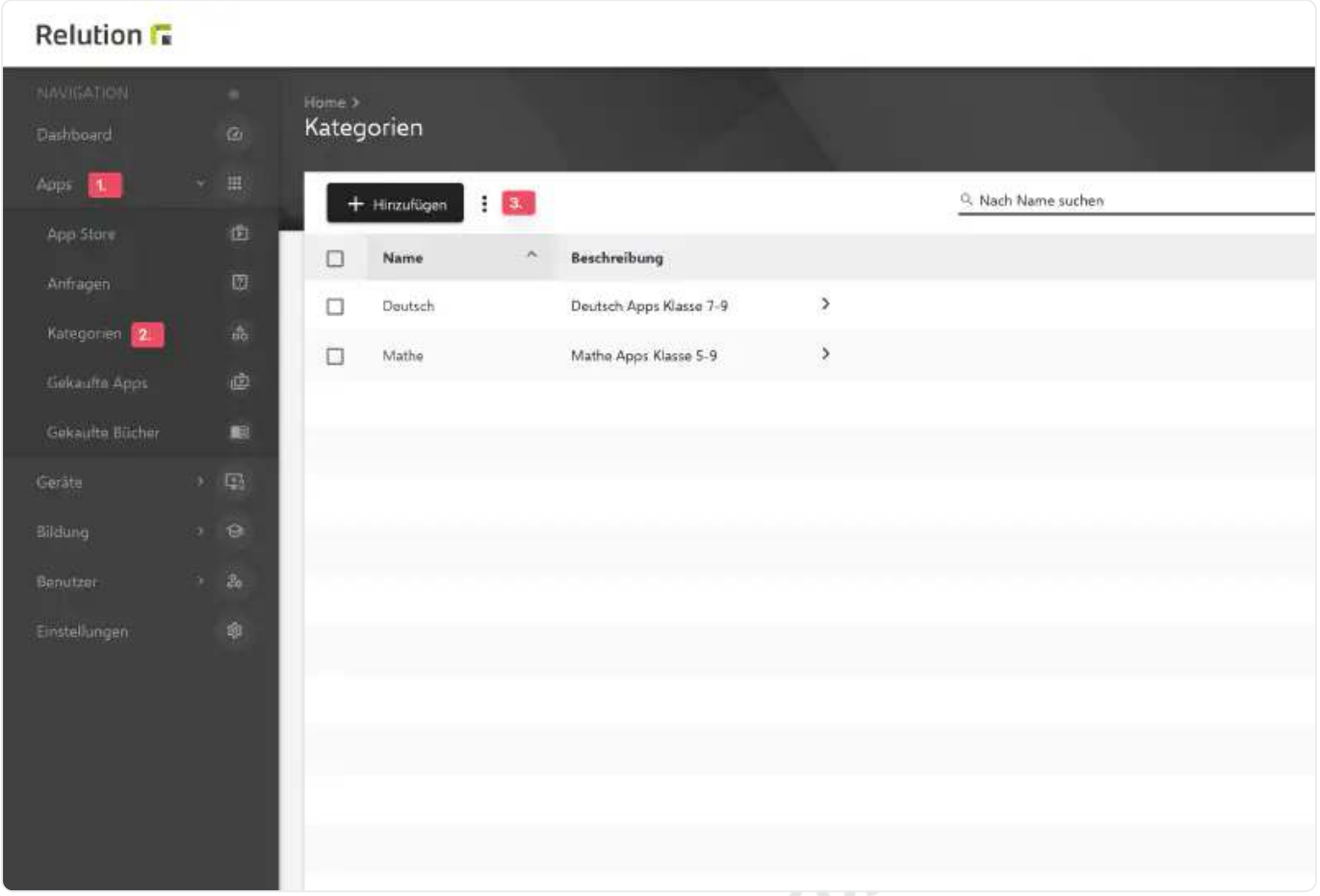
Für Version 26.4.0



Durch Stillhalten der Maus bei einer Drag & Drop-Aktion auf eine andere App wird automatisch ein Ordner erzeugt. Das Homescreen Layout ist auf 20 Apps Pro Seite begrenzt.

Apps nach Kategorie gruppieren

Dieses Layout gruppiert installierte Apps entsprechend der im Relution-Portal erstellten Kategorien. System-Apps werden automatisch gruppiert.



Für Version 26

Relution Decon (Inhaltsfilter)

Ab Version 5.27 ermöglicht Relution für iOS die Einrichtung eines DNS-basierten Inhaltsfilters. Diese Funktion sorgt für einen sicheren und fokussierten Internetzugang, indem der Zugriff auf ausgewählte Webseiten und Apps eingeschränkt wird. Dank der KI-gestützten Kategorisierung von Inhalten bietet Relution Decon einen umfassenden Jugendschutzfilter mit erweiterten Einstellungsmöglichkeiten.

Was ist Relution Decon?

Relution Decon ist ein KI-gestütztes Add-on für iOS und iPadOS, das Inhalte in Echtzeit filtert und ein sicheres digitales Umfeld schafft. Mithilfe der DNS-basierten Inhaltskontrolle blockiert Decon unerwünschte Webseiten und Apps, sodass Nutzer in einem geschützten, ablenkungsfreien Raum arbeiten und lernen können.

Relution Decon nutzt einen DNS-Proxy, um alle Anfragen an den Decon-Server weiterzuleiten. Dort werden Webseiten klassifiziert und gemäß den Richtlinien entweder erlaubt oder blockiert. Dank SSL-Verschlüsselung bleiben alle Datenübertragungen sicher, und die Nutzeraktivitäten geschützt.

Decon App

Für Version 26.4.0

Die Decon-App wird bei der Richtlinieninstallation automatisch auf iOS-Geräten bereitgestellt. Sie überwacht die DNS-Anfragen des Geräts und stellt sicher, dass nur zugelassene Inhalte aufgerufen werden können.

Funktionen der App:

- Aktiviert einen systemweiten DNS-Proxy, der vom Benutzer nicht deaktiviert werden kann
- Zeigt den aktuellen Status von Relution Decon an
- Gibt Einsicht in blockierte Webseiten und die angewendeten Filterkategorien

> Empfehlenswert: Vor der Verteilung ausreichend VPP-Lizenzen für die App bereitstellen.

VPP-Einrichtung in Relution →
Relution Decon im Apple App Store →

Decon Richtlinie

In der Geräte-Richtlinie auf `Hinzufügen` → `Relution Decon` klicken. Mit dieser Richtlinie wird die Decon-App automatisch auf den Geräten installiert und fungiert als Proxy für alle DNS-Anfragen.

Die Konfiguration wird mit der Veröffentlichung der Richtlinie abgeschlossen.

Hierarchie der Richtlinienkonfiguration (höchste zu niedrigste Priorität)

1. Allow-Apps
2. Block-Apps
3. Allow-Webseiten
4. Block-Webseiten
5. Blockierte Kategorien

Decon in Relution Teacher

Decon kann mit Relution Server 5.32.0 und Relution Agent 5.19.0 in Unterrichtsprofilen ausgewählt und gesteuert werden. Voraussetzung: Schülergeräte müssen mit einer Decon-Richtlinie versehen sein.

Mehr zu Relution Teacher →

Hinweis: Für die Dauer der Unterrichtsstunde wird die sonst gültige Decon-Konfiguration überschrieben.

Klassifizierung nach Kategorien

Relution Decon ordnet Webseiten automatisch einer Kategorie zu. Administratoren legen fest, welche Kategorien blockiert werden:

Für Version 26.4.0

Kategorie	Beschreibung	Beispiele
Nicht jugendfrei	Nicht für Jugendliche geeignete Seiten	Pornografie, Gewalt, Waffen, Drogen, Gambling, Adult Entertainment, Adult Shopping, Dating, Google Safe Search
Werbung	Werbeseiten	Ad Providers
Kommunikation	Kommunikationsdienste	Email, Messenger, (Video) Calling
Social Media	Social-Media-Inhalte	Facebook, Instagram, TikTok, etc.
Entertainment	Unterhaltung, z. B. Streaming oder Spiele	Movies, Games, Videos
Musik	Musik-Streaming-Anbieter	Spotify, Tidal, etc.
News	Nachrichten und Magazine	News, Wetter
Shopping	Online-Shops (außer adult content)	Amazon, eBay, etc.
Arbeit	Arbeitsrelevante Webseiten	Office, File Sharing, Intranet
Bildung	Lerninhalte	Wikipedia, Google Scholar
Generative AI	KI-spezifische Webseiten	ChatGPT, Perplexity.ai, etc.
Phishing	Potenzielle Phishing-Webseiten	Potential scams, Data theft
Sonstiges	Alles Andere	Rest

Allow- und Block-Listen

- Allow-Webseiten / Block-Webseiten: Spezifische Domains gezielt freigeben oder sperren (keine Pfadunterscheidung).
- Allow-Apps / Block-Apps: Internetzugang für Apps gezielt steuern, Basisfunktionen bleiben erhalten.

Erweiterte DNS-Konfiguration

DNS-Server auf dem Gerät: Alternative DNS-Server können hinterlegt werden, falls Relution Decon DNS nicht erreichbar ist. Fallback: Cloudflare Families DNS (1.1.1.3).

DNS-Server auf dem Relution Decon Server: Ersetzt den Standard-DNS für den Decon-Server. IP-Adressen (UDP) oder DNS-over-HTTPS (DoH) wie Zero oder Quad9 sind möglich.

Limitierungen

- Zwischenspeicherung: Blockierungen und Richtlinienänderungen können bis zu 1 Minute verzögert umgesetzt werden.
- Pfadunabhängigkeit: DNS arbeitet auf Domain-Ebene, keine Unterscheidung von Unterseiten.
- App-Blockierung: Nur Internetzugang wird gesperrt, Basisfunktionen und zwischengespeicherte Inhalte bleiben verfügbar.

Für Version 26.4.0

Relution Shared Device

Relution bringt einen eigenen Mehrbenutzermodus für iOS-Geräte mit. Anders als der Mehrbenutzermodus von Apple, `Geteiltes iPad` (Shared iPad), zeichnet sich der `Relution Shared Device`-Modus durch Folgendes aus:

- Benutzer melden sich über den `Relution Agent` mit einem vorhandenen Relution-Benutzer (Account) auf den Geräten an.
- Eine (Managed) Apple-ID ist dafür nicht notwendig.
- Auch die Anmeldung mit einem LDAP-Benutzerkonto ist mit Relution möglich.
- Der Modus kann bequem über die entsprechende Richtlinien-Konfiguration aktiviert und deaktiviert werden.

Voraussetzung für den Einsatz dieser Konfiguration ist, dass sich die Zielgeräte in Überwachter Modus (Supervised Mode) → befinden.

Verhalten beim Benutzerwechsel

Der `Relution Shared Device`-Modus installiert beim Benutzer-Login alle erforderlichen Apps und deinstalliert diese beim Benutzer-Logout automatisch wieder:

- Beim Login werden alle erforderlichen Apps automatisch installiert.
- Beim Logout werden diese Apps automatisch wieder deinstalliert.
- Dadurch werden alle Inhalte, die temporär in den Apps erzeugt wurden, automatisch auf den Geräten gelöscht.
- So stellt Relution bei einer benutzerübergreifenden Verwendung über den `Relution Shared Device`-Modus die datenschutzkonforme Nutzung der Geräte sicher.

Für Version 26.4.0

Ausnahme System-Apps: System-Apps, wie z.B. der Safari Browser oder die Photos App, können Apple-seitig nicht deinstalliert werden. Dadurch lassen sich für diese Apps somit auch keine temporär erzeugten Daten löschen. Hier empfiehlt es sich, auf alternative Apps wie beispielsweise den Firefox Browser oder die Relution-Foto-Funktion auszuweichen.

Datensicherung: Daten, die gesichert werden sollen, müssen entweder über `Relution Files` auf einem externen Server gespeichert oder über Dienste wie Own- bzw. Nextcloud auf einem externen System abgelegt werden.

Netzwerklast durch Neuinstallationen vermeiden

Durch die Neuinstallation von Apps können erhebliche Lastspitzen im Netzwerk auftreten. Daher sollte die Konfiguration `App-Konformität` möglichst schlank gehalten werden:

- Die `Positivliste (Allowlist)` sollte nur sehr wenige und kleine Apps als erforderliche Apps beinhalten.
- Benutzer können sich bei Bedarf über den `Relution Agent` Apps bequem aus dem Relution App Store nachinstallieren.
- Im Schulkontext kann eine Lehrkraft benötigte Apps mittels der `Relution Teacher App` und eines `Unterrichtsprofils` installieren lassen.

Im Sinne des Datenvolumens im Netzwerk ist es nicht ratsam, auf einem Relution Shared Device zu jeder Zeit jede App installiert zu haben.

Kombination mit Apple „Geteiltes iPad“

Wird der `Relution Shared Device`-Modus in Kombination mit der Apple `Geteiltes iPad`-Funktionalität eingesetzt, gelten folgende Besonderheiten:

- Es findet keine Deinstallation der installierten Apps statt.
- Ein datenschutzkonformes Arbeiten ist in diesem Anwendungsfall nur möglich, wenn sich Benutzer im Apple `Geteiltes iPad`-Modus als Gast anmelden.
  - Im `Gast-Modus` werden nach Gast-Abmeldung alle temporären Daten auf den Geräten automatisch durch die Apple `Geteiltes iPad`-Funktionalität gelöscht.

Zusätzlich gelten folgende Einschränkungen für diese Kombination:

- Der Gast-Modus von Apple Geteiltes iPad ist nicht mit der Apple Classroom App kompatibel. Im Schulkontext bedeutet dies, dass Schüler-iPads in dem oben beschriebenen Setup in der Apple Classroom App der Lehrkraft nicht als online angezeigt werden.
- Eine App-Konformität funktioniert nur in Form einer Positivliste in Kombination mit dem Relution Shared Device-Modus. Sperrlisten zeigen keinerlei Wirkung.

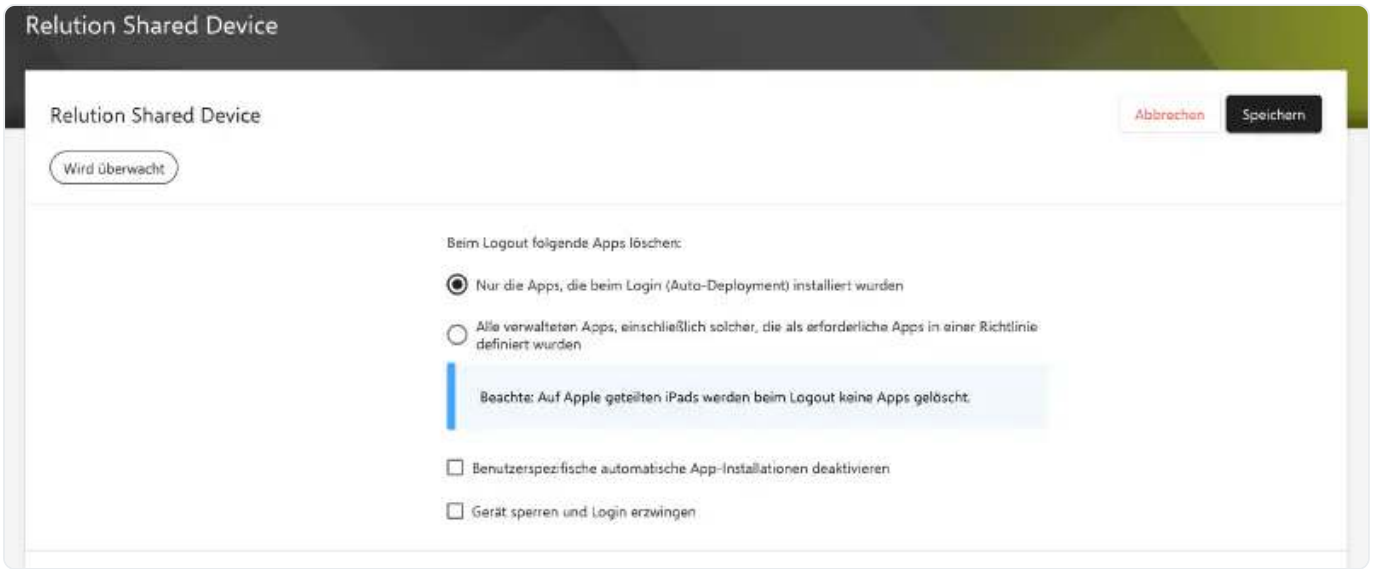
Für Version 26.4.0

Bekannte Einschränkungen

Mit iOS 17.x bewirkt das Festlegen der Restriktionskonfiguration `Synchronisierung des iCloud-Schlüsselbunds erlauben` auf `nein`, dass die Anmeldung auf gemeinsam genutzten Geräten verlangsamt wird.

Um dieses Verhalten zu umgehen, muss in der angewendeten Konfiguration der `Restriktion` der Punkt `Synchronisierung des iCloud-Schlüsselbunds erlauben` auf `ja` gesetzt werden.

Relution Shared Device Einstellungen



Die ersten vier Optionen der `Relution Shared Device`-Konfiguration sind die wichtigsten:

- Zuerst ist zu entscheiden, ob beim Logout der Benutzer nur die benutzerspezifischen Apps, die über `Auto-Deployments` installiert wurden, oder alle Apps, die über Relution installiert wurden, gelöscht werden sollen. Je nach Konfiguration sorgt die zweite Konfiguration dafür, dass mehr Apps deinstalliert werden.
- `Benutzerspezifische automatischen App-Installation`
  - Deaktiviert vorhandene Auto-Deployments auf Benutzer- oder Gruppenebene.
- `Gerät sperren und Login erzwingen`
  - Setzt den `Relution Agent` vor dem Benutzer-Login in den `Single-App-Modus`. Benutzer müssen somit erst eine erfolgreiche Benutzer-Anmeldung durchführen, um den Relution Agent verlassen zu können, um anschließend auf das Gerät zuzugreifen. Dieser Schalter hat auf Apple Shared iPads keine Funktion.

Für Version 26.4.0

> Es ist nicht empfehlenswert, die letzte Option zu nutzen, da in diesem Modus kein Zugriff auf die Einstellungen des Geräts besteht und u.a. keine WLAN-Verbindung manuell eingerichtet werden kann, wenn keine Netzwerk-Konfiguration angewendet wird. Ist die Option deaktiviert, können Benutzer die Einstellungen auf dem Gerät ohne Benutzer-Anmeldung öffnen.

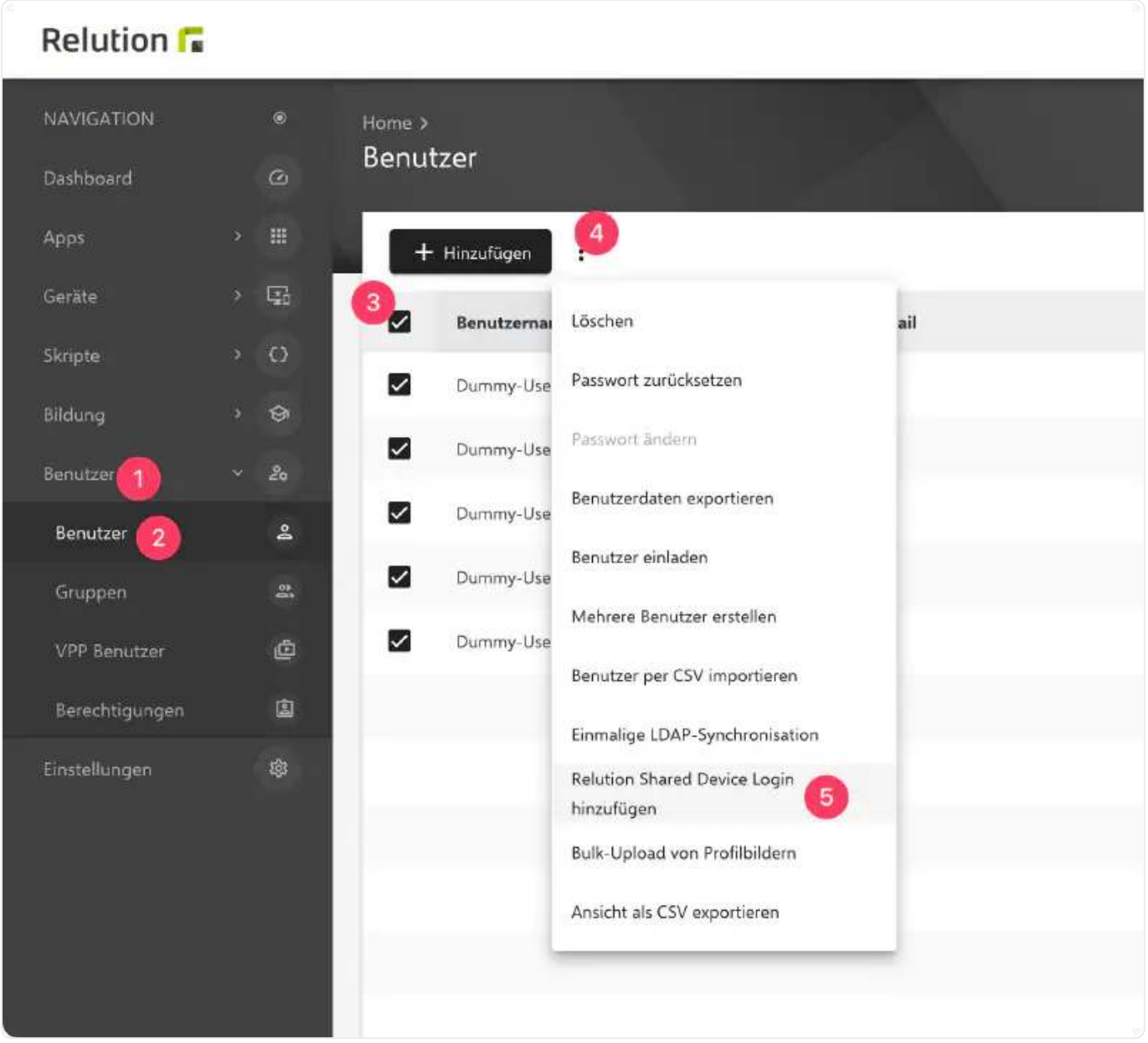
Anmeldung per QR-Code

Neben Benutzername und Passwort ist im `Relution Agent` auch eine Anmeldung per QR-Code möglich. Jeder QR-Code enthält ein persönliches Zugangstoken (Access Token) eines Benutzers. Das erleichtert die Anmeldung überall dort, wo die Eingabe von Zugangsdaten mühsam ist, z. B. bei Grundschülern.

Voraussetzung ist, dass in der `Relution Shared Device`-Konfiguration die Option Anmeldung mit Zugangstoken (QR-Codes) zulassen aktiviert ist. Ohne diese Option wird im `Relution Agent` keine Anmeldung per QR-Code angeboten.

QR-Codes für mehrere Benutzer erzeugen

QR-Codes lassen sich für beliebig viele Benutzer in einem Schritt erzeugen und gesammelt drucken. Dazu werden unter `Benutzer` → `Benutzer` die gewünschten Benutzer in der Liste markiert. Über das Drei-Punkte-Menü neben Hinzufügen wird anschließend Relution Shared Device Login hinzufügen ausgewählt.



Im folgenden Dialog wird ein Name für die Zugangstoken vergeben. Über den Schalter Gültigkeitsdauer lässt sich optional ein Ablaufdatum festlegen, ohne Ablaufdatum bleiben die Tokens unbegrenzt gültig. Durch Klick auf Hinzufügen wird für jeden markierten Benutzer ein eigenes Token mit diesem Namen erzeugt.

Im Bereich QR-Codes drucken öffnet die Schaltfläche Drucken den Druckdialog des Browsers mit allen erzeugten QR-Codes. Unter jedem QR-Code stehen der Benutzername und das Ablaufdatum (`EXP` mit Datum) bzw. der Hinweis `Läuft nicht ab`.

> Die Tokens werden aus Sicherheitsgründen nur in diesem Dialog angezeigt. Nach Klick auf Schließen lassen sich die QR-Codes nicht erneut drucken. Die QR-Codes sollten daher direkt gedruckt oder über den Druckdialog als PDF gespeichert werden. Geht ein QR-Code verloren, wird für den betroffenen Benutzer ein neues Token erzeugt.

Für einzelne Benutzer kann ein Token auch im Benutzerprofil erzeugt werden.

QR-Codes platzsparend drucken

Die Druckansicht gibt jeden QR-Code auf einer eigenen Seite aus. Sollen die QR-Codes als kleine Karten ausgeschnitten werden, lassen sich über den Druckdialog mehrere Seiten auf ein Blatt drucken:

- Google Chrome und Microsoft Edge: `Weitere Einstellungen` → `Seiten pro Blatt`
- macOS-Druckdialog: `Layout` → `Seiten pro Blatt`

Alternativ wird die Druckausgabe zunächst als PDF gespeichert und anschließend mit mehreren Seiten pro Blatt gedruckt. Bis zu neun QR-Codes pro DIN-A4-Blatt bleiben in der Regel gut scanbar. Die Lesbarkeit sollte vor dem Druck aller Karten mit einem Testausdruck am Gerät geprüft werden.

Weiterführende Informationen

Weiterführende Informationen zu dieser Konfiguration bietet die Entscheidungshilfe zum Mehrbenutzermodus →

Für Version 26.4.0

Relution Files

Relution bietet für iOS die Möglichkeit, lokale Dateifreigaben, auch Netzwerklaufwerke genannt, über SMB und WebDAV zu integrieren. Über die Anbindung von beispielsweise Schul- oder Unternehmens-Serverlösungen kann so auf relevante Dokumente und Inhalte zugegriffen sowie Daten und Arbeitsergebnisse sicher auf einem zentralen Server abgespeichert werden.

Vorteile von Relution Files

Daten sollten nicht in einer ungesicherten Cloud mit Servern außerhalb der EU gespeichert werden, wenn DSGVO-konform gearbeitet werden muss. Ebenso ist es ratsam, die Daten nicht direkt auf Geräten zu speichern, wenn Geräte von mehreren Benutzer genutzt werden. Durch das Speichern und Ablegen von Dokumenten auf eigenen lokalen Servern über `Relution Files` wird die Datensicherheit und Datenhoheit für alle Benutzer gewährleistet.

Lokale Netzlaufwerke für Relution Files konfigurieren

Lokale Dateifreigaben können auf zwei Arten in Relution eingerichtet werden:

Für die manuelle Einrichtung die Dokumentation der App selbst beachten -> Relution Files →

Für Version 26.4.0

Automatische Konfiguration von Relution Files über Richtlinien

Durch eine verwaltete Konfiguration, die der Administrator über das Relution Portal vornimmt, entfällt für den Endanwender nahezu jede Hürde bei der Einrichtung des Gerätes. Auf diese Weise lässt sich die Dateifreigabe nahtlos nutzen.

Mit der Konfiguration von `Relution Dateifreigaben` in einer Richtlinie kann eine WebDAV- oder SMB-Verbindung für die Nutzung vorbereitet werden. Hierfür ist es erforderlich, ein Protokoll zu wählen und den Pfad zur Freigabe einzugeben.

Zudem besteht die Option, den bereits am Gerät `angemeldeten Relution-Benutzer zu verwenden`, was eine zusätzliche Anmeldung zur Dateifreigabe bei der Nutzung von `Relution geteiltes Gerät` überflüssig macht.

Alternativ kann bei 1:1-Geräten der dem Gerät zugewiesene Benutzer sich mit seinen Benutzerdaten anmelden. Durch die Verwendung von Platzhaltern wie beispielsweise `${user.fullname}` kann in diesem Fall der Anmeldeprozess vereinfacht werden.

Weiter kann zwischen zwei Erweiterungstypen gewählt werden: Klassisch und Modern. Diese Einstellung definiert den intern verwendeten Erweiterungstyp von Relution Files, um die Freigaben in die native Apple Files-App zu integrieren. Der `Klassische` Typ sollte in seltenen Fällen verwendet werden, in denen der Standardtyp `Modern` nicht wie erwartet funktioniert (z. B. gibt es unter iOS 18+ einen Fehler bei Shared iPads, bei dem der `Moderne`-Erweiterungstyp Dateien nicht anzeigt).

Apple Configurator 2

Mit dieser Richtlinien-Konfiguration können `.mobileconfig`-Dateien auf Apple-Geräte übertragen werden. Diese kann beispielsweise eine WLAN-Verbindung und das entsprechende Zertifikat enthalten.

Konfiguration

Um eine `.mobileconfig`-Datei auf Geräte übertragen zu können, müssen die entsprechenden Informationen direkt in der Relution-Konfiguration hinterlegt und benannt werden.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
 <key>PayloadContent</key>
 <array>
  </array>
 <key>PayloadDescription</key>
 <string>Dies ist eine leere Konfigurationsdatei.</string>
 <key>PayloadDisplayName</key>
 <string>Leere Konfiguration</string>
 <key>PayloadIdentifier</key>
 <string>com.example.emptyconfig</string>
 <key>PayloadOrganization</key>
 <string>Deine Organisation</string>
 <key>PayloadType</key>
 <string>Configuration</string>
 <key>PayloadUUID</key>
 <string>DEINE-EINDEUTIGE-UUID</string>
 <key>PayloadVersion</key>
 <integer>1</integer>
</dict>
</plist>
```

Es ist nicht möglich, eine mobileconfig-Datei zu verwenden, in der eine Vielzahl an Konfigurationen hinterlegt sind.

Managed App Konfiguration iOS

Es ist möglich, einige Apps mit der Richtlinien-Konfiguration `Verwaltete App (Managed App)` vorzukonfigurieren. Diese Konfiguration ist nur für iOS-Geräte ab Version 7 und macOS-Geräte ab Version 11+ verfügbar.

Konfiguration

Die Bundle-ID der zu konfigurierenden App angeben und eine gültige App-Konfigurations-Payload hinzufügen. In der Payload lassen sich die Platzhalter verwenden, die unten auf der Seite angezeigt werden. So kann zum Beispiel eine E-Mail-Client-App konfiguriert werden, indem der Platzhalter `${user.email}` verwendet wird. So lässt sich die Konfiguration für verschiedene Benutzer nutzbar machen. Die Platzhalter werden ausgefüllt, wenn die Konfiguration auf die Geräte übertragen wird.

> Die zu konfigurierende App muss im Vorfeld bereits auf den Geräten installiert sein, bevor die App-Konfiguration Anwendung findet. Wird die App in der gleichen Richtlinie auf den Geräten installiert, sicherstellen, dass die App-Konfiguration nach der Installation der App ausgeführt wird, indem sie später in die Liste der Konfigurationen eingefügt wird.

Grundsätzlich ist der Hersteller der jeweiligen App für die Konfigurationsmöglichkeiten verantwortlich. Wir haben hier einige Beispiele aufgeführt, die mit den Apps zum Zeitpunkt der Erstellung dieses Dokuments funktioniert haben. Wir geben keinerlei Garantie, dass dies weiterhin gewährleistet ist.

Für Version 26.4.0

Goodnotes 6

```
com.goodnotesapp.x
```

```xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>ManagedAppConfigurationVersion</key>
    <string>1</string>
    <key>LicenseKey</key>
    <string>AAAAAA-BBBBBB-CCCCCC-DDDDDD-123456-V3</string>
</dict>
</plist>
```

Zusätzliche Informationen sind vom Hersteller hier aufgeführt: Goodnotes Webseite →

Microsoft Outlook für Office365

```
com.microsoft.Office.Outlook
```

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
 <key>com.microsoft.outlook.EmailProfile.AccountType</key>
 <string>ModernAuth</string>
 <key>com.microsoft.outlook.EmailProfile.EmailAccountName</key>
 <string>${user.fullname}</string>
 <key>com.microsoft.outlook.EmailProfile.ServerHostName</key>
 <string>outlook.office365.com</string>
 <key>com.microsoft.outlook.EmailProfile.EmailAddress</key>
 <string>${user.email}</string>
 <key>com.microsoft.outlook.EmailProfile.EmailUPN</key>
 <string>${user.email}</string>
 <key>com.microsoft.outlook.EmailProfile.AccountDomain</key>
 <string></string>
 <key>com.microsoft.outlook.EmailProfile.ServerAuthentication</key>
 <string>Username and Password</string>
 <key>IntuneMAMAllowedAccountsOnly</key>
 <string>Enabled</string>
 <key>IntuneMAMUPN</key>
 <string>${user.email}</string>
</dict>
</plist>
```

Microsoft Outlook für einen On-Premise Exchange Server

```
com.microsoft.Office.Outlook
```

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
 <key>com.microsoft.outlook.EmailProfile.AccountType</key>
 <string>BasicAuth</string>
 <key>com.microsoft.outlook.EmailProfile.EmailAccountName</key>
 <string>${user.fullname}</string>
 <key>com.microsoft.outlook.EmailProfile.ServerHostName</key>
 <string>exchange.server.name</string>
 <key>com.microsoft.outlook.EmailProfile.AccountDomain</key>
 <string>domainname</string>
 <key>com.microsoft.outlook.EmailProfile.EmailAddress</key>
 <string>${user.email}</string>
 <key>com.microsoft.outlook.EmailProfile.EmailUPN</key>
 <string>${user.email}</string>
 <key>com.microsoft.outlook.EmailProfile.ServerAuthentication</key>
 <string>Username and Password</string>
 <key>IntuneMAMAllowedAccountsOnly</key>
 <string>Disabled</string>
 <key>IntuneMAMUPN</key>
 <string>${user.email}</string>
</dict>
</plist>
```

Für Versi

SecurePIM für Office365

```
com.virtual-solution.securepim-enterprise
```

```
<?xml version="1.0" ?>
<!DOCTYPE plist PUBLIC "-//Apple Inc//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
 <dict>
  <key>license</key>
    <string>your-license-key</string>
    <key>activeSyncServer</key>
    <string>outlook.office365.com</string>
    <key>userEmail</key>
    <string>${user.email}</string>
    <key>activeSyncUser</key>
    <string>${user.email}</string>
    <key>deviceSerialNumber</key>
    <string>${device.serialnumber}</string>
    <key>recipientCertificateEmail</key>
    <string>${user.email}</string>
    <key>allowTouchIDAuthentication</key>
    <string>true</string>
    <key>callKitEnabled</key>
    <string>true</string>
  </dict>
 </plist>
```

Konfiguration unvollständig

Beim Export einer bestehenden Konfiguration aus einem anderen MDM-System als XML und der anschließenden Umwandlung in eine `plist`-Datei kann aus einem als optional markierten, leeren Wert ein leerer `<string></string>`-Wert in der `plist` werden. Betroffen ist unter anderem der Key `subscriptionWebServiceEndPointURL`.

SecurePIM meldet in diesem Fall beim App-Start dauerhaft die Meldung „Konfiguration unvollständig", obwohl der Key im ursprünglichen System ohne Wert funktioniert hat. Abhilfe schafft das Eintragen eines beliebigen, nicht-leeren Werts in den betroffenen Key oder das vollständige Entfernen des Keys aus der `plist`.

FileBrowser for Education

```
com.stratospherix.filebrowsereducation
```

Konfiguration eines SMB-Share

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>mdm-enforce</key>
  <integer>1</integer>
  <key>lockdown</key>
  <integer>1</integer>
  <key>1displayname</key>
  <string>My NAS</string>
  <key>1domain</key>
  <string>office.mwaysolutions.com</string>
  <key>1flags</key>
  <integer>1746</integer>
  <key>1machinename</key>
  <string>smb://yoursmbservershare/</string>
  <key>1username</key>
  <string>${user.email}</string>
  <key>1vpntype</key>
  <integer>0</integer>
  <key>waitForSearchButton</key>
  <integer>0</integer>
</dict>
</plist>
```

Für Versi

IBM Verse client

```
com.ibm.lotus.traveler
```

Vollständiges Konfigurationsbeispiel anzeigen

Einzel App Modus

Mit dieser Konfiguration wird festgelegt, dass ein Gerät ausschließlich eine bestimmte App ausführt. In diesem Modus können Benutzer die Anwendung nicht verlassen oder zu anderen Funktionen des Geräts wechseln.

Vorbereitung & Konfiguration

> Die gewünschte App vorab über eine Aktion oder eine App verwalten-Richtlinie installieren. Wenn der Single App Mode aktiviert wird, ohne dass die App auf dem Gerät vorhanden ist, kann das Gerät durch eine Fehlermeldung blockiert werden. In diesem Fall muss die App nachträglich installiert und das Gerät neu gestartet werden.

Die auf dem Gerät angezeigte Fehlermeldung lautet:

```
Der geführte Zugriff ist nicht verfügbar. Bitte wenden sie sich an deine:n Admin.
```

1. App-Auswahl: Zunächst die Anwendung auswählen, die im Einzel-App-Modus ausgeführt werden soll.
2. Einschränkungen: Anschließend die zusätzlichen Optionen definieren, um die Nutzung der App weiter einzugrenzen.

Für Version 26.4.0

Gerätesteuerung

Mit diesen Optionen wird die physische Interaktion mit dem Gerät eingeschränkt:

- Touch-Eingaben deaktivieren: Unterbindet jegliche Berührungseingaben auf dem Bildschirm.
- Bewegung (Bildschirm drehen) deaktivieren: Verhindert den Wechsel zwischen Hoch- und Querformat.
- Lautstärketasten deaktivieren: Sperrt die physischen Tasten zur Lautstärkeregelung.
- Seitenschalter deaktivieren: Deaktiviert den Stummschalter. Das Verhalten richtet sich nach der Position, in der sich der Schalter zum Zeitpunkt der Aktivierung befand.
- Ein-/Ausschalter deaktivieren: Verhindert das Ausschalten oder Sperren des Geräts über die Power-Taste.
- Automatische Sperre deaktivieren: Das Gerät wechselt bei Inaktivität nicht automatisch in den Ruhezustand (Bildschirm bleibt dauerhaft an).

Bedienungshilfen

Folgende Bedienungshilfen lassen sich für Benutzer während des Modus freigeben:

- VoiceOver: Erlaubt die Nutzung der Bildschirmvorlesefunktion.
- Zoom: Gestattet das Vergrößern von Bildschirminhalten.
- Farben umkehren: Erlaubt die Invertierung der Displayfarben.
- AssistiveTouch: Aktiviert die digitale Bedienhilfe auf dem Bildschirm.
- Auswahl vorlesen: Ermöglicht es, markierten Text laut vorzulesen.
- Mono Audio: Schaltet die Audioausgabe auf Mono um.

Bedienungshilfen-Kurzbefehl

Hier wird festgelegt, welche Funktionen über den Kurzbefehl (z. B. Dreifachklick auf die Seitentaste) verfügbar sein sollen. Standardmäßig sind diese Optionen deaktiviert:

- VoiceOver: Aktiviert den Kurzbefehl für die Vorlesefunktion.
- Zoom: Aktiviert den Kurzbefehl für die Zoom-Funktion.
- Farben umkehren: Aktiviert den Kurzbefehl für die Farbinvertierung.
- AssistiveTouch: Aktiviert den Kurzbefehl für AssistiveTouch.

Filter für Inhalte

Hierbei handelt es sich um einen Jugendschutzfilter, der auf iOS- und macOS-Geräten aktiviert oder deaktiviert werden kann.

> Relution hat keinen Einfluss auf die gefilterten Inhalte. Die Verwaltung des Filters obliegt Apple. Zudem kann nicht festgelegt werden, ob Inhalte einer bestimmten Altersfreigabe entsprechen oder nicht.

Konfiguration

Für Version 26.4.0

Trotzdem können Webseiten zu einer `Sperrliste (Gesperrte URLs)` oder einer `Positivliste (Erlaubte URLs)` hinzugefügt werden. In der Konfiguration ist der Filter grundsätzlich aktiv, wenn der Haken `Auto-Filter aktivieren` gesetzt ist:

Unter Umständen wird durch den Filter nicht immer das gewünschte Ergebnis erzielt, da teilweise auch URLs gefiltert werden, die keine jugendgefährdenden Inhalte aufweisen.

Wenn eine bestimmte URL gefiltert werden soll, die nicht durch den automatischen Filter geblockt wird, muss diese auf die `Gesperrte URLs`-Liste gesetzt werden. Soll eine gefilterte URL freigegeben werden, wird sie auf die `Erlaubte URLs`-Liste gesetzt.

Ein besonderes Augenmerk sollte auf die Liste der `Bestimmten Lesezeichen` geworfen werden. Wenn hier Eintragungen gemacht werden, sind ausschließlich diese URLs erlaubt. Unabhängig davon, was in der `Erlaubte URLs`-Liste konfiguriert wurde. Zudem werden diese `Bestimmten Lesezeichen` im Safari als Bookmarks angelegt.

> Ist der Filter für Inhalte aktiv, kann auf den Geräten in den Safari-Einstellungen Verlauf und Webseitendaten die Funktion Löschen nicht mehr ausgeführt werden.

Geräte Sperrzeit

Durch das Festlegen von Sperrzeiten für iOS-Geräte kann die aktive Verwendung unterbunden werden. Ist die Richtlinien-Konfiguration aktiv, werden alle Apps ausgeblendet und stehen nach Ablauf der Endzeit wieder zu Verfügung.

Benachrichtigungen

Ab Version 5.25 lassen sich mit Relution für iOS die Einstellungen für Benachrichtigungen einzelner Apps vorkonfigurieren. Hierzu steht die Richtlinienkonfiguration `Benachrichtigungen` zur Auswahl bereit.

Konfiguration

Um Benachrichtigungseinstellungen zu konfigurieren, muss eine App gewählt werden, auf die die Einstellung angewendet werden soll. Dazu stehen die gewohnten Auswahlmöglichkeiten `Relution App Store`, `Apple App Store`, `iOS System Apps` und `Manueller Eintrag` zur Verfügung. Wurde eine App ausgewählt, kann diese entsprechend konfiguriert werden.

An dieser Stelle lassen sich Mitteilungen auf dem Gerät für die entsprechende App aktivieren. Dazu gehört die Anzeige in CarPlay, auf dem Sperrbildschirm oder im Mitteilungscenter. Als Hinweistyp lässt sich temporärer oder dauerhafter Banner einstellen.

Zudem können kritische Warnmeldungen aktiviert und Töne eingeschaltet werden.

Der Vorschautyp lässt sich ebenfalls einstellen. Hier kann zwischen `Immer`, `Entsperrt` und `Nie` gewählt werden.

Auch eine Gruppierung nach pro App ist möglich.

Für Version 26.4.0

Exchange

Mit Relution kann eine Microsoft Exchange Konfiguration für iOS-Geräte in die native Mail-App übergeben werden. Somit entfällt für den Endanwender die komplexe Einrichtung. Je nach gewählter Authentifizierung → ist am Gerät nur noch die Eingabe des Benutzerkennwortes, eine Anmeldung über OAuth oder gar keine Eingabe erforderlich.

Allgemein

- Secure Mail Gateway verwenden: Wird diese Funktion aktiviert, werden die URL und Domäne des Secure Mail Gateway anstelle der Exchange-URL und Exchange-Domäne auf die Geräte verteilt. Dadurch kommunizieren die Geräte über das Secure Mail Gateway mit dem Exchange Server.
- Exchange Host
- Exchange Domäne
- Exchange Server verwendet SSL für die Authentifizierung

Kontoeinstellungen

Für Version 26.4.0

- Kontoname
- E-Mail-Adresse des Benutzers verwenden `${user.email}`
- E-Mail-Adresse

Benutzername

- Manuell
- Benutzername des Benutzers verwenden `${user.name}`
- E-Mail-Adresse des Benutzers verwenden `${user.email}`

Die Felder OAuth, Passwort und Zertifikat legen fest, wie sich das Gerät am Exchange-Server anmeldet. Sie sind im Abschnitt Authentifizierung → beschrieben.

Eingeschaltete Services

- Kalender aktivieren
  - Benutzer kann den Kalender ein- und ausschalten
- E-Mail aktivieren
  - Benutzer kann die E-Mails ein- und ausschalten
- Notizen aktivieren
  - Benutzer kann die Notizen ein- und ausschalten
- Erinnerungen aktivieren
  - Benutzer kann die Erinnerungen ein- und ausschalten
- Kontakte aktivieren
  - Benutzer kann die Kontakte ein- und ausschalten

Synchronisationseinstellungen

- Bewegen zulassen
- Mail-Versand via Share-Sheet verhindern
- Letzte E-Mail-Adressen synchronisieren
- S/MIME Signierung aktivieren
- S/MIME Signierung vom Benutzer überschreibbar
- S/MIME-Verschlüsselung standardmäßig aktivieren
- Pro Nachricht Verschlüsselungsoption aktivieren
- S/MIME-Verschlüsselung vom Benutzer überschreibbar
- Synchronisationszeitraum
  - Kein Limit
  - 1 Tag
  - 3 Tage
  - 1 Woche
  - 2 Wochen
  - 1 Monat

Authentifizierung

Für die Anmeldung am Exchange-Server stehen drei Wege zur Verfügung: ein Passwort, OAuth oder ein Zertifikat. Relution kennt die Passwörter der Benutzer nicht und kann sie daher nicht pro Benutzer übertragen.

Passwort

Für Version 26.4.0

Ein im Feld Passwort eingetragener Wert wird unverändert an alle Geräte übertragen, denen die Richtlinie zugewiesen ist. Einen Platzhalter für das Passwort des jeweiligen Benutzers gibt es nicht. Für persönliche Konten bleibt das Feld daher in der Regel leer, und das Passwort wird am Gerät eingegeben.

Ob iOS dabei von sich aus nach dem Passwort fragt, steuert das Betriebssystem. Relution kann keine Passwortabfrage in der Mail-App auslösen.

OAuth

Ist OAuth aktiviert, meldet sich der Benutzer über die Anmeldeseite des Identitätsanbieters an, z. B. bei Microsoft Entra ID für Exchange Online oder Exchange Server mit Hybrid Modern Authentication. Das Feld Passwort ist in diesem Fall gesperrt.

Zertifikat

Mit einem Zertifikat meldet sich das Gerät ohne Passwort am Exchange-Server an. Voraussetzung ist, dass der Exchange-Server die Anmeldung per Zertifikat akzeptiert. Es gibt zwei Varianten:

- Zertifikat wählen: Ein bestimmtes Zertifikat oder eine Zertifikatsvorlage aus der Zertifikatsverwaltung → wird verwendet.
- Benutzerdefiniertes Zertifikat verwenden: Das Zertifikat des jeweiligen Benutzers wird verwendet. Besitzt ein Benutzer mehrere Zertifikate dieses Typs, wählt das Feld Zertifikatsname eines davon aus. Bleibt es leer, wird das am längsten gültige Zertifikat verwendet.

Für die direkte Anmeldung per Zertifikat am Exchange-Server bleibt OAuth deaktiviert.

Relution verhindert nicht, dass OAuth und ein Zertifikat gleichzeitig konfiguriert werden. Das Zertifikat wird in diesem Fall trotzdem an das Gerät übertragen.

Aktualisierungsmodus

Wenn diese Einstellung auf Nur bei Veröffentlichung von neuen Richtlinienversionen gesetzt wird, werden Updates für diese Konfiguration nur dann verschickt, wenn sich die veröffentlichte Richtlinienversion geändert hat. Aus anderen Gründen, wie z. B. geänderter Gerätebenutzer oder Platzhalter, ausgelöste Updates werden nicht auf die Geräte ausgespielt.

Dadurch wird die Anzahl der Synchronisierungen für diese Konfiguration reduziert, was die Ressourcennutzung auf dem Gerät verringern kann, während gleichzeitig das Risiko verpasster Aktualisierungen besteht.

Aktualisierungsmodus

- Standard
- Nur bei Veröffentlichung von neuen Richtlinienversionen

Für Version 26.4.0

Softwareupdates

Mit Relution 26.1.0 wurde die neue Apple-Konfiguration Softwareupdates für Geräte ab iOS 18 eingeführt. Diese Konfiguration kann zusätzlich zur bestehenden System-Updates Konfiguration verwendet werden. Sie ersetzt unter anderem das Verzögern von Updates in den Restriktionen sowie das Update-Verhalten aus der alten System-Updates Konfiguration, welche in Relution als veraltet gekennzeichnet ist.

Um Updates zuverlässig über den gesamten Gerätepool sicherzustellen, können die Konfigurationen Softwareupdates und System-Updates parallel konfiguriert und auf alle iOS-Geräte verteilt werden.

> Die veraltete Konfiguration System-Updates wird von Apple mittelfristig eingestellt.

Konfiguration

Allgemein

Einschreibungen in das Beta-Programm

- Erlaubt
- Immer aus

Benachrichtigungen zu Softwareupdates

- Alle Benachrichtigungen anzeigen
- Dem Benutzer angezeigte Updates:
  - Alle
  - Neueste
  - Älteste

Für Version 26.4.0

Aktionen für automatische Softwareupdates

Automatisches Herunterladen verfügbarer Betriebssystem-Updates

- Wahl durch Benutzer
- Immer aus
- Immer an

Verfügbare Betriebssystem-Updates automatisch installieren

- Wahl durch Benutzer
- Immer aus
- Immer an

Automatisches Installieren verfügbarer Sicherheitsupdates

- Wahl durch Benutzer
- Immer aus
- Immer an

Aufschub von Betriebssystem-Updates

- Verzögerung in Tagen: Anzahl der Tage, um ein größeres oder kleineres Betriebssystem-Update auf dem Gerät zu verschieben.

Schnelle Reaktion auf Sicherheitsupdates

- Erlaubt dem Benutzer Sicherheitsverbesserungen im Hintergrund zu installieren
- Ermöglicht dem Benutzer, Rollbacks von Sicherheitsupdates im Hintergrund durchzuführen

Verwaltete Softwareupdates

Neu in 26.4

Die Konfiguration Verwaltete Softwareupdates erzwingt Betriebssystemupdates und gibt dabei eine Zielversion bis zu einer Frist vor. Sie ist der Nachfolger der veralteten Konfiguration System-Updates und ergänzt die oben beschriebenen Softwareupdates-Einstellungen: Während dort das Update-*Verhalten* gesteuert wird (automatisches Laden, Aufschub, Benachrichtigungen), legt Verwaltete Softwareupdates verbindlich fest, *welche* Version bis *wann* installiert sein muss.

Voraussetzung ist iOS 17 oder neuer im überwachten Modus (Supervised). Die Konfiguration steht außerdem für tvOS ab 18.4 und visionOS ab 26 zur Verfügung.

Für Version 26.4.0

Zielversion

- Zu erzwingende Version
  - Neueste Hauptversion — das Gerät wird auf die aktuellste verfügbare Hauptversion gehoben.
  - Neueste Nebenversion — es wird innerhalb der installierten Hauptversion aktualisiert.
  - Bestimmte Mindestversion — eine konkrete Version wird als Mindeststand vorgegeben.
- URL der Detailseite — optionaler Link, den iOS den Benutzern zur Update-Ankündigung anzeigt.

Durchsetzung

- Durchsetzungsplan
  - Relativ zum Veröffentlichungsdatum — die Frist ergibt sich aus Tage nach Veröffentlichung und Uhrzeit. Damit gilt für jede künftige Version automatisch dieselbe Regel.
  - Bestimmtes Datum und Uhrzeit — die Frist wird als fester Zeitpunkt gesetzt.
- Karenzzeit nach der Einschreibung — optional. Verschiebt die Frist auf so viele Tage nach der Einschreibung eines Geräts, damit neu eingeschriebene Geräte nicht sofort zum Update gezwungen werden. Die Angabe gilt für beide Durchsetzungspläne und verlängert eine Frist immer nur, verkürzt sie nie. Bleibt das Feld leer, ist die Funktion deaktiviert.

Lassen sich die verfügbaren Betriebssystemversionen im Portal nicht laden, meldet die Konfiguration dies beim Öffnen. Die Auswahl einer bestimmten Mindestversion ist dann nicht möglich, die beiden anderen Modi bleiben

nutzbar.

Update auslösen

Es gibt zwei Möglichkeiten, iOS-Updates durchzuführen:

Richtlinien-Konfiguration Über die Richtlinien System-Updates kann der Zeitraum für System-Updates festgelegt werden.

Geräte-Aktion Über Aktionen im Geräte-Inventar können Geräte unverzüglich auf die jeweils aktuellste verfügbare Update-Version aktualisiert werden.

Damit iOS-Geräte ein Update erfolgreich durchführen können, müssen folgende Bedingungen erfüllt sein:

- Die Geräte müssen ausreichend geladen oder an eine Stromquelle angeschlossen sein.
- Die Geräte müssen entsperrt sein; andernfalls müssen Benutzer ihr Gerätepasswort eingeben.
- Das installierte Update entspricht immer der neuesten öffentlich verfügbaren iOS-Version.
- Unterstützte iOS-Geräte prüfen unabhängig von dieser Richtlinien-Konfiguration einmal täglich auf Updates.
- Diese Konfiguration überschreibt vorhandene Restriktionen zum Verzögern von Updates.
- Bei geteilten Geräten dürfen keine Benutzer angemeldet sein.

Für Version 26.4.0

Hintergrundbild

Mit der Konfiguration „Hintergrundbild“ für iOS-Geräte lässt sich ein Bild für den Homescreen und/oder Sperrbildschirm hinterlegen, der nach Anwendung der Richtlinie auf den Geräten erscheint. So können beispielsweise Schülergeräte einer Schule oder Geräte eines Unternehmens mit einem einheitlichen Hintergrundbild und/oder mit einem Bild auf dem Sperrbildschirm versehen werden.

Wird das Hintergrundbild über die Richtlinie festgelegt, wird das ursprüngliche Hintergrundbild des Geräts verworfen und kann mit Relution nicht wiederhergestellt werden.

Welche Ansichten auf den Geräten lassen sich konfigurieren?

Es lässt sich definieren, ob nur beim Sperrbildschirm oder Homescreen nach Anmeldung das Hintergrundbild angezeigt wird oder es für beide Ansichten verwendet werden soll.

Kalender (CalDAV)

Mit der Richtlinie Kalender wird ein CalDAV-Konto per Konfigurationsprofil an die native Kalender-App von iOS und iPadOS übergeben. Für den Endanwender entfällt damit die manuelle Einrichtung. Die zum Konto gehörenden Kalenderpfade werden auf aktuellen iOS-Versionen automatisch nach RFC 6764 über eine Umleitung unter `/.well-known/caldav` ermittelt. Eine korrekt eingerichtete serverseitige `/.well-known/caldav`-Umleitung ist deshalb auf aktuellen iOS-Versionen zwingende Voraussetzung; die alleinige Angabe einer Principal-URL genügt dort nicht mehr.

Konfigurationsmöglichkeiten

Die folgenden Felder stehen für das CalDAV-Konto zur Verfügung. Sie entsprechen den Schlüsseln des Apple-CalDAV-Payloads (`com.apple.caldav.account`).

Kontoeinstellungen

- Kontobeschreibung — Anzeigename des Kontos auf dem Gerät.
- Host — Serveradresse ohne Schema und ohne Pfad (z. B. `kalender.example.com`).
- Port — in der Regel `443`.
- SSL verwenden — bei Erreichbarkeit über HTTPS zwingend zu aktivieren. Ohne aktives SSL wird bei Port `443` ein unverschlüsselter Verbindungsaufbau versucht, der fehlschlägt.
- Benutzername — manuell oder über die Platzhalter `${user.name}` bzw. `${user.email}`.
- Passwort — bei fehlender Angabe erfolgt die Abfrage bei der Profilinstallation am Gerät.
- Principal-URL *(optional)* — der Pfad zum Benutzer-Principal (z. B. `/remote.php/dav/principals/users/${user.name}/`).

Für Version 26.4.0

> Die Principal-URL ist als reiner Pfad anzugeben, nicht als vollständige URL mit Schema und Host (nicht `https://host/...`). Host, Port und Verschlüsselung ergeben sich aus Host, Port und SSL verwenden. Auf aktuellen iOS-Versionen ersetzt eine gesetzte Principal-URL die automatische Erkennung jedoch nicht mehr — maßgeblich ist eine korrekt eingerichtete `/.well-known/caldav`-Umleitung. Das Feld kann daher leer bleiben.

Automatische Erkennung über .well-known

Aktuelle iOS-Versionen richten CalDAV-Konten nach RFC 6764 ein. Der Ablauf ist dabei:

1. Anfrage `PROPFIND /.well-known/caldav` an den unter Host hinterlegten Server.
2. Der Server antwortet mit einer Umleitung (`301`) auf seinen DAV-Endpunkt (bei ownCloud/Nextcloud `/remote.php/dav`).
3. Über den DAV-Endpunkt wird der `current-user-principal` und darüber der Kalender-Bereich des Benutzers ermittelt.

Die zuverlässige Einrichtung hängt damit vollständig von einer korrekten `/.well-known`-Umleitung ab. Auf neueren iOS-Versionen lässt sich die automatische Erkennung nicht mehr durch Angabe einer Principal-URL umgehen — ohne funktionierende `/.well-known`-Umleitung schlägt die Einrichtung fehl, selbst wenn eine Principal-URL hinterlegt ist.

Neuere iOS-Versionen sind bei der Auswertung der Umleitung strenger als iOS 17. Eine fehlerhafte Umleitung (z. B. auf `http://` statt `https://`), die unter iOS 17 noch toleriert wurde, führt auf aktuellen Versionen zum Abbruch der Erkennung. Bereits unter iOS 17 eingerichtete Konten auf Altgeräten können dabei weiterhin funktionieren, während Neueinrichtungen fehlschlagen.

Serverseitige Einrichtung der Umleitung

`/.well-known/caldav` und `/.well-known/carddav` müssen per `301` auf den DAV-Endpunkt des Servers umleiten. Die Ziel-Adresse muss zwingend mit **`https://`** beginnen und darf keinen internen Port enthalten.

Für nginx:

```
location = /.well-known/caldav  { return 301 https://$host/remote.php/dav; }
location = /.well-known/carddav { return 301 https://$host/remote.php/dav; }
```

Für Apache (im vHost):

```
Redirect 301 /.well-known/caldav  https://kalender.example.com/remote.php/dav
Redirect 301 /.well-known/carddav https://kalender.example.com/remote.php/dav
```

Betrieb hinter einem Reverse-Proxy / TLS-Terminierung: Terminiert ein vorgelagerter Proxy die TLS-Verbindung und leitet intern per HTTP an einen anderen Port weiter (z. B. `8080`), kennt der Webserver seine öffentliche Adresse häufig nur als `http` auf dem internen Port. Eine daraus erzeugte Umleitung lautet dann fehlerhaft z. B. `http://kalender.example.com:8080/remote.php/dav`. Da aktuelle iOS-Versionen einem Wechsel von `https` auf `http` nicht folgen, schlägt die Erkennung fehl. In diesem Fall ist die Umleitung mit vollständiger **`https://`**-Zieladresse zu setzen — entweder direkt am TLS-terminierenden Proxy oder als absolute Ziel-URL wie im Apache-Beispiel.

Verifizierung

Die Umleitung lässt sich mit `curl` prüfen:

```
curl -sI https://kalender.example.com/.well-known/caldav
```

Die Antwort muss eine Umleitung mit korrektem `location`-Header enthalten:

```
HTTP/2 301
location: https://kalender.example.com/remote.php/dav
```

Der `location`-Header muss mit `https://` beginnen und darf keinen internen Port (z. B. `:8080`) enthalten.

Fehlerbehebung

Symptom	Ursache	Lösung
Einrichtung schlägt nur auf neueren iOS-Versionen fehl; ältere Geräte funktionieren weiter	Die Umleitung verweist auf `http://` (Downgrade); ältere iOS-Versionen tolerierten dies	Umleitung auf `https://` korrigieren
`301` verweist auf einen internen Port (z. B. `:8080`)	Reverse-Proxy/TLS-Terminierung, der Webserver kennt seine öffentliche Adresse nicht	Umleitung mit vollständiger `https://`-Adresse am Proxy oder Webserver setzen
`405 Method Not Allowed` auf Pfaden wie `/` oder `/principals/`	Die automatische Erkennung greift nicht und probiert Standardpfade, die auf dem Server nicht existieren	`/.well-known`-Umleitung korrekt einrichten (auf neueren iOS-Versionen zwingend)
Der ermittelte Pfad ist offensichtlich falsch	Principal-URL als vollständige URL statt als reiner Pfad hinterlegt oder SSL verwenden nicht aktiviert	Principal-URL als reinen Pfad angeben und SSL verwenden aktivieren

Eingrenzung am Gerät

Zur Eingrenzung kann ein CalDAV-Konto testweise direkt am Gerät unter `Einstellungen` → `Kalender` → `Accounts` eingerichtet werden. Verbindet sich das manuell eingerichtete Konto, während das per Profil verteilte Konto fehlschlägt, liegt die Ursache in der automatischen Erkennung (`/.well-known`) bzw. in der über das Profil verteilten Principal-URL — nicht am Server selbst.

Verwendung unter macOS

Die CalDAV-Konfiguration und die serverseitige `/.well-known`-Voraussetzung gelten für macOS identisch:

- Kalender (CalDAV) für macOS →

Administrierte Domänen

Mit der Konfiguration Administrierte Domänen wird festgelegt, welche E-Mail- und Web-Domänen iOS als Domänen des Unternehmens behandelt. Die Konfiguration steht für Geräte mit Geräteregistrierung zur Verfügung, für Geräte mit Benutzerregistrierung (User Enrollment/BYOD) nicht.

E-Mail-Domänen

In der Liste E-Mail Domänen werden die Domänen des Unternehmens eingetragen, z. B. `relution.io`. Beim Verfassen einer Nachricht markiert die Mail-App alle Empfängeradressen rot, deren Domäne nicht in der Liste steht. So ist sofort erkennbar, wenn eine Nachricht das Unternehmen verlässt.

Der Versand an diese Adressen wird dabei nicht blockiert. Die Markierung ist ein reiner Hinweis.

Web-Domänen

Für Version 26.4.0

URLs aus den Domänen in der Liste Web-Domänen behandelt iOS als verwaltet. Inhalte, die in Safari von diesen Seiten heruntergeladen werden, gelten damit als Unternehmensdaten, z. B. ein PDF aus dem Intranet.

Eine sichtbare Wirkung hat diese Liste erst zusammen mit den Einschränkungen zum Öffnen von Dokumenten in der Konfiguration Restriktionen →:

- Öffnen von verwalteten Dokumenten in nicht verwalteten Apps erlauben
- Öffnen von nicht verwalteten Dokumenten in verwalteten Apps erlauben

Ist das Öffnen verwalteter Dokumente in nicht verwalteten Apps verboten, lässt sich ein PDF aus dem Intranet anschließend nur noch in verwalteten Apps öffnen. Weitere Hintergründe zur Trennung von verwalteten und nicht verwalteten Daten sind im Artikel Datentrennung → beschrieben.

Intelligence-Einstellungen

Mit Relution lässt sich die Konfiguration Intelligence-Einstellungen zentral verwalten, um die Funktionen von Apple Intelligence auf verwalteten iOS-Geräten zu steuern. Über die Richtlinie lassen sich einzelne KI-gestützte Funktionen wie der Apple-Intelligence-Bericht, Genmoji, Image Playground, Image Wand, personalisierte Handschriftergebnisse, die Visual-Intelligence-Zusammenfassung und die Schreibwerkzeuge erlauben oder unterbinden. Zusätzlich lassen sich appspezifische Intelligence-Funktionen in Mail, Notizen und Safari steuern sowie Diktier- und Übersetzungsfunktionen ausschließlich lokal auf dem Gerät erzwingen, ohne Verbindung zu Apple-Servern.

Die Konfiguration steht für iOS-Geräte ab Version 26.4 zur Verfügung und kann ausschließlich im Rahmen der Geräteregistrierung angewendet werden, nicht bei der Benutzerregistrierung (BYOD). In gleicher Form ist sie für macOS und visionOS ab Version 26.4 verfügbar.

Nicht alle Optionen werden von jeder Plattform unterstützt. Das Formular zeigt sie dennoch für alle Plattformen an.

- visionOS: nicht unterstützt werden Personalisierte Handschriftergebnisse erlauben, Visual-Intelligence-Zusammenfassung erlauben, Übersetzung nur auf dem Gerät erzwingen sowie Transkription erlauben und Transkriptionszusammenfassung erlauben im Abschnitt Notizen.
- macOS: nicht unterstützt werden Image Wand erlauben, Personalisierte Handschriftergebnisse erlauben, Visual-Intelligence-Zusammenfassung erlauben und Übersetzung nur auf dem Gerät erzwingen.

Für Version 26.4.0

Einstellungen

- Apple-Intelligence-Bericht erlauben
  - Wenn deaktiviert, wird der Apple-Intelligence-Bericht auf dem Gerät deaktiviert. Standardmäßig aktiviert.
- Genmoji erlauben
  - Wenn deaktiviert, wird die Genmoji-Funktion deaktiviert. Standardmäßig aktiviert.
- Image Playground erlauben
  - Wenn deaktiviert, wird Image Playground deaktiviert. Standardmäßig aktiviert.
- Image Wand erlauben
  - Wenn deaktiviert, wird Image Wand deaktiviert. Standardmäßig aktiviert.
- Personalisierte Handschriftergebnisse erlauben
  - Wenn deaktiviert, werden personalisierte Handschriftergebnisse deaktiviert. Standardmäßig aktiviert.
- Visual-Intelligence-Zusammenfassung erlauben
  - Wenn deaktiviert, wird die Visual-Intelligence-Zusammenfassung deaktiviert. Standardmäßig aktiviert.
- Schreibwerkzeuge erlauben
  - Wenn deaktiviert, werden die Schreibwerkzeuge (Writing Tools) deaktiviert. Standardmäßig aktiviert.
- Diktat nur auf dem Gerät erzwingen
  - Wenn aktiviert, wird Diktieren ausschließlich lokal auf dem Gerät verarbeitet, ohne Verbindung zu Apple-Servern. Standardmäßig deaktiviert.
- Übersetzung nur auf dem Gerät erzwingen
  - Wenn aktiviert, wird Übersetzen ausschließlich lokal auf dem Gerät verarbeitet, ohne Verbindung zu Apple-Servern. Standardmäßig deaktiviert.

Mail

- Intelligente Antworten erlauben
  - Wenn deaktiviert, werden intelligente Antworten (Smart Replies) in Mail deaktiviert. Standardmäßig aktiviert.
- Zusammenfassung erlauben
  - Wenn deaktiviert, wird die Zusammenfassungsfunktion in Mail deaktiviert. Standardmäßig aktiviert.

Notizen

- Transkription erlauben
  - Wenn deaktiviert, wird die Transkription in Notizen deaktiviert. Standardmäßig aktiviert.
- Transkriptionszusammenfassung erlauben
  - Wenn deaktiviert, wird die Zusammenfassung von Transkriptionen in Notizen deaktiviert. Standardmäßig aktiviert.

Safari

- Zusammenfassung erlauben
  - Wenn deaktiviert, wird die Zusammenfassungsfunktion in Safari deaktiviert. Standardmäßig aktiviert.

Für Version 26.4.0

Externe Intelligenz-Einstellungen

Mit der Konfiguration „Externe Intelligenz-Einstellungen“ wird zentral gesteuert, ob und wie externe, cloudbasierte KI-Dienste (z. B. ChatGPT) über Siri und Apple Intelligence auf iOS-Geräten genutzt werden dürfen. Die Richtlinie steht ab iOS 26.4 zur Verfügung — ausschließlich für Geräte mit vollständiger Geräteregistrierung, nicht im User Enrollment/BYOD-Modus — und wird per Deklarativer Geräteverwaltung (DDM) auf das Gerät übertragen. Dieselbe Konfiguration steht in gleicher Form auch für macOS- und visionOS-Geräte ab der jeweiligen Version 26.4 zur Verfügung.

Diese Konfiguration ist eine eigenständige, DDM-basierte Richtlinie und ergänzt die bereits bestehenden Felder zu externen Intelligenz-Integrationen innerhalb der iOS-Restriktionen →. Beide Konfigurationstypen können im Portal parallel angezeigt werden, decken jedoch dieselben Funktionen ab.

Externe KI-Integrationen

- Externe KI-Integrationen erlauben
  - Wenn deaktiviert, werden externe KI-Integrationen vollständig unterbunden. Standardmäßig aktiviert.
- Anmeldung für externe KI-Integrationen erlauben
  - Wenn deaktiviert, ist die Anmeldung (Sign-In) bei externen KI-Integrationen nicht möglich. Standardmäßig aktiviert.
- Erlaubte Workspace-ID
  - Legt die Workspace-ID fest, auf die die externe KI-Integration beschränkt wird. Derzeit auf eine einzelne Workspace-ID begrenzt.

Für Version 26.4.0

Tastatur-Einstellungen

Ab iOS 26.4 und Relution 26.3 steht die Konfiguration „Tastatur-Einstellungen“ zur Verfügung, die über die Deklarative Geräteverwaltung (DDM) umgesetzt wird. Mit dieser Richtlinie lassen sich Tastaturfunktionen wie Autokorrektur, Diktat, Rechtschreibprüfung, Texterkennung, Textersetzung, Wischgesten zum Tippen und mathematische Tastaturvorschläge zentral aktivieren oder deaktivieren – nützlich etwa für Bildungseinrichtungen oder Unternehmen, die eine einheitliche und kontrollierte Texteingabe auf verwalteten Geräten sicherstellen möchten.

Die Konfiguration erfordert iOS 26.4 oder neuer und steht ausschließlich für Geräte zur Verfügung, die per Geräteregistrierung (Device Enrollment) verwaltet werden. Alle Einstellungen sind standardmäßig aktiviert; ein Deaktivieren schränkt die jeweilige Tastaturfunktion ein.

Einstellungen für die Tastatur

- Nachschlagen von Definitionen zulassen
  - Wenn deaktiviert, steht das Nachschlagen von Wortdefinitionen (Look Up) auf der Tastatur nicht mehr zur Verfügung.
- Diktat zulassen
  - Wenn deaktiviert, kann die Diktierfunktion der Tastatur nicht mehr verwendet werden.
- Mathematische Tastaturvorschläge zulassen
  - Wenn deaktiviert, zeigt die Tastatur keine automatischen Lösungsvorschläge für mathematische Ausdrücke mehr an.
- Autokorrektur zulassen
  - Wenn deaktiviert, korrigiert die Tastatur Tippfehler nicht mehr automatisch.
- Texterkennung zulassen
  - Wenn deaktiviert, werden während der Eingabe keine vorausschauenden Wortvorschläge (Predictive Text) mehr über der Tastatur angezeigt.
- Wischgesten zum Tippen zulassen
  - Wenn deaktiviert, kann nicht mehr per Wischgeste über die Tastatur getippt werden (Slide to Type / Gleitgesten-Eingabe).
- Rechtschreibprüfung zulassen
  - Wenn deaktiviert, unterstreicht die Tastatur falsch geschriebene Wörter nicht mehr.
- Textersetzung zulassen
  - Wenn deaktiviert, werden konfigurierte Textersetzungen/-kürzel beim Tippen nicht mehr automatisch eingesetzt.

Für Version 26.4.0

Siri-Einstellungen

Ab iOS 26.4 und Relution 26.3 steht die Konfiguration „Siri-Einstellungen“ zur Verfügung, die über die Deklarative Geräteverwaltung (DDM) umgesetzt wird. Mit dieser Richtlinie lassen sich die grundsätzliche Verfügbarkeit von Siri, der Obszönitätsfilter sowie – ausschließlich unter iOS – die Verarbeitung nutzergenerierter Inhalte und der Zugriff auf Siri im gesperrten Zustand zentral steuern.

Die Konfiguration erfordert iOS 26.4 oder neuer und steht ausschließlich für Geräte zur Verfügung, die per Geräteregistrierung (Device Enrollment) verwaltet werden; für Geräte mit Benutzerregistrierung (User Enrollment/BYOD) ist sie nicht verfügbar.

Vergleichbare Siri-Schalter existieren bereits innerhalb der iOS-Restriktionen →. Die „Siri-Einstellungen“ sind eine eigenständige, zusätzliche Konfiguration und ersetzen die Restriktionen nicht.

Einstellungen für Siri

- Siri aktivieren
  - Aktiviert oder deaktiviert Siri auf dem Gerät. Standardmäßig aktiviert.
- Obszönitätsfilter erzwingen
  - Erzwingt den Obszönitätsfilter von Siri. Standardmäßig deaktiviert.
- Nutzergenerierte Inhalte zulassen
  - Erlaubt Siri den Zugriff auf nutzergenerierte Inhalte. Standardmäßig aktiviert.
- Siri im gesperrten Zustand zulassen
  - Erlaubt die Nutzung von Siri, während das Gerät gesperrt ist. Standardmäßig aktiviert.

Für Version 26.4.0

Safari-Einstellungen

Mit der Konfiguration „Safari-Einstellungen“ lässt sich das Verhalten des Safari-Browsers auf verwalteten iOS-Geräten zentral steuern. Dazu zählen unter anderem der Umgang mit Cookies, die Betrugswarnung, JavaScript und Pop-ups sowie das Löschen des Verlaufs, privates Surfen, die Zusammenfassung von Inhalten und die Startseite, die beim Öffnen eines neuen Tabs angezeigt wird. Auf macOS-Geräten stehen ausschließlich die vier zuletzt genannten Optionen zur Verfügung – Cookies, Betrugswarnung, JavaScript und Pop-ups lassen sich dort nicht konfigurieren.

Die Konfiguration steht ausschließlich für Geräte mit einem Device-Enrollment-Profil zur Verfügung (kein User Enrollment/BYOD) und setzt mindestens iOS 26 voraus.

Für Version 26.4.0

Einstellungen für den Safari-Browser

- Cookies erlauben
  - Legt fest, wie Safari mit Cookies umgeht.
    - Immer – Safari erlaubt immer Cookies. *(Standardwert)*
    - Von bereits besuchten Seiten – Safari erlaubt nur Cookies von Websites, die bereits besucht wurden.
    - Von der aktuellen Website – Safari erlaubt nur Cookies von der aktuell geöffneten Website.
    - Nie – Safari blockiert Cookies grundsätzlich.
- Deaktivierung der Betrugswarnung zulassen
  - Wenn deaktiviert, erzwingt das System die Betrugswarnung in Safari; Benutzer können sie nicht abschalten. Standardmäßig aktiviert.
- JavaScript erlauben
  - Wenn deaktiviert, wird JavaScript in Safari systemweit deaktiviert. Standardmäßig aktiviert.
- Pop-Ups erlauben
  - Wenn deaktiviert, werden Pop-up-Fenster in Safari systemweit deaktiviert. Standardmäßig aktiviert.
- Löschen des Verlaufs zulassen
  - Wenn deaktiviert, kann der Browser-Verlauf in Safari nicht gelöscht werden. Standardmäßig aktiviert.
- Privates Surfen zulassen
  - Wenn deaktiviert, ist der private Surfmodus in Safari nicht verfügbar. Standardmäßig aktiviert.
- Zusammenfassung von Inhalten zulassen
  - Wenn deaktiviert, wird die automatische Zusammenfassung von Inhalten in Safari deaktiviert. Standardmäßig aktiviert.
- Startseite *(Pflichtfeld)*
  - Legt fest, welche Seite beim Öffnen eines neuen Tabs in Safari angezeigt wird.
    - Start – Safari verwendet die Standard-Startseite; die Homepage wird deaktiviert. *(Standardwert)*
    - Erweiterung – Safari verwendet die über den angegebenen Bezeichner referenzierte Safari-Erweiterung als Startseite; die Homepage wird deaktiviert. Erfordert die Angabe eines Erweiterungs-Bezeichners im Format `Identifier (TeamIdentifier)`, z. B. `com.example.app (ABCD1234)`.
    - Home – Safari verwendet die angegebene URL sowohl als Startseite für neue Tabs als auch als Homepage. Erfordert die Angabe einer Homepage-URL, die mit `https://` oder `http://` beginnen muss.

Für Version 26.4.0

Safari-Erweiterungen

Mit der Konfiguration „Safari-Erweiterungen“ lässt sich das Verhalten einzelner Safari-Erweiterungen auf verwalteten iOS-Geräten zentral steuern. Für jede Erweiterung wird über ihren eindeutigen Identifier festgelegt, ob sie generell erlaubt, dauerhaft aktiviert oder dauerhaft deaktiviert ist, ob sie auch im privaten Surfen verwendet werden darf und auf welche Domains sie zugreifen darf bzw. nicht zugreifen darf. Pro Richtlinie lassen sich mehrere Erweiterungen konfigurieren.

Diese Konfiguration steht nur für überwachte (supervised) iOS-Geräte ab iOS 18 zur Verfügung, die über das Device Enrollment eingebunden wurden; für Geräte im User Enrollment (BYOD) kann sie nicht verwendet werden.

Einstellungen je Safari-Erweiterung

- Identifier der Erweiterung
  - Der Identifier der Safari-Erweiterung, oder „*“, um Einstellungen für alle Erweiterungen zu treffen. Um die Erweiterung zu verwalten, muss die App, zu der sie gehört, auf dem Gerät installiert sein. Dieser Identifier lässt sich via `codesign -dv <Pfad zur Erweiterung (im PlugIns-Verzeichnis innerhalb der App)>` auf einem macOS-Gerät bestimmen, falls die Erweiterung auf macOS verfügbar ist. Ansonsten muss diese Information vom Entwickler der Erweiterung zur Verfügung gestellt werden.
- Status
  - Steuert, ob die Erweiterung zugelassen ist. Optionen: Erlaubt / Immer an / Immer aus.
- Privates Surfen
  - Erweiterung auch im Modus „Privates Surfen“ zulassen. Optionen: Erlaubt / Immer an / Immer aus.
- Erlaubte Domains
  - Steuert die (Sub-)Domains, auf welche die Safari-Erweiterung Zugriff hat. Domains ohne Prefix haben Vorrang vor solchen mit Prefix, nicht zugelassene Domains haben Vorrang vor erlaubten Domains. Alle nicht über die beiden Listen konfigurierten Domains können von Benutzer auf dem Gerät konfiguriert werden.
- Abgelehnte Domains
  - Steuert die (Sub-)Domains, auf welche die Safari-Erweiterung keinen Zugriff hat. Domains ohne Prefix haben Vorrang vor solchen mit Prefix, nicht zugelassene Domains haben Vorrang vor erlaubten Domains. Alle nicht über die beiden Listen konfigurierten Domains können von Benutzer auf dem Gerät konfiguriert werden.

Für Version 26.4.0

Audio-Zubehör-Einstellungen

Ab Version 26.1.0 von Relution wurde die neue Konfiguration „Audio-Zubehör-Einstellungen“ für Geräte ab iOS 26+ eingeführt.

Diese Funktion ermöglicht das temporäre Pairing von Audiozubehör (z. B. Kopfhörer oder Lautsprecher) mit verwalteten Geräten. So kann Audiozubehör zeitlich begrenzt gekoppelt und anschließend automatisch oder manuell wieder entkoppelt werden.

Deaktivieren der temporären Kopplung von Audiozubehör „Ein/Aus“

Mit diesem Schalter wird die temporäre Kopplung von Audiozubehör aktiviert oder deaktiviert.

- Aktiviert: Temporäres Pairing ist erlaubt.
- Deaktiviert: Es ist keine temporäre Kopplung von Audiozubehör möglich.

Richtlinie zum Entkoppeln

Für Version 26.4.0

Hier wird definiert, wie und wann ein temporär gekoppeltes Audiozubehör wieder getrennt wird:

- Keine automatische Entkopplung Das Gerät hebt die Kopplung nicht automatisch auf.

  Diese Option sollte nur verwendet werden, wenn ein Gerät gelöscht und erneut registriert wird (z. B. *Return to Service*) oder wenn ein Benutzerwechsel stattfindet.

- Automatische Entkopplung zu einer bestimmten Uhrzeit Das Gerät hebt die Kopplung von vorübergehend gekoppeltem Audiozubehör automatisch zu einem definierten Zeitpunkt auf.

Zeit zum Entkoppeln

- Uhrzeit festlegen (z. B. 16:30 Uhr) Definiert den Zeitpunkt, zu dem das Gerät die Kopplung von temporär verbundenem Audiozubehör automatisch beendet.

  Zum festgelegten Zeitpunkt wird ausschließlich die Kopplung von zuvor temporär verbundenem Audiozubehör aufgehoben.

Bedingter Zugriff

Ergänzend zu folgendem Artikel Microsoft Bedingter Zugriff → gibt es mit Relution 5.33 für iOS eine Richtlinie Bedingter Zugriff.

Hier gibt es folgende 2 Optionen:

- Gerät wird als nicht konform gekennzeichnet, wenn der Nutzer dieses noch nicht über den Relution Agent registriert hat
- Informiert den Nutzer per Push-Benachrichtigung, damit er sein Gerät registriert

Für Version 26.4.0

Mathematische Einstellungen

Ab Version 26.1.0 von Relution steht die neue Konfiguration Mathematische Einstellungen für Geräte ab iOS 18+ zur Verfügung.

Mit dieser Richtlinie lassen sich die Funktionen und Modi der Apple Taschenrechner App zentral steuern und an pädagogische oder organisatorische Anforderungen anpassen.

Einstellungen für die Apple Taschenrechner App

Basis-Modus

- Quadratwurzel hinzufügen: Fügt dem Basisrechner eine Quadratwurzel-Taste hinzu, indem die Taste „+/-“ ersetzt wird. Standardmäßig ist die Quadratwurzel-Funktion nur im wissenschaftlichen Modus verfügbar. Diese Option ermöglicht den Zugriff auf die Quadratwurzel auch dann, wenn der wissenschaftliche Modus eingeschränkt ist.

Mathematik-Notizen-Modus

- Aktivieren / Deaktivieren: Legt fest, ob der Mathematik-Notizen-Modus in der Taschenrechner App verwendet werden darf.

Wissenschaftlicher Modus

- Aktivieren / Deaktivieren: Bestimmt, ob der wissenschaftliche Modus der Taschenrechner App verfügbar ist.

Globale Eingabeoptionen des Taschenrechners

- Einheitenumrechnung aktivieren: Ermöglicht die Nutzung der integrierten Einheitenumrechnung innerhalb der App.

Für Version 26.4.0

Systemverhalten

Tastaturvorschläge aktivieren

- Aktivieren / Deaktivieren: Steuert, ob in Tastaturvorschlägen automatisch mathematische Lösungen angezeigt werden.

Mathe-Notizen für andere Apps aktivieren

- Aktivieren / Deaktivieren: Legt fest, ob die Funktion „Math Notes“ auch in anderen Apps (z. B. Notizen) verwendet werden darf.

AirPrint

Mit der Richtlinienkonfiguration AirPrint werden AirPrint-fähige Drucker per Konfigurationsprofil auf iOS- und iPadOS-Geräte übertragen. Die hinterlegten Drucker erscheinen anschließend im Druckdialog des Geräts, ohne dass sie im lokalen Netzwerk über Bonjour gefunden werden müssen.

Anwendungsfall

AirPrint-Drucker werden standardmäßig per Bonjour (mDNS) erkannt. Bonjour-Ankündigungen reichen jedoch nicht über Subnetz- bzw. VLAN-Grenzen hinaus — in Schul- und Unternehmensnetzen mit getrennten Netzen für Geräte und Drucker sind die Drucker deshalb im Druckdialog häufig nicht sichtbar. Über die Konfiguration AirPrint wird die Adresse des Druckers direkt vorgegeben, sodass das Gerät ihn gezielt ansprechen kann.

Die Konfiguration ist auch für Geräte mit User Enrollment verfügbar und wird neben iOS und iPadOS auch in macOS-Richtlinien angeboten (siehe AirPrint für macOS →).

Voraussetzungen

- Ein AirPrint-fähiger Drucker oder Druckserver (z. B. CUPS), der über IPP bzw. IPPS erreichbar ist.
- Netzwerkverbindung zwischen Gerät und Drucker auf dem verwendeten Port (Standard für IPP: `631`); Firewalls zwischen den Netzsegmenten müssen diesen Port zulassen.
- Hostname oder IP-Adresse sowie der Ressourcenpfad des Druckers.

Für Version 26.4.0

Konfiguration

Die Konfiguration wird unter `Geräte` → `Richtlinien` in einer iOS-Richtlinie über Konfiguration hinzufügen → AirPrint angelegt. Im Abschnitt Allgemein werden die Drucker in einer Tabelle aufgelistet; über Hinzufügen öffnet sich der Dialog Drucker hinzufügen. Eine Konfiguration kann beliebig viele Drucker enthalten, gespeichert werden kann sie erst, sobald mindestens ein Drucker eingetragen ist.

Pro Drucker stehen folgende Felder zur Verfügung:

Feld	Pflicht	Beschreibung
Hostname oder IP-Adresse	ja	Adresse des Druckers bzw. Druckservers, z. B. `192.168.10.25` oder `drucker01.example.com`.
Port	nein	Port des IPP-Dienstes (`0` – `65535`). Ohne Angabe wird der Standardport verwendet.
Pfad der Ressource	ja	Ressourcenpfad der Druckwarteschlange, z. B. `ipp/print` bei vielen Netzwerkdruckern oder `printers/<Warteschlange>` bei CUPS-Servern.
TLS verwenden	nein	Erzwingt eine TLS-verschlüsselte Verbindung (IPPS) zum Drucker. Standardmäßig deaktiviert.

Bereits eingetragene Drucker lassen sich über das Kontextmenü in der Tabelle mit Bearbeiten ändern oder mit Löschen entfernen; mehrere Drucker können per Mehrfachauswahl gleichzeitig gelöscht werden.

> Den Ressourcenpfad kündigt der Drucker im Bonjour-TXT-Eintrag `rp` an. Auf einem Mac im selben Netz wie der Drucker lässt er sich mit `dns-sd -B _ipp._tcp` (Drucker suchen) und anschließend `dns-sd -L "<Druckername>" _ipp._tcp` auslesen. Alternativ ist er häufig in der Weboberfläche des Druckers hinterlegt.

Für Version 26.4.0

Zugehörige Einschränkungen

Ergänzend zur Konfiguration AirPrint enthält die Richtlinienkonfiguration Restriktionen im Abschnitt Einschränkungen der Einstellungen weitere AirPrint-bezogene Optionen, u. a. AirPrint erlauben, Speicherung der AirPrint-Anmeldeinformationen erlauben, iBeacon-Erkennung von AirPrint-Druckern erlauben und Vertrauenswürdiges TLS-Zertifikat für AirPrint erfordern. Ist AirPrint erlauben deaktiviert, steht das Drucken auf dem Gerät auch mit hinterlegten Druckern nicht zur Verfügung.

- Restriktionen für iOS →

> Ist Vertrauenswürdiges TLS-Zertifikat für AirPrint erfordern aktiv, akzeptiert das Gerät nur Drucker mit einem vertrauenswürdigen Zertifikat. Drucker mit selbstsignierten Zertifikaten sind dann nicht mehr nutzbar, sofern das ausstellende Zertifikat nicht zusätzlich per Richtlinie auf dem Gerät installiert wird.

Setup-Assistent

Mit der Konfiguration Setup-Assistent lassen sich Einrichtungsschritte ausblenden, die iOS auf einem bereits eingerichteten Gerät anzeigt, z. B. nach einem Softwareupdate. Die Konfiguration steht ab iOS 14 zur Verfügung und wirkt nur auf betreuten Geräten. Für Geräte mit Benutzerregistrierung (User Enrollment/BYOD) ist sie nicht verfügbar.

Unterschied zum DEP-Profil

Die Schritte des Einrichtungsassistenten lassen sich an zwei Stellen überspringen, die zu unterschiedlichen Zeitpunkten wirken:

	DEP-Profil	Konfiguration Setup-Assistent
Zeitpunkt	Ersteinrichtung des Geräts	Nach der Einschreibung, z. B. nach einem Softwareupdate
Wo konfiguriert	Konfigurationsprofil → der Automatischen Geräteregistrierung (ADE, im Portal: DEP)	Richtlinie mit der Konfiguration Setup-Assistent

Für Version 26

Die im DEP-Profil gewählten Schritte gelten nur für die Ersteinrichtung. Zeigt iOS später erneut Einrichtungsschritte an, z. B. zu Darstellung, Siri oder Bildschirmzeit nach einem Update, werden diese nur über die Konfiguration Setup-Assistent ausgeblendet. Ohne diese Konfiguration erscheinen solche Schritte wie von Apple vorgesehen.

Die Konfiguration ist damit keine Voraussetzung für die Einschreibung. Sie wird nur benötigt, wenn auch nach der Ersteinrichtung keine zusätzlichen Einrichtungsschritte angezeigt werden sollen.

Einstellungen

Im Bereich Überspringe folgende Setup-Schritte werden die Schritte aktiviert, die ausgeblendet werden sollen. Die Auswahl entspricht den Setup-Schritten im DEP-Profil.

Die Schalter im Bereich Allgemein, z. B. Barrierefreiheit überspringen oder Siri-Einrichtung überspringen, gelten nur für macOS und haben auf iOS-Geräten keine Wirkung. Siehe Setup-Assistent (macOS) →.

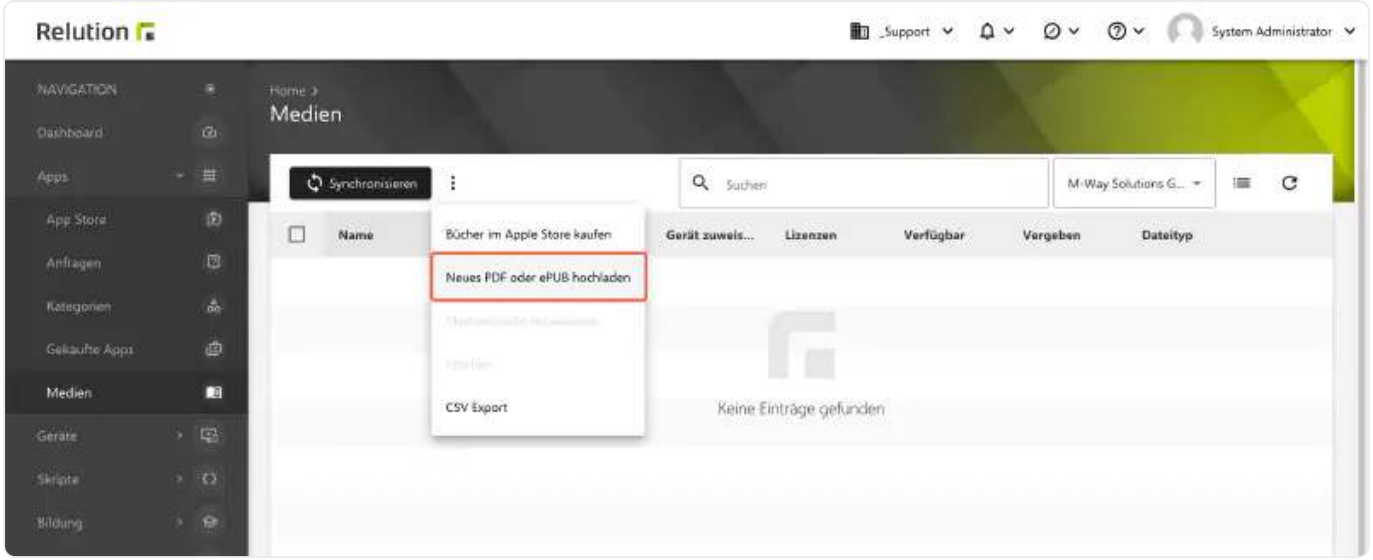
> Apple erlaubt pro Gerät nur eine Konfiguration Setup-Assistent. Einem Gerät sollten daher nicht mehrere Richtlinien mit dieser Konfiguration gleichzeitig zugewiesen werden.

Managed Media

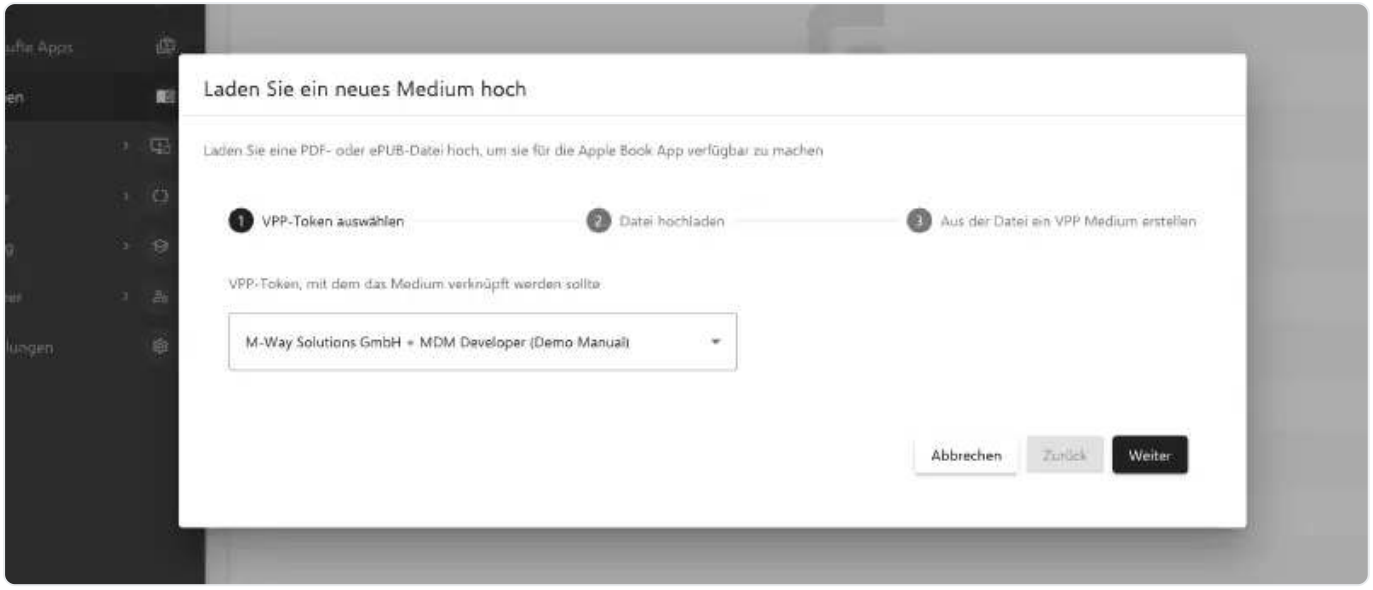
Ab Relution 5.20 ist es möglich, über die Richtlinienkonfiguration Managed Media PDF- oder ePUB Dateien direkt an iOS-Geräte zu verteilen und diese in der Bücher App auf dem iPad anzuzeigen. VPP Bücher können nur mit VPP Benutzern und nicht mit Geräten verknüpft werden.

Vorbereitung und Upload von Medien

Um PDF- und ePUB Dateien verteilen zu können, müssen diese zuerst in Relution hochgeladen werden. Dies wird über die Übersicht der Bücher getan. Hierzu muss im Seitenmenü in den entsprechenden Bereich gewechselt werden.

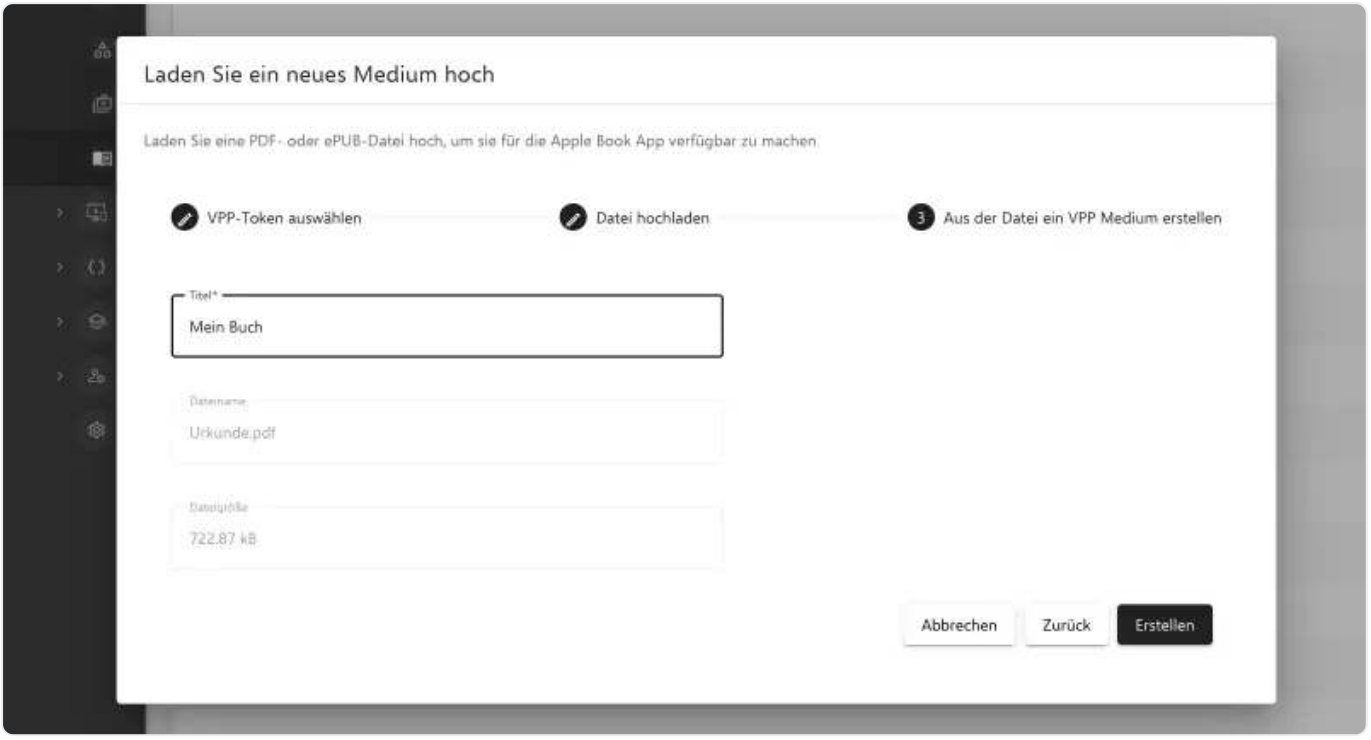


Über das Menü hinter den drei Punkten kann Neues Buch hochladen gewählt werden.



In diesem Schritt muss das VPP Token ausgewählt werden, das mit der Mediendatei verknüpft werden soll.

Anschließend muss die Datei (pdf oder epub) gewählt und hochgeladen werden.



Im letzten Schritt kann das Buch mit einem Titel versehen werden.

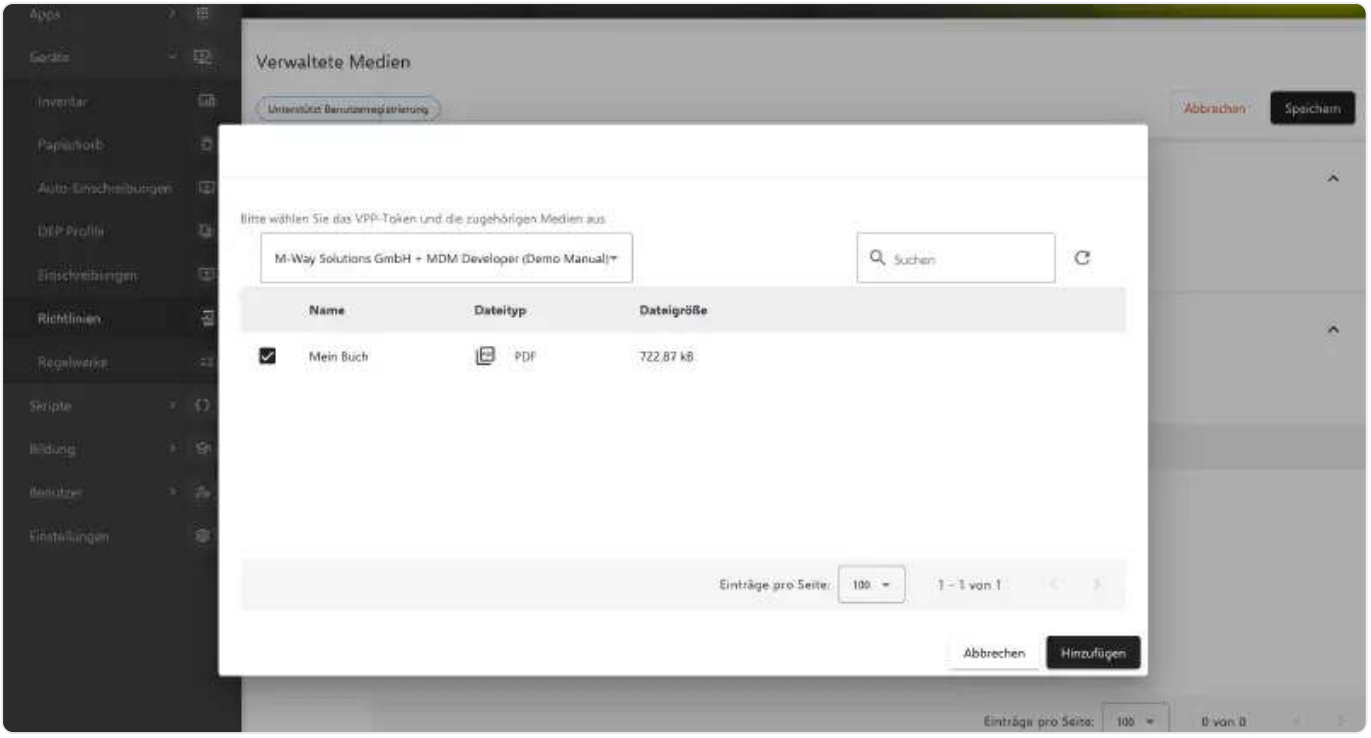
In der Übersicht der Bücher ist die PDF-Datei nun sichtbar.

Für Version 26.4.0

Konfiguration der Richtlinie

Wie bereits beschrieben, ist diese Richtlinienkonfiguration ab Relution Server 5.20 verfügbar und somit in einer iOS-Richtlinie auswählbar.

In der Managed Media Konfiguration können die zuvor hinzugefügten Dateien verknüpft und über die Richtlinie auf das Gerät gebracht werden.



Es steht zusätzlich ein Konfigurationsparameter zur Verfügung, der das automatische Entfernen der Dateien nach entfernen der Richtlinie vom Gerät erzwingt oder unterbindet.

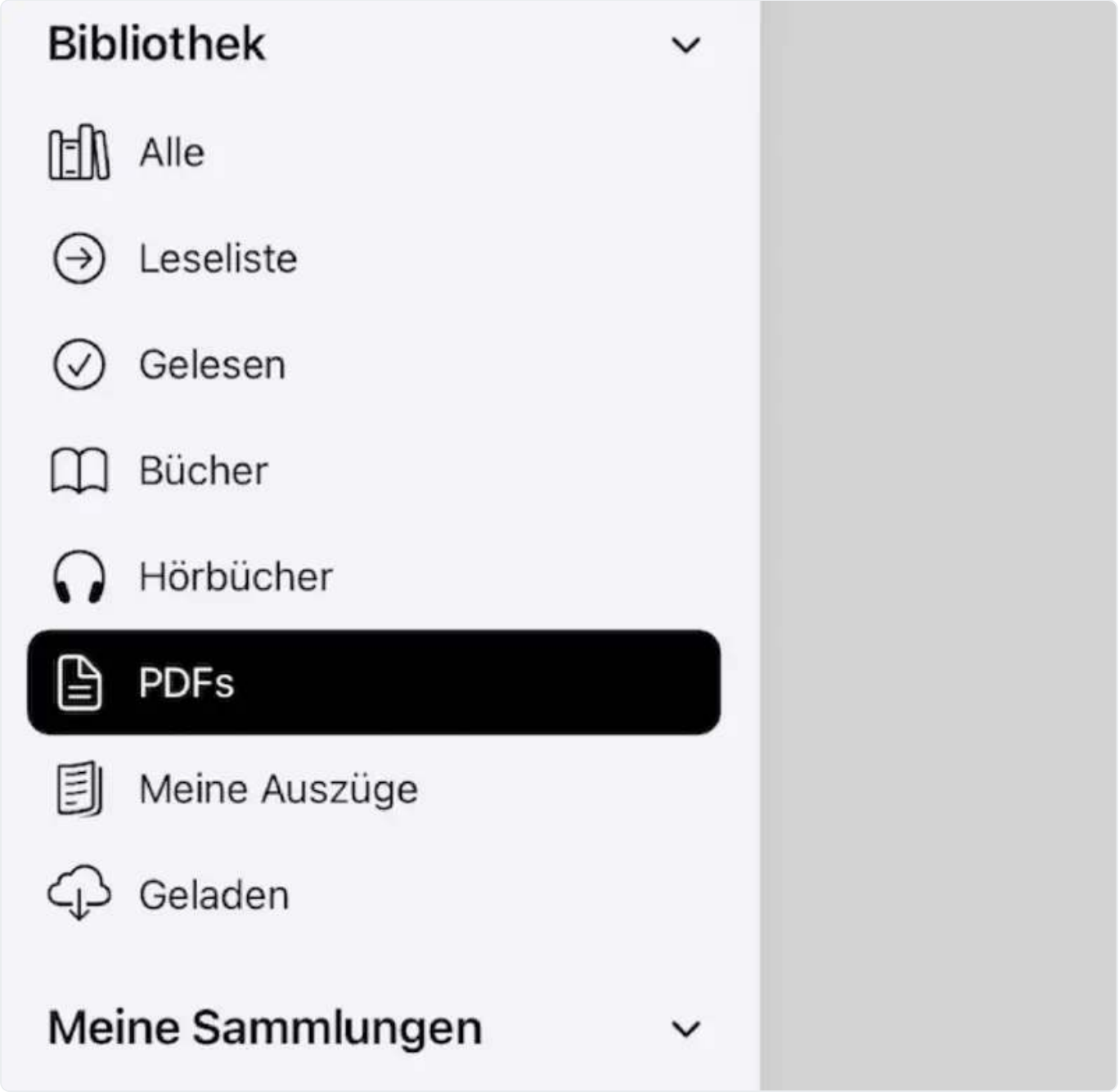
Für Version 26.4.0

Als Aktion ausführen

Neben der Richtlinienkonfiguration lassen sich zuvor hochgeladene Medien auch direkt per Aktion auf einem Gerät installieren oder entfernen. Die entsprechenden Aktionen heißen Medien installieren bzw. Medien entfernen.

Auf dem iPad

Auf dem iPad steht das verknüpfte PDF dann unter der entsprechenden Kategorie zur Verfügung.


Bibliothek
Alle
Leseliste
Gelesen
Bücher
Hörbücher
PDFs
Meine Auszüge
Geladen
Meine Sammlungen

Restriktionen

Folgend eine Übersicht der verfügbaren iOS/iPadOS Restriktionen in Relution `5.28.3` Zu beachten sind die zusätzlichen Hinweise an den einzelnen Konfigurationspunkten in Relution, wie z.B. `supervised / wird überwacht`, `User Enrollment / Unterstützt Benutzerregistrierung`, `deprecated / veraltet`, `deprecated on non-supervised Devices / veraltet auf nicht überwachten Geräten` sowie die min. OS Version wie z.B. `iOS 16+`

Empfohlene Restriktionen →

Gerät

Alle Restriktionen anzeigen

Safari

Alle Restriktionen anzeigen

Für Version 26.4.0

SIRI

Alle Restriktionen anzeigen

Andere Apps

Alle Restriktionen anzeigen

Einschränkungen für verwaltete Apps und Dokumente

Alle Restriktionen anzeigen

Einschränkungen der Einstellungen

Alle Restriktionen anzeigen

Classroom Einschränkungen

Alle Restriktionen anzeigen

Einschränkungen für die Medien

Alle Restriktionen anzeigen

Einschränkungen bei Änderungen

Alle Restriktionen anzeigen

Für Version 26.4.0

iCloud-Einschränkungen

Alle Restriktionen anzeigen

Lockscreen-Einschränkungen

Alle Restriktionen anzeigen

Einschränkungen für Backups und Synchronisierung

Alle Restriktionen anzeigen

Allgemein

Alle Restriktionen anzeigen

Für Version 26.4.0

App Verteilung

Unternehmen entscheiden sich immer öfter, bestimmte Arbeitsprozesse mit einer mobilen App zu unterstützen. Schnell stellt sich die Frage, wie diese App an die Nutzer verteilt werden soll. Oftmals sieht der Anwendungsfall so aus, dass nicht nur Mitarbeiter, sondern auch externe Personen die App bekommen sollen – dazu können zum Beispiel Dienstleister, Partner oder Kunden gehören. Diese App ist in den meisten Fällen auch explizit nicht für einen breiten Kundenkreis gedacht, sondern richtet sich an ausgewählte professionelle Benutzer. Folgende Abschnitte sollen bei der Entscheidung helfen, die beste Distributionsmethode zu finden.

Verteilung über öffentliche App Stores

Apple und Google stellen zur Verteilung von Apps jeweils eine Infrastruktur zur Verfügung. Bei Apple werden Apps für Endanwender über den Apple App Store bereitgestellt. Auf jedem iOS-Gerät ist die App Store App vorinstalliert.

Die Verwaltung und die Veröffentlichung von Apps erfolgt hierfür über das Developer-Portal und App Store Connect. Bei Google werden Apps für Endanwender über den Play Store bereitgestellt. Auf jedem Android Gerät ist die App Play Store vorinstalliert.

Die Verwaltung und die Veröffentlichung von Apps erfolgt hierfür über das Developer-Portal. Apple und Google definieren die Rahmenbedingungen für die Veröffentlichung von Apps über ihre Systeme.

Sofern ein Gerät über ein MDM System verwaltet wird, kann die Store App für den Benutzer auch gesperrt werden und steht somit unter Umständen für den Endanwender nicht zur Verfügung.

Für Version 26.4.0

Verteilung über Apple App Store – Vorteile

- Apps stehen für Endanwender über den Standard-Mechanismus von Apple zur Verfügung.
- Apps müssen nach einem Jahr nicht mit einem aktualisierten Provisioning Profile neu signiert und bereitgestellt werden.
- Apps können selektiv für einzelne Länder freigeschaltet bzw. gesperrt werden.
- Apps können in definierten Strukturen kostenpflichtig angeboten werden (Apple verlangt hierfür eine prozentuale Provisionsgebühr von 15%).
- Apple stellt die Infrastruktur für die Verteilung und Abrechnung bereit.

Verteilung über Apple App Store – Nachteile

- Benutzer benötigen eine Apple-ID auf den Endgeräten, um Apps aus dem Apple App Store zu installieren.
- Bei Unternehmenskunden mit verwalteten Geräten ist der Apple App Store unter Umständen per MDM gesperrt.
- Es müssen sämtliche Apple Vorgaben eingehalten werden, wie bspw. Unterstützung neuer Geräteklassen wie iPhone X.
- Apple behält sich in einem Review vor, die App nicht zu veröffentlichen bzw. nachträglich zu entfernen.
- Durch den Review kann es zu Verzögerungen von bis zu 10 Tagen kommen (derzeit liegt die durchschnittliche Review Dauer bei etwa 3 Arbeitstagen).
- Apps können nur stark eingeschränkt ausgewählten Benutzergruppen bereitgestellt werden.

Verteilung über Google Play Store – Vorteile

- Apps stehen für Endanwender über den Standard-Mechanismus von Google zur Verfügung.
- Apps können selektiv für einzelne Länder freigeschaltet bzw. gesperrt werden.
- Apps können in definierten Strukturen kostenpflichtig angeboten werden (Google verlangt hierfür eine prozentuale Provisionsgebühr von 15%).
- Google stellt die Infrastruktur für die Verteilung und Abrechnung bereit.

Verteilung über Google Play Store – Nachteile

- Benutzer benötigen einen Google Account, um Apps aus dem Play Store zu installieren.
- Bei Unternehmenskunden mit verwalteten Geräten ist der Play Store unter Umständen per MDM gesperrt.
- Es müssen sämtliche Google Vorgaben eingehalten werden – wie bspw. die Cordova Version.
- Google behält sich nach automatisierten App-Scans vor, die App auch nachträglich aus dem Store zu entfernen.
- Durch technische Scans kann sich die Veröffentlichung von Apps um wenige Stunden verzögern.
- Apps können nur stark eingeschränkt ausgewählten Benutzergruppen bereitgestellt werden.

Verteilung über Beta-Programme der öffentlichen App Stores

Apple und Google bieten zusätzlich zur Verteilung von öffentlichen Apps jeweils auch ein Beta-Testprogramm zur Verfügung. Bei Apple werden Apps für einen Beta-Test für Endanwender über die TestFlight App bereitgestellt. Auf iOS-Geräten kann diese App aus dem Apple Store App nachinstalliert werden.

Die Verwaltung und die Veröffentlichung von Apps erfolgen hierfür über das Developer-Portal und App Store Connect im Bereich TestFlight. Bei Google werden Apps für einen Alpha- oder Beta-Test über den Play Store bereitgestellt. Auf jedem Android Gerät ist der Play Store vorinstalliert.

Für Version 26.4.0

Die Verwaltung und die Veröffentlichung von Apps erfolgen hierfür über das Developer-Portal im Bereich Alpha- und Beta-Testing. Apple und Google definieren die Rahmenbedingungen für die Veröffentlichung von Apps über ihre Systeme.

Verteilung über Apple Testflight – Vorteile

- Apps stehen für Benutzer über einen von Apple bereitgestellten Mechanismus zur Verfügung.
- Apps können selektiv für einzelne Benutzer freigeschaltet werden.
- Apple stellt die Infrastruktur für die Verteilung und Abrechnung bereit.

Verteilung über Apple Testflight – Nachteile

- Benutzer benötigen eine Apple-ID, um Apps aus dem Apple App Store zu installieren.
- Für die Installation der App ist die einmalige Installation der TestFlight App notwendig.
- Apple behält sich in einem „reduzierten“ Review vor, die App nicht zu veröffentlichen.
- Durch den Review kann es zu Verzögerungen von bis zu 10 Tagen kommen (derzeit liegt die durchschnittliche Review Dauer bei etwa zwei Arbeitstagen).
- Die Signatur von Apps läuft nach 90 Tagen ab.

Der TestFlight-Dienst ist primär für eine kurze Testphase vor der Veröffentlichung einer iOS-App gedacht. Für einen dauerhaften Betrieb ist die Lösung wegen der kurzen Gültigkeit der Signatur nicht geeignet.

Verteilung über Google Alpha- und Beta-Testing – Vorteile

- Apps stehen für Benutzer über einen von Google bereitgestellten Mechanismus zur Verfügung.
- Apps können selektiv für einzelne Benutzer freigeschaltet werden.
- Google stellt die Infrastruktur für die Verteilung und Abrechnung bereit.

Verteilung über Google Alpha- und Beta-Testing – Nachteile

- Benutzer benötigen eine Google-ID, um Apps aus dem Play Store zu installieren.
- Bei Unternehmenskunden mit verwalteten Geräten ist der Play Store unter Umständen per MDM gesperrt.

Verteilung über internen Enterprise App Store

Apple und Google bieten neben der Verteilung von Apps über die jeweiligen öffentlichen Stores auch Mechanismen zur internen Verteilung von Apps primär für Unternehmen. Bei Apple wird als Voraussetzung das Apple Enterprise Programm und ein Enterprise App Store wie bspw. Relution benötigt.

Die Apps werden für Endanwender über eine separate App Store App oder eine mobile Webseite bereitgestellt. Die Verwaltung von Apps erfolgt über das Developer-Portal.

Die Verteilung der Apps über den jeweiligen Anbieter des Enterprise App Store. Bei Google können Apps über einen Webservice zum Download und zur Installation bereitgestellt werden.

Für spezielle Geräte wie beispielsweise Samsung können optimierte Installations- und Verteilungsmechanismen genutzt werden. Apple und Google definieren die Möglichkeiten für die Verteilung von Apps parallel zu ihren Systemen.

Für Version 26.4.0

Verteilung von iOS Apps über Enterprise App Store – Vorteile

- Apps können an ausgewählte Benutzergruppen bspw. als Deeplink oder nach Anmeldung mit zuvor konfigurierten Benutzernamen und Passwort verteilt werden.
- Benutzer benötigen keine Apple-ID, um Apps aus einem internen Enterprise App Store zu installieren.
- Sämtliche Apple Vorgaben müssen nicht eingehalten werden.
- Die Veröffentlichung von App Updates wird nicht durch ein Review von Apple verzögert.
- Einige Enterprise App Stores (wie beispielsweise Relution) sind auch ohne Geräteverwaltung (MDM) nutzbar.
- Ein existierendes Benutzerverwaltungssystem (ActiveDirectory/LDAP) kann angeschlossen werden, so dass die Nutzer keine neuen Zugangsdaten benötigen.

Verteilung von iOS Apps über Enterprise App Store – Nachteile

- Apps stehen für Endanwender über einen speziellen Mechanismus zur Verfügung, der von Apple genehmigt ist, jedoch eine initiale Konfiguration durch den Benutzer benötigt (siehe hier →).
- *Apps müssen nach einem Jahr mit einem aktualisierten Provisioning Profile neu signiert und bereitgestellt werden. Dies kann jedoch mit Relution automatisiert werden, so dass hier eigentlich kein Nachteil entsteht.*
- Die Infrastruktur für die Verteilung kann beispielsweise als Cloud-Dienst oder On-Premise bereitgestellt werden
- Die Verteilung von Apps darf gemäß Apple Richtlinien nur an Mitarbeiter, Interessenten und Partner, aber vor allem an einen bekannten Nutzerkreis, erfolgen.

Verteilung von Android Apps über Enterprise App Store – Vorteile

- Apps können an ausgewählte Benutzergruppen beispielsweise als Deeplink oder nach Anmeldung mit zuvor konfigurierten Benutzernamen und Passwort verteilt werden.
- Benutzer benötigen keine Google-ID, um Apps aus einem internen Enterprise App Store zu installieren.
- Sämtliche Google Vorgaben müssen nicht eingehalten werden.
- Die Veröffentlichung von App Updates wird nicht durch technische Scans von Google verzögert.
- Einige Enterprise App Stores (wie beispielsweise Relution) sind auch ohne Geräteverwaltung (MDM) nutzbar.
- Ein existierendes Benutzerverwaltungssystem (ActiveDirectory/LDAP) kann angeschlossen werden, so dass die Nutzer keine neuen Zugangsdaten benötigen.

Verteilung von Android Apps über Enterprise App Store – Nachteile

- Apps stehen für Endanwender über einen speziellen Mechanismus zur Verfügung, der von Google genehmigt ist, jedoch eine initiale Konfiguration durch den Benutzer benötigt.
- Die Infrastruktur für die Verteilung muss bspw. als Cloud-Dienst bereitgestellt werden.

Für Version 26.4.0

Identitätszertifikat

Ein abgelaufenes Identitätszertifikat blockiert die sichere Kommunikation zwischen Relution und den Geräten. Dieser Artikel beschreibt, wie betroffene Apple- und Windows-Geräte identifiziert und die Zertifikate manuell verlängert werden.

In Relution eingeschriebene Apple- und Windows-Geräte erhalten ein Identitätszertifikat. Dieses ist ein Jahr gültig und wird automatisch verlängert, solange eine aktive Kommunikation zum Gerät besteht.

Es kann jedoch vorkommen, dass Geräte eingelagert oder inaktiv sind und das Identitätszertifikat dadurch nicht rechtzeitig verlängert werden kann. Aus Sicherheitsgründen verweigert Relution bei einem abgelaufenen Identitätszertifikat jegliche Kommunikation mit dem betreffenden Gerät.

Identitätszertifikat prüfen und verlängern

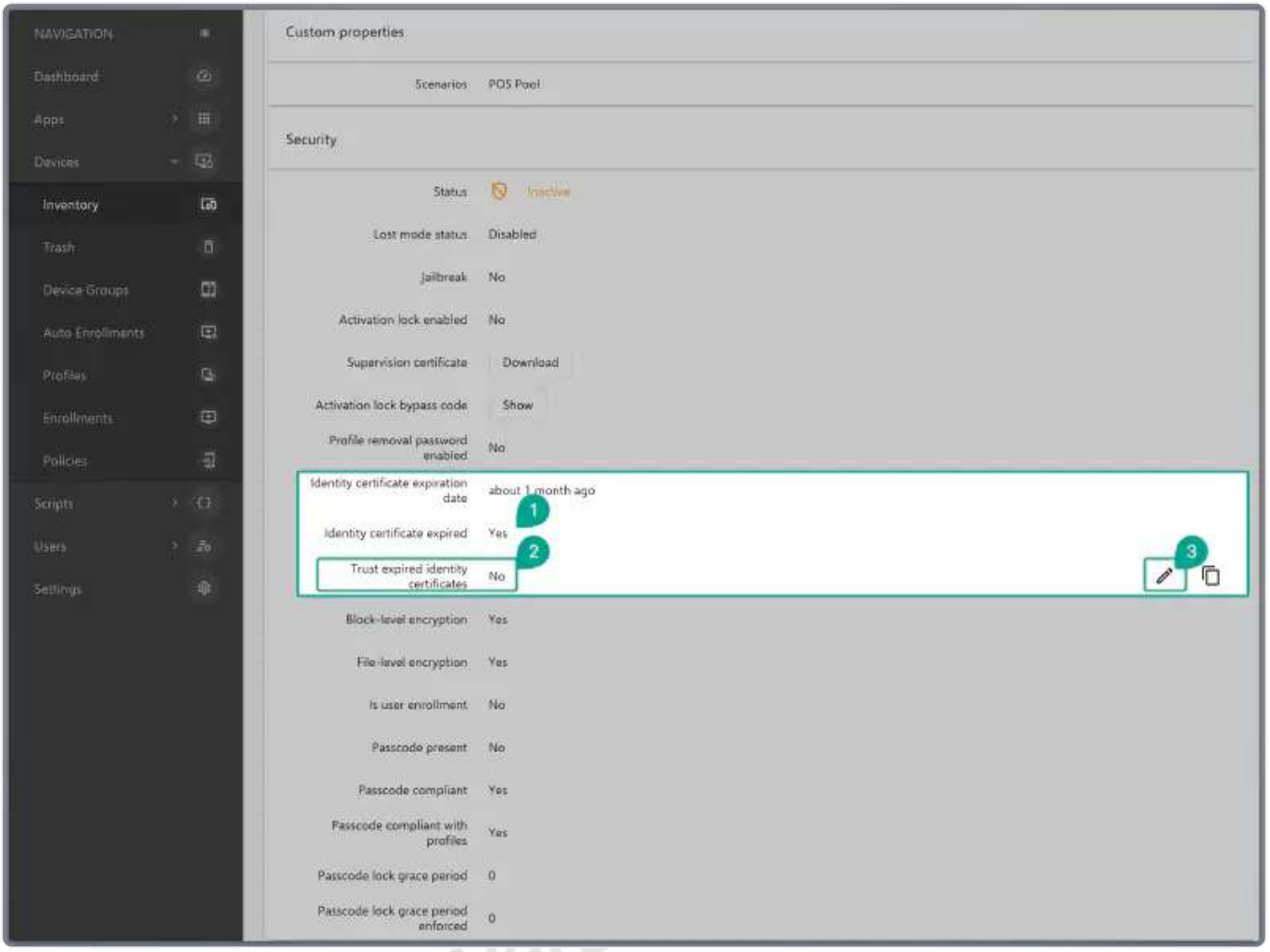
Betroffene Geräte können unter `Navigation` → `Geräte` → `Inventar` → `[Gerät]` im Reiter `Informationen` im Block `Sicherheit` geprüft werden.

Hier befinden sich drei relevante Felder:

- Ablaufdatum des Identitätszertifikats
- Identitätszertifikat ist abgelaufen
- Abgelaufenen Identitätszertifikaten vertrauen

Ist ein Identitätszertifikat abgelaufen, kann der Bearbeitungsmodus durch Überfahren des Punktes Abgelaufenen Identitätszertifikaten vertrauen mit der Maus aktiviert und das Zertifikat verlängert werden. Dadurch wird die Kommunikation zum Gerät wieder als vertrauenswürdig eingestuft, und es können MDM-Befehle verarbeitet werden.

Für Version 26.4.0



Wichtiger Hinweis: Diese Aktion kann jederzeit im Portal ausgeführt werden. Sobald die Geräte online sind, aktualisieren sie selbstständig auf das gültige Zertifikat.

Alternative App Marktplätze

iOS 17.4 führt die Unterstützung für App-Marktplätze von Drittanbietern für Geräte in der Europäischen Union (EU) ein. Mit der Einführung einer speziellen Entwicklerberechtigung können Drittanbieter nun ihre eigenen alternativen App-Marktplätze erstellen, die auf Geräten mit iOS 17.4 und höher heruntergeladen und installiert werden können. Alternative App-Marktplätze bieten eine neue Vertriebsmethode für Anwendungen, die es Nutzer in der EU ermöglicht, Apps außerhalb des App Store von Apple herunterzuladen

Konfiguration via Relution Restriktion

In den Restriktionen wurde die Konfiguration `Installation alternativer App-Marktplätze zulassen` hinzugefügt. Hiermit kann in Relution der Wert einfach angepasst werden.

Konfiguration via Apple Configurator 2 in Relution

1. Neue Richtlinie mit dem Namen `Restrict Marketplace` erstellen.
2. In dieser Richtlinie eine `Apple Configurator 2 configuration` hinzufügen.
3. Eine leere Textdatei mit folgendem Inhalt erstellen und als `restrictMarket.mobileconfig` speichern.

> Vollständiges Konfigurationsbeispiel anzeigen

1. In der `Apple Configurator 2 configuration` einen Namen vergeben und die erstellte mobileconfig-Datei hochladen.
2. Die Richtlinie veröffentlichen und an Geräte ab iOS 17.4 zuweisen

Wichtig! Ist die Richtlinie Geräten unter iOS 17.4 zugewiesen, muss diese entfernt und anschließend neu zugewiesen werden.

Für Version 26.4.0

Datentrennung

Bei der Nutzung von mobilen Geräten wird auf Daten aller Art zugegriffen. Dabei muss die Datenschutzkonformität gewährleistet werden. Hierbei unterscheidet man zwischen firmeneigenen Geräten, sogenannten „Corporate Owned Devices“ (COD) und benutzereigenen Geräten, sogenannten „Bring Your Own Devices“ (BYOD). Für beide Nutzungsarten bieten die Hersteller der Mobilgeräte-Betriebssysteme iOS und Android inzwischen eigene Technologien zur Separierung der Daten an. Nachfolgend werden diese „Bordmittel“ und ihre Implementierung in Relution beschrieben.

iOS – Corporate Owned Devices

Unterscheidung managed / unmanaged

Seit iOS 12 unterscheidet Apple grundsätzlich zwischen „managed“ und „unmanaged“ für folgende Objekte:

Managed Devices

1. Apps - von Relution gepushed oder über den Relution Enterprise Appstore installiert, serverseitig konfigurierbar.
2. Mail Accounts - von Relution über eine Richtlinie konfiguriert.
3. Kontakte - vom managed Mail Account auf das Gerät geladen (synchronisiert).
4. Dokumente - vom managed Mail Account auf das Gerät geladen (synchronisiert).

Für Version 26.4.0

Unmanaged Devices

1. Apps - vom Benutzer aus dem Apple AppStore installiert, nicht serverseitig konfigurierbar.
2. Mail Accounts - vom Benutzer selbst auf dem Gerät konfiguriert.
3. Kontakte - vom Benutzer selbst angelegt.
4. Dokumente - vom Benutzer in unmanaged Apps erzeugt oder in unmanaged Mail Accounts empfangen.

Dabei kann eine unmanaged App in eine managed App umgewandelt werden, indem sie von Relution neu gepushed wird. Sie ersetzt dabei die unmanaged App gleichen Namens auf dem Gerät. Unmanaged Mail-Accounts, Kontakte und Dokumente lassen sich jedoch nicht nach managed überführen.

Zugriffs-Einschränkungen

Die Trennung der Daten erfolgt in iOS systemseitig, indem per Richtlinie eingestellt werden kann, ob der Zugriff auf managed Daten aus unmanaged Apps heraus erlaubt sein soll oder nicht. Dazu bietet die Konfiguration „Restriktionen“ als Teil einer Richtlinie in Relution folgende Einschränkungsmöglichkeiten:

- Öffnen von managed Dokumenten in unmanaged Apps verbieten.
- Öffnen von unmanaged Dokumenten in managed Apps erlauben.
- Unmanaged Apps den Zugriff auf managed Kontakte verbieten.
- Managed Apps erlauben, unmanaged Kontakte zu schreiben.
- AirDrop-Ziele grundsätzlich als unmanaged betrachten.
- Verschieben von Mails in unmanaged Mail Accounts verbieten.

Damit lässt sich beispielsweise verhindern, dass:

- Eine private App (z.B. WhatsApp) die geschäftlichen (Exchange-)Kontakte sieht.
- Eine geschäftliche Mail beliebig weitergeleitet wird.
- Ein Anhang einer geschäftlichen Mail in einer beliebigen App geöffnet wird (z.B. Dropbox).

Welche Web-Inhalte iOS dabei als managed behandelt, z. B. Downloads aus dem Intranet, wird über die Konfiguration Administrierte Domänen → festgelegt. Dort lassen sich außerdem E-Mail-Domänen hinterlegen, damit die Mail-App externe Empfänger kennzeichnet.

---

iCloud-Einschränkungen

Um das unkontrollierte Abfließen von Daten zu verhindern, bietet Relution die Möglichkeit, Cloud-Accounts ganz zu verbieten oder zumindest einzuschränken. Im Einzelnen lassen sich folgende Funktionen abschalten:

- iCloud-Backups.
- Synchronisierung des iCloud-Schlüsselbunds.
- Managed Apps erlauben, Daten in der iCloud abzulegen.
- Fotos in der iCloud speichern.
- Synchronisierung von iCloud-Dokumenten.

Funktions-Einschränkungen

Für Version 26.4.0

Schließlich gibt es einige iOS-Systemfunktionen, die unter Datensicherheitskriterien betrachtet und per Restriktion ebenfalls abgeschaltet werden können:

- App Block-/Allow-Listing
- Web-URL Block-/Allow-Listing
- AirDrop (komplett abschaltbar)
- Passwort teilen
- Zugriff zum Apple AppStore
- Bildschirmfotos und -aufzeichnungen.
- Kamera (komplett abschaltbar, auch für in-App-Funktionen)
- Erstellen und Modifizieren von Accounts (Mail, Apple IDs)
- Bluetooth
- Installation von VPN-Profilen
- USB-Verbindungen.

Per App VPN

Als wichtige Datenschutzmaßnahme bietet iOS die Möglichkeit, die Datenverbindung von Apps fest an eine VPN-Verbindung zu koppeln, die ihrerseits wieder vom Relution-Server konfiguriert werden kann. So ist sichergestellt, dass bestimmte Apps nur über das firmeneigene Netz laufen und externe Zugriffe unterbunden werden (intranet-only).

iOS – Bring Your Own Devices

Bis iOS 12 war es üblich, auf iOS-BYOD-Geräten eine Container-App einzusetzen, die serverseitig konfiguriert werden konnte und somit eine Trennung von geschäftlichen und privaten Daten sicherstellte.

Zwischenzeitlich bietet iOS jedoch eine eingebaute „Container-Lösung“, um geschäftliche von private Anwendungen und Daten zu trennen. Hierzu wird ein iOS-Gerät in Relution über eine (BYOD) Einschreibung im Inventar aufgenommen. Dadurch wird auf dem Gerät ein MDM-Profil installiert, wodurch eine Verwaltung über Relution ermöglicht wird. Technisch wird dann zwischen „verwalteten“ und „nicht verwalteten“ Apps und Inhalten unterschieden. Damit wird das iOS-Gerät zum „Dual Persona“-Gerät und die Daten werden komplett separiert. Mittels Restriktionen lässt sich zusätzlich steuern, ob Daten zwischen „verwalteten“ und „nicht verwalteten“ Apps geteilt werden dürfen.

Auf den Geräten können verschiedene Konfigurationen eingespielt und über Relution verwaltet werden:

- Apps
- VPN-Konfiguration
- Notizen (weitere System-Apps werden in zukünftigen iOS-Versionen folgen)
- iCloud-Account
- Keychain
- Mail Accounts / Attachments
- Kalender Accounts / Attachments.

Für Version 26.4.0

Wird das MDM-Profil entfernt, werden alle verwalteten Apps und Inhalte gelöscht. Diese Aktion kann per Relution oder am Gerät selbst erfolgen.

Klassenlisten (Geteiltes iPad)

Durch die Funktion der Klassenlisten für Shared iPads in Relution wird die Anmeldung mit verwalteten Apple Accounts für Schüler optimiert. Anstatt den vollständigen, oft langen verwalteten Apple Account (Managed Apple ID) manuell einzutippen, können Schüler einfach ihre Klasse und ihren Namen oder ihre Initialen auswählen.

Voraussetzungen

Um diese Funktion nutzen zu können, müssen folgende Bedingungen erfüllt sein:

- DEP-Token: Mindestens ein gültiger DEP-Token am jeweiligen Standort.
- Managed Apple IDs: Vorhandensein von verwalteten Apple Accounts.
- Passendes Endgerät: Ein Apple Shared iPad, das über denselben DEP-Token eingerichtet wurde, über den auch die verwalteten Apple Accounts verwaltet werden.

Konfiguration

Für Version 26.4.0

Mit folgenden Schritten lassen sich die Klassenlisten aktivieren:

1. Richtlinien öffnen: In Relution zum Bereich Richtlinien navigieren.
2. Richtlinie erstellen: Eine neue iOS-Richtlinie erstellen oder eine bestehende bearbeiten.
3. Konfiguration hinzufügen: Die Konfiguration Geteiltes iPad hinzufügen.
4. Klassen auswählen: Die Klassen auswählen, die für die Anmeldung auf dem Shared iPad freigeschaltet werden sollen.
5. Abschluss: Nach dem Zuweisen der Richtlinie werden die verfügbaren Klassen auf dem Sperrbildschirm des iPads zur Auswahl angeboten.

Wichtige Hinweise zur Fehlerbehebung

Sollten Probleme bei der Anmeldung auftreten, liegt dies häufig an einer Diskrepanz der Account-Daten:

- Account-Abgleich: Den in Relution hinterlegten Apple Account des Benutzers überprüfen.
- Beispiel für Unstimmigkeiten:
  - Account in Relution: `Schueler@relution.io`
  - Account im Apple School Manager: `Schueler@appleid.relution.io`
- Lösung: Die Accounts müssen exakt übereinstimmen, damit die Anmeldung über die Klassenliste funktioniert.

> Tipp: Die Anmeldung manuell über den herkömmlichen Weg Am iPad anmelden testen. Funktionieren die Zugangsdaten dort, aber nicht über die Klassenliste, liegt mit hoher Wahrscheinlichkeit eine Diskrepanz bei den hinterlegten Benutzerdaten vor.

Empfohlene Restriktionen

Für iOS-Geräte können eine Vielzahl an Restriktionen konfiguriert werden. Nicht immer ist jede Einstellung sinnvoll oder führt zum gewünschten Ergebnis. Teilweise bringen die Einstellungen auch Probleme mit sich, wenn man nicht genau weiß, wie sie sich auswirken. In diesem Artikel beschränken wir uns auf einige potenzielle Problemstellungen, in die man als Benutzer geraten kann und nennen empfehlenswerte Einstellungen.

Viele Restriktionen lassen sich nur auf Geräten im Überwachten Modus (Supervised Mode) konfigurieren. Diese sind durch den Hinweis `Wird überwacht` gekennzeichnet.

Verbinden mit Macs oder PCs erlauben

Diese Einstellung zeigt nur Wirkung, wenn im DEP-Profil die Verbindung mit Macs oder PCs grundsätzlich erlaubt wurde. Ist dies nicht der Fall, ist die entsprechende Einstellung in den Restriktionen wirkungslos.

Verzögerung von Betriebssystem-Updates aktivieren

Hier kann ein Wert zwischen einem und 90 Tagen definiert werden. In dieser Zeit werden den Benutzer neue System-Updates nicht angezeigt und somit nicht installiert. Dies beinhaltet auch Sicherheits-Updates.

Für Version 26.4.0

USB-Verbindung in gesperrtem Zustand erlauben

Sind Geräte nicht mehr online, können sie z.B. durch eine externe Netzwerk-Karte (Lightning/ Ethernet-Adapter) wieder online genommen werden. Sind Geräte aber gesperrt, z.B. im Lost Mode, kann das externe Zubehör nicht durch Benutzer freigegeben werden und funktioniert somit nicht. Diese Einstellung verhindert dies.

Alle Inhalte & Einstellungen löschen erlauben

Hierbei handelt es sich um den Factory Reset. Soll dieser nicht verfügbar sein, muss der Haken entfernt werden.

Ausschalten des WLAN verbieten

Ist diese Option aktiviert, können Benutzer das WLAN nicht abschalten, auch im Flugmodus. Der Wechsel zwischen WLAN-Netzwerken ist weiterhin erlaubt.

Automatische Datums- und Zeiteinstellung erzwingen

Die Einstellung funktioniert nur, wenn auf den Geräten die Ortungsdienste aktiviert wurden. Die Geräte werden das Datum und die Uhrzeit automatisch einstellen. Dies geschieht auch auf Basis der Zeitzone, in der es sich befindet. Diese kann bei deaktivierten Ortungsdiensten nicht ermittelt werden.

WLAN-Whitelisting erzwingen

Wird diese Option aktiviert, können sich Geräte nur noch mit Netzwerken verbinden, die über eine Richtlinie auf die Geräte gebracht wurden. Vor der Aktivierung dieser Funktion sicherstellen, dass die übertragenen Netzwerke auf den Geräten funktionieren. Es ist nicht möglich, im Anschluss manuell WLAN-Verbindungen hinzuzufügen.

App-Installation ohne Eingabe

Um auf iOS-Geräten Apps `silent` zu installieren, ist es notwendig, dass die Geräte sich im `Überwachten Modus (Supervised Mode)` → befinden und für die App entweder VPP-Lizenzen → verfügbar sind, oder Benutzer mit einer Apple ID an den Geräten angemeldet sind.

Sind diese Bedingungen erfüllt, können über Relution Apps auf Geräten installiert werden, ohne dass Benutzer dies auf den Endgeräten bestätigen müssen. Sicherstellen, dass ausreichend VPP-Lizenzen verfügbar sind.

Für Version 26.4.0

> Fehlt es an VPP-Lizenzen, erscheint auf den Geräten ggf. eine Aufforderung, sich am App Store anzumelden. Dies kann auch passieren, wenn Relution und der Apple VPP Server nicht synchron laufen. In diesem Fall in den Bereich Gekaufte Apps wechseln und dort eine Synchronisierung durchführen.

Native Apps verwalten

Mit Relution ist es möglich, auch native iOS-Apps zu verteilen und ein Release-Management zu betreiben. Dies bedeutet, dass verschiedene Versionen für verschiedene Personengruppen bereitgestellt werden können. So können zum Beispiel Benutzer die Version 1.0 einer App im produktiven Einsatz haben, während eine Gruppe von Key-Benutzer die Version 1.1 testet, ohne dass die Benutzer dies bemerken. Hierzu muss zu Beginn die Version 1.0 in Relution hochgeladen und in den Status `Produktiv` versetzt werden.

> Ein automatisches Verteilen und Installieren von nativen Apps ist bei Android Enterprise nicht möglich.

Neue App anlegen

Dazu im Menu auf `Apps` → `App Store` klicken. Hier lässt sich über die Schaltfläche Hinzufügen ein `App-Typ` wählen. Auf `Native App` klicken. Nun die entsprechende Datei der hochzuladenden App auswählen.

> Auf die Größe der Datei achten. Bei großen Apps kommt es eventuell zu Problemen, falls die Datenbank oder der Reverse Proxy dies nicht zulässt. In diesem Fall muss die Konfiguration angepasst werden.

Den entsprechenden Freigabestatus angeben und auf `Speichern` klicken. Diese App kann nun im `Relution Agent` der entsprechenden Plattform von Mitgliedern der Gruppen `Appstore User` und `Device Manager` gesehen und installiert werden. Die Berechtigungen lassen sich an dieser Stelle auch anpassen. Unabhängig von dieser Berechtigung können Administratoren diese App auch über das Relution-Portal an Geräte verteilen.

Für Version 26.4.0

App updaten

Soll für die App eine neue Version getestet werden, kann diese vorab in den Status `Entwicklung` oder `Prüfung` versetzt werden. Vorher muss die neue Version über die Schaltfläche Neue Version ausgewählt und hochgeladen werden. Im Beispiel befindet sich die App im Status `Prüfung`. Sie wird automatisch am 31.5.2022 in den Status `Produktiv` versetzt. Das `Freigabedatum` kann optional verwendet werden. In den App-Eigenschaften können beide Versionen eingesehen werden. Benutzer mit entsprechender Berechtigung können die App auch auf Endgeräten sehen, installieren und testen.

Manuelle Produktivnahme der neuen Version

Im Relution-Portal können die jeweiligen Versionen angeschaut und konfiguriert werden. Durch einen Klick auf die Schaltfläche Produktiv wird die neue Version in diesen Status verschoben. Befindet sich bereits eine Version im produktiven Status, wird diese automatisch ins `Archiv` verschoben.

Die App wird auf den Endgeräten nicht automatisch aktualisiert. Dies muss durch die Benutzer manuell über den Relution Agent durchgeführt werden oder durch die Administratoren durch eine manuelle App installieren-Aktion ausgelöst werden.

Für Version 26.4.0

App-Store-Apps verwalten

Apps aus dem Apple App Store lassen sich über Relution auf verwalteten Geräten verteilen. Voraussetzung ist in jedem Fall eine App-Lizenz — auch für kostenlose Apps.

Lizenzen beziehen

Eine App-Lizenz kann auf zwei Wegen bezogen werden:

- über das Apple `Volume Purchase Program` (VPP),
- oder über eine Apple-ID, die auf dem Gerät angemeldet ist.

Welcher Weg sinnvoll ist, hängt vom Einsatzszenario ab. Auf Geräten, die ohne Apple-ID betrieben werden, ist eine VPP-Lizenz zwingend erforderlich.

VPP einrichten →

Apps aus dem Apple School Manager und Business Manager

Für Version 26.4.0

Apps, die im Apple School Manager oder Apple Business Manager erworben werden, werden automatisch nach Relution synchronisiert (ab Version 5.10). Sie erscheinen dort im Freigabestatus produktiv und stehen damit unmittelbar zur Verteilung bereit.

Soll eine App nicht allen Benutzern zugänglich sein, lässt sich der Freigabestatus manuell ändern.

Apps manuell hinzufügen

Apps lassen sich jederzeit auch von Hand zum Relution App Store hinzufügen. Dabei gelten zwei Einschränkungen:

- Für manuell angelegte Apps stehen keine VPP-Lizenzen automatisch zur Verfügung.
- Die Installation gelingt nur auf Geräten, auf denen ein Benutzer mit einer Apple-ID angemeldet ist.

VPP-Lizenzen für solche Apps lassen sich nachträglich beschaffen.

Aktualisierung erzwingen

App-Store-Apps werden vom Betriebssystem selbständig aktualisiert. In seltenen Fällen bleibt das aus. Über die Geräteaktion App installieren lässt sich ein Update anstoßen: Das Gerät startet die Installation erneut und gleicht die App-Version mit dem App Store ab. Ist dort eine neuere Version verfügbar, wird die vorhandene App aktualisiert.

Aktionen gehen nicht durch

In Schulumgebungen und anderen Einsatzszenarien, in denen iOS-Geräte zentral über Mobile Device Management (MDM) verwaltet werden, kann es gelegentlich zu Störungen kommen. Insbesondere die fehlende Verarbeitung von MDM-Aktionen kann zu erheblichen Problemen führen – sei es im laufenden Unterricht oder im allgemeinen Betrieb der Geräte. In diesem Beitrag werden mögliche Fehlerbilder beschrieben und die zugrunde liegenden Ursachen analysiert, um Lösungsansätze für solche Situationen aufzuzeigen.

Siehe auch: Nicht jetzt → — dort werden ausstehende Aktionen mit Status `Not Now` und weitere gerätebedingte Ursachen behandelt.

Abgelaufene Zertifikate

Fehlerbild: MDM-Aktionen bleiben im Status `ausstehend` und werden vom Gerät nicht ausgeführt.

Ursache: Das Identitätszertifikat des iOS-Geräts ist abgelaufen. Dieser Zustand tritt häufig bei Geräten auf, die über einen längeren Zeitraum eingelagert wurden und kurz vor der automatischen Verlängerung des Zertifikats keinen Kontakt mehr zum MDM-Server hatten.

Siehe auch: Identitätszertifikat → — dort werden Gültigkeitsdauer und automatische Verlängerung sowie die manuelle Verlängerung eines abgelaufenen Zertifikats über die `Geräteinformationen` beschrieben.

Für Version 26.4.0

VPN-Apps

Fehlerbild: iOS-Geräte bleiben während des Unterrichts hängen, oder zeitbasierte Konfigurationen, wie z. B. der Start oder das Ende eines Unterrichts, werden nicht ausgeführt.

Ursache: Häufig installieren Endanwender, insbesondere in schulischen Kontexten, eigenständig VPN-Apps, wodurch die Kommunikation mit dem MDM-Server blockiert wird. Einige VPN-Apps bieten zudem einen sogenannten `Kill-Switch`, mit dem Benutzer gezielt die gesamte Internetkommunikation trennen können. Dadurch werden MDM-Aktionen, wie das Starten oder Beenden eines Unterrichts, unterbrochen. Auf betroffenen Geräten kann in Relution unter `Installierte Apps` gezielt nach VPN-Anwendungen gesucht werden, um eine solche App zu identifizieren.

Lösung: In Relution besteht die Möglichkeit, die Installation oder Nutzung von VPNs durch Restriktionen zu unterbinden. Dazu kann in den Restriktionen die Option `VPN-Konfiguration deaktivieren` ausgewählt werden. Mit dieser Einstellung können auf den Geräten keine nicht verwalteten VPN-Konfigurationen mehr eingerichtet werden.

DNS

Fehlerbild: iOS-Geräte bleiben während des Unterrichts hängen, oder zeitbasierte Konfigurationen – wie beispielsweise der Start oder das Ende eines Unterrichts – werden nicht ausgeführt.

Ursache: Ein häufiger Grund ist, dass Endanwender, insbesondere in schulischen Kontexten, eigenständig einen alternativen DNS-Server konfigurieren. Dies kann die Kommunikation mit dem MDM-Server blockieren und dazu führen, dass MDM-Aktionen nicht korrekt ausgeführt werden. Abweichende Konfigurationen können auf betroffenen Geräten unter `Einstellungen` → `WiFi` → `DNS` überprüft werden.

Lösung: Um derartigen Problemen vorzubeugen, kann in Relution eine Konfiguration für `verschlüsselte DNS-Einstellungen` angewendet werden. Dadurch wird sichergestellt, dass Änderungen am DNS durch Endanwender nicht angewendet werden (die Änderung selbst bleibt möglich) und die Kommunikation über den verwalteten DNS-Server Priorität hat.

Zuverlässige Anbieter und Konfigurationen

- Google DNS →
- Cloudflare DNS →

Für Version 26.4.0

Relution Shared Device optimieren

Bei einem Benutzerwechsel im `Relution Shared Device-Modus` werden, je nach Konfiguration, viele Apps bzw. mehrere Gigabyte an Daten neu heruntergeladen. Hierbei kann es aufgrund des hohen Datenvolumens bei einer Vielzahl von Downloads und Installationen zu Verzögerungen im Unterricht kommen.

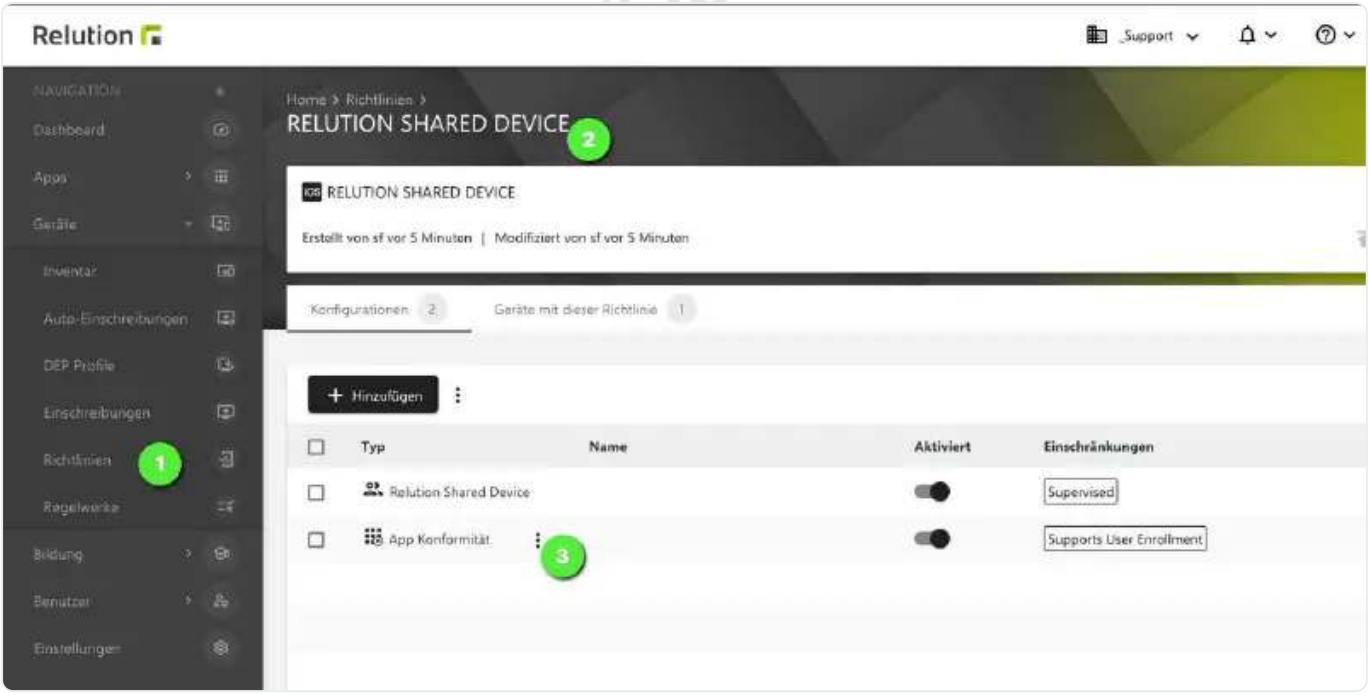
Um temporäre Inhalte aus verwendeten Apps bei einer benutzerübergreifenden Nutzung der Geräte entfernen zu können, muss Relution während einer Benutzerabmeldung die Apps von den Geräten löschen. Mehr dazu unter folgendem Link
Mehrbenutzermodus →

Optimierungen

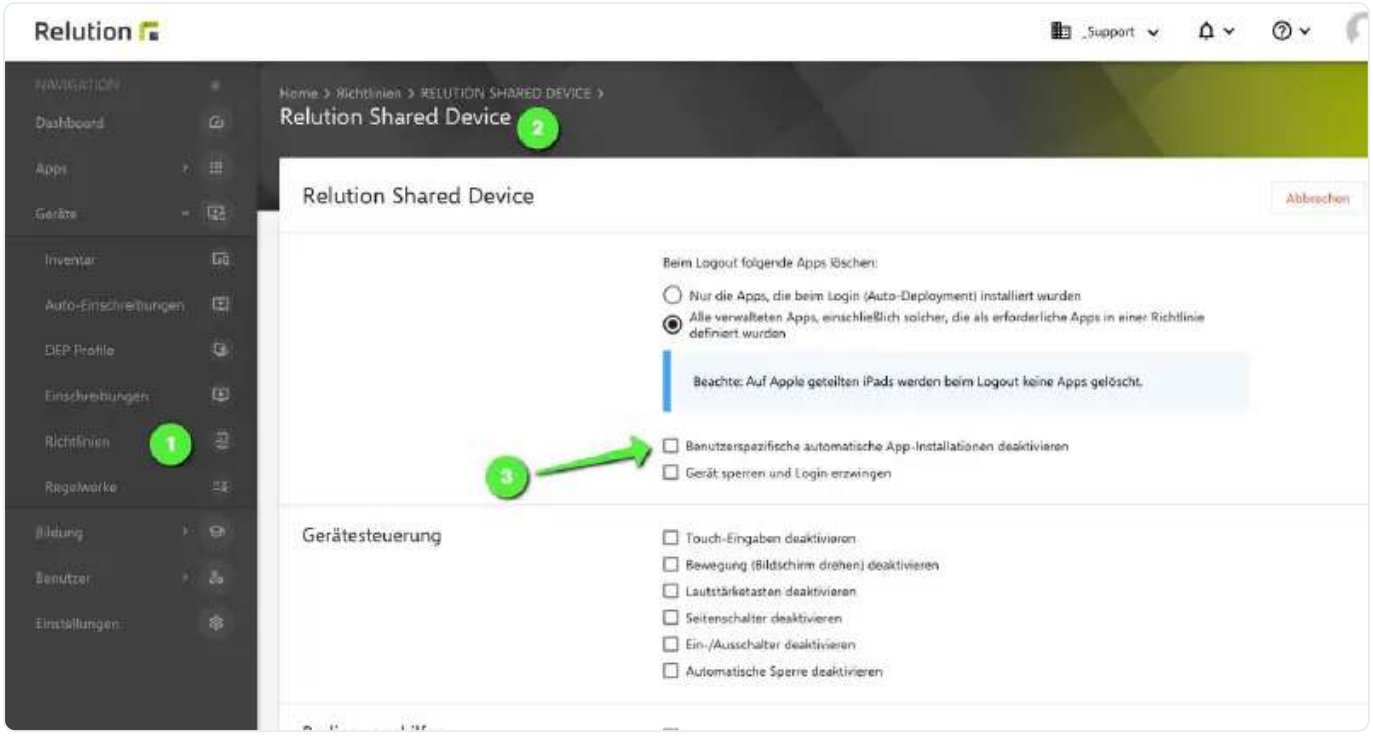
Um Verzögerungen im Unterricht so minimal wie möglich zu halten, werden folgende Maßnahmen empfohlen:

App Konformität und Auto Deployments minimieren

Die Liste `Erforderliche Apps` in der Richtlinienkonfiguration `App Konformität` relativ klein halten. Eine kleine Basisausstattung an Apps für alle Geräte ist in der Regel ausreichend. Jede App muss mehrfach durchs Netz übertragen werden, und zwar einmal für jedes Gerät, auf dem die Richtlinie Anwendung findet. So werden aus 50 MB schnell 5 GB, wenn der Unterricht beginnt.



Zudem lassen sich `Auto-Deployments` für benutzerspezifische Apps unterbinden, um den Fußabdruck beim Benutzer-Login so gering wie möglich zu halten.



Alternativ können benötigte Apps jederzeit über den Relution Agent auf den Geräten von Benutzer nachträglich installiert werden.

Unterrichtsprofile über Relution Teacher

Wurde die obere Maßnahme befolgt und sind keine oder nur wenige Apps in `App-Konformität` und `Auto-Deployments` hinterlegt, können Lehrkräfte über die Relution Teacher App und der Verwendung von `Unterrichtsprofilen` alle benötigten Apps für den Unterricht vorgeben. Damit werden nur die für die jeweilige Unterrichtseinheit benötigten Apps geladen.

Für Version 26.4.0

Nicht jetzt

Aktionen für iOS-Geräte stehen auf `Ausgeliefert` und werden nicht abgearbeitet

Aktionen sind Kommandos, die von Relution auf eingeschriebenen Geräten ausgeführt werden. Diese können entweder implizit über Richtlinienkonfiguration oder explizit durch das Anwenden einer Aktion ausgelöst werden. Die Übersicht aller ausstehenden und ausgeführten Aktionen befindet sich in den Gerätedetails im Tab `Aktionen`.

Siehe auch: Aktionen gehen nicht durch → — dort werden abgelaufene Zertifikate und weitere serverseitige Ursachen behandelt.

Gerät wurde neu gestartet

- Das Gerät wurde neu gestartet und bisher noch nicht entsperrt
  - Der digitale Schlüsselbund (Keychain) ist gesperrt, bis ein Gerät nach einem Neustart zum ersten Mal entsperrt wird. In Folge kann das Betriebssystem noch nicht auf gespeicherte Kennwörter zugreifen und sich daher nicht mit einem verschlüsselten WLAN verbinden

Aktion im Kanal Benutzer

- Die Aktion wurde auf dem Benutzer-Kanal versendet und aktuell ist kein Benutzer am Gerät angemeldet

Für Version 26.4.0

Gerät hat den Verbindungsstatus Nicht jetzt

In manchen Fällen beantworten iOS/iPadOS Geräte Kommandos vom MDM Server mit `Nicht jetzt`. Das ist immer dann der Fall, wenn das Gerät zum aktuellen Zeitpunkt nicht bereit ist mit dem MDM Server zu kommunizieren

Es gibt diverse Gründe die zu einem `Nicht jetzt` führen können. Die folgende Liste enthält die uns derzeit bekannten Auslöser, die Liste erhebt dabei keinen Anspruch auf Vollständigkeit.

- Das Gerät ist gesperrt / eine Benutzerinteraktion ist erforderlich
  - Einige Kommandos können nicht ausgeführt werden, solange das Gerät gesperrt ist, unter anderem
    - Anwenden bestimmter Restriktionen
    - Konfiguration einer WLAN Verbindung
    - Installation oder Update von Apps
    - Installation von Zertifikate die Benutzerzustimmung benötigen
- Netzwerk- oder Batteriezustand
  - Das Gerät hat einen zu niedrigen Batteriestand um den Vorgang zu starten
  - Die Netzwerkverbindung des Geräts ist instabil
- Benutzer verzögert Softwareupdates
  - Ein Update soll eingeplant werden (`ScheduleOSUpdate` oder `InstallLater`) und der Benutzer verzögert das Update explizit
- Das Gerät ist noch nicht vollständig eingeschrieben
  - Einige Kommandos können erst ausgeführt werden, nachdem das Gerät die DEP-Einschreibung und/oder den Supervision-Prozess abgeschlossen hat
- Das Gerät ist anderweitig beschäftigt
  - Das System führt aktuell einen kritischen Task aus (Update, iCloud Backup oder Restore)

Lösung

- Die Geräte entsperren und eine stabile WLAN-Verbindung herstellen
- Sofern notwendig mit einem Benutzer am Gerät anmelden
- Potentielle Dialoge vom Betriebssystem bestätigen
- Das Gerät bei Bedarf vorher aufladen

Für Version 26.4.0

Weitere Informationen

Der `Nicht jetzt` Status ist reguläres Verhalten von iOS/iPadOS und nicht Relution-spezifisch.

Seit Version 5.8.1 ist Relution in der Lage `Nicht jetzt` Antworten von Geräten zu verstehen. Beantwortet ein Gerät ein Kommando mit `Nicht jetzt` stellt Relution den Verbindungsstatus für das jeweilige Gerät im Inventar entsprechend um. Um Geräte in diesem Zustand wieder dazu zu bringen mit dem MDM zu kommunizieren müssen diese in aller Regel entsperrt und zum Beispiel ausstehende Betriebssystemupdates ausgeführt werden.

Einige Aktionen, wie etwa `Verlorener Modus (Lost Mode)` und `Passwort zurücksetzen`, werden vom Gerät priorisiert behandelt und auch in diesem Zustand entgegengenommen. Seit Version 5.9 behandelt Relution diese Aktionen ebenfalls priorisiert und überspringt alle derzeit ausstehenden Aktionen. Damit ist sichergestellt, dass Geräte die vorherige Aktionen mit `Nicht jetzt` beantwortet haben trotzdem in den Lost Mode versetzt werden können oder dass ein vergessenes Kennwort dennoch geändert werden kann.

Apple Dev-Doku Not Now Status →

Gerätenamen

- DEP-Geräte verlieren nach dem Zurücksetzen den zuvor vergebenen Gerätenamen im Geräteinventar.
- Der Export der `CSV`-Datei aus `Geräte` → `Inventar` kann nicht bei `Geräte` → `Auto-Einschreibung` importiert werden und umgekehrt.

Ursache

- Der Name aus dem Bereich `Auto-Einschreibungen` überschreibt den nachträglich geänderten Gerätenamen aus dem Geräteinventar.
- Das Format der exportierten `CSV`-Datei ist unterschiedlich zu dem Format der importierten `CSV`-Datei und beinhaltet andere Felder.

Lösung

Die `CSV`-Datei mit den gewünschten Gerätenamen aus dem `Inventar` exportieren und die Daten in das Template-Format der zu importierenden `CSV`-Datei von `Auto-Einschreibungen` überführen.

Es lassen sich für `Auto-Einschreibungen` und `Inventar` `CSV`-Datei-Vorlagen herunterladen. So steht jeweils die richtige Format-Vorlage für die Namensänderungen zur Verfügung.

Für Version 26.4.0

> Die erste Zeile der Format-Vorlage ist notwendig und sollte nicht geändert werden.

Die Seriennummer und den Gerätenamen aus den exportierten Daten kopieren und anschließend bei `Auto-Einschreibungen` importieren. Werden Geräte neu eingeschrieben, wird nun der richtige Gerätename bei der `Auto-Einschreibung` verwendet.

Anleitung

1. Die Inventarliste exportieren.
2. Die Format-Vorlage für den Import bei `Auto-Einschreibungen` herunterladen.
3. Die entsprechenden Daten aus dem Export in die Format-Vorlage für den Import importieren.
4. Die befüllte Format-Vorlage bei `Auto Einschreibungen` importieren.

Mehrbenutzermodus

Relution und Apple bieten jeweils einen eigenen Mehrbenutzermodus an.

Relution shared Device und Apple geteiltes iPad.

Beide Modi bringen unterschiedliche Eigenschaften mit.

Relution Shared Device →

> Mit iOS 17.x führt die Verwendung der Restriktionskonfiguration Synchronisierung des iCloud-Schlüsselbunds erlauben nein zu einer verlangsamten Anmeldung bei Apple-geteilten-Geräten.

Definierte Anforderungen als Entscheidungshilfe

Die eigenen Anforderungen an Geräte im Mehrbenutzermodus definieren, um sich für eine der beiden Lösungen zu entscheiden. Folgende Punkte geben Orientierung:

- DSGVO-konformes Arbeiten
- Verfügbarkeit von `Apple Classroom` für Lehrkräfte
- Einfache Anmeldung ohne Benutzernamen und Kennwort
- Niedrige zur Verfügung stehende Bandbreite
- Keine Benutzer und/oder Klassen in Relution angelegt
- Möglichst kurze Login-Zeiten
- Nutzung von System-Apps notwendig
- Nutzung von persönlichen Laufwerken
- Nutzung von `Relution Teacher`

Für Version 26.4.0

Gegenüberstellung der Anforderungen

Die Anforderungen werden nur teilweise von beiden Modi unterstützt:

Funktion	Relution Shared Device	Apple Shared iPad
DSGVO-konformes Arbeiten	Ja	Nur im Gastmodus
Werden Schüler in der Classroom App online angezeigt?	Ja	Nicht im Gastmodus
Anmeldung ohne Benutzernamen und Kennwort	Nein	Ja
Niedrige zur Verfügung stehende Bandbreite	Konfigurationsabhängig	Ja
Keine Benutzer und/oder Klassen in Relution angelegt	Nein	Ja
Möglichst kurze Loginzeiten	Konfigurationsabhängig	Ja
Nutzung von Systemapps notwendig	Nein	Ja
Nutzung von persönlichen Laufwerken	Ja	Nein
Nutzung der Relution Teacher Console	Ja	Nur in Kombination mit Relution Shared Device
Verwendung einer SIM/eSIM	Ja	Nein

Für Version

Gast-Modus

Wird eine möglichst schnelle Anmeldezeit gewünscht und steht wenig Bandbreite zur Verfügung, eignet sich Apple `Geteiltes iPad`. Es ermöglicht die Anmeldung im sogenannten `Gast-Modus`, wodurch eine anonyme Nutzung gewährleistet wird. Als `Gast` werden die Geräte in `Apple Classroom` allerdings nicht als `online` angezeigt. Soll DSGVO-konform gearbeitet und `Apple Classroom` verwendet werden, kommt der Mehrbenutzermodus von Apple nicht in Frage. Mit dem `Relution Shared Device`-Modus ist diese Kombination möglich.

System-Apps

Da Relution temporäre Daten und Inhalte aus Apps nur löschen kann, indem diese von Geräten deinstalliert werden, ist es nicht empfehlenswert, auf System-Apps zurückzugreifen, in denen Daten gespeichert werden. Der Safari Browser ist beispielsweise eine solche System-App. Diese lässt sich nicht deinstallieren, wodurch Inhalte und geöffnete Tabs vorheriger Benutzer bei einem Benutzerwechsel noch vorhanden sind und eingesehen werden können. Um dieses Problem zu umgehen, bietet sich die Nutzung von alternativen Apps an, wie beispielsweise den Firefox Browser, der vom Gerät gelöscht werden kann.

Fotos

Auch beim Thema Fotos sollte die native Kamera auf den iOS-Geräten deaktiviert werden. Erstelle Bilder werden ansonsten automatisch in der System-App `Photos` gespeichert, welche sich ebenfalls nicht löschen lässt. Somit können erzeugte Fotos durch Relution nicht entfernt werden. Alternativ bietet die Relution Kamera die Möglichkeit, erstellte Fotos nicht auf den Geräten, sondern auf einem konfigurierten Netzlaufwerk zu speichern.

Microsoft-Anwendungen

Beim Einsatz von Microsoft Apps wie `Teams` oder `Excel` gilt es folgende Besonderheit zu beachten:

Werden Geräte im `Relution Shared Device`-Modus betrieben und Benutzer melden sich nicht von diesen Apps ab, werden die Anmeldungen im digitalen Schlüsselbund (Keychain) der Geräte gespeichert und können nicht durch eine Deinstallation entfernt werden. Benutzer müssen dafür sensibilisiert werden, dass eine Abmeldung von diesen Apps zwingend erforderlich ist. Alternativ kann Apple `Geteiltes iPad` verwendet werden.

Kombination beider Mehrbenutzer-Modi

Es ist möglich, `Relution Shared Device` und `Apple Shared iPad` gleichzeitig zu aktivieren. Die Kombination vereint die Vorteile beider Lösungen. Durch den Apple `Gast-Modus` können System-Apps genutzt werden, ohne dass Daten auf den Geräten zurückbleiben. Zugleich können über den `Relution Agent` Lehrkräfte `Unterrichtsprofile` mit relevanten Apps und Funktionen auf Schülergeräten anwenden.

Für Version 26.4.0

> Bei der Verwendung des Gast-Modus auf Schülergeräten kann Apple Classroom von Lehrkräften nicht eingesetzt werden.

Ordner Homescreen Layout

Mit dem Relution Homescreen Layout ist es möglich, Apps anzuordnen und diese in verschiedenen Ordnern übersichtlich zu platzieren.

Problem

Bei der Einrichtung der Richtlinienkonfiguration `Homescreen Layout` werden im Simulator keine Ordner erstellt.

Lösung

Um einen Ordner zu erstellen, muss bei der `Drag & Drop`-Funktionalität des Simulators darauf geachtet werden, die App für eine kurze Zeit absolut still über einem anderen App-Icon zu positionieren, damit automatisch ein Ordner erstellt wird.

> Das Homescreen Layout ist aktuell auf 20 Apps pro Seite begrenzt.

Für Version 26.4.0

Apple Case anlegen

Nach Betriebssystem-Updates von Apple-Geräten kann es in manchen Fällen zu unerwarteten Fehlfunktionen oder Problemen kommen. In solchen Situationen empfehlen wir, direkt einen Case bei Apple zu eröffnen, um die Analyse und Behebung des Fehlers zu beschleunigen.

Anschließend die Case-ID des Apple-Tickets über unseren Support senden. Wir reichen diese zusätzlich an unsere Apple-Kontakte weiter, um den Prozess weiter zu unterstützen und zu beschleunigen.

Apple Case erstellen

1. Die Website öffnen: Feedbackassistant von Apple →
2. Mit der eigenen ASM/ABM-ID anmelden.
3. Beim ersten Besuch erscheint die Auswahl zwischen:
   - Beta Program
   - Developer Program

   Hier Beta Program wählen.

Für Version 26.4.0

Welche Themen können gemeldet werden?

Es können Cases zu folgenden Apple-Plattformen eingereicht werden:

- iOS / iPadOS
- watchOS
- tvOS
- macOS
- HomePod
- visionOS

Für uns besonders relevant sind iOS / iPadOS sowie macOS.

Wichtige Angaben beim Einreichen eines Cases

Am Beispiel von *iOS / iPadOS* sollten folgende Felder ausgefüllt werden:

- Titel des Problems
- Kategorie: `Something Else Not on the List`
- Type of Issue: `Incorrect / Unexpected Behaviour`
- Fehlerbeschreibung (auf Englisch) → möglichst detailliert und präzise

Notwendige Informationen in der Fehlerbeschreibung

Sicherstellen, dass folgende Punkte enthalten sind:

- Betriebssystemversion der betroffenen Geräte
- Zeitpunkt/Umstände, wann das Problem auftritt
- Reproduzierbarkeit: Wie genau lässt sich der Fehler nachstellen?
- Systemdiagnose anhängen → Wie diese erstellt wird, wird über das ?-Symbol im Formular erklärt.

Filter für Inhalte (Built-In)

Google-Suchergebnisse enthalten trotz aktiviertem `Auto-Filter` unangemessene Suchergebnisse. Webseiten, die unangemessene Inhalte enthalten, sind erwartungsgemäß gesperrt. Unter der Kategorie `Bilder und Videos` werden im Suchergebnis jedoch weiterhin nicht passende und nicht jugendfreie Inhalte dargestellt.

Problem

Der Inhaltsfilter von Apple bietet keine Möglichkeit, die Suche von Google einzuschränken (z.B. Safe-Search). Der automatische Filter von Apple filtert Webseiten anhand `Erwachsenen-Sprache` (adult language) und nicht anhand medialer Inhalte wie Bilder oder Videos. Googles Bildersuche wird dadurch nicht eingeschränkt.

Für Version 26.4.0

Lösung

Um die Suchergebnisse weiter einzuschränken, sind entsprechende Apps von Drittanbietern oder ein Inhaltsfilter auf Netzwerkebene (Proxy/VPN) notwendig.

Linksammlung

Die folgenden Webseiten geben einen Überblick über Apps, die zum Filtern unangemessener Inhalte verwendet werden können. Seitens Relution wurden die empfohlenen Apps der externen Seiten nicht getestet - daher kann ausdrücklich keine verbindliche Aussage zu Qualität und/oder Tauglichkeit dieser Apps getan werden.

wondershare →

WithSecure →

QR Code lässt sich nicht scannen

Bei iOS-Geräten kann es vorkommen, dass im Zuge einer angewendeten Richtlinienkonfiguration mit `App-Konformität` der QR Code Scanner der Kamera deaktiviert wird. Die Kamera erkennt zwar einen vorhandenen QR Code, bietet aber den Link zum Öffnen im Browser nicht an. Das Problem tritt nur in Verbindung mit einer `Positivliste` in der Konfiguration `App-Konformität` auf.

Anleitung

Die App bzw. das Plugin muss manuell zur `Positivliste` der `App-Konformität` hinzugefügt werden.

1. In die Konfiguration der entsprechenden Richtlinie gehen.
2. Einen neuen `Positivliste`-Eintrag für `App manuell hinzufügen` erzeugen.
3. Der Name kann frei gewählt werden. Als `internen Namen` `com.apple.barcodesupport` eingeben.
4. Die Richtlinie speichern und veröffentlichen.

Für Version 26.4.0

Gesperrtes Gerät

Wenn iOS-Geräte mit einer PIN geschützt sind und neu gestartet werden, können sie bis zum Entsperren nicht mit einem passwortgeschützten WLAN verbunden werden, da das OS nicht auf die Keychain zugreifen kann. Ein ähnlicher Zustand kann durch Aktivierung des Lost Mode herbeigeführt werden. Ohne Netzwerkverbindung werden daher keine Aktionen wie das Zurücksetzen des Passwortes oder das Deaktivieren des Lost Mode durchgeführt.

LAN auf Lightning / USB-C Adapter

Hiermit kann über einen RJ45 Adapter eine LAN Verbindung zum Endgerät hergestellt werden, so dass das Gerät eine Internetverbindung aufbauen und MDM Aktionen verarbeiten kann. Voraussetzung hierfür ist jedoch, dass vor dem Sperren des Gerätes in den Restriktionen die Option `USB-Zubehör im gesperrten Zustand zulassen` gesetzt wurde.

Bekanntes offenes WLAN

Wenn dem Gerät vor dem Sperren ein offenes / ungeschütztes WLAN bekannt war, kann die Verbindung zu diesem ohne Entsperren automatisch vom Gerät aufgebaut werden und MDM Aktionen können wieder verarbeitet werden.

Veraltet für iOS 18.x

Für Version 26.4.0

Gerät zurücksetzen

Eine immer gültige Option ist das Zurücksetzen der betroffenen Geräte auf die Werkseinstellungen. Es ist immer möglich iOS Geräte über DFU Modus → komplett zurückzusetzen.

Weblinks

Weblinks können in Relution als App bereitgestellt werden. Dies ist sinnvoll, wenn beispielsweise ein Weblink benutzer- bzw. gruppenspezifisch verteilt (Auto-Deployments) oder in der Richtlinienkonfiguration `Homescreen Layout` platziert werden soll.

1. Weblink anlegen

1. In Relution unter `App Store` auf `Hinzufügen` klicken
2. `Weblink` auswählen
3. Auf `Weiter` klicken
4. Die URL des Links eingeben
5. Auf `Details hinzufügen` klicken
6. Den Freigabestatus `Produktiv` aktivieren
7. Einen Namen vergeben
8. Optional die Option Im Vollbildmodus öffnen aktivieren, damit der Weblink als Web App startet (siehe Weblink als Web App öffnen →)
9. Oben rechts auf `Speichern` klicken.

Weblinks auf Geräte verteilen

Für Version 26.4.0

Hier muss sich für Option “2a” oder “2b” entschieden werden. Werden Weblinks über die Autodeployments verteilt, besteht die Möglichkeit, diese im Homescreen Layout anzuordnen (3).

2a. Weblink per Auto Deployments verteilen

Weblinks können nicht als `Erforderliche App` in der Richtlinienkonfiguration `App-Konformität` bereitgestellt werden. Es ist aber möglich, Weblink per `Auto-Deployments` automatisch an bestimmte Benutzer oder Benutzergruppen zu verteilen.

1. Das entsprechende Benutzerkonto oder die entsprechende Gruppe öffnen.
2. Unten im Bereich `Auto-Deployments` auf `Hinzufügen` klicken.
3. Den erzeugten Weblink auswählen und auf `Hinzufügen` klicken.
4. Oben auf `Speichern` klicken.

Der hinzugefügte Weblink wird unverzüglich auf den Geräten angezeigt, auf denen sich die entsprechenden Benutzer oder ein Mitglied der jeweiligen Benutzergruppe angemeldet hat.

2b. Weblink über Richtlinie bereitstellen

Weblinks können ebenfalls mit der Konfiguration `Weblink` bereitgestellt werden, hierzu muss wie folgt eine Konfiguration über Richtlinien angelegt werden

1. In der Seitennavigation `Geräte` → `Richtlinien` → `Hinzufügen` oder eine bestehende Richtlinie öffnen
2. Über den Button Hinzufügen → Weblink → Details hinzufügen eine Weblink Konfiguration erstellen
3. Bezeichnung und URL (z. B. `https://relution.io`) sind Pflichtangaben.
4. App zum Öffnen des Weblinks: Hier kann eine Drittanbieter-Browser-App gewählt werden, z. B. Firefox. Ohne Eingabe wird Safari verwendet. Für die Darstellung als Web App bleibt das Feld leer.
5. Entfernbar: Der Weblink kann vom Benutzer entfernt werden.
6. Vorbereitetes Icon: Ist die Option aktiviert, legt iOS keine zusätzlichen Effekte über das hochgeladene Icon. Die Option stammt aus älteren iOS-Versionen, die Icons mit einem Glanzeffekt versehen haben.
7. Vollbild: Der Weblink startet als Web App statt in Safari (siehe Weblink als Web App öffnen →).

Mit Relution 5.32.0 können bei Weblinks Platzhalter verwendet werden um so z.B. einen Benutzernamen mitzugeben.

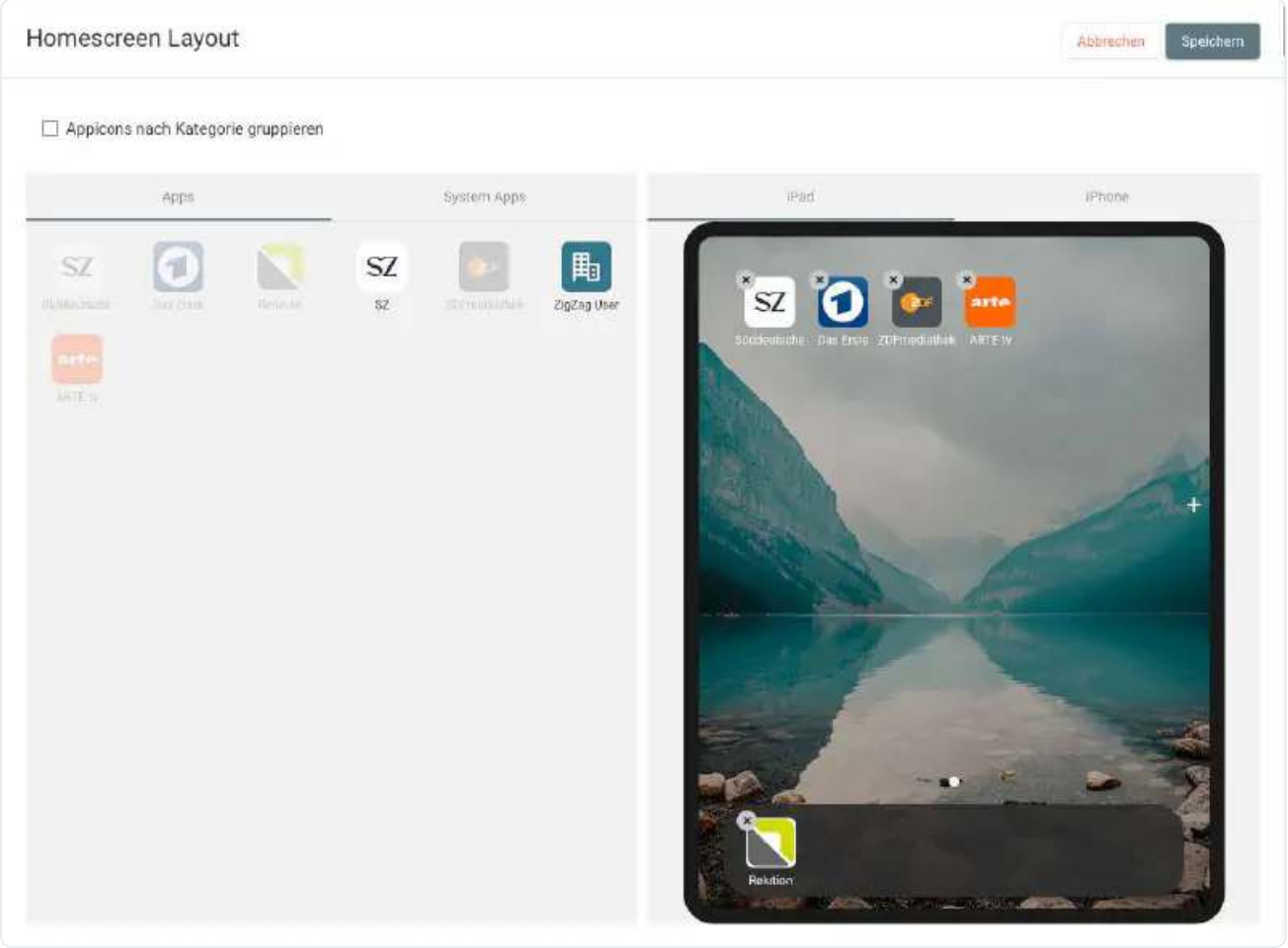
---

3. Optional: Weblink im Homescreen Layout anordnen

Über die Richtlinienkonfiguration `Homescreen Layout` lassen sich Apps und Weblink gezielt auf dem Homescreen von iOS-Geräten platzieren.

Für Version 26.4.0

1. Im Relution-Portal zum Menüpunkt `Geräte` → `Richtlinien` navigieren und auf Hinzufügen klicken.
2. Eine iOS-Richtlinie erstellen und einen `Namen` vergeben. Auf `Speichern` klicken.
3. Nach Klick auf `Hinzufügen` anschließend die Option `Homescreen Layout` auswählen und mit `Details hinzufügen` fortfahren.
4. Wurden vorhandene Weblink zuvor einer Kategorie zugeordnet, lassen sich diese automatisch in erzeugten Ordnern auf dem Homescreen platzieren. Für eine manuelle Anordnung die Option `App Icons nach Kategorie gruppieren` deaktivieren.
5. Anschließend die relevanten Apps und Weblink per Drag & Drop in der gewünschten Reihenfolge platzieren.



6. Auf `Speichern` klicken und die aktuelle Version der Richtlinie veröffentlichen.
7. Um die Richtlinie auf iOS-Geräten anzuwenden, die gewünschten Geräte über das Tab `Geräte mit dieser Richtlinie` hinzufügen. Die gewählten Einstellungen werden anschließend automatisch auf den Geräten ausgeführt.

> Damit Weblink im Homescreen Layout angezeigt werden sind die Schritte 1+2 oder 1+3 notwendig. Die URL im Weblink muss beim Erstellen im Relution Store sowie in der Weblink Konfiguration identisch sein.

Weblink als Web App öffnen

Ein Weblink kann auf dem Gerät entweder als Lesezeichen in Safari oder als eigenständige Web App starten. Gesteuert wird das über die Option Im Vollbildmodus öffnen (Weblink im App Store) bzw. Vollbild (Konfiguration `Weblink` in einer Richtlinie):

- Option deaktiviert: Der Weblink öffnet die Seite in Safari, mit Adressleiste und Tabs.
- Option aktiviert: iOS startet die Seite als Web App in einem eigenen Fenster ohne Safari-Oberfläche. In der App-Übersicht erscheint sie als eigene App.

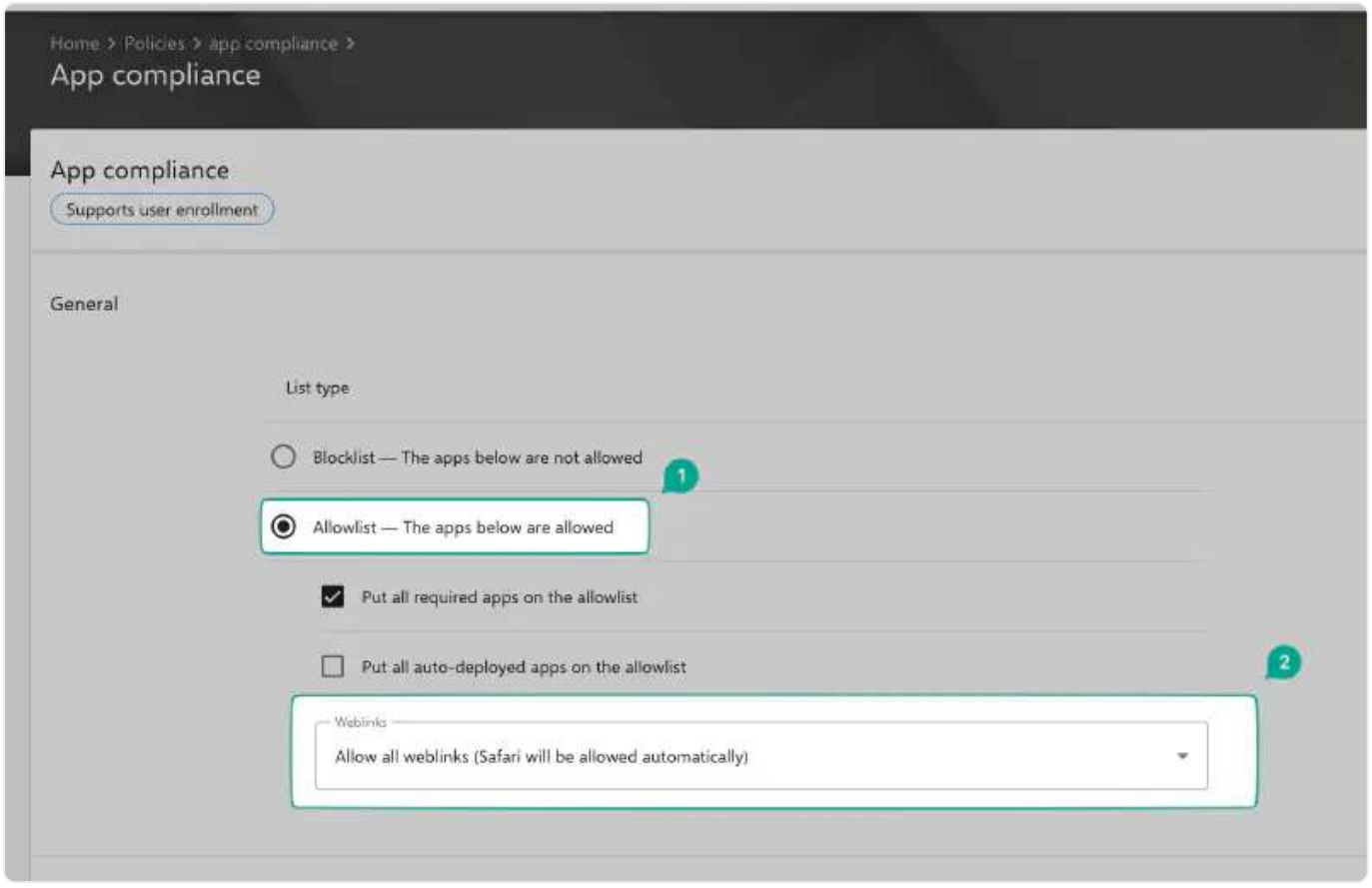
Ob die Seite tatsächlich als Web App dargestellt wird, hängt auch von der Webseite selbst ab. Sie muss den Web-App-Modus unterstützen, z. B. über ein Web App Manifest mit `"display": "standalone"` oder das Meta-Tag `apple-mobile-web-app-capable`. Fehlt diese Unterstützung, zeigt iOS die Seite trotz aktivierter Option wie in Safari an.

In der Richtlinienkonfiguration bleibt App zum Öffnen des Weblinks für die Darstellung als Web App leer. Ist dort eine App gewählt, öffnet sich der Weblink in dieser App.

Weblink bei Relution Shared Device

Damit Weblink bei Relution Shared Devices angezeigt und verwendet werden können, muss den Geräten eine App-Konformität zugewiesen werden. Diese wiederum muss wie folgt konfiguriert sein:

- Listen-Typ auf `Erlaubt` setzen
- Weblink auf `Erlaube alle Weblink (Safari wird automatisch erlaubt)` stellen



Backup

Dieser Artikel behandelt zwei zusammenhängende, aber unterschiedliche Vorgänge bei supervised (vollständig verwalteten) Apple-Geräten:

- Sicherung: Ein Backup eines supervised Geräts wird erstellt, um dessen Daten vor Verlust zu schützen.
- Umzug: Die Daten eines alten supervised Geräts werden auf ein neues, ebenfalls supervised Gerät übertragen.

Beide Geräte müssen dafür über Apple School Manager (ASM) oder Apple Business Manager (ABM) per DEP bei Relution registriert und im Modus `Supervised` betrieben werden.

Ein Umzug von oder auf ein nicht überwachtes (unsupervised) Gerät ist nicht Gegenstand dieses Artikels. Wie ein nicht überwachtes Gerät nachträglich ohne Datenverlust supervised gemacht werden kann, beschreibt Nicht überwachtes Gerät supervised registrieren →.

iCloud- oder lokales Backup?

Kriterium	iCloud-Backup	Lokales Backup (Mac/PC)
Speicherort	In iCloud	Auf dem Mac oder PC
Verbindung	WLAN	Kabelverbindung zum Mac/PC
Voraussetzung im DEP-Profil	Setup-Schritt `Mit Apple ID anmelden` darf nicht übersprungen werden	`Verbinden mit Macs oder PCs und Konfigurieren mit Apple Configurator erlauben` muss aktiviert sein.
Typischer Einsatzzweck	Laufende Sicherung, teilweise Wiederherstellung	geplanter Geräteumzug mit nahezu voller Datenübernahme

> Da sich diese DEP-Profil-Einstellung später nicht mehr ändern lässt, empfiehlt es sich, die Verbindung mit Computern generell zu aktivieren und über eine Restriktion in den Richtlinien zu unterbinden.

Empfehlung: Für die laufende Absicherung eines Geräts reicht in der Regel ein iCloud-Backup. Für einen geplanten Umzug auf ein neues Gerät - insbesondere bei größeren Datenmengen - ist ein lokales Backup über einen Mac oder PC oft die zuverlässigere Wahl. Details zu beiden Verfahren beschreibt Apple unter Backup-Methoden für iPhone, iPad und iPod touch →.

Voraussetzungen im DEP-Profil

Damit die Wiederherstellung eines Backups im Einrichtungsassistenten des neuen Geräts überhaupt angeboten wird, muss das dem Gerät zugewiesene DEP-Profil in Relution entsprechend konfiguriert sein:

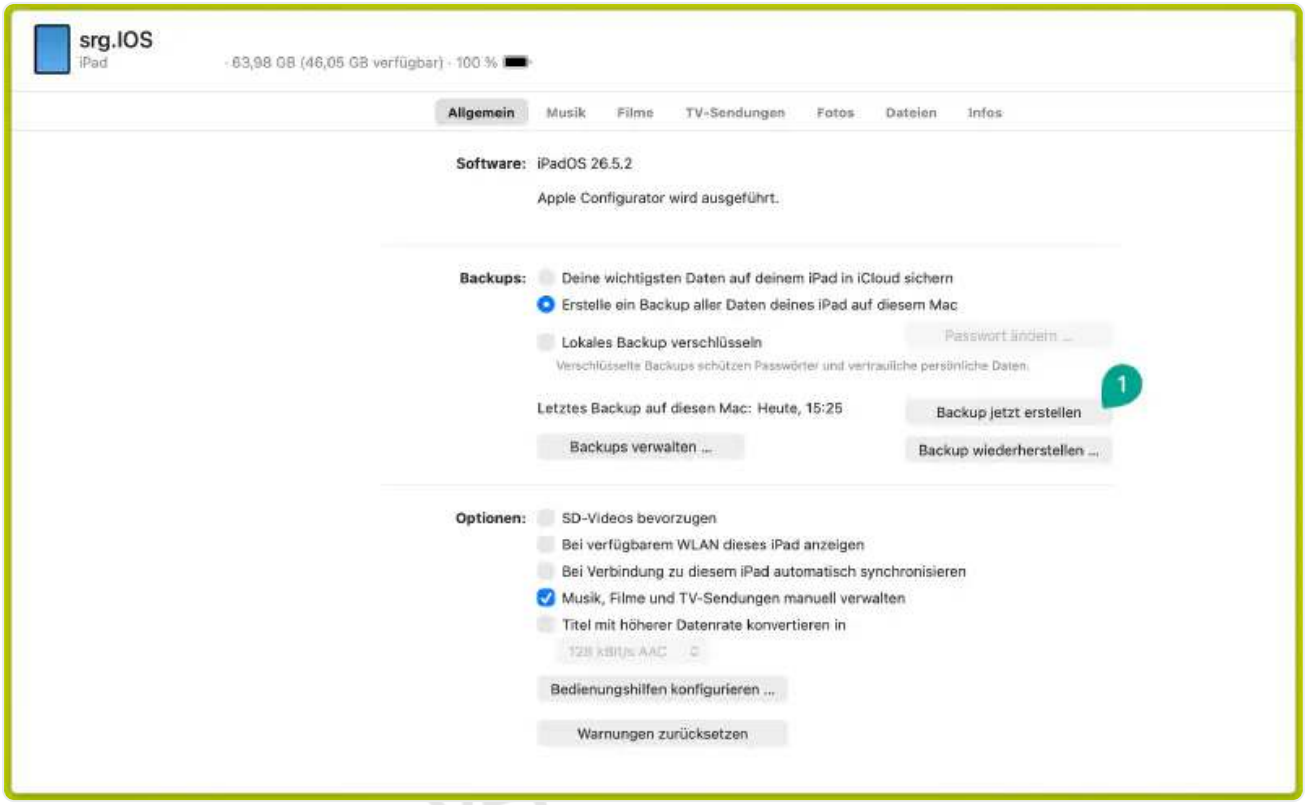
Einstellung im DEP-Profil	Erforderlicher Zustand	Zweck
Setup-Schritt `Backup einspielen`	Nicht aktivieren	Wird diese Option aktiviert, überspringt der Einrichtungsassistent den Wiederherstellen-Schritt vollständig - eine Wiederherstellung aus einem Backup ist dann nicht mehr möglich.
Setup-Schritt `Mit Apple ID anmelden`	Nicht aktivieren	Für ein iCloud-Backup muss sich das Gerät mit derselben Apple ID anmelden können, mit der das Backup erstellt wurde.
`Verbinden mit Macs oder PCs und Konfigurieren mit Apple Configurator erlauben`	Aktivieren	Nur für ein lokales Backup über einen Mac oder PC nötig. Ohne diese Option kann das Gerät nicht mit einem Computer verbunden werden.

Mehr zur Konfiguration eines DEP-Profils in Relution: Konfigurationsprofil für ADE →

Für Version 26.4.0

Ablauf

1. Auf dem alten Gerät ein Backup erstellen - per iCloud oder lokal über einen Mac oder PC. Eine Anleitung dazu bietet Apple unter Ein Backup für dein iPhone oder iPad mit deinem Mac erstellen →.

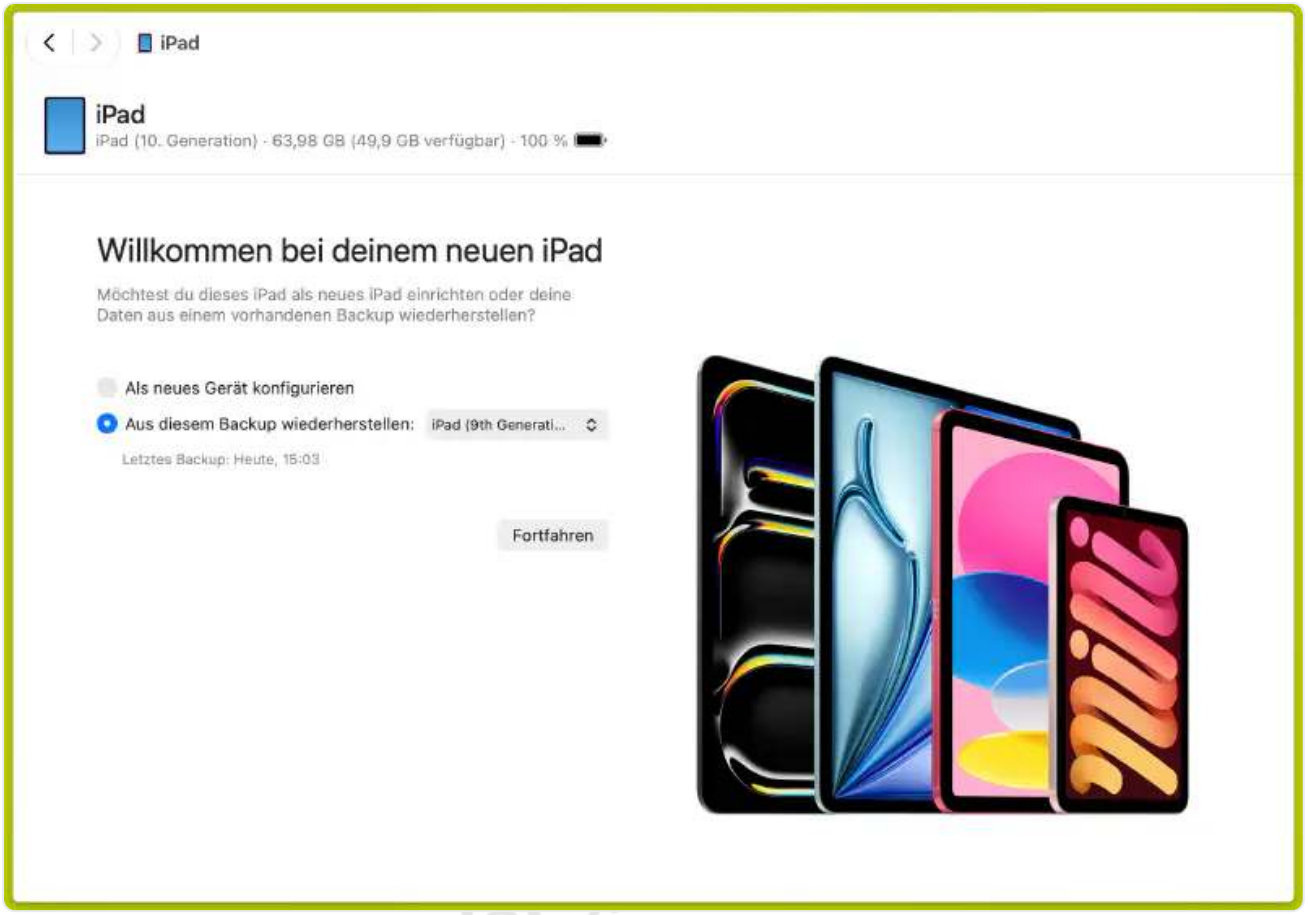


2. Das neue Gerät in Betrieb setzen und dem Einrichtungsassistenten folgen.

3. Im Einrichtungsassistenten `Wiederherstellung von Apps und Daten` bzw. die entsprechende Option für ein iCloud- oder Computer-Backup wählen.

4. Bei einem iCloud-Backup: Mit derselben Apple ID anmelden, mit der das Backup erstellt wurde.

5. Bei einem Backup von einem Mac/PC erscheint eine Aufforderung, das neue Gerät zu verbinden. Im Finder kann anschließend das zuvor erstellte Backup des alten Geräts ausgewählt werden.



6. Das Gerät durchläuft anschließend automatisch die DEP-Registrierung bei Relution und wird supervised eingeschrieben.

Kein Profil aus dem Backup verwenden

Für DEP-Profile, die für iOS/iPadOS 26 bzw. visionOS 26 oder höher konfiguriert sind, steht im Relution Portal beim DEP-Profil zusätzlich die Option `Kein Profil aus dem Backup verwenden` zur Verfügung. Der zugehörige Hinweistext im Portal lautet:

```
Falls gesetzt, verwendet das Gerät das Profil nicht, wenn es ein Backup
wiederherstellt.
```

In der Praxis bedeutet das:

- Deaktiviert (Standard): Beim Wiederherstellen eines Backups kann das neue Gerät die im Backup enthaltenen Angaben zum Verwaltungsprofil übernehmen. Das ist für den klassischen 1:1-Umzug von einem alten auf ein neues Gerät der passende Zustand.
- Aktiviert: Das Gerät ignoriert beim Wiederherstellen etwaige Profilangaben aus dem Backup und wird stattdessen ausschließlich über das aktuell in Relution hinterlegte DEP-Profil verwaltet. Das ist sinnvoll, wenn ein Gerät zwar aus einem Backup wiederhergestellt wird, aber bewusst eine andere oder aktualisierte Verwaltungskonfiguration erhalten soll.

Diese Option ist neu und betrifft nur DEP-Profile für iOS/iPadOS 26 bzw. visionOS 26 oder höher. Das Verhalten vor einem Rollout an einem Testgerät prüfen, da sich Details je nach Apple-Betriebssystemversion ändern können.

Nach dem Umzug

Im Relution Portal unter `Geräte` prüfen, ob das neue Gerät korrekt als supervised und eingeschrieben angezeigt wird und die erwarteten Konfigurationen, Apps und Richtlinien erhalten hat. Das alte Gerät kann anschließend regulär außer Betrieb genommen bzw. aus Relution entfernt werden.

Schnellstart (Quick Start)

Für ein neues Gerät, das bereits bei Apple School Manager oder Apple Business Manager registriert ist - also praktisch jedes Relution-verwaltete supervised Gerät -, funktioniert die Datenübertragung per „Schnellstart“ nicht. Das ist eine Einschränkung von Apple selbst und lässt sich nicht über das DEP-Profil umgehen.

Für Version 26.4.0

Apple beschreibt Schnellstart als Funktion, mit der ein neues iPhone oder iPad automatisch anhand eines vorhandenen Geräts eingerichtet wird, indem beide Geräte nebeneinandergelegt werden.

Für Privatgeräte ohne DEP-Registrierung funktioniert das inklusive direkter Datenübertragung. Für Geräte, die einer Organisation zugewiesen sind, gilt jedoch ausdrücklich:

```
Wenn dein neues Gerät bei Apple School Manager oder Apple Business registriert ist,
kannst du mit „Schnellstart“ keine Daten von deinem aktuellen Gerät übertragen.
```

Mit „Schnellstart“ Daten auf ein neues iPhone oder iPad übertragen →

Für den Umzug zwischen zwei supervised Geräten ist daher immer eine Wiederherstellung aus einem Backup (iCloud oder lokal) der richtige Weg.

Teamviewer Support Einladung

Mit TeamViewer lassen sich Remote Support Sessions erstellen und mit Empfängern teilen. Über Relution kann ein Session-Link per Nachricht an ein Gerät geschickt werden. Voraussetzung: Auf dem Gerät ist die TeamViewer QuickSupport App installiert.

In dieser Anleitung wird beschrieben, wie eine Session erstellt, der Link geteilt und der Empfänger zur Verbindung gebracht wird.

Voraussetzungen

- TeamViewer
- TeamViewer QuickSupport App auf dem Zielgerät (z. B. iPhone oder iPad)
- Zugriff auf Relution zum Versenden der Nachricht
- Berechtigung zur Nutzung von Remote Support

Schritte zur Erstellung einer Remote Session

1. Nachricht mit Link erstellen:
    - Man meldet sich bei Relution an.
    - Unter `Geräte` → `Inventar` → `Gerät auswählen` → `Aktion auswählen` → `Nachricht senden` kann eine Nachricht versendet werden.
    - Ein Link zur TeamViewer-Sitzung wird in die Nachricht eingefügt.
    - Die Nachricht wird an das gewünschte Gerät gesendet.
2. Link auf dem Gerät öffnen:
    - Der Empfänger erhält die Nachricht auf seinem Gerät.
    - Der Empfänger öffnet die Nachricht und klickt auf den Link.
    - Die TeamViewer QuickSupport App öffnet sich automatisch.
3. Sitzung starten:
    - Der Absender der Nachricht kann nun die Sitzung auf seinem Computer starten.
    - Der Empfänger auf dem Gerät muss die Verbindung bestätigen.

Für Version 26.4.0

Hinweise

- Es muss sichergestellt werden, dass die TeamViewer QuickSupport App auf dem neuesten Stand ist.
- Der Link zur TeamViewer-Sitzung ist nur für eine begrenzte Zeit gültig.
- Der Empfänger muss über eine stabile Internetverbindung verfügen.

Sonstiges

- Weitere Informationen zu TeamViewer findet man auf der offiziellen Website: teamviewer.com →

Sicherheitshinweis

- Links zu TeamViewer-Sitzungen sollten nur mit vertrauenswürdigen Personen geteilt werden.
- Verbindungen von unbekannten Absendern sollten nicht bestätigt werden.

Für Version 26.4.0

Airdrop

Seit der Aktualisierung auf iOS 26.2 (sowie iPadOS 26.2 und macOS 26.2) hat Apple die Sicherheitsanforderungen für den Datenaustausch via AirDrop verschärft. Viele Nutzer, insbesondere in Schulen und Unternehmen, stellen fest, dass beim Versenden von Dateien plötzlich die Eingabe eines Codes verlangt wird – ein Verhalten, das unter iOS 18.x noch nicht existierte.

Beim Versuch, eine Datei an eine Person zu senden, die nicht in den eigenen Kontakten gespeichert ist, wird der Transfer blockiert, bis ein numerischer Code eingegeben wurde. Dies erschwert den schnellen Datenaustausch im Unterricht oder in Arbeitsgruppen erheblich.

Ursache

Laut offizieller Apple-Dokumentation ist dies eine bewusste Sicherheitsfunktion zum Schutz der Privatsphäre:

- Identitätsprüfung: Wer nicht in den eigenen Kontakten hinterlegt ist, muss nun zwingend einen AirDrop-Code verwenden, um Objekte senden zu können.
- Ablauf: Der Empfänger muss Fortfahren wählen, woraufhin ein Code auf seinem Display erscheint. Dieser muss vom Sender eingegeben werden, um die Übertragung zu autorisieren.
- MDM-Einschränkung: Administratoren haben derzeit keine Möglichkeit, diese Abfrage über Mobile Device Management (MDM) global zu deaktivieren. Apple bietet MDM-Anbietern hier keine erweiterten Optionen gegenüber dem Endanwender an.

Für Version 26.4.0

Voraussetzung: Apple Account und iCloud

> Wichtig: Die Nutzung von AirDrop im Modus Nur Kontakte sowie die dauerhafte Code-freie Verbindung zu bekannten Kontakten erfordern einen angemeldeten Apple Account (iCloud) auf dem Gerät. Weitere Informationen dazu bietet die Apple Dokumentation →

Auf iPads ohne Apple Account erscheint beim Umstellen von AirDrop auf Nur Kontakte ein Bestätigungsfenster mit dem Hinweis, dass hierfür iCloud benötigt wird. Ohne Anmeldung ist diese Einstellung nicht nutzbar.

Damit AirDrop im Modus Nur Kontakte zuverlässig funktioniert, muss außerdem die E-Mail-Adresse oder Mobiltelefonnummer des Apple Accounts der sendenden Person in deren Kontaktkarte beim Empfänger hinterlegt sein.

Workaround

Um die ständige Code-Eingabe zu umgehen, gibt es folgende Ansätze:

Temporäre Lösung: AirDrop auf 10 Minuten für alle stellen

Die einfachste kurzfristige Lösung ist, AirDrop vorübergehend auf 10 Minuten für alle zu stellen. In diesem Modus ist keine Kontaktbeziehung oder Code-Eingabe erforderlich. Die Einstellung kehrt nach 10 Minuten automatisch auf den vorherigen Wert zurück.

Die 30-Tage-Regel nutzen

Sobald ein Code einmal erfolgreich eingegeben wurde, merkt sich das System die Verbindung. Nun lassen sich 30 Tage lang weitere Objekte mit dieser Person austauschen, ohne dass erneut ein Code verlangt wird.

Dauerhafte Lösung: Zu Kontakten hinzufügen

Die Codeabfrage wird dauerhaft unterdrückt, wenn sich Sender und Empfänger gegenseitig in ihren Kontakten speichern.

- Nach einem Empfang die Option Neuen Kontakt erstellen oder Zu Kontakt hinzufügen wählen.
- Sobald die Person als bekannter Kontakt hinterlegt ist, erfolgt der Austausch wie gewohnt ohne zusätzliche Verifizierung.

Bekannte Kontakte verwalten oder ignorieren

Um eine Verbindung vor Ablauf der 30 Tage zu trennen:

- Die App Kontakte öffnen.
- In der Liste unter Andere bekannte Kontakte nach der entsprechenden Person suchen.
- Dort Diese Person ignorieren wählen, um den automatisierten Austausch zu beenden.

Für Version 26.4.0

Bei iTunes anmelden

Wenn Apple Appstore Apps über ein MDM verteilt werden (in Relution über eine App-Installations-Aktion, über eine Richtlinie oder über ein Auto-Deployment), kann folgende Meldung auf dem Endgerät erscheinen.

App-Installation - Melde dich bei iTunes an, damit deine Organisation Apps verwalten und installieren kann.

Für Version 26.4.0

09:59
Wetter
Aktien
Wo ist?
Home
Bücher
iTunes Store
Fitness
Watch
App-Installation
Melde dich bei iTunes an, damit „support.relution.io“ Apps verwalten und installieren darf.
Abbrechen
Anmelden
Relution Agent

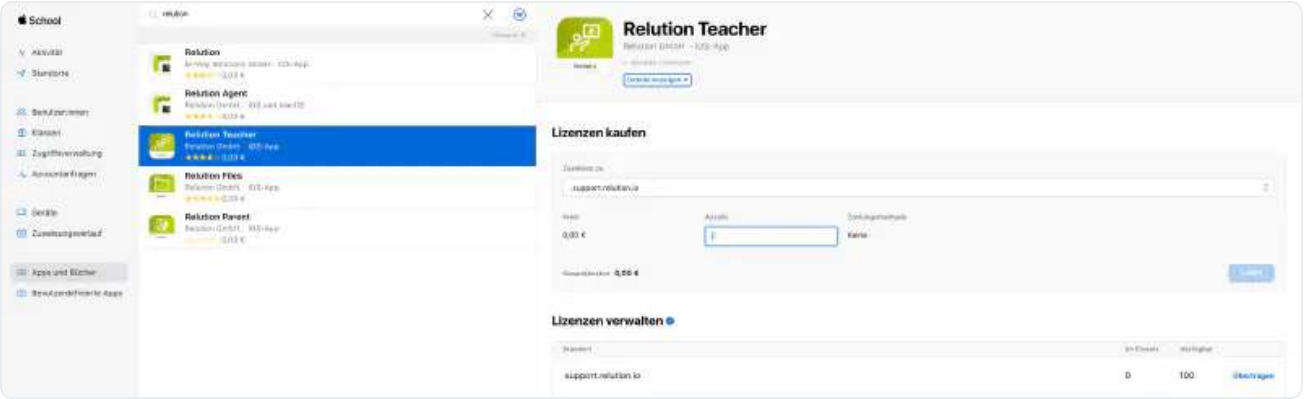
Für Version

Ursache

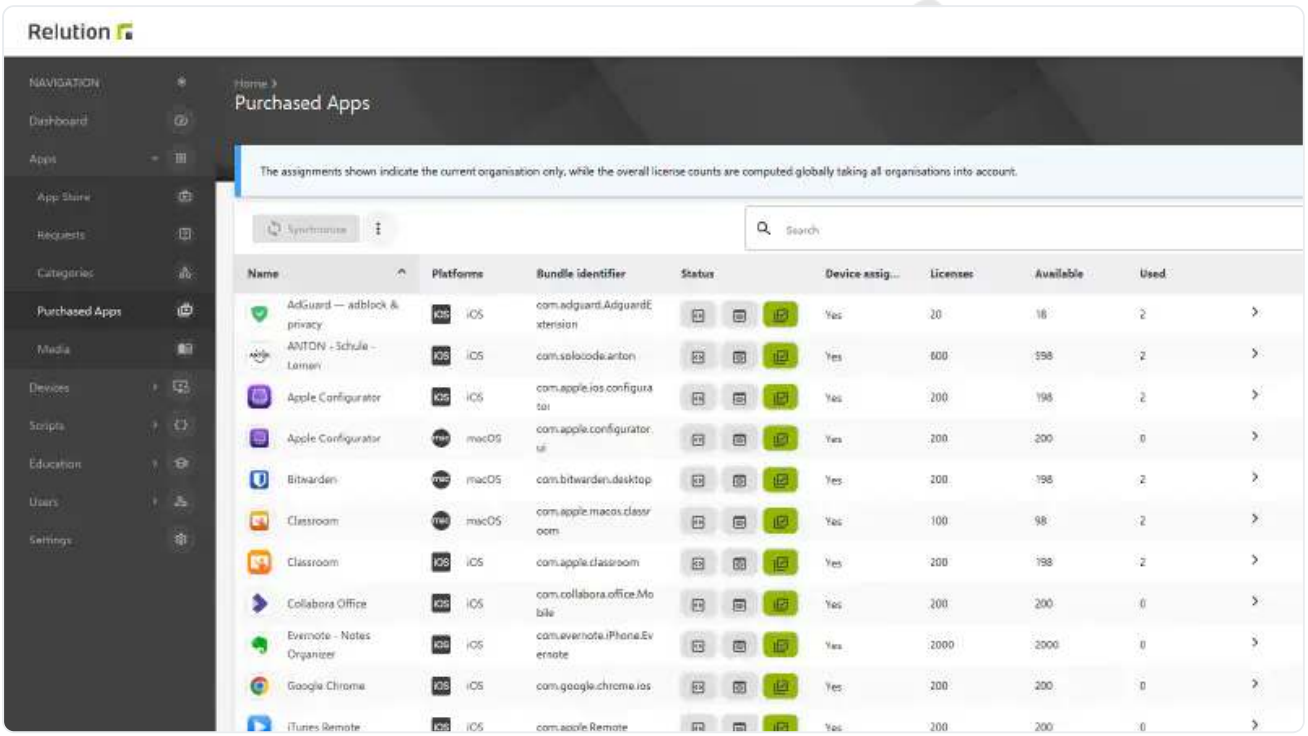
Appstore Apps (auch kostenlose) benötigen immer eine Lizenz.
Im privaten Umfeld wird das über die AppleID realisiert und beim Download einer App aus dem Store automatisch erledigt.
Bei MDM Anbietern funktioniert das über das Apple VPP (Volume Purchase Program) Hierzu müssen im ASM / ABM (Apple School / Business Manager) entsprechend Lizenzen für jede zu verteilende App im Vorfeld erworben werden.

Lösung

1. Dazu muss man sich im ASM / ABM Portal anmelden und dort unter Apps & Books Lizenzen für die gewünschte App in ausreichender Stückzahl für die (verteilende) Organisation erwerben.



2. Nach kurzer Zeit ist die App auch in Relution unter `Gekaufte Apps` im Seitenmenü sichtbar.



3. Auf den Endgeräten mit der Meldung müssen alle PopUps (eine Meldung pro unlizenzierter App) abgebrochen werden. Danach kann die Aktion oder Policy erneut ausgeführt werden und die Apps werden ohne Meldung installiert.

VPP einrichten→

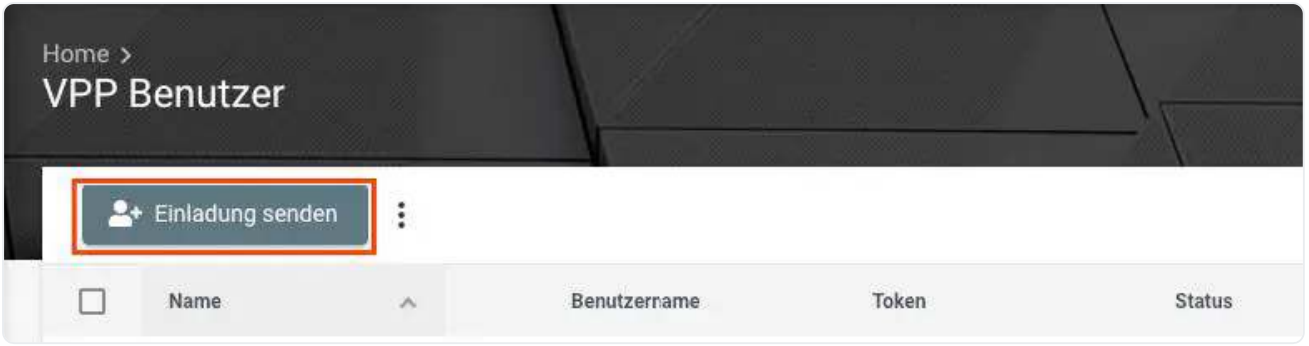
Gekaufte Bücher zuweisen

Über Apple gekaufte Bücher können in Relution einzelnen Benutzer zugewiesen werden. Es reicht nicht aus, für diese Benutzer eine Managed Apple-ID zu hinterlegen; sie müssen über Relution eine Einladung erhalten und anschließend den Anweisungen auf dem Bildschirm folgen.

Für Version 26.4.0

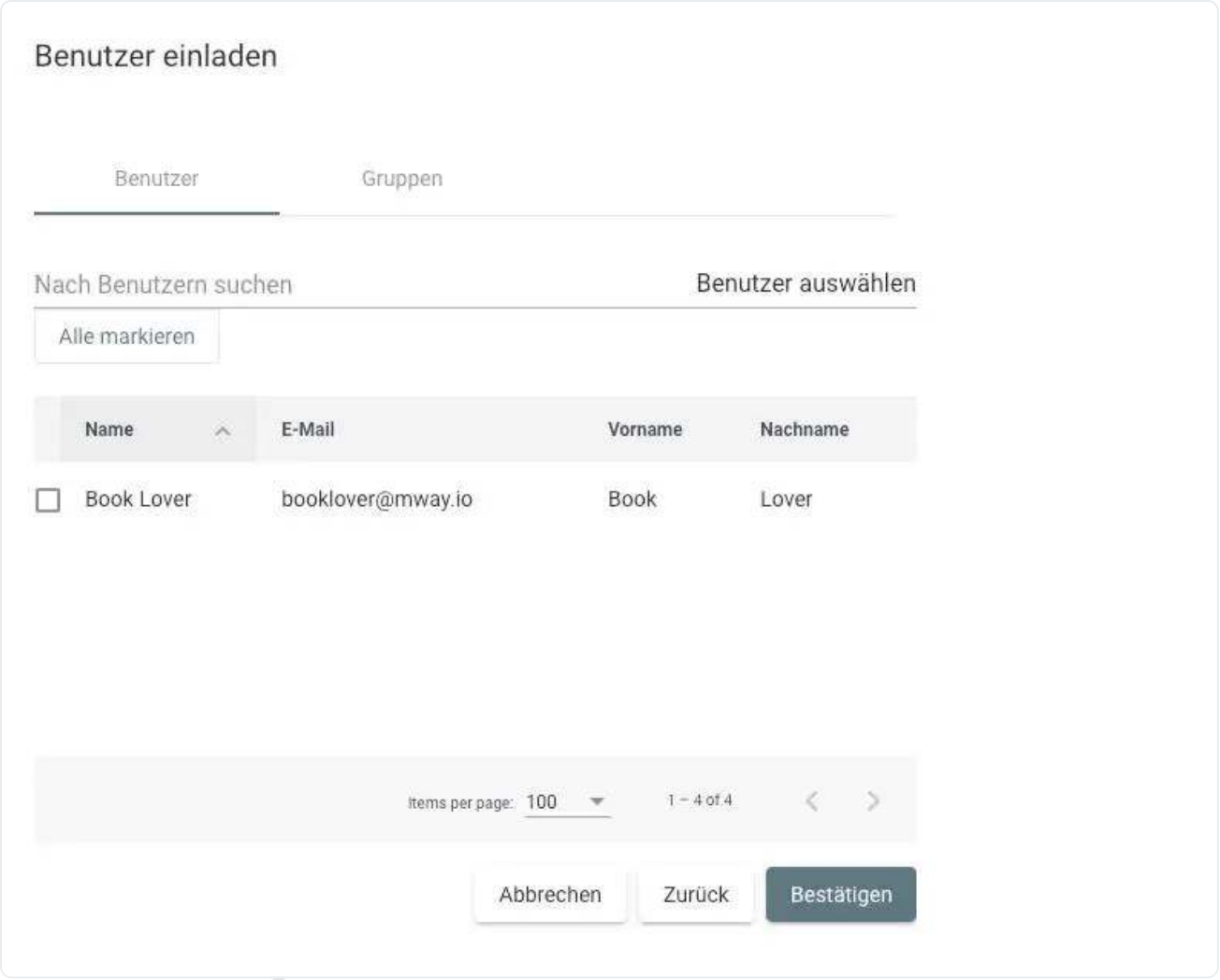
Anleitung

1. Die gewünschten Benutzer, sofern nicht schon geschehen, in Relution anlegen.
2. In den Bereich `Benutzer` → `VPP Benutzer` wechseln.
3. `Einladung senden` wählen.

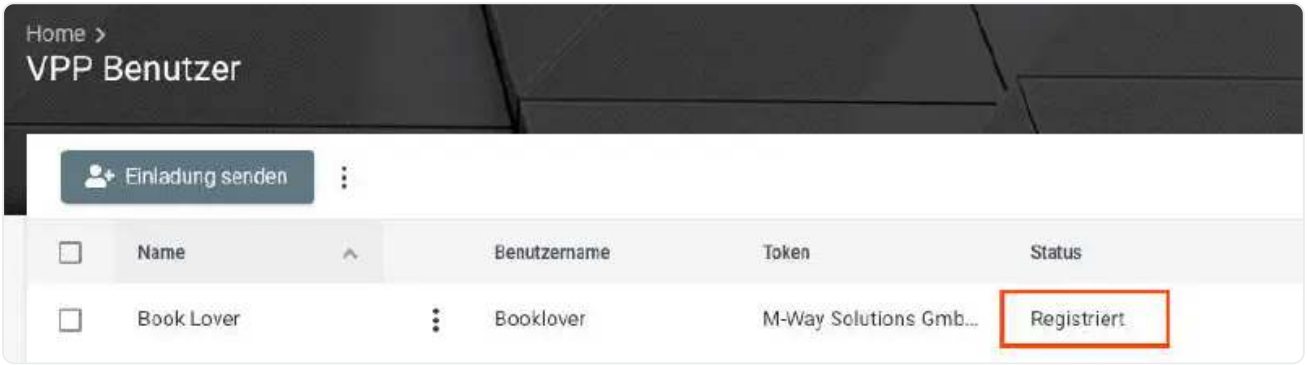


4. Das gewünschte VPP-Token wählen und auf `Weiter` klicken.

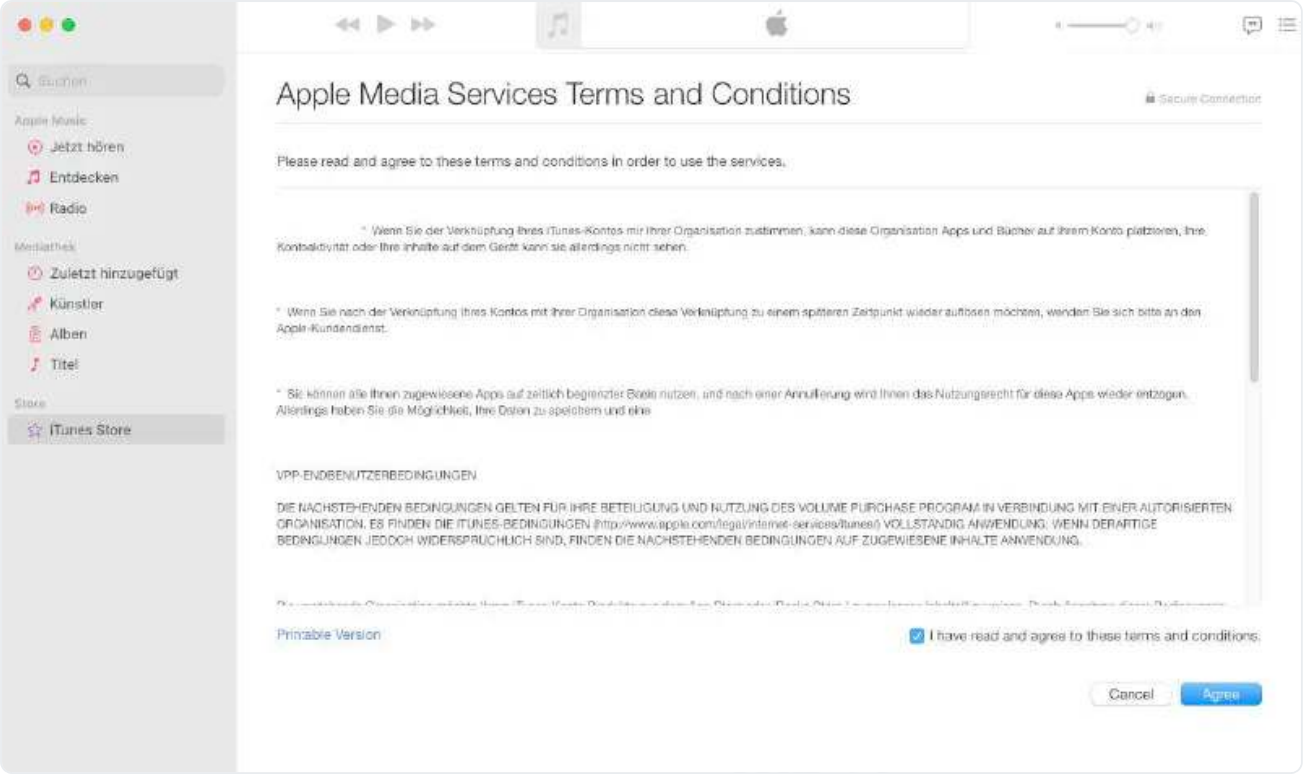
5. Die gewünschte, einzuladende Benutzer auswählen und auf `Bestätigen` klicken.



6. Der Benutzer wird mit dem Status `Registriert` in der Liste hinterlegt. Der Benutzer sollte eine E-Mail bekommen.

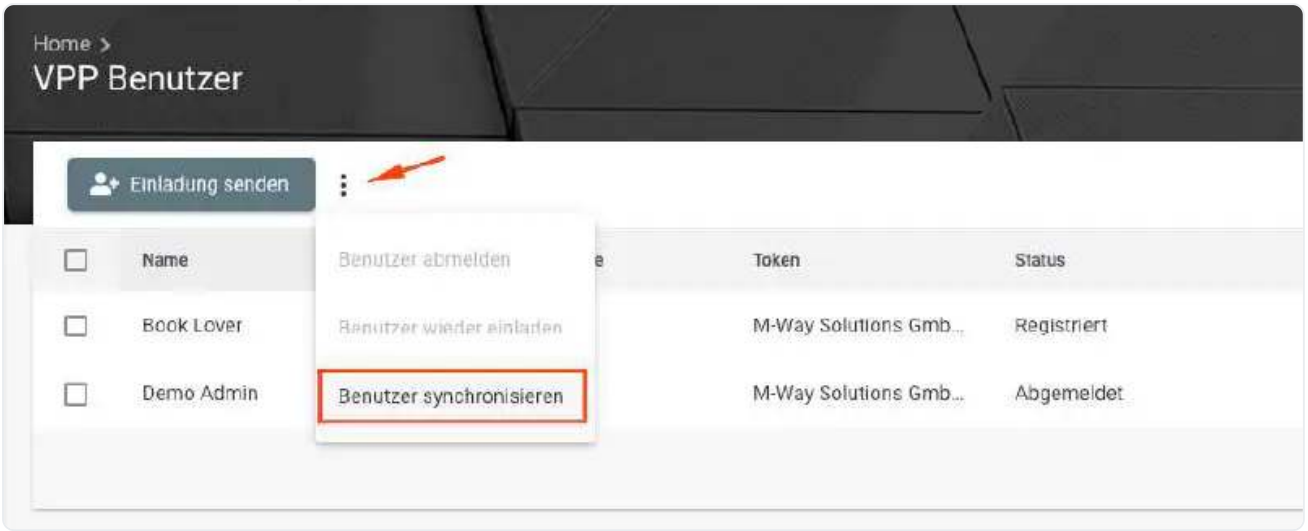


7. In der E-Mail befindet sich ein Link, der geöffnet werden muss - wahlweise mit `iTunes` bzw. `Apple Music`. Hier muss der Benutzer die AGB akzeptieren und bestätigen. Wenn noch kein Benutzer auf dem Gerät angemeldet ist, muss ggf. ein Benutzername und ein Kennwort eingegeben werden.



8. Im Anschluss muss die Zuweisung von Apps nochmals erlaubt werden.

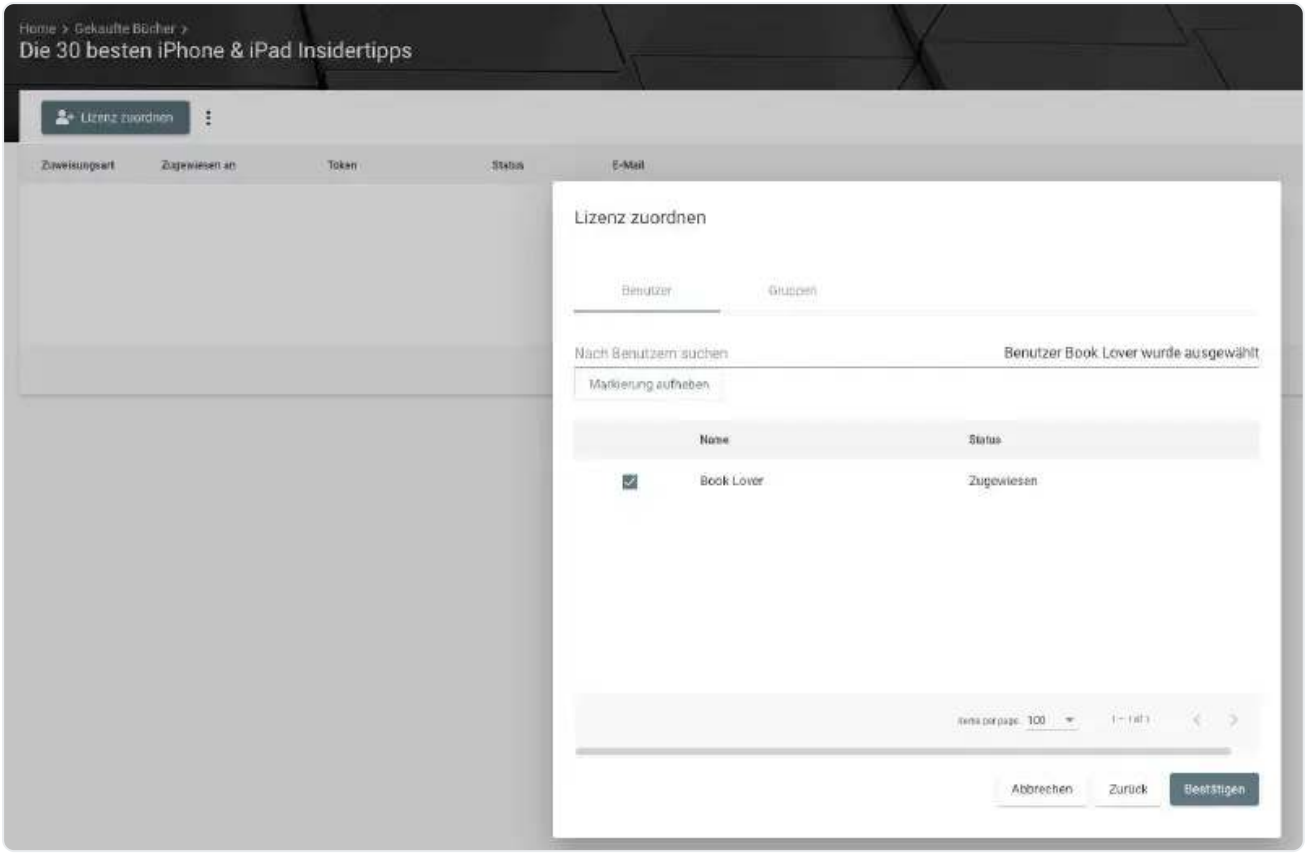
9. In Relution müssen die VPP-Benutzer nun synchronisiert werden.



10. Wird die Anzeige im Anschluss aktualisiert, wird der Benutzer als `Zugewiesen` angezeigt.

11. Unter `Gekaufte Bücher` auf das gewünschte, zuzuweisende Buch klicken.

12. Im nächsten Schritt auf `Lizenz zuweisen` klicken, das entsprechende Token und im Anschluss den gewünschten Benutzer wählen. Die Auswahl mit Klick auf Bestätigen abschließen.



Nun ist der Benutzer ein Buch zugewiesen.

Übersicht Einschreibungen

Apple TVs entwickeln sich zu einer bedeutenden Einheit in Organisationen. Sie sind eines der vielversprechendsten Streaming Tools, die heute in Organisationsinfrastrukturen eingesetzt werden. Relution unterstützt die Verwaltung von Apple TVs mit mehreren Einschreibeverfahren: der Automatischen Geräteregistrierung (ADE, im Portal: DEP), der nachträglichen Aufnahme über `Apple Configurator 2` und der manuellen Einschreibung.

Automatische Geräteregistrierung (ADE) mit DEP-Profil

Der Apple School- oder Business Manager wurde von Apple eingeführt, um Organisationen und Bildungseinrichtungen bei der Bereitstellung von Apple-Geräten aus der Ferne zu unterstützen. Mithilfe von ASM/ABM können brandneue Apple-Geräte in Relution registriert werden, ohne dass ein Techniker sie jemals in die Hand nehmen muss.

Konfigurationsprofil für ADE →
DEP Allgemein →

Voraussetzungen

- tvOS 10.2 oder höher.
- Die Organisation sollte im Apple School/ Apple Business Manager angemeldet sein.
- Geräte müssen nach dem 1. März 2011 bestellt worden sein, unabhängig davon, ob sie direkt von Apple oder einem autorisierten Wiederverkäufer gekauft wurden.
- Wenn Geräte direkt bei Apple gekauft wurden, ist die Apple-Kundennummer, die der eigenen Organisation zugewiesen ist, erforderlich, um berechtigte Bestellungen und Geräte mit dem Apple School/ Business Manager zu verbinden.
- Wurden Geräte direkt von einem autorisierten Wiederverkäufer oder Netzbetreiber beschafft, müssen die Geräte mit der Reseller-ID dieses Händlers verknüpft sein. Das tatsächliche Datum der Berechtigung wird durch die Verkaufshistorie des autorisierten Wiederverkäufers oder Netzbetreibers bestimmt.
- Ein in Relution hinterlegtes APNs-Zertifikat (APNS Push Zertifikate →).
- Ein in Relution eingebundenes DEP-Konto und ein DEP-Profil, das den Geräten zugewiesen ist. Eine Mindest-Betriebssystemversion lässt sich im DEP-Profil für tvOS nicht festlegen.

Für Version 26.4.0

Optionen für Apple TVs im DEP-Profil

Zwei Einstellungen im DEP-Profil betreffen speziell Apple TVs:

- Automatische Voreinstellung für macOS und tvOS: Der Einrichtungsassistent wechselt automatisch zwischen seinen Bildschirmen. Das Apple TV benötigt dafür eine Ethernet-Verbindung. Solange der Schalter aktiviert ist, lassen sich die zu überspringenden Setup-Schritte nicht auswählen.
- Unter den zu überspringenden Setup-Schritten enthält die Gruppe tvOS spezifisch die Bildschirme, die nur auf Apple TVs vorkommen: Aerial Screensavers konfigurieren und Tap To Set Up konfigurieren (ab tvOS 10.2) sowie TV Home Screen Layout synchronisieren, TV provider login und „Wo befindet sich dieser Apple TV?“ (ab tvOS 11). Aktivierte Schritte werden bei der Einrichtung übersprungen.

Nachträgliche Einschreibung über den Apple Configurator 2

`Apple Configurator 2` ist eine kostenlose App aus dem Mac App Store, mit der Apple TVs, die nicht bereits von einem autorisierten Wiederverkäufer für die ADE registriert wurden, nachträglich zum Apple School/ Business Manager hinzugefügt werden können. Anschließend werden sie wie andere ADE-Geräte eingeschrieben.

Voraussetzungen

- Apple TV mit tvOS 10.2 oder höher.
- macOS-Gerät mit `Apple Configurator 2.5` oder höher.
- Das macOS-Gerät und das Apple TV sind mit demselben WLAN- oder Ethernet-Netzwerk verbunden.

Für tvOS-Geräte muss folgender Pfad als MDM-Server-URL angegeben werden, sofern die Geräte auf dem Relution-Livesystem verwaltet werden sollen. Bei einer eigenen Relution-Instanz wird `live.relution.io` durch den Hostnamen des eigenen Servers ersetzt.

```
https://live.relution.io/api/enrollment/v1/appleMdm/depenroll
```

Nachträglich zur ADE hinzufügen →
Überwachter Modus / Supervision →

Für Version 26.4.0

Manuelle Einschreibung

Apple TVs lassen sich auch ohne ADE über eine manuelle Einschreibung in Relution aufnehmen. Dazu wird unter `Geräte` → `Einschreibungen` eine Einschreibung mit der Plattform tvOS angelegt. Die Plattform ist nur auswählbar, wenn in Relution ein APNs-Zertifikat hinterlegt ist. Da Apple TVs keinen Webbrowser besitzen, wird das MDM-Profil der Einschreibung mit `Apple Configurator 2` auf dem Apple TV installiert.

Manuelle Einschreibung →

Verfügbare Aktionen

Relution stellt eine Auswahl an Aktionen bereit, um Apple TV-Geräte direkt zu kontrollieren und zu lenken. Die Aktionen lassen sich gezielt auf ein einzelnes Gerät oder über die Mehrfachauswahl in der Geräteliste auf mehrere Geräte gleichzeitig anwenden. Zusätzlich können sie über die Mitgliedschaft in Gerätegruppen ereignis- oder zeitgesteuert ausgelöst werden: Aktionen mit Gerätegruppen →

Der Aktionsdialog wird unter `Geräte` → `Inventar` über Aktion anwenden geöffnet, entweder für die in der Liste ausgewählten Geräte oder in der Detailansicht eines Geräts. Angeboten werden nur Aktionen, die alle ausgewählten Geräte unterstützen.

Für Version 26.4.0

Aktionsübersicht

Aktion	Beschreibung
App entfernen	Deinstalliert eine App vom Gerät.
Gerät auf Werkszustand zurücksetzen	Setzt das Gerät auf den Werkszustand zurück und löscht alle Daten vom Gerät.
Gerät neu starten	Das Gerät wird neu gestartet. Nur für überwachte (supervised) Geräte verfügbar.
Geräteinformationen aktualisieren	Aktualisiert alle verfügbaren Informationen zu dem Gerät, die unter Details aufgelistet sind.
Im Geräte-Setup-Assistenten fortfahren	Informiert das Gerät, dass die Vorkonfiguration abgeschlossen ist und es im Setup-Assistenten fortfahren kann. Nur für Geräte verfügbar, die über die Automatische Geräteregistrierung (ADE, im Portal: DEP) registriert wurden. Wirkt nur, wenn im DEP-Profil die Option Konfiguration abwarten aktiviert ist.
MDM Profil aktualisieren	Installiert das MDM-Profil auf dem Gerät neu. Dabei werden das Identitätszertifikat erneuert und aktuelle Einstellungen wie das Certificate Pinning übernommen. Die MDM-Server-URL bleibt unverändert; eine geänderte externe URL wird so nicht auf das Gerät übertragen. Relution erneuert das MDM-Profil automatisch, bevor das Identitätszertifikat abläuft. Die manuelle Aktion ist daher nur in Sonderfällen erforderlich.
Relution Store App bereitstellen	Nach einer App im Relution Store suchen und diese auf den Geräten installieren.
Return to Service	Setzt das Gerät auf die Werkseinstellungen zurück; anschließend versucht es, sich automatisch wieder anzumelden. Voraussetzung ist tvOS 18 oder neuer, bei älteren Versionen schlägt die Aktion fehl. Im Aktionsdialog muss eine Richtlinie mit einer tvOS-WLAN-Konfiguration ausgewählt werden. Die Aktion steht nur zur Verfügung, wenn alle ausgewählten Geräte derselben Plattform angehören.
Update Installieren	Installiert ein gewünschtes Update auf dem ausgewählten Gerät. Nur für überwachte (supervised) Geräte verfügbar. Die Aktion wird nur angeboten, wenn Relution für alle ausgewählten Geräte ein verfügbares Update ermittelt hat. Die verfügbaren Updates werden neu ermittelt, sobald die Geräteinformationen aktualisiert werden, z. B. über Geräteinformationen aktualisieren.

Ist mindestens eines der ausgewählten Geräte nicht überwacht, werden Gerät neu starten und Update Installieren im Aktionsdialog nicht angezeigt. Entsprechendes gilt für Im Geräte-Setup-Assistenten fortfahren, sobald ein ausgewähltes Gerät nicht über die Automatische Geräteregistrierung registriert wurde.

Verfügbare Konfigurationen

Eine Richtlinie ist eine Sammlung einer oder mehrerer Konfigurationen. Jede Richtlinie kann auf einem oder mehreren Geräten gleichzeitig angewendet werden. Zudem können mit jedem Gerät eine oder mehrere Richtlinien verknüpft sein.

Konfigurationen im Überblick

Konfiguration	Beschreibung
AirPlay-Sicherheit →	AirPlay-Sicherheitseinstellungen, um unautorisiertes Streamen auf Apple TVs über AirPlay zu verhindern
App Konformität →	Verwaltung appspezifischer Einschränkungen
Apple Configurator 2 Konfiguration →	Wendet ein mit Apple Configurator 2 erstelltes Konfigurationsprofil (`.mobileconfig`) auf Geräte an
Einzel-App-Modus	Geräte auf eine einzige App begrenzen
Geräteeinstellungen	Allgemeine Geräteeinstellungen konfigurieren (nur überwachte Geräte)
Gerätename	Konfigurieren des Gerätenamens (nur überwachte Geräte)
Konferenzraum →	Konferenzraum-Modus verwalten
Restriktionen	Verwaltung von Geräterestriktionen
Softwareupdates-Einstellungen →	Update-Verhalten der Geräte steuern, z. B. automatische Installation und Aufschub von Updates (ab tvOS 18.4)
System-Updates	Aktualisierungen von Apple-Geräten verwalten (nur überwachte Geräte; veraltet, Nachfolger: Verwaltete Softwareupdates)
Verwaltete Softwareupdates →	Betriebssystemupdates erzwingen und eine Zielversion bis zu einer Frist vorgeben (ab tvOS 18.4, nur überwachte Geräte)
WLAN	Verwaltung der WLAN-Einstellungen
Zeitzone	Konfiguration der Zeitzone (ab tvOS 14, nur überwachte Geräte)
Zertifikat	Zertifikat auswählen, das standardmäßig auf dem Gerät installiert werden soll

Die Konfigurationen WLAN, Zertifikat und Apple Configurator 2 Konfiguration können mehrfach in einer Richtlinie angelegt werden, alle übrigen jeweils nur einmal.

Apple Configurator 2 Konfiguration

Mit dieser Richtlinien-Konfiguration können `.mobileconfig`-Dateien auf Apple-Geräte übertragen werden. Eine solche Datei kann beispielsweise eine WLAN-Verbindung samt zugehörigem Identitätszertifikat (PKCS#12, `.p12`) enthalten.

Konfiguration

Im Feld Name wird eine Bezeichnung für die Konfiguration vergeben. Über .mobileconfig Datei auswählen wird die Datei hochgeladen. Danach erscheint ihr Inhalt anstelle der Dateiauswahl im Feld Payload Inhalt und kann dort bearbeitet werden. Der Inhalt muss gültiges XML sein. Signierte Profile sind kein lesbares XML und lassen sich daher nicht verwenden. In Apple Configurator 2 wird die Datei deshalb ohne Signatur gesichert. Wird das Feld Payload Inhalt geleert, kann erneut eine Datei ausgewählt werden.

Im Feld Payload Inhalt können Benutzer-, Geräte- und Zertifikatsplatzhalter verwendet werden. Die verfügbaren Platzhalter werden unterhalb des Formulars angezeigt und beim Übertragen auf das Gerät ersetzt, siehe Erweiterte Platzhalter →.

Pro Richtlinie können mehrere Apple-Configurator-2-Konfigurationen angelegt werden. Auf diese Weise lassen sich mehrere Konfigurationstypen auf getrennte Konfigurationen verteilen.

Anforderungen an die Datei

Für Version 26.4.0

Beim Speichern wird der Inhalt geprüft. Die Datei muss folgende Bedingungen erfüllen:

- Auf der obersten Ebene sind die Schlüssel `PayloadType`, `PayloadVersion` (als Zahl), `PayloadIdentifier`, `PayloadUUID` und `PayloadDisplayName` vorhanden.
- `PayloadContent` enthält genau einen Konfigurationstyp. Zusätzlich dürfen Zertifikat-Payloads enthalten sein.

Dateien, die sich nicht auslesen lassen, denen einer dieser Schlüssel fehlt, die keinen Payload oder mehrere Konfigurationstypen enthalten, werden beim Speichern abgelehnt.

> Mit übertragen werden nur Zertifikate im Format PKCS#12 (`com.apple.security.pkcs12`). PKCS#1-Zertifikate (`com.apple.security.pkcs1`) werden bei der Prüfung zwar akzeptiert, aber nicht an das Gerät übertragen. Andere Zertifikate wie Root-Zertifikate (`com.apple.security.root`) zählen als eigener Konfigurationstyp. Zusammen mit einer weiteren Konfiguration führen sie zu einem Fehler beim Speichern und werden daher in einer eigenen Konfiguration hinterlegt.
>
> Die eigentliche Konfiguration muss in `PayloadContent` an erster Stelle stehen. Enthält die Datei mehrere Payloads desselben Typs, wird nur der erste auf das Gerät übertragen.

Enthält die Datei einen Konfigurationstyp, den Relution auch als eigene, nur einmal pro Richtlinie zulässige Konfiguration anbietet, lässt sich diese Konfiguration in derselben Richtlinie nicht mehr hinzufügen. Unter tvOS betrifft das:

Payload-Typ in der Datei	Gesperrte Konfiguration
`com.apple.airplay.security`	AirPlay-Sicherheit →
`com.apple.conferenceroomdisplay`	Konferenzraum →
`com.apple.applicationaccess`	Restriktionen
`com.apple.app.lock`	Einzel-App-Modus

Umgekehrt wird eine solche Datei beim Speichern abgelehnt, wenn die Richtlinie die entsprechende Konfiguration oder eine weitere aktive Apple-Configurator-2-Konfiguration mit demselben Payload-Typ bereits enthält.

Beispiel

Die folgende Datei überträgt eine WLAN-Verbindung (`com.apple.wifi.managed`). SSID, Passwort, Bezeichner und UUIDs sind Beispielwerte und werden durch eigene Werte ersetzt. Jede `PayloadUUID` muss eindeutig sein.

Für Version 26.4.0

```xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
 <key>PayloadContent</key>
 <array>
  <dict>
   <key>AutoJoin</key>
   <true/>
   <key>EncryptionType</key>
   <string>WPA2</string>
   <key>HIDDEN_NETWORK</key>
   <false/>
   <key>Password</key>
   <string>WLAN-Passwort</string>
   <key>PayloadDisplayName</key>
   <string>WLAN</string>
   <key>PayloadIdentifier</key>
   <string>com.example.wifi.payload</string>
   <key>PayloadType</key>
   <string>com.apple.wifi.managed</string>
   <key>PayloadUUID</key>
   <string>8D2E4C1A-3B5F-4A7E-9C6D-1F0B2A3C4D5E</string>
   <key>PayloadVersion</key>
   <integer>1</integer>
   <key>SSID_STR</key>
   <string>Firmen-WLAN</string>
  </dict>
 </array>
 <key>PayloadDescription</key>
 <string>WLAN-Konfiguration für Apple-Geräte</string>
 <key>PayloadDisplayName</key>
 <string>WLAN</string>
 <key>PayloadIdentifier</key>
 <string>com.example.wifi</string>
 <key>PayloadOrganization</key>
 <string>Beispiel GmbH</string>
 <key>PayloadType</key>
 <string>Configuration</string>
 <key>PayloadUUID</key>
 <string>4A7B1C2D-5E6F-4890-A1B2-C3D4E5F60718</string>
 <key>PayloadVersion</key>
 <integer>1</integer>
</dict>
</plist>
```

Überwachter Modus entfernen

Hin und wieder kann es notwendig sein, Apple-Geräten, welche im überwachten Modus (Supervised Mode) betrieben werden, diesen Modus zu entziehen.

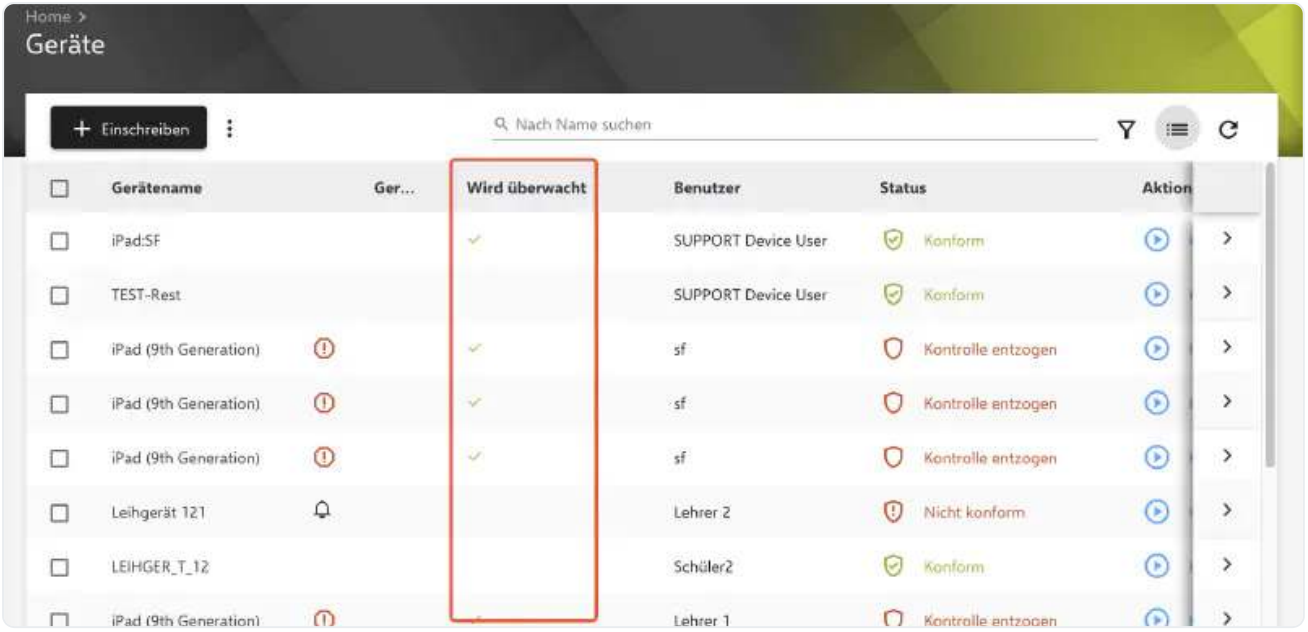
> Für iOS- und tvOS-Geräte kann dieser Zustand rückgängig gemacht werden. macOS-Geräte hingegen können ab Version 11 nur noch im überwachten Modus betrieben werden.

Überwachte Geräte identifizieren

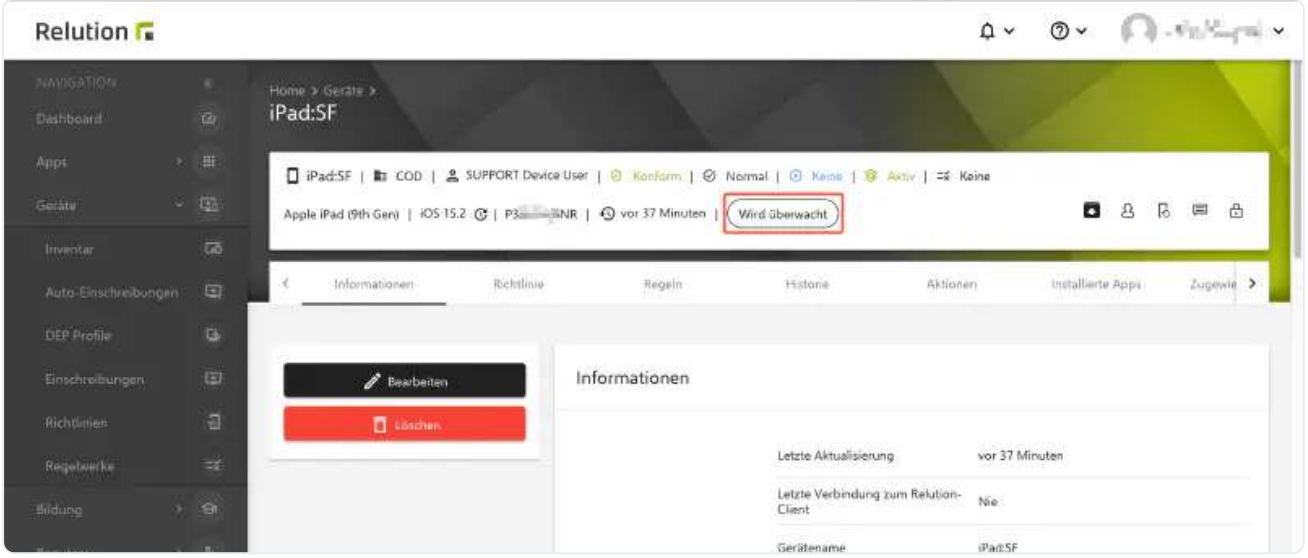
Überwachte Geräte lassen sich wie folgt ausfindig machen:

Für Version 26.4.0

1. Im Inventar die Spalte Wird überwacht einblenden. Die entsprechenden Geräte sind mit einem Haken markiert. Alternativ lässt sich die Liste über den gleichnamigen Filter Wird überwacht eingrenzen.



2. In den Gerätedetails lässt sich der Status über die entsprechende Badge Wird überwacht in der Infobox ablesen.



Über den Apple Configurator eingeschriebene Geräte

Durch diesen Vorgang wird auch das MDM-Profil von den Geräten entfernt, sodass sie im Anschluss nicht mehr verwaltet werden können, ohne sie erneut einzuschreiben. Zudem werden alle Apps und Daten von den Geräten entfernt.

Die Geräte lassen sich mit einer der folgenden Möglichkeiten zurücksetzen:

1. Eine Gerät auf Werkszustand zurücksetzen-Aktion an die Geräte schicken.
2. Am Gerät selbst zurücksetzen: auf iPhone und iPad unter `Einstellungen` → `Allgemein` → `iPhone/iPad übertragen/zurücksetzen` → `Alle Inhalte & Einstellungen löschen`, auf Apple TV unter `Einstellungen` → `System` → `Zurücksetzen`.
3. Geräte an einen Mac Computer anschließen und die Anwendung Apple Configurator 2 öffnen. Rechtsklick auf die Geräte machen und Erweitert und dort Alle Inhalte & Einstellungen löschen wählen.

Die Aktion Return to Service eignet sich nicht zum Entfernen des überwachten Modus: Sie setzt das Gerät zwar zurück, schreibt es anschließend aber automatisch wieder ein (siehe Verfügbare Aktionen →).

Per ADE über Apple School/Business Manager eingeschriebene Geräte

Sind Geräte über die Automatische Geräteregistrierung (ADE, im Portal: DEP) im Apple School/Business Manager zum MDM-System hinzugefügt worden, muss die Verknüpfung dort rückgängig gemacht werden, da sich die Geräte sonst nach dem Zurücksetzen auf Werkseinstellungen immer wieder automatisch bei dem MDM-System melden und erneut in den überwachten Modus versetzt werden. Das gilt auch für Geräte, die über einen autorisierten Händler hinzugefügt wurden.

1. Im Apple School/Business Manager einloggen und auf Geräte klicken.
2. Das entsprechende Gerät auswählen und auf der rechten Seite auf Gerätezuweisung bearbeiten klicken.
3. Auf Zuweisung aufheben klicken.
4. Das Gerät auf Werkseinstellungen zurücksetzen.

Für Version 26.4.0

ADE-Geräte, die nachträglich über den Apple Configurator hinzugefügt wurden

Das Entfernen des überwachten Modus bei Geräten, die über den Apple Configurator zum Apple School/Business Manager hinzugefügt wurden, funktioniert analog zu den über einen autorisierten Händler eingeschriebenen ADE-Geräten.

> Jedoch können Endanwender innerhalb der ersten 30 Tage nach Hinzufügen der Geräte zur Automatischen Geräteregistrierung (ADE) das MDM-Profil auf den Geräten manuell entfernen. Dadurch geht die MDM-Einschreibung sowie auch der überwachte Modus verloren.

Konferenzraum-Konfiguration

Für Apple TV kann der Bildschirm eines AirPlay-unterstützten Gerätes freigegeben werden, ohne dass Benutzer Zugriff auf andere Funktionen des Apple TVs erhalten. Wenn das Konferenzraum-Display eingeschaltet wird, zeigt es Netzwerkdetails und Anweisungen zur Verbindung mit Apple TV über AirPlay an, ergänzt um die in der Konfiguration hinterlegte Nachricht.

Die Konfiguration Konferenzraum steht nur in tvOS-Richtlinien zur Verfügung und kann je Richtlinie einmal hinzugefügt werden.

Konferenzraum für Apple TV einrichten

1. Die Konfiguration wird im Relution-Portal über `Geräte` → `Richtlinien` → `{tvOS-Richtlinie}` → `Hinzufügen` → `Konferenzraum` → `Details hinzufügen` angelegt. Konfigurationen lassen sich nur in einer Entwurfsversion der Richtlinie hinzufügen.

2. Im Abschnitt Allgemein wird im Pflichtfeld Nachricht der Text eingetragen, der auf dem Konferenzraum-Bildschirm des Apple TV angezeigt wird. Der Text kann Benutzer- und Geräteplatzhalter enthalten (z. B. `${device.name}`), die in der Karte Verfügbare Platzhalter aufgeführt sind; sie werden bei der Übertragung an das Gerät durch die jeweiligen Werte ersetzt. Ohne Nachricht lässt sich die Konfiguration nicht speichern.

3. Anschließend muss die Richtlinie veröffentlicht werden, um sie Geräten zuweisen zu können.

tvOS-Geräte in Relution →

Für Version 26.4.0

AirPlay-Sicherheits-Konfiguration

AirPlay-Sicherheit verhindert das unbefugte Streaming auf Apple TV über AirPlay. Administratoren können somit kontrollieren, wer sich über die AirPlay-Funktionalität mit Apple TV verbinden kann. Es lässt sich entweder ein AirPlay-Passwort einrichten oder die Verbindung von Geräten in einem anderen Netzwerk mit dem Fernseher einschränken. AirPlay-Sicherheit kann auf Apple TVs mit tvOS 11 oder höher verwendet werden.

Konfiguration hinzufügen

Die Konfiguration wird im Relution-Portal über `Geräte` → `Richtlinien` → `{tvOS-Richtlinie}` → `Hinzufügen` → `AirPlay-Sicherheit` → `Details hinzufügen` angelegt. Konfigurationen lassen sich nur in einer Entwurfsversion der Richtlinie hinzufügen. AirPlay-Sicherheit steht nur in tvOS-Richtlinien zur Verfügung und kann je Richtlinie einmal hinzugefügt werden.

Verfügbare AirPlay-Sicherheits-Einstellungen

Für Version 26.4.0

- Zugang (Standard: Geräte in allen WLANs) – legt fest, aus welchem Netzwerk sich ein AirPlay-unterstütztes Apple-Gerät über AirPlay mit einem Apple TV verbinden kann. Folgende Optionen stehen zur Auswahl:
    - Geräte in allen WLANs: Erlaubt die Verbindung zwischen Apple TV und AirPlay-unterstützten Apple-Geräten in verschiedenen Netzwerken.
    - Geräte im selben WLAN: Erlaubt die Verbindung zwischen AirPlay-unterstützten Apple-Geräten und Apple TV, die sich im selben Netzwerk befinden (dasselbe WLAN oder Ethernet).
- Sicherheit (Standard: Einmaliger Code) – legt fest, wie die Verbindung abgesichert wird. Folgende Optionen stehen zur Auswahl:
    - Einmaliger Code: Beim Herstellen einer Verbindung zwischen einem Apple TV und einem AirPlay-unterstützten Apple-Gerät wird ein Code auf dem Fernsehbildschirm angezeigt, der auf dem AirPlay-unterstützten Apple-Gerät eingegeben wird, um das Streaming zu starten. Bei einer erneuten Verbindung zwischen denselben Geräten ist der Code nicht mehr erforderlich.
    - Code: Bei jedem Versuch, Inhalte über AirPlay zu streamen, wird ein Code auf dem Fernsehbildschirm angezeigt, der auf dem AirPlay-unterstützten Apple-Gerät eingegeben wird, um das Streaming zu starten.
    - Passwort: Für die Verbindung zwischen einem AirPlay-unterstützten Apple-Gerät und einem Apple TV wird ein festes AirPlay-Passwort verlangt. Bei Auswahl dieser Option erscheint in der Konfiguration das Pflichtfeld Passwort, in dem das AirPlay-Passwort hinterlegt wird; ohne Passwort lässt sich die Konfiguration nicht speichern. Beim Verbindungsaufbau fragt das Gerät nach diesem Passwort, nach Eingabe des Passworts aus der Richtlinie startet das Streaming. Im Gegensatz zu Einmaliger Code wird auf dem Fernseher kein Code angezeigt.

Anschließend muss die Richtlinie veröffentlicht werden, um sie Geräten zuweisen zu können.

tvOS-Geräte in Relution →

App Konformität

Die Installation von Apps aus Apps und Bücher (im Portal: VPP) auf Apple TV Geräten gestaltet sich dank der App Konformität-Richtlinie von Relution besonders unkompliziert. Diese Konfiguration ermöglicht eine einfache und zentrale Verteilung von Anwendungen auf eine Vielzahl von Geräten.

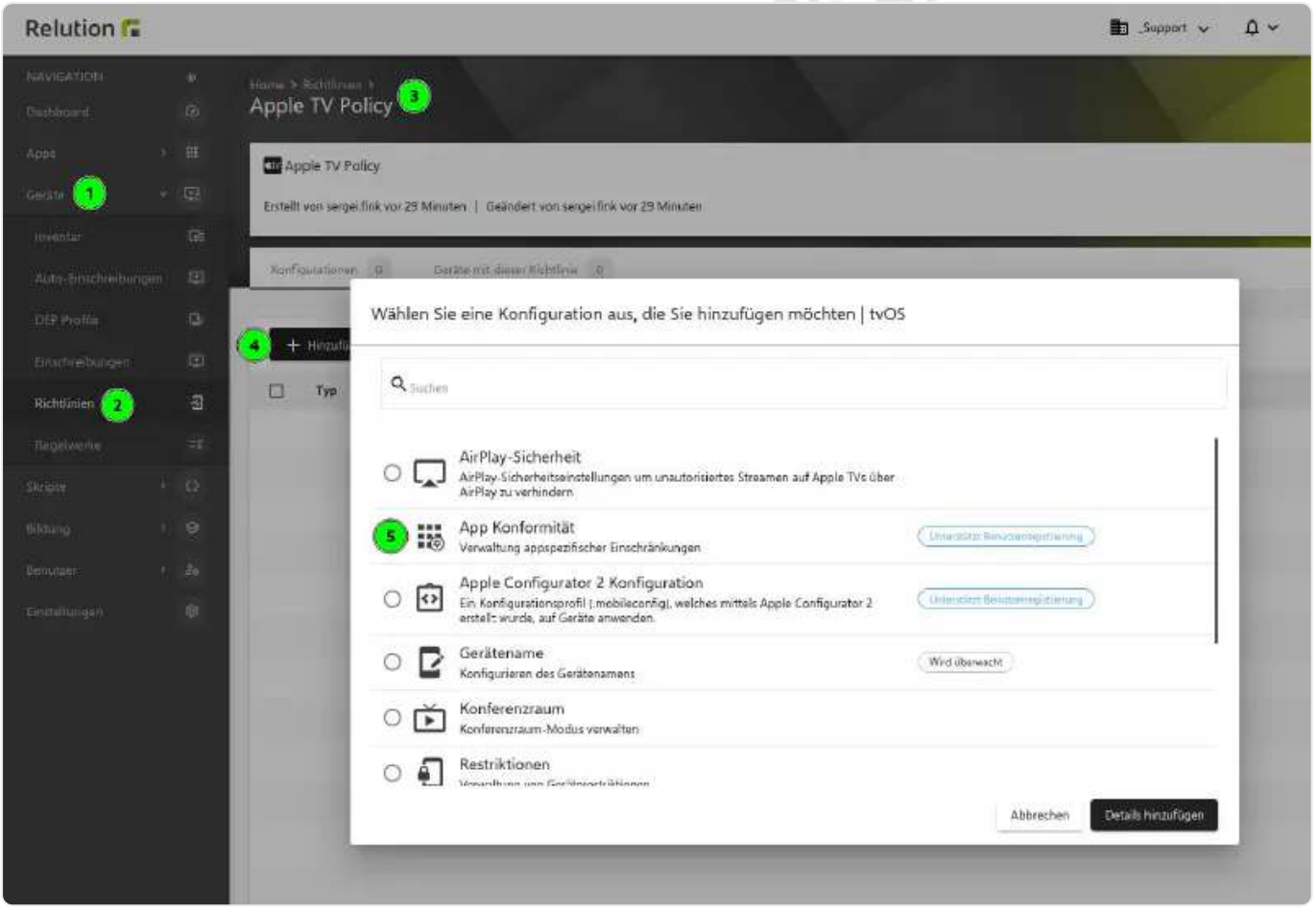
Um mit der Verteilung zu beginnen, ist lediglich Folgendes erforderlich:

- Ein Apple School- oder Apple Business-Konto.
- Die Einbindung des eigenen Tokens für Apps und Bücher → in Relution.
- Erworbene Lizenzen für die gewünschten Apps aus dem Apple School Manager (ASM) oder Apple Business Manager (ABM).

tvOS-Geräte in Relution →

Konfiguration der App Konformität

Die Verteilung von Apps auf Apple TV Geräten (analog zu iOS-Geräten) erfolgt über die Richtlinien-Konfiguration App Konformität. Sie wird unter `Geräte` → `Richtlinien` in einer tvOS-Richtlinie über Konfiguration hinzufügen ausgewählt und mit Details hinzufügen angelegt.



Ähnlich wie bei iOS-Geräten wird die Verfügbarkeit von Apps im Abschnitt Allgemein unter Listenart gesteuert: entweder als Sperrliste (Alle Apps in der folgenden Liste sind nicht erlaubt, Standard bei neuen Konfigurationen) oder als Positivliste (Alle Apps in der folgenden Liste sind erlaubt). Pro Konfiguration ist nur eine der beiden Listenarten aktiv. Die Apps werden im darunterliegenden Abschnitt Apps auf der Sperrliste bzw. Apps auf der Positivliste über Hinzufügen eingetragen.

Positiv- und Sperrliste werden nur auf betreuten (supervised) Geräten angewendet.

Positivliste (erlaubte Apps)

Mit der Positivliste wird explizit definiert, welche Apps auf den Geräten verfügbar sein dürfen. Zusätzlich stehen zwei Optionen zur Verfügung:

- Alle Auto-Deployments hinzufügen: Apps, die über Auto-Deployments an die Benutzer der Geräte verteilt werden, werden automatisch in die Positivliste aufgenommen.
- Lokale Sicherheitsabfrage-Dialoge erlauben (z.B. iCloud- oder Google-Login): Der Systemdialog für lokale Sicherheitsabfragen wird in die Positivliste aufgenommen, damit solche Abfragen nicht blockiert werden.

Für Version 26.4.0

Home > Richtlinien > srg.tvOS.handbuch >

App Konformität

App Konformität

Unterstützt Benutzerregistrierung

Abbrechen | Speichern

Allgemein

Listenart

- ○ Alle Apps in der folgenden Liste sind nicht erlaubt
- ◉ Alle Apps in der folgenden Liste sind erlaubt
  - ☑ Alle Auto-Deployments hinzufügen
  - ☐ Lokale Sicherheitsabfrage-Dialoge erlauben (z.B. iCloud- oder Google-Login)

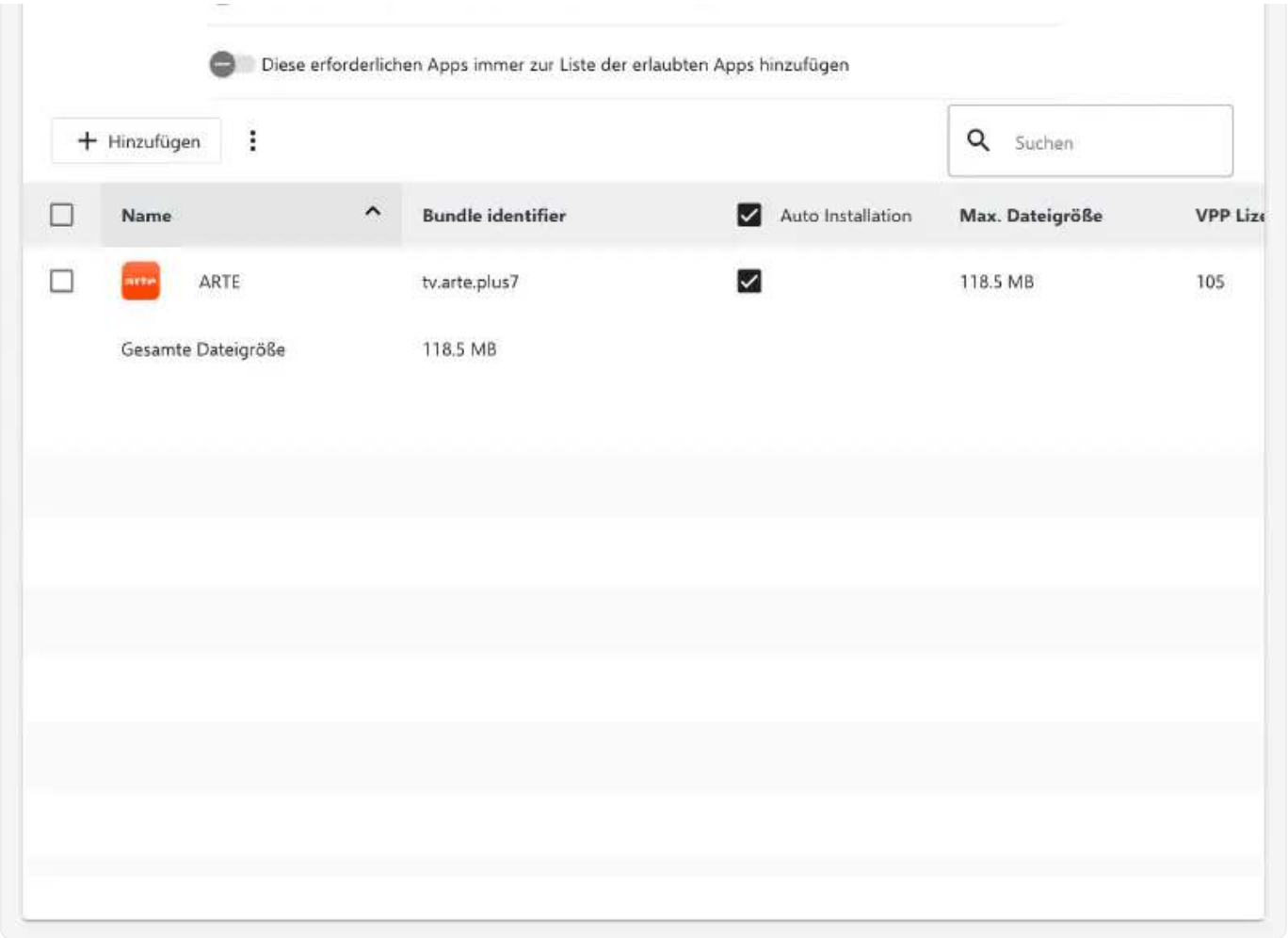
Apps auf der Positivliste

+ Hinzufügen ⋮ 🔍 Suchen

	Name	Bundle identifier
☐	Apple Podcasts	com.apple.podcasts
☐	Tips	com.apple.tips
☐	WWDC	com.apple.wwdc

Erforderliche Apps

⊖ Nicht länger erforderliche Apps automatisch deinstallieren



Sperrliste (blockierte Apps)

Die Sperrliste wird verwendet, um bestimmte Apps auf den tvOS-Geräten auszublenden oder zu sperren.

Für Version 26.4.0

Home > Richtlinien > srg.tvOS.handbuch >

App Konformität

App Konformität

Unterstützt Benutzerregistrierung

Abbrechen | Speichern

Allgemein

Listenart

- (●) Alle Apps in der folgenden Liste sind nicht erlaubt
- ( ) Alle Apps in der folgenden Liste sind erlaubt

Apps auf der Sperrliste

+ Hinzufügen

Suchen

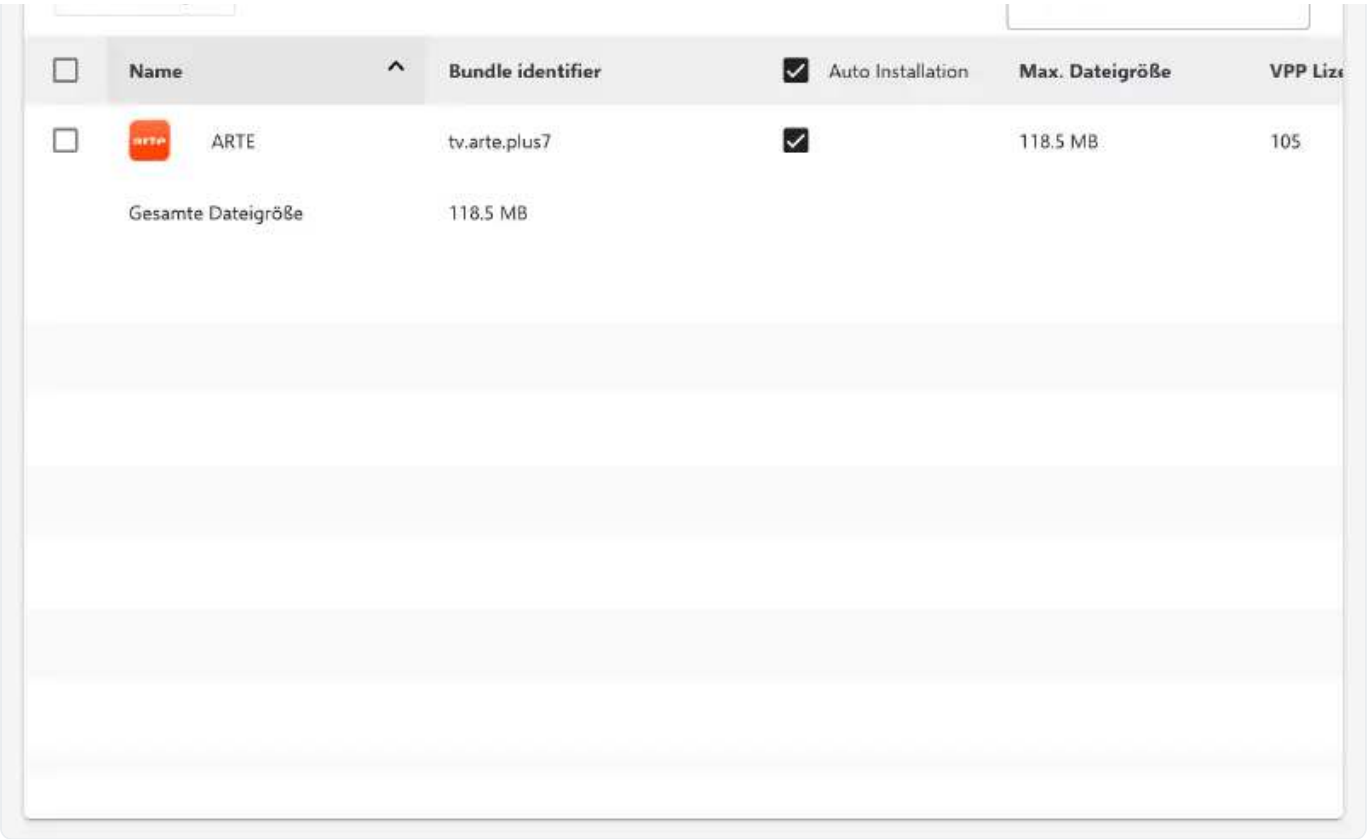
Name	Bundle identifier
Apple Podcasts	com.apple.podcasts
Tips	com.apple.tips
WWDC	com.apple.wwdc

Erforderliche Apps

- Nicht länger erforderliche Apps automatisch deinstallieren
- Diese erforderlichen Apps immer zur Liste der erlaubten Apps hinzufügen

+ Hinzufügen

Suchen

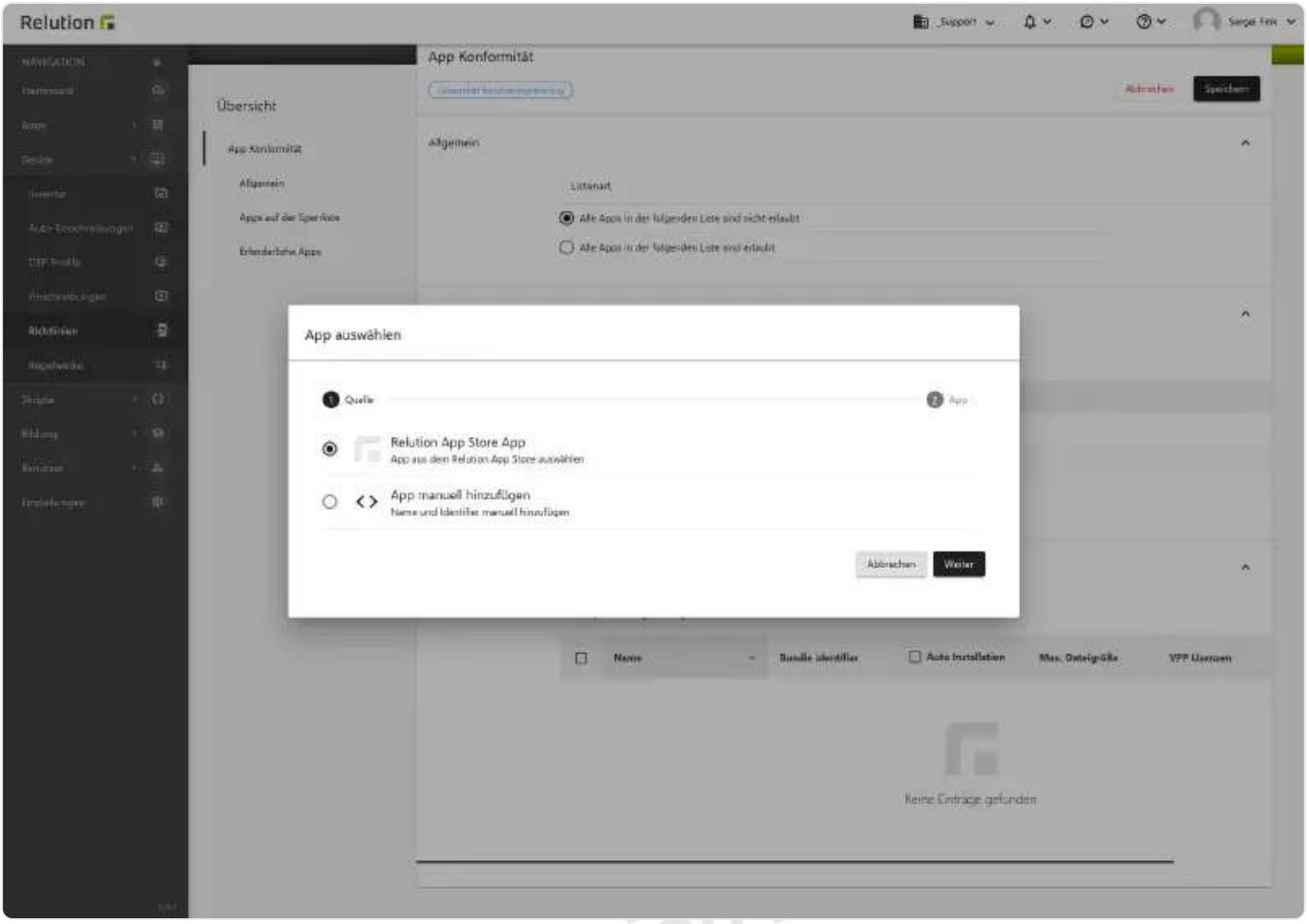


Erforderliche Apps

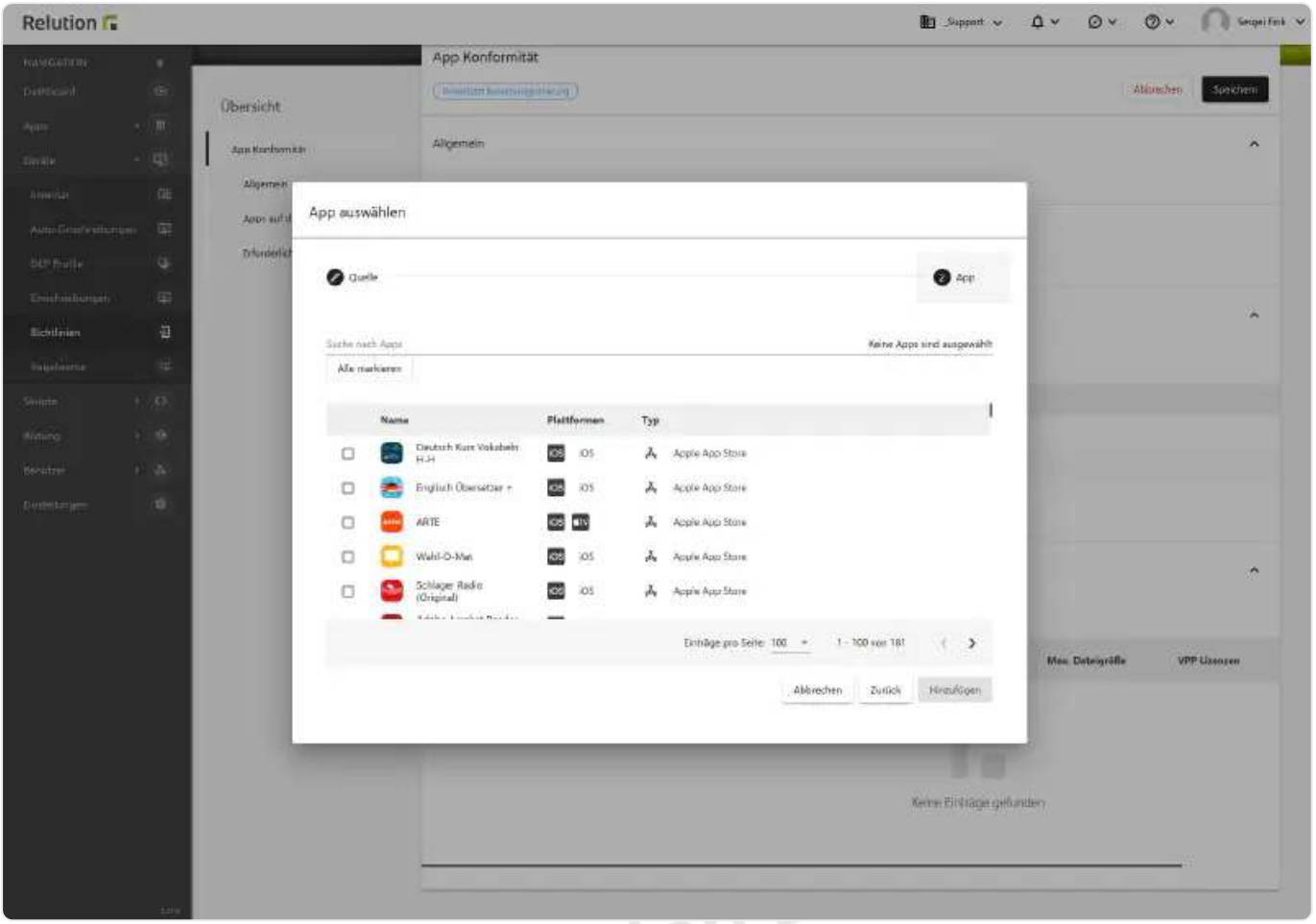
Für Version 26.4.0

Im Abschnitt Erforderliche Apps wird festgelegt, welche Anwendungen verpflichtend auf den Geräten installiert werden sollen. Über Hinzufügen stehen folgende Quellen zur Verfügung (dieselben gelten auch für Positiv- und Sperrliste):

- Relution App Store App: Auswahl von Apps der Plattformen tvOS und iOS aus dem Relution App Store. Für erforderliche Apps werden native, selbst hochgeladene Apps sowie öffentliche Apps angeboten, für die in der Organisation Lizenzen aus Apps und Bücher vorhanden sind. Eine direkte Suche im öffentlichen Apple App Store gibt es für tvOS nicht.
- App manuell hinzufügen: Eintrag einer App über Name und Interner Name (Bundle-ID).


Relution
App Konformität
Übersicht
App Konformität
Allgemein
Apps auf der Sperrliste
Erforderliche Apps
Allgemein
Listenart
Alle Apps in der folgenden Liste sind nicht erlaubt
Alle Apps in der folgenden Liste sind erlaubt
App auswählen
Quelle
App
Relution App Store App
App aus dem Relution App Store auswählen
App manuell hinzufügen
Name und Identifier manuell hinzufügen
Abbrechen
Weiter
Name
Bundle identifier
Auto Installation
Max. Dateigröße
VPP Lizenzen
Keine Einträge gefunden

Für Version



Ist eine erforderliche App nicht auf dem Gerät installiert, gilt das Gerät als nicht konform. Aktiv installiert wird die App nur, wenn in der Spalte Auto Installation das Häkchen gesetzt ist; beim Hinzufügen einer App ist es standardmäßig gesetzt. Die Spalten VPP Lizenzen und Verfügbare VPP Lizenzen zeigen die vorhandenen und die noch freien Lizenzen je App.

Oberhalb der Liste stehen zwei Schalter zur Verfügung:

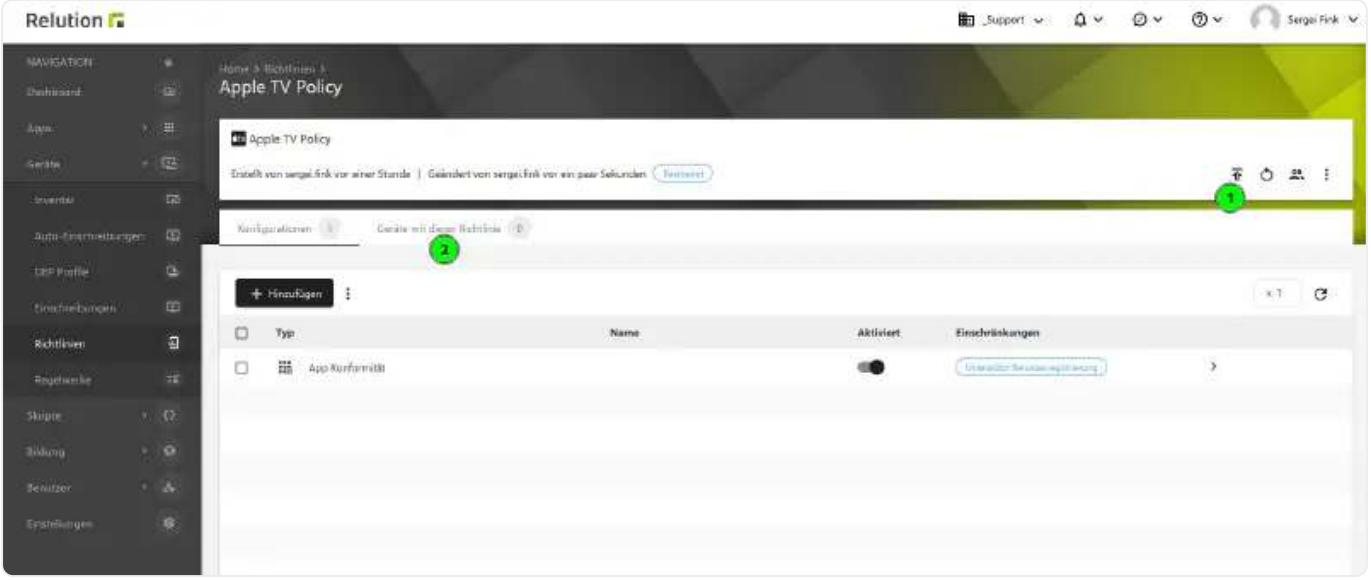
- Nicht länger erforderliche Apps automatisch deinstallieren: Wird eine automatisch installierte erforderliche App aus der Konfiguration entfernt oder die Konfiguration vom Gerät entfernt, wird die App deinstalliert. Bei neuen Konfigurationen ist der Schalter ausgeschaltet.
- Diese erforderlichen Apps immer zur Liste der erlaubten Apps hinzufügen: Wird durch diese oder eine andere Richtlinie eine Positivliste für das Gerät konfiguriert, werden die erforderlichen Apps dort ergänzt.

Beim Speichern wird geprüft, ob sich die Listen widersprechen: Eine erforderliche App darf nicht auf der Sperrliste stehen. Ist bei einer Positivliste der zweite Schalter ausgeschaltet, müssen alle erforderlichen Apps auch auf der Positivliste eingetragen sein.

Auch iOS-Apps können unter tvOS genutzt werden, sofern sie für tvOS geeignet sind. Nicht kompatible Apps werden zwar auf dem Gerät installiert, verschwinden jedoch nach dem Installationsvorgang wieder und sind nicht verfügbar.

> Öffentliche Apps ohne Lizenzen aus Apps und Bücher sowie Weblinks (Browser) können nicht auf tvOS-Geräten installiert werden.

Sobald die Konfiguration abgeschlossen ist, kann sie gespeichert, veröffentlicht und den entsprechenden Geräten zugewiesen werden.



Für Version 26.4.0

App Verteilung

Unternehmen entscheiden sich immer öfter, bestimmte Arbeitsprozesse mit einer mobilen App zu unterstützen. Neben vielen anderen konzeptionellen Fragen, stellt sich schnell die Frage, wie diese App an die Nutzer verteilt werden soll. Oftmals sieht der Anwendungsfall so aus, dass nicht nur Mitarbeiter, sondern auch externe Personen die App bekommen sollen – dazu können zum Beispiel Dienstleister, Partner oder Kunden gehören. Diese App ist in den meisten Fällen auch explizit nicht für einen breiten Kundenkreis gedacht, sondern richtet sich an ausgewählte professionelle Benutzer. Folgende Abschnitte sollen bei der Entscheidung helfen, die beste Distributionsmethode zu finden.

Auf Apple-TV-Geräte gelangen Apps aus Relution ausschließlich über die Geräteverwaltung (MDM). Eine Installation durch Benutzer über eine Webseite, einen Deeplink oder eine Store-App ist auf tvOS nicht möglich, Web-Clips werden an tvOS-Geräte nicht verteilt. In Relution werden tvOS-Apps unter der Plattform iOS geführt (Native Apps verwalten →). Apps aus dem App Store lassen sich auf Apple TV nur mit einer Lizenz aus Apps und Bücher (im Portal: VPP) installieren (App-Store-Apps verwalten →, App Konformität →). Die folgenden Abschnitte beschreiben die Verteilwege allgemein für iOS und Android.

Verteilung über öffentliche App Stores

Für Version 26.4.0

Apple und Google stellen zur Verteilung von Apps jeweils eine Infrastruktur zur Verfügung. Bei Apple werden Apps für Endanwender über den Apple App Store bereitgestellt. Auf jedem iOS Gerät ist die App Store App vorinstalliert.

Die Verwaltung und die Veröffentlichung von Apps erfolgt hierfür über das Developer-Portal und App Store Connect. Bei Google werden Apps für Endanwender über den Play Store bereitgestellt. Auf jedem Android Gerät ist die App Play Store vorinstalliert.

Die Verwaltung und die Veröffentlichung von Apps erfolgt hierfür über das Developer-Portal. Apple und Google definieren die Rahmenbedingungen für die Veröffentlichung von Apps über ihre Systeme.

Sofern ein Gerät über ein MDM System verwaltet wird, kann die Store App für den Benutzer auch gesperrt werden und steht somit u.U. für den Endanwender nicht zur Verfügung.

Verteilung über Apple App Store – Vorteile

- Apps stehen für Endanwender über den Standard-Mechanismus von Apple zur Verfügung
- Apps müssen nicht nach einem Jahr mit einem aktualisierten Provisioning Profile neu signiert und bereitgestellt werden
- Apps können – sofern notwendig – selektiv für einzelne Länder freigeschaltet bzw. gesperrt werden
- Apps können – sofern gewünscht – in definierten Strukturen kostenpflichtig angeboten werden (Apple verlangt hierfür eine prozentuale Provisionsgebühr von 15%)
- Apple stellt die Infrastruktur für die Verteilung und Abrechnung bereit

Verteilung über Apple App Store – Nachteile

- Benutzer benötigen eine Apple-ID auf den Endgeräten, um Apps aus dem Apple App Store zu installieren
- Bei Unternehmenskunden mit verwalteten Geräten ist der Apple App Store u.U. per MDM gesperrt
- Es müssen sämtliche Apple Vorgaben eingehalten werden, wie bspw. Unterstützung neuer Geräteklassen wie iPhone X
- Apple behält sich in einem Review vor, die App nicht zu veröffentlichen bzw. nachträglich zu entfernen
- Durch den Review kann es zu Verzögerungen von bis zu 10 Tagen kommen (derzeit liegt die durchschnittliche Review Dauer bei etwa 3 Arbeitstagen)
- Apps können nur stark eingeschränkt ausgewählten Benutzergruppen bereitgestellt werden

Verteilung über Google Play Store – Vorteile

- Apps stehen für Endanwender über den Standard-Mechanismus von Google zur Verfügung
- Apps können – sofern notwendig – selektiv für einzelne Länder freigeschaltet bzw. gesperrt werden
- Apps können – sofern gewünscht – in definierten Strukturen kostenpflichtig angeboten werden (Google verlangt hierfür eine prozentuale Provisionsgebühr von 15%)
- Google stellt die Infrastruktur für die Verteilung und Abrechnung bereit

Verteilung über Google Play Store – Nachteile

- Benutzer benötigen einen Google Account, um Apps aus dem Play Store zu installieren
- Bei Unternehmenskunden mit verwalteten Geräten ist der Play Store u.U. per MDM gesperrt
- Es müssen sämtliche Google Vorgaben eingehalten werden – wie bspw. die Cordova Version
- Google behält sich nach automatisierten App-Scans vor, die App auch nachträglich aus dem Store zu entfernen
- Durch technische Scans kann sich die Veröffentlichung von Apps um wenige Stunden verzögern
- Apps können nur stark eingeschränkt ausgewählten Benutzergruppen bereitgestellt werden

Für Version 26.4.0

Verteilung über Beta-Programme der öffentlichen App Stores

Apple und Google bieten zusätzlich zur Verteilung von öffentlichen Apps jeweils auch ein Beta-Testprogramm zur Verfügung. Bei Apple werden Apps für einen Beta-Test für Endanwender über die TestFlight App bereitgestellt. Auf iOS Geräten kann diese App aus dem App Store App nachinstalliert werden.

Die Verwaltung und die Veröffentlichung von Apps erfolgen hierfür über das Developer-Portal und App Store Connect im Bereich TestFlight. Bei Google werden Apps für einen Alpha- oder Beta-Test über den Play Store bereitgestellt. Auf jedem Android Gerät ist der Play Store vorinstalliert.

Die Verwaltung und die Veröffentlichung von Apps erfolgen hierfür über das Developer-Portal im Bereich Alpha- und Beta-Testing. Apple und Google definieren die Rahmenbedingungen für die Veröffentlichung von Apps über ihre Systeme.

Verteilung über Apple Testflight – Vorteile

- Apps stehen für Benutzer über einen von Apple bereitgestellten Mechanismus zur Verfügung
- Apps können selektiv für einzelne Benutzer freigeschaltet werden
- Apple stellt die Infrastruktur für die Verteilung und Abrechnung bereit

Verteilung über Apple Testflight – Nachteile

- Benutzer benötigen eine Apple-ID, um Apps aus dem Apple App Store zu installieren
- Für die Installation der App ist die einmalige Installation der TestFlight App notwendig
- Apple behält sich in einem „reduzierten“ Review vor, die App nicht zu veröffentlichen
- Durch den Review kann es zu Verzögerungen von bis zu 10 Tagen kommen (derzeit liegt die durchschnittliche Review Dauer bei etwa zwei Arbeitstagen)
- Die Signatur von Apps läuft nach 90 Tagen ab

Der TestFlight-Dienst ist primär für eine kurze Testphase vor der Veröffentlichung einer iOS App gedacht. Für einen dauerhaften Betrieb ist die Lösung wegen der kurzen Gültigkeit der Signatur nicht geeignet.

Verteilung über Google Alpha- und Beta-Testing – Vorteile

- Apps stehen für Benutzer über einen von Google bereitgestellten Mechanismus zur Verfügung
- Apps können selektiv für einzelne Benutzer freigeschaltet werden
- Google stellt die Infrastruktur für die Verteilung und Abrechnung bereit

Verteilung über Google Alpha- und Beta-Testing – Nachteile

- Benutzer benötigen eine Google-ID, um Apps aus dem Play Store zu installieren
- Bei Unternehmenskunden mit verwalteten Geräten ist der Play Store u.U. per MDM gesperrt

Für Version 26.4.0

Verteilung über internen Enterprise App Store

Apple und Google bieten neben der Verteilung von Apps über die jeweiligen öffentlichen Stores auch Mechanismen zur internen Verteilung von Apps primär für Unternehmen. Bei Apple wird als Voraussetzung das Apple Enterprise Programm und ein Enterprise App Store wie bspw. Relution benötigt.

Die Apps werden für Endanwender über eine separate App Store App oder eine mobile Webseite bereitgestellt. Hochgeladen und verwaltet werden die Apps im Enterprise App Store (in Relution unter `Apps` → `App Store`). Bei Apple werden lediglich Zertifikate und Provisioning Profiles im Apple Developer-Portal erstellt.

Die Verteilung der Apps erfolgt über den jeweiligen Anbieter des Enterprise App Store. Bei Google können Apps über einen Webservice zum Download und zur Installation bereitgestellt werden.

Für spezielle Geräte wie bspw. Samsung können optimierte Installations- und Verteilungsmechanismen genutzt werden. Apple und Google definieren die Möglichkeiten für die Verteilung von Apps parallel zu ihren Systemen.

Verteilung von iOS Apps über Enterprise App Store – Vorteile

- Apps können an ausgewählte Benutzergruppen bspw. als Deeplink oder nach Anmeldung mit zuvor konfigurierten Benutzernamen und Passwort verteilt werden
- Benutzer benötigen keine Apple-ID, um Apps aus einem internen Enterprise App Store zu installieren
- Es müssen nicht sämtliche Apple Vorgaben eingehalten werden
- Die Veröffentlichung von App Updates wird nicht durch ein Review von Apple verzögert
- Einige Enterprise App Stores (wie bspw. Relution) sind auch ohne Geräteverwaltung (MDM) nutzbar
- Ein existierendes Benutzerverwaltungssystem (ActiveDirectory/LDAP) kann angeschlossen werden, so dass die Nutzer keine neuen Zugangsdaten benötigen

Verteilung von iOS Apps über Enterprise App Store – Nachteile

- Apps stehen für Endanwender über einen speziellen Mechanismus zur Verfügung, der von Apple genehmigt ist, jedoch eine initiale Konfiguration durch den Benutzer benötigt (siehe hier →)
- Apps müssen nach einem Jahr mit einem aktualisierten Provisioning Profile neu signiert und als neue Version in Relution hochgeladen werden.
- Die Infrastruktur für die Verteilung kann bspw. als Cloud-Dienst oder On-Premise bereitgestellt werden
- Die Verteilung von Apps darf gemäß Apple Richtlinien nur an Mitarbeiter, Interessenten und Partner, aber vor allem an einen bekannten Nutzerkreis, erfolgen

Verteilung von Android Apps über Enterprise App Store – Vorteile

- Apps können an ausgewählte Benutzergruppen bspw. als Deeplink oder nach Anmeldung mit zuvor konfigurierten Benutzernamen und Passwort verteilt werden
- Benutzer benötigen keine Google-ID, um Apps aus einem internen Enterprise App Store zu installieren
- Es müssen nicht sämtliche Google Vorgaben eingehalten werden
- Die Veröffentlichung von App Updates wird nicht durch technische Scans von Google verzögert
- Einige Enterprise App Stores (wie bspw. Relution) sind auch ohne Geräteverwaltung (MDM) nutzbar
- Ein existierendes Benutzerverwaltungssystem (ActiveDirectory/LDAP) kann angeschlossen werden, so dass die Nutzer keine neuen Zugangsdaten benötigen

Verteilung von Android Apps über Enterprise App Store – Nachteile

- Apps stehen für Endanwender über einen speziellen Mechanismus zur Verfügung, der von Google genehmigt ist, jedoch eine initiale Konfiguration durch den Benutzer benötigt
- Die Infrastruktur für die Verteilung muss bspw. als Cloud-Dienst bereitgestellt werden

Für Version 26.4.0

Native Apps verwalten

Mit Relution lassen sich auch native Apps für tvOS verteilen und mit einem Release-Management versehen. Eine eigene tvOS-Plattform gibt es dafür nicht: tvOS-Apps werden als `.ipa`-Datei hochgeladen und in Relution unter der Plattform iOS geführt. Apple-TV-Geräte erhalten sie über diese iOS-App. Voraussetzung ist, dass die App für tvOS erstellt wurde.

Zu einer App können mehrere Versionen in unterschiedlichen Freigabestatus vorliegen, etwa eine Version 1.0 im Status Produktiv und eine Version 1.1, die im Status Entwicklung oder Prüfung vorbereitet und geprüft wird. Auf Apple-TV-Geräte verteilt wird immer die Version im Status Produktiv. Zu Beginn wird deshalb die Version 1.0 in Relution hochgeladen und in den Status Produktiv versetzt.

Neue App anlegen

Native Apps werden im Menü unter `Apps` → `App Store` angelegt. Die Schaltfläche Hinzufügen öffnet den Dialog Neue Apps hinzufügen. Unter Quelle wird Native App gewählt.

Nach einem Klick auf Weiter wird über Datei wählen die Datei der App (`.ipa`) hochgeladen. Details hinzufügen öffnet anschließend das App-Formular.

> Die Größe der Datei ist zu beachten. Bei großen Apps kommt es eventuell zu Problemen, falls die Datenbank oder der Reverse Proxy dies nicht zulässt. In diesem Fall muss die Konfiguration angepasst werden.

Für Version 26.4.0

Im App-Formular wird der Freigabestatus angegeben und die App über Speichern angelegt. Mit Ausnahme des Status Archiv kann sich in jedem Freigabestatus nur eine Version der App befinden.

Im Abschnitt Rechte wird festgelegt, wer die App im Relution-Portal bearbeiten darf:

- Eigentümer dürfen alle Operationen auf die App in jedem Status anwenden.
- Prüfer dürfen die App bearbeiten und Versionen in den Status Produktiv oder Entwicklung verschieben.
- Entwickler dürfen Versionen im Status Entwicklung hochladen, bearbeiten und in den Status Prüfung oder ins Archiv verschieben.
- Benutzer dürfen Versionen im Status Produktiv herunterladen, bewerten und kommentieren.

Unabhängig von diesen Rechten können Administratoren die App über das Relution-Portal an Geräte verteilen.

Native Apps auf Apple TV verteilen

Für tvOS gibt es keinen Relution Agent und damit keinen Self-Service-Store auf dem Gerät. Benutzer können native Apps nicht selbst auf dem Apple TV installieren. Die Verteilung erfolgt ausschließlich über das Relution-Portal:

- über die Geräteaktion Relution Store App bereitstellen (Aktionen →),
- unter Erforderliche Apps in der Konfiguration App Konformität, sofern in der Spalte Auto Installation das Häkchen gesetzt ist (App Konformität →),
- in der App-Ansicht unter Geräte mit dieser App über die Schaltfläche App aktualisieren für Geräte, auf denen die App bereits installiert ist.

Verteilt wird dabei immer die Version im Status Produktiv. Eine Version im Status Entwicklung oder Prüfung lässt sich über das Relution-Portal nicht auf ein Apple TV verteilen. Auto-Deployments berücksichtigen für tvOS nur öffentliche Apps, keine nativen Apps.

App updaten

Soll für die App eine neue Version vorbereitet werden, kann diese vorab in den Status Entwicklung oder Prüfung versetzt werden. Vorher muss die neue Version über die Schaltfläche Neue Version ausgewählt und hochgeladen werden.

Für die neue Version lässt sich im Feld Go-Live Datum ein Termin hinterlegen. Automatisch in den Status Produktiv wechselt die Version an diesem Tag nur, wenn ein App-Freigabeprozess → aktiv ist und die Version im Status Prüfung alle Freigabeschritte durchlaufen hat. Ohne aktiven Freigabeprozess dient das Datum nur als Wunschtermin, und die Version wird manuell in den Status Produktiv versetzt (siehe unten).

In den App-Eigenschaften können beide Versionen eingesehen werden.

Manuelle Produktivnahme der neuen Version

Im Relution-Portal können die jeweiligen Versionen angeschaut und konfiguriert werden. Liegt die neue Version im Status Prüfung, wird sie durch einen Klick auf die Schaltfläche Produktiv in diesen Status verschoben. Liegt sie noch in Entwicklung, erfolgt der Wechsel über `Verschieben` → `Produktiv`. Befindet sich bereits eine Version im Status Produktiv, wird diese automatisch ins Archiv verschoben.

Für Version 26.4.0

> Die App wird auf den Geräten nicht automatisch aktualisiert. Das Update wird durch die Administratoren über die Geräteaktion Relution Store App bereitstellen oder in der App-Ansicht unter Geräte mit dieser App über die Schaltfläche App aktualisieren ausgelöst.

App-Store-Apps verwalten

Mit Relution ist es möglich, Apps aus dem Apple App Store auf Geräten zu verteilen. Hierzu muss immer eine App-Lizenz erworben werden – unabhängig davon, ob die App kostenpflichtig ist oder nicht. Auf iOS-Geräten kann eine App-Lizenz entweder über Apps und Bücher (im Portal: VPP) erworben oder über eine auf dem Gerät angemeldete Apple-ID bezogen werden. Auf Apple-TV-Geräten lassen sich Apps aus dem App Store dagegen nur mit einer Lizenz aus Apps und Bücher installieren, der Weg über eine Apple-ID steht hier nicht zur Verfügung. Wie Apps und Bücher eingerichtet wird, ist dem entsprechenden Kapitel → zu entnehmen.

Apps, die im Apple School/Business Manager erworben werden, werden automatisch nach Relution synchronisiert (ab Version 5.10). Die Apps werden in Relution im Status Produktiv veröffentlicht und können im Anschluss auf Geräte verteilt werden. Apps, die nicht allen Benutzern zugänglich gemacht werden sollen, können auch manuell einem anderen Freigabestatus zugewiesen werden. Es kann jederzeit auch eine App manuell zum Relution App Store hinzugefügt werden. Für diese Apps sind jedoch keine Lizenzen aus Apps und Bücher automatisch verfügbar. Auf Apple-TV-Geräten lassen sie sich erst installieren, wenn für sie Lizenzen aus Apps und Bücher vorhanden sind. Es ist möglich, diese Lizenzen nachträglich zu beschaffen.

Apps verteilen

Regulär werden Apps aus dem App Store über die Richtlinien-Konfiguration App Konformität → als erforderliche Apps auf Apple-TV-Geräte verteilt.

Einzelnen Geräten wird eine App über die Geräteaktion Relution Store App bereitstellen zugewiesen. Dort stehen neben nativen Apps auch die Apps aus dem App Store zur Auswahl, die im Relution App Store unter der Plattform iOS geführt werden. Die Aktion App vom Apple App Store installieren gibt es für tvOS-Geräte nicht.

Für Version 26.4.0

Apps managen

Apps aus dem App Store werden vom Betriebssystem selbständig aktualisiert. In seltenen Fällen funktioniert dies jedoch nicht. Für diesen Fall gibt es zwei Wege, ein Update anzustoßen:

- In der Detailansicht der App werden im Reiter Geräte mit dieser App die betroffenen Geräte ausgewählt und über App aktualisieren aktualisiert. Die Schaltfläche ist deaktiviert, sobald auf einem der ausgewählten Geräte bereits die Version im Status Produktiv installiert ist.
- Alternativ wird auf den betroffenen Geräten die Aktion Relution Store App bereitstellen mit der betreffenden App ausgeführt.

In beiden Fällen wird eine erneute Installation angestoßen und die Geräte validieren die App-Version mit dem App Store von Apple. Ist die verfügbare Version aktueller als die installierte Version, wird die vorhandene App aktualisiert.

Benutzer-Einschreibung

Mit der Benutzer-Einschreibung, auch User Enrollment genannt, lassen sich private Macs einschreiben, ohne dass Besitzer die gesamte Kontrolle über die Geräte abgeben müssen. So lassen sich basierend auf dem Bring Your Own Device-Ansatz (BYOD) private Geräte von Schülern oder Mitarbeitern im Schul- bzw. Unternehmenskontext unter Einhaltung des Schutzes privater Daten einbinden und nutzen. Die Benutzer-Einschreibung von iPhone und iPad beschreibt der Artikel Benutzer-Einschreibung für iOS →.

Geräte dürfen sich für eine Apple-Benutzer-Einschreibung nicht im Überwachten Modus/Supervised Mode → befinden.

Es gibt zwei Varianten der Benutzer-Einschreibung: die kontogesteuerte Benutzer-Einschreibung, bei der die Anmeldung auf dem Mac mit einem verwalteten Apple Account (im Portal: Managed Apple ID) erfolgt, und die profilbasierte Benutzer-Einschreibung über einen Einschreibungslink.

Die profilbasierte Benutzer-Einschreibung wird ab macOS 15 nicht mehr unterstützt. Für diese Macs wird die kontogesteuerte Benutzer-Einschreibung → verwendet.

Vorteile

- Administratoren können privat installierte Apps nicht einsehen.
- Geräte bleiben unter Kontrolle der Benutzer.

Für Version 26.4.0

Nachteile

- Nicht alle Aktionen und Richtlinien-Konfigurationen sind möglich.
- Verwaltete Apple Accounts sind notwendig.
- Der macOS Companion wird auf Macs mit Benutzer-Einschreibung nicht bereitgestellt. Apps vom Typ DMG lassen sich auf diesen Macs daher nicht installieren.

Kontogesteuerte Benutzer-Einschreibung

Relution unterstützt die kontobasierte Benutzer-Registrierung von Macs, die sich nicht im Überwachten Modus → (Supervised Mode) befinden.

Die Anmeldung erfolgt auf dem Mac in den Systemeinstellungen über die Anmeldung mit einem Geschäfts- oder Schulaccount, also mit dem verwalteten Apple Account. Über die Service Discovery ermittelt der Mac den zuständigen MDM-Server und leitet auf die Anmeldeseite von Relution weiter, auf der die Anmeldung mit dem Relution-Benutzerkonto erfolgt. Anschließend wird auf dem Mac die Anmeldung mit dem verwalteten Apple Account bestätigt, das MDM-Profil installiert, und der Mac erscheint im Geräte-Inventar der entsprechenden Relution-Organisation.

Voraussetzungen

- macOS 14 oder höher.
- Ein in Relution hinterlegtes APNs-Zertifikat (APNS Push Zertifikate →).
- Ein verwalteter Apple Account und ein Relution-Benutzerkonto für den jeweiligen Benutzer. In den Benutzer-Details ist dafür die Managed Apple ID hinterlegt; ohne Managed Apple ID verwendet Relution die E-Mail des Benutzers. Dieser Wert muss dem verwalteten Apple Account entsprechen, mit dem die Anmeldung auf dem Mac erfolgt.
- Entweder die aktivierte Einstellung Kontobasierte Apple-Benutzerregistrierung in der Organisation oder eine für den Benutzer angelegte Benutzer-Einschreibung →.
- Eine Service Discovery für die Domain der verwalteten Apple Accounts, entweder automatisch über den Apple School/Business Manager oder über eine Well-Known-Datei.

Kontobasierte Apple-Benutzerregistrierung aktivieren

Die Einstellung befindet sich unter `Einstellungen` → `Geräteverwaltung` im Bereich Kontobasierte Apple-Benutzerregistrierung. Sie gilt je Organisation; in der globalen Organisation wird der Bereich nicht angezeigt.

Bei der Anmeldung eines Benutzers verwendet Relution zuerst eine für diesen Benutzer angelegte macOS-Benutzer-Einschreibung mit dem Status Erstellt, die noch mindestens fünf Minuten gültig ist. Ist keine solche Einschreibung vorhanden und der Schieberegler Kontobasierte Apple-Benutzerregistrierung aktiviert, legt Relution automatisch eine Benutzer-Einschreibung mit der Eigentümerschaft Gerät in Mitarbeiterbesitz (BYOD) und einer Gültigkeit von fünf Tagen an. Standardmäßig ist der Schieberegler deaktiviert; ohne passende Benutzer-Einschreibung schlägt die Einschreibung des Mac dann fehl.

Service Discovery einrichten

Für Version 26.4.0

Eine Service Discovery muss konfiguriert werden, damit Apple die Geräte an den richtigen MDM Server übertragen kann. Dafür stehen zwei Wege zur Verfügung.

Automatisch über den Apple School/Business Manager

Ab macOS 15.2 ist keine eigene Datei erforderlich, wenn der Apple School/Business Manager für die Automatische Geräteregistrierung (ADE, im Portal: DEP) über ein DEP-Konto in Relution eingebunden ist. Relution hinterlegt die Service-Discovery-URL bei jeder Synchronisation der ADE-Geräte automatisch im Apple School/Business Manager. Voraussetzung ist, dass dort unter `Preferences` → `Your MDM Servers` → `MDM Server Assignment` → `Default MDM Server Assignment` Relution als Standard-MDM-Server für Mac festgelegt ist.

Über eine Well-Known-Datei

Für Macs mit einer älteren macOS-Version als 15.2 oder ohne eingebundenen Apple School/Business Manager muss eine HTTP Well-Known-Ressourcen-Datei an der Domain hinterlegt werden, mit der sich die Benutzer anmelden. Für den eigenen Hostnamen beantwortet Relution diese Anfrage bereits selbst; eine eigene Datei ist daher nur erforderlich, wenn die Domain der verwalteten Apple Accounts davon abweicht. Apple muss diese Datei über einen HTTP GET unter folgender URL abrufen können:

```
https://yourdomain.com/.well-known/com.apple.remotemanagement
```

Unter dem Punkt `yourdomain.com` muss die Domain hinterlegt werden, die auch für die verwalteten Apple Accounts verwendet wird. Die Datei muss auf einer Domain hinterlegt werden, die mit HTTP-GET-Anfragen umgehen kann.

Die Datei wird im JSON-Format mit dem Content-Type `application/json` angelegt. Um die richtigen Informationen in die Datei einzutragen, lassen sich die benötigten Informationen direkt aus dem Relution Portal kopieren:

1. `Einstellungen` → `Geräteverwaltung` öffnen.
2. Im Bereich Kontobasierte Apple-Benutzerregistrierung den unter Antwort angezeigten JSON-Text vollständig, einschließlich der äußeren geschweiften Klammern, kopieren (Schaltfläche In Zwischenablage kopieren) und in die Datei einfügen. Der JSON-Text wird unabhängig vom Schieberegler angezeigt.

> Damit die Datei richtig funktioniert, darf sie keine Dateiendung haben.

Beispiel: maxmustermann@musterhausen.de

In diesem Beispiel wäre die Domain `musterhausen.de`. Dort müsste die Service Discovery hinterlegt werden.

Benutzer-Einschreibung in Relution anlegen

Eine Benutzer-Einschreibung wird unter `Geräte` → `Einschreibungen` über Hinzufügen angelegt. Als Plattform wird macOS und als Typ die Schaltfläche Benutzereinschreibung gewählt. Der Typ ist nur auswählbar, wenn die Berechtigung zum Lesen von Benutzern besteht.

Eine Benutzer-Einschreibung ist immer genau einem Benutzer zugeordnet; für mehrere Benutzer wird je eine eigene Einschreibung angelegt. Für den Benutzer muss entweder eine Managed Apple ID oder eine E-Mail in den Benutzer-Details hinterlegt sein. Ist keine Managed Apple ID hinterlegt, wird die E-Mail als verwalteter Apple Account verwendet. Geräten zugewiesene Benutzer lassen sich bei eingeschriebenen Geräten via Benutzer-Einschreibung nicht mehr ändern bzw. entfernen.

Eine so angelegte Benutzer-Einschreibung wird für die kontogesteuerte Benutzer-Einschreibung verwendet, wenn sich der Benutzer auf dem Mac anmeldet. Auf Macs bis macOS 14 lässt sie sich außerdem für die profilbasierte Benutzer-Einschreibung nutzen.

Für Version 26.4.0

Profilbasierte Benutzer-Einschreibung (bis macOS 14)

Der Einschreibungslink der angelegten Benutzer-Einschreibung wird an den jeweiligen Schüler oder Mitarbeiter gesendet. Über den Link wird die Einschreibung auf dem Mac unter Verwendung des verwalteten Apple Accounts des Benutzers durchgeführt, und das Gerät erscheint automatisch im Geräte-Inventar der entsprechenden Relution-Organisation.

Manuelle Einschreibung

Die Einschreibung wird durch ein manuell auf den Mac heruntergeladenes und installiertes MDM-Profil vorgenommen. Hierzu wird entweder ein QR-Code gescannt oder die entsprechende URL manuell im Browser aufgerufen. Im Anschluss wird das MDM-Profil in den Systemeinstellungen installiert.

Vorteile

- Die Einschreibung kann vorgenommen werden, ohne die Geräte auf Werkseinstellungen zurücksetzen zu müssen.

Nachteile

- Die Einschreibung kann jederzeit in den Einstellungen auf den Geräten entfernt werden (MDM-Profil), sofern in der Einschreibung nicht Passwort zum Entfernen des Profils verwenden aktiviert ist.
- Nur bedingt für BYOD-Geräte geeignet, da Administratoren sehen können, welche Apps installiert sind. Für private Geräte ist die Benutzer-Einschreibung → vorgesehen.
- Nicht alle Aktionen und Richtlinien-Konfigurationen sind möglich.
- Geräte sind häufig nicht überwacht (Supervised Mode).

Für Version 26.4.0

Einschreibung in Relution anlegen

Voraussetzung ist ein in Relution hinterlegtes APNs-Zertifikat (APNS Push Zertifikate →). Fehlt es, lassen sich die Apple-Plattformen beim Anlegen einer Einschreibung nicht auswählen.

Um eine manuelle Einschreibung durchzuführen, muss diese in Relution zuerst angelegt werden. Hierzu wird im Menü `Geräte` → `Einschreibungen` geöffnet und anschließend auf Hinzufügen geklickt.

Einschreibungen sind abhängig vom Betriebssystem. Als Plattform wird daher macOS gewählt und als Typ die Geräteeinschreibung (Schaltfläche macOS, nicht Benutzereinschreibung). Die Eigentümerschaft wird entsprechend gewählt.

Soll ein `Benutzer` mit dem einzuschreibenden Gerät verknüpft werden, wird dieser unter Benutzer ausgewählt. Optional lassen sich ein Gerätename und eine Gerätebeschreibung für die Anzeige im Geräte-Inventar vorgeben; ohne Gerätename erzeugt Relution den Namen automatisch.

Im Abschnitt Konfiguration stehen für macOS folgende Optionen zur Verfügung:

- Passwort zum Entfernen des Profils verwenden: Das MDM-Profil lässt sich dann nur mit einem automatisch generierten Passwort vom Mac entfernen. Das Passwort lässt sich in den Gerätedetails im Bereich Sicherheit unter Passwort zum Entfernen des Profils abrufen (siehe auch Sicherheitsoptimierungen für Einschreibungen →).
- Statische Gerätegruppen: Das Gerät wird direkt diesen Gruppen zugeordnet; die den Gruppen zugewiesenen Richtlinien werden nach der Einschreibung angewendet.
- Vereinbarungen: Auswahl von Vereinbarungen, die unter `Einstellungen` → `Allgemein` → `Vereinbarungen` angelegt wurden. Relution stellt deren Texte dem Gerät während der Einschreibung bereit.

Jede Einschreibung ist nur einmalig nutzbar, es sei denn, der Schalter für die Mehrfach-Einschreibung wird aktiviert. Ist dies der Fall, können über den Einschreibungslink so lange neue Geräte eingeschrieben werden, bis entweder das Gültigkeitsdatum überschritten wurde oder keine Geräte-Lizenzen mehr in Relution verfügbar sind. Das Gültigkeitsdatum wird unter Gültig bis festgelegt und ist mit einem Datum sieben Tage nach dem Anlegen vorbelegt. Mehrfach-Einschreibung lässt sich nach dem Speichern nicht mehr ändern.

Sind in den Einstellungen der Organisation Einschreibungsbenachrichtigungen per E-Mail oder SMS aktiviert, kann der Einschreibungslink im Abschnitt Benachrichtigung direkt an den zugeordneten Benutzer versendet werden.

Nach dem Speichern und Anlegen der Einschreibung kann die angezeigte URL auf dem Mac im Browser aufgerufen oder der erstellte QR-Code gescannt werden. Das MDM-Profil wird über die Schaltfläche Einschreibung heruntergeladen und anschließend in den Systemeinstellungen installiert (siehe Schritte unten).

Schritt für Schritt Anleitung

1. Die Einschreibung starten, indem auf Einschreibung gedrückt wird
2. Dann auf Zulassen drücken
3. Das nächste Fenster über Schließen schließen
4. In die Systemeinstellungen wechseln
5. Dort in den Bereich Profile
6. Das geladene MDM-Profil auswählen
7. Das MDM-Profil prüfen, auf Installieren drücken und den Dialog erneut durch Drücken auf Installieren bestätigen
8. Es wird eine Sicherheitsmeldung eingeblendet. Auch hier auf Installieren drücken
9. Der entfernten Verwaltung vertrauen
10. Mit der Bestätigung auf Fertig ist das MDM-Profil installiert

Damit ist die Einschreibung abgeschlossen.
Im Geräte-Inventar des Relution-Portals sollte nun ein neuer Eintrag erscheinen. Sind für den Relution Agent Lizenzen aus Apps und Bücher (im Portal: VPP) vorhanden, wird der Relution Agent anschließend automatisch auf dem Gerät installiert.

> Der verwaltete Benutzer sollte erst gelöscht werden, wenn bereits ein weiterer Benutzer (idealerweise mit Administratorrechten) auf dem Gerät vorhanden ist. Andernfalls kann der Zugriff auf das Gerät verloren gehen und ein Zurücksetzen des Macs erforderlich werden.

Für Version 26.4.0

Verfügbare Aktionen

Relution stellt eine Auswahl an Aktionen bereit, um Macs direkt zu kontrollieren und zu lenken. Die Aktionen lassen sich gezielt auf ein einzelnes Gerät oder über die Mehrfachauswahl in der Geräteliste auf mehrere Geräte gleichzeitig anwenden. Zusätzlich können sie über die Mitgliedschaft in Gerätegruppen ereignis- oder zeitgesteuert ausgelöst werden: Aktionen mit Gerätegruppen →

Der Aktionsdialog wird unter `Geräte` → `Inventar` über Aktion anwenden geöffnet, entweder für die in der Liste ausgewählten Geräte oder in der Detailansicht eines Geräts. Angeboten werden nur Aktionen, die alle ausgewählten Geräte unterstützen.

Für Version 26.4.0

Aktionen für macOS

Aktion	Beschreibung
AirPlay Wiedergabe starten	Ermöglicht kabellose Bildschirmübertragung. Anwendungsfall: Präsentationen auf einem Großbildschirm.
AirPlay Wiedergabe stoppen	Beendet die AirPlay-Übertragung. Nur für überwachte Geräte verfügbar. Anwendungsfall: Beenden der Bildschirmübertragung.
App entfernen	Deinstalliert eine App. Anwendungsfall: Entfernen nicht benötigter Apps.
App vom Apple App Store installieren	Installiert Apps aus dem App Store. Anwendungsfall: Verteilung von Standard-Apps.
Bildschirmfreigabe aktivieren	Aktiviert die Bildschirmfreigabe. Ab macOS 10.14.4. Anwendungsfall: Fernwartung.
Bildschirmfreigabe deaktivieren	Deaktiviert die Bildschirmfreigabe. Ab macOS 10.14.4. Anwendungsfall: Beenden der Fernwartung.
Bluetooth ein- oder ausschalten	Schaltet Bluetooth auf dem Gerät ein oder aus. Ab macOS 10.13.4. Anwendungsfall: Steuerung aus Sicherheitsgründen.
Gerät auf Werkszustand zurücksetzen	Setzt das Gerät auf den Werkszustand zurück und löscht alle Daten. Beim Auslösen der Aktion muss eine 6-stellige numerische PIN festgelegt werden. Anwendungsfall: Vorbereitung zur Weitergabe.
Gerät herunterfahren	Fährt das Gerät herunter. Nur für überwachte Geräte verfügbar, ab macOS 10.13. Anwendungsfall: Geräte zentral ausschalten, z. B. nach Unterrichts- oder Arbeitsende.
Gerät neu starten	Startet das Gerät neu. Ab macOS 10.13. Mit der Option Den Benutzer benachrichtigen, um das Gerät neu zu starten (kein erzwungener Neustart) wird der Benutzer nur zum Neustart aufgefordert (ab macOS 11). Anwendungsfall: Behebung von Software-Problemen.
Gerät vollständig sperren	Startet das Gerät neu und sperrt es vollständig für jede Benutzung oder Anmeldung. Zum Entsperren ist die beim Auslösen der Aktion festgelegte 6-stellige PIN erforderlich. Auf Macs mit Apple Silicon und einer macOS-Version vor 11.5 deaktiviert die Aktion den Mac; zur Reaktivierung sind eine Netzwerkverbindung und die Anmeldung eines lokalen Administrators mit aktiviertem Secure Token erforderlich. Anwendungsfall: Schutz sensibler Daten.
Geräteinformationen aktualisieren	Aktualisiert alle verfügbaren Informationen zu dem Gerät, die unter Details aufgelistet sind. Anwendungsfall: Aktuelle Informationen in Relution.
Im Geräte-Setup-Assistenten fortfahren	Informiert das Gerät, dass die Vorkonfiguration abgeschlossen ist und es im Setup-Assistenten fortfahren kann. Nur für Geräte verfügbar, die über die Automatische Geräteregistrierung (ADE, im Portal: DEP) registriert wurden. Wirkt nur, wenn im DEP-Profil die

Aktion	Beschreibung
	Option Konfiguration abwarten aktiviert ist. Anwendungsfall: Automatisierte Einrichtung.
Lokales Administratorkennwort aktualisieren	Ändert das Kennwort eines lokalen Administratorkontos. Das Konto wird aus den vom Gerät gemeldeten lokalen Benutzern ausgewählt oder über Manuelle Eingabe mit seiner GUID angegeben. Nur verfügbar, wenn genau ein Gerät ausgewählt ist. Anwendungsfall: Erhöhung der Sicherheit.
MDM Profil aktualisieren	Installiert das MDM-Profil auf dem Gerät neu. Dabei werden das Identitätszertifikat erneuert und aktuelle Einstellungen wie das Certificate Pinning übernommen. Die MDM-Server-URL bleibt unverändert; eine geänderte externe URL wird so nicht auf das Gerät übertragen. Relution erneuert das MDM-Profil automatisch, bevor das Identitätszertifikat abläuft. Die manuelle Aktion ist daher nur in Sonderfällen erforderlich.
Nachricht senden	Zeigt eine Textnachricht auf dem Gerät an. Anwendungsfall: Kurzfristige Information der Nutzer.
Relution Store App bereitstellen	Installiert eine App aus dem Relution Store. Apps vom Typ DMG lassen sich nur mit aktiviertem macOS Companion installieren. Anwendungsfall: Verteilung eigener Apps.
Shell-Skript ausführen	Führt ein verwaltetes Shell-Skript auf dem Gerät aus. Voraussetzung ist der aktivierte macOS Companion (`Einstellungen` → `Relution Client Apps`, Abschnitt macOS Companion, Schalter macOS Companion aktivieren). Der macOS Companion wird nur auf Macs ab macOS 12 bereitgestellt. Anwendungsfall: Automatisierte Wartungsaufgaben.
Update Installieren	Installiert ein ausgewähltes macOS-Update aus der Liste der vom Gerät gemeldeten verfügbaren Updates. Zusätzlich wird festgelegt, wie das Update ausgeführt wird, z. B. nur herunterladen, herunterladen und den Benutzer benachrichtigen oder installieren mit anschließend erzwungenem Neustart. Nur für überwachte Geräte verfügbar. Die Aktion wird nur angeboten, wenn Relution für alle ausgewählten Geräte ein verfügbares Update ermittelt hat. Die verfügbaren Updates werden neu ermittelt, sobald die Geräteinformationen aktualisiert werden, z. B. über Geräteinformationen aktualisieren.
Wiederherstellungssperre setzen →	Setzt, ändert oder entfernt das Passwort der Wiederherstellungssperre. Nur für überwachte Geräte verfügbar, ab macOS 11.5. Anwendungsfall: Schutz vor dem Start im Wiederherstellungsmodus oder von einem externen Datenträger ohne Kenntnis des Passworts.
Wiederherstellungssperre verifizieren →	Überprüft, ob ein bekanntes Passwort mit der auf dem Gerät gesetzten Wiederherstellungssperre übereinstimmt. Nur für überwachte Geräte verfügbar, ab macOS 11.5. Anwendungsfall: Kontrolle, ob das hinterlegte Passwort der Wiederherstellungssperre noch gültig ist.

Ist mindestens eines der ausgewählten Geräte nicht überwacht, werden AirPlay Wiedergabe stoppen, Gerät herunterfahren, Update Installieren sowie die beiden Aktionen zur Wiederherstellungssperre im Aktionsdialog nicht angezeigt. Entsprechendes gilt für Im Geräte-Setup-Assistenten fortfahren, sobald ein ausgewähltes Gerät nicht über die Automatische Geräteregistrierung registriert wurde. Shell-Skript ausführen erscheint nur, wenn der macOS Companion aktiviert ist.

Für Macs, die per Benutzer Einschreibung → registriert wurden, stehen nur folgende Aktionen zur Verfügung: AirPlay Wiedergabe starten, App vom Apple App Store installieren, Geräteinformationen aktualisieren, MDM Profil aktualisieren, Nachricht senden und Relution Store App bereitstellen.

Für Version 26.4.0

Wiederherstellungssperre

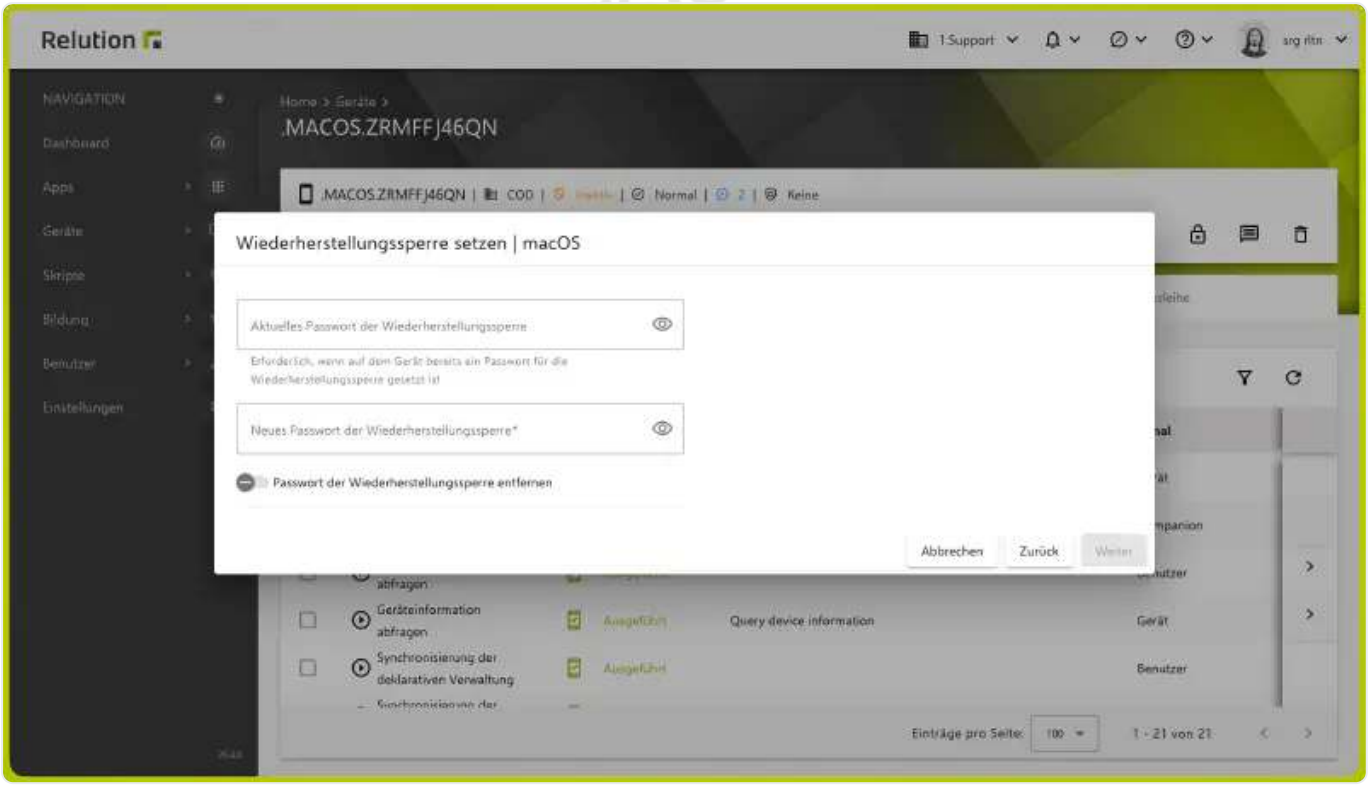
Die Wiederherstellungssperre (Recovery Lock) verhindert, dass ein Mac ohne Kenntnis eines Passworts im Wiederherstellungsmodus gestartet oder von einem externen Datenträger gebootet wird. Zur Verwaltung dieser Sperre stehen in Relution zwei Aktionen bereit. Beide setzen ein überwachtes (supervised) Gerät mit macOS 11.5 oder neuer voraus und werden im Aktionsdialog angeboten, entweder für ein einzelnes Gerät oder über die Mehrfachauswahl in der Geräteliste für mehrere Geräte gleichzeitig: Verfügbare Aktionen →

Die in diesen Aktionen eingegebenen Passwörter gibt Relution nicht wieder aus; sie lassen sich später im Portal nicht einsehen und sind daher separat aufzubewahren.

Wiederherstellungssperre setzen

Neu in 26.4

Ab Version 26.4 lässt sich das Passwort der Wiederherstellungssperre über die Aktion Wiederherstellungssperre setzen direkt aus Relution heraus setzen, ändern oder entfernen. Ist auf dem Gerät bereits ein Passwort für die Wiederherstellungssperre gesetzt, muss dieses im Feld Aktuelles Passwort der Wiederherstellungssperre angegeben werden. Das neue Passwort wird im Pflichtfeld Neues Passwort der Wiederherstellungssperre eingetragen. Ist der Schalter Passwort der Wiederherstellungssperre entfernen aktiviert, wird das bestehende Passwort entfernt, ohne ein neues zu vergeben; das Feld für das neue Passwort entfällt dann, und das Feld Aktuelles Passwort der Wiederherstellungssperre muss ausgefüllt werden.



Wiederherstellungssperre verifizieren

Neu in 26.5

Mit der Aktion Wiederherstellungssperre verifizieren wird überprüft, ob ein bekanntes Passwort mit der auf dem Gerät gesetzten Wiederherstellungssperre übereinstimmt. Das zu prüfende Passwort wird im Feld Passwort der Wiederherstellungssperre eingegeben; ist auf dem Gerät kein Passwort gesetzt, bleibt das Feld leer. Stimmt das Passwort überein, erhält die Aktion den Status Ausgeführt. Stimmt es nicht überein, erhält sie den Status Fehler mit der Fehlermeldung `The Recovery Lock password does not match`.

Status der Wiederherstellungssperre

Ob auf einem Gerät überhaupt eine Wiederherstellungssperre aktiv ist, lässt sich in den Gerätedetails in der Karte Sicherheit über den Wert Ist die Wiederherstellungssperre aktiviert einsehen.

Für Version 26.4.0

Verfügbare Konfigurationen

Relution bietet eine Vielzahl von Konfigurationsmöglichkeiten an, um macOS-Geräte effizient zu steuern. Diese Konfigurationen können in Richtlinien ausgewählt und angepasst werden. Der große Vorteil besteht darin, dass Richtlinien und die enthaltenen Konfigurationen problemlos auf eine Vielzahl von Geräten verteilt werden können.

Für Version 26.4.0

Übersicht der Konfigurationen

Konfiguration	Beschreibung
Active Directory →	Die Integration von Active Directory konfigurieren
Administrierte Domänen	Administrierte E-Mail-Domänen definieren
AirPlay	Verwaltung der kabellosen Übertragung von Inhalten auf AirPlay-fähige Empfängergeräte
AirPrint →	Verwaltung von AirPrint-Druckereinstellungen
Anmeldefenster	Verwalten des Anmeldefensters auf dem Gerät
App Konformität	Verwaltung appspezifischer Einschränkungen
App Store Restriktionen	Verwaltung von App Store Restriktionen
App zu VPN Zuordnung →	Konfiguration des verwendeten VPN einzelner Apps
Apple Configurator 2 Konfiguration →	Wendet ein mit Apple Configurator 2 erstelltes Konfigurationsprofil (`.mobileconfig`) auf Geräte an
Barrierefreiheit	Die Barrierefreiheitsfunktionen des Geräts konfigurieren
Bedingter Zugriff →	Einrichtung des Bedingten Zugriffs auf dem Gerät über den Relution Agent erfordern, um geschützte Ressourcen nutzen zu können
Benachrichtigungen	Benachrichtigungseinstellungen für Apps konfigurieren
Bildschirmschoner	Konfiguration eines passwortgeschützten Bildschirmschoners
Bildschirmzeit	Konfiguriert die Einstellungen der Kindersicherung
Desktop →	Konfiguration der Desktop-Einstellungen
DNS Proxy	DNS Proxy Konfiguration
DNS-Verschlüsselungs-Einstellungen	Konfigurieren der DNS-Verschlüsselungs-Einstellungen (ab macOS 11)
Dock	Das Dock konfigurieren
E-Mail	E-Mail Konfigurationen für mehrere Benutzer hinzufügen
Einstellungen für die Festplattenverwaltung	Festplattenverwaltungseinstellungen auf dem Gerät installieren (ab macOS 15, nur überwachte Geräte)
Erweiterbares Single Sign On	Eine App-Erweiterung konfigurieren, die Single Sign On durchführt
Exchange	Verwaltung von Exchange-Konten

Konfiguration	Beschreibung
Externe Intelligenz-Einstellungen →	Externe, cloudbasierte KI-Integrationen über Siri und Apple Intelligence steuern (ab macOS 26.4)
FileVault →	Die Festplattenverschlüsselung eines macOS-Geräts konfigurieren
Filter für Inhalte →	Spezifizierte URLs erlauben oder verbieten (nur überwachte Geräte)
Finder-Einstellungen	Konfigurieren der Finder-Einstellungen eines macOS-Geräts
Firewall	Konfiguration der Firewall
Geräteeinstellungen	Allgemeine Geräteeinstellungen konfigurieren (nur überwachte Geräte)
Gerätename →	Konfigurieren des Gerätenamens (nur überwachte Geräte)
Globale Einstellungen	Konfigurieren der globalen Einstellungen
Globale Ethernet-Einstellungen	Verwalten der globalen Ethernet-Verbindungseinstellungen
Globaler HTTP Proxy	Globale Proxy-Einstellungen konfigurieren (nur überwachte Geräte)
Inhaltscaching	Funktionen des Inhaltscaching konfigurieren
Intelligence-Einstellungen →	Apple-Intelligence-Funktionen wie Genmoji, Image Playground und Schreibwerkzeuge zentral steuern (ab macOS 26.4)
Kalender →	Verwaltung von CalDAV-Kalendern
Kernel-Erweiterungen →	Kernel-Erweiterungen verwalten
Kontakt	Verwaltung von CardDAV-Konten
Konten	Konteneinstellungen konfigurieren
Login-Elemente	Automatisch gestartete Elemente bei der Anmeldung verwalten
Managed App →	App Konfigurationen für gemanagte Apps pushen
Mathematische Einstellungen →	Funktionen und Modi der Apple Taschenrechner App zentral konfigurieren (ab macOS 15)
Migrationsassistent-Einstellungen →	Verhalten des Migrationsassistenten steuern, u. a. verwaltete Migration sowie ausgeschlossene Konten und Pfade (ab macOS 26.4, nur überwachte Geräte)
Passwort	Passwortrichtlinie für Apple-Geräte
Proxies	Konfigurieren von Proxies
Relution Decon →	DNS-basierter Inhaltsfilter für Webseiten und Apps
Restriktionen →	Verwaltung von Geräterestriktionen
Safari-Einstellungen →	Verhalten des Safari-Browsers zentral steuern, z. B. Verlauf, privates Surfen und Startseite (ab macOS 26)

Konfiguration	Beschreibung
Safari-Erweiterungen	Einstellungen für Safari-Erweiterungen (ab macOS 15, nur überwachte Geräte)
SCEP	Verwaltung der SCEP-Einstellungen
Schriftart	Schriftarten auf dem Gerät hinzufügen
Script	Planmäßige Skriptausführung über den macOS Companion verwalten (nur auswählbar, wenn der macOS Companion aktiviert ist)
Setup-Assistent →	Einrichtungsschritte ausblenden, die nach der Ersteinrichtung angezeigt werden
Sicherheitseinstellungen	Konfigurieren der Sicherheitseinstellungen
Siri-Einstellungen →	Verhalten von Siri zentral steuern, u. a. Obszönitätsfilter (ab macOS 26.4)
Softwareupdates-Einstellungen →	Update-Verhalten der Geräte steuern, z. B. automatisches Laden, Aufschub und Benachrichtigungen (ab macOS 15, nur überwachte Geräte)
Steuerung der Systemrichtlinien	Einstellungen für die Steuerung der Systemrichtlinien konfigurieren
Stromspareinstellungen	Stromspareinstellungen konfigurieren
System-Erweiterungen	Systemerweiterungen verwalten
System-Updates →	Updates von macOS-Geräten verwalten (veraltet, Nachfolger: Verwaltete Softwareupdates)
Systemeinstellungen	Konfigurieren der Systemeinstellungen
Tastatur-Einstellungen →	Tastaturfunktionen wie Diktat und mathematische Tastaturvorschläge zentral steuern (ab macOS 26.4)
Time Machine	Verwalten der Time Machine-Einstellungen auf dem Gerät
Verwaltete Softwareupdates →	Betriebssystemupdates erzwingen und eine Zielversion bis zu einer Frist vorgeben (ab macOS 14, nur überwachte Geräte)
VPN	Verwaltung von VPN Einstellungen
Weblink	Einen Weblink auf Geräte hinzufügen
WLAN	Verwaltung der WLAN-Einstellungen
Zertifikat	Ein Zertifikat wählen, das standardmäßig auf dem Gerät installiert werden soll

Die Konfigurationen Active Directory, Apple Configurator 2 Konfiguration, DNS-Verschlüsselungs-Einstellungen, E-Mail, Erweiterbares Single Sign On, Exchange, Filter für Inhalte, Kalender, Kontakt, Managed App, Safari-Erweiterungen, SCEP, Schriftart, Script, Steuerung der Systemrichtlinien, VPN, Weblink, WLAN und Zertifikat können mehrfach in einer Richtlinie angelegt werden, alle übrigen jeweils nur einmal. Ist eine nur einmal erlaubte Konfiguration bereits in der Richtlinie enthalten, wird sie im Auswahldialog nicht mehr angeboten. Dasselbe gilt, wenn eine Apple Configurator 2 Konfiguration bereits ein Profil dieses Typs enthält.

Im Auswahldialog weisen Badges auf Voraussetzungen hin, etwa auf eine Mindestversion von macOS, auf überwachte Geräte (Wird überwacht) oder auf die Unterstützung der Benutzer Einschreibung → (Unterstützt Benutzerregistrierung). Auf Macs aus der Benutzer Einschreibung wird nur ein Teil der Konfigurationen angewendet.

Die Konfiguration Script erscheint im Auswahldialog nur, wenn unter `Einstellungen` → `Relution Client Apps` die Option macOS Companion aktivieren eingeschaltet ist (Standard: aktiviert).

Für Version 26.4.0

Intelligence-Einstellungen

Mit der Konfiguration Intelligence-Einstellungen lassen sich die Funktionen von Apple Intelligence auf verwalteten macOS-Geräten zentral steuern. Über die Richtlinie lassen sich einzelne KI-gestützte Funktionen wie der Apple-Intelligence-Bericht, Genmoji, Image Playground und die Schreibwerkzeuge sowie appspezifische Intelligence-Funktionen in Mail, Notizen und Safari erlauben oder unterbinden. Zusätzlich lässt sich erzwingen, dass Diktieren ausschließlich lokal auf dem Gerät verarbeitet wird, ohne Verbindung zu Apple-Servern.

Die Konfiguration steht für macOS-Geräte ab Version 26.4 zur Verfügung und kann ausschließlich im Rahmen der Geräteregistrierung angewendet werden, nicht bei der Benutzerregistrierung (BYOD). Pro Richtlinie ist eine Konfiguration dieses Typs möglich. Geräte, die die Einstellungen nicht unterstützen, erhalten die Konfiguration nicht.

> Das Formular ist für iOS, macOS und visionOS gleich aufgebaut. Die Optionen Image Wand erlauben, Personalisierte Handschriftergebnisse erlauben, Visual-Intelligence-Zusammenfassung erlauben und Übersetzung nur auf dem Gerät erzwingen werden auch für macOS angezeigt, von macOS aber nicht unterstützt. Sie sind deshalb hier nicht beschrieben, siehe Intelligence-Einstellungen für iOS →.

Genmoji, Image Playground, die Schreibwerkzeuge, der Apple-Intelligence-Bericht und das Diktat nur auf dem Gerät lassen sich auch über die Konfiguration Restriktionen → steuern. Die entsprechenden Felder sind dort als Veraltet gekennzeichnet und werden durch diese Konfiguration abgelöst. Für Geräte vor macOS 26.4 bleiben sie der einzige Weg, diese Funktionen zu steuern. Die Zusammenfassungen in Mail und Safari sowie die Transkriptionszusammenfassung in Notizen bieten die Restriktionen ebenfalls an. Die Anbindung externer KI-Dienste wird über die Konfiguration Externe Intelligenz-Einstellungen → verwaltet.

Für Version 26.4.0

Einstellungen

- Apple-Intelligence-Bericht erlauben
  - Wenn deaktiviert, wird der Apple-Intelligence-Bericht auf dem Gerät deaktiviert. Standardmäßig aktiviert.
- Genmoji erlauben
  - Wenn deaktiviert, wird die Genmoji-Funktion deaktiviert. Standardmäßig aktiviert.
- Image Playground erlauben
  - Wenn deaktiviert, wird Image Playground deaktiviert. Standardmäßig aktiviert.
- Schreibwerkzeuge erlauben
  - Wenn deaktiviert, werden die Schreibwerkzeuge (Writing Tools) deaktiviert. Standardmäßig aktiviert.
- Diktat nur auf dem Gerät erzwingen
  - Wenn aktiviert, wird Diktieren ausschließlich lokal auf dem Gerät verarbeitet, ohne Verbindung zu Apple-Servern. Standardmäßig deaktiviert.

Mail

- Intelligente Antworten erlauben
  - Wenn deaktiviert, werden intelligente Antworten (Smart Replies) in Mail deaktiviert. Standardmäßig aktiviert.
- Zusammenfassung erlauben
  - Wenn deaktiviert, wird die Zusammenfassungsfunktion in Mail deaktiviert. Standardmäßig aktiviert.

Notizen

- Transkription erlauben
  - Wenn deaktiviert, wird die Transkription in Notizen deaktiviert. Standardmäßig aktiviert.
- Transkriptionszusammenfassung erlauben
  - Wenn deaktiviert, wird die Zusammenfassung von Transkriptionen in Notizen deaktiviert. Standardmäßig aktiviert.

Safari

- Zusammenfassung erlauben
  - Wenn deaktiviert, wird die Zusammenfassungsfunktion in Safari deaktiviert. Standardmäßig aktiviert.

Externe Intelligenz-Einstellungen

Mit der Konfiguration Externe Intelligenz-Einstellungen lässt sich zentral steuern, ob und wie externe, cloudbasierte KI-Dienste (z. B. ChatGPT) über Siri und Apple Intelligence auf macOS-Geräten genutzt werden dürfen. Die Richtlinie steht ab macOS 26.4 zur Verfügung — ausschließlich für Geräte mit vollständiger Geräteregistrierung, nicht im User Enrollment/BYOD-Modus — und wird per Deklarativer Geräteverwaltung (DDM) auf das Gerät übertragen. Geräte, die die Einstellungen nicht unterstützen, erhalten die Konfiguration nicht. Pro Richtlinie ist eine Konfiguration dieses Typs möglich. Dieselbe Konfiguration steht in gleicher Form auch für iOS- und visionOS-Geräte ab der jeweiligen Version 26.4 zur Verfügung.

Für Version 26.4.0

> Hinweis: Diese DDM-basierte Konfiguration löst die Felder zu externen KI-Integrationen in der Konfiguration Restriktionen → ab. Diese Felder sind im Portal seit Relution 26.3 als Veraltet gekennzeichnet. Für Geräte vor macOS 26.4 lassen sich externe KI-Integrationen weiterhin nur über diese Restriktionsfelder steuern.

Externe KI-Integrationen

- Externe KI-Integrationen erlauben
  - Wenn deaktiviert, werden externe KI-Integrationen vollständig unterbunden. Standardmäßig aktiviert.
- Anmeldung für externe KI-Integrationen erlauben
  - Wenn deaktiviert, ist die Anmeldung (Sign-In) bei externen KI-Integrationen nicht möglich. Standardmäßig aktiviert.
- Erlaubte Workspace-ID
  - Legt die Workspace-ID fest, auf die die externe KI-Integration beschränkt wird. Derzeit auf eine einzelne Workspace-ID begrenzt. Leerzeichen am Anfang und Ende werden entfernt. Bleibt das Feld leer, wird keine Workspace-ID vorgegeben.

Tastatur-Einstellungen

Ab macOS 26.4 und Relution 26.3 steht die Konfiguration Tastatur-Einstellungen zur Verfügung, die über die Deklarative Geräteverwaltung (DDM) umgesetzt wird. Mit dieser Richtlinie lassen sich unter macOS das Nachschlagen von Definitionen, das Diktat sowie mathematische Tastaturvorschläge zentral aktivieren oder deaktivieren. Weitere Tastaturoptionen wie Autokorrektur, Texterkennung, Rechtschreibprüfung, Wischgesten zum Tippen oder Textersetzung stehen über diese Richtlinie ausschließlich für iOS-Geräte → zur Verfügung.

> Hinweis: Die Konfiguration erfordert macOS 26.4 oder neuer und steht ausschließlich für Geräte zur Verfügung, die per Geräteregistrierung (Device Enrollment) verwaltet werden. Alle Einstellungen sind standardmäßig aktiviert; ein Deaktivieren schränkt die jeweilige Tastaturfunktion ein.

Pro Richtlinie ist eine Konfiguration Tastatur-Einstellungen möglich. Relution überträgt sie nur an Geräte, die diesen Konfigurationstyp melden; Geräte mit älteren macOS-Versionen erhalten sie ohne Fehlermeldung nicht.

Einstellungen für die Tastatur

- Nachschlagen von Definitionen zulassen
  - Wenn deaktiviert, steht das Nachschlagen von Wortdefinitionen (Look Up) auf der Tastatur nicht mehr zur Verfügung.
- Diktat zulassen
  - Wenn deaktiviert, kann die Diktierfunktion der Tastatur nicht mehr verwendet werden.
- Mathematische Tastaturvorschläge zulassen
  - Wenn deaktiviert, zeigt die Tastatur keine automatischen Lösungsvorschläge für mathematische Ausdrücke mehr an.
  - Die Konfiguration Mathematische Einstellungen → enthält mit Tastaturvorschläge aktivieren ebenfalls eine Option für mathematische Tastaturvorschläge.

Für Version 26.4.0

Siri-Einstellungen

Ab macOS 26.4 und Relution 26.3 steht die Konfiguration Siri-Einstellungen zur Verfügung, die über die Deklarative Geräteverwaltung (DDM) umgesetzt wird. Mit dieser Richtlinie lassen sich die grundsätzliche Verfügbarkeit von Siri sowie der Obszönitätsfilter zentral steuern. Weitere Optionen dieser Konfiguration – die Verarbeitung nutzergenerierter Inhalte und der Zugriff auf Siri im gesperrten Zustand – stehen ausschließlich unter iOS zur Verfügung und werden im Formular für macOS nicht angezeigt. Pro Richtlinie ist eine Konfiguration dieses Typs möglich.

Hinweis: Die Konfiguration erfordert macOS 26.4 oder neuer und steht ausschließlich für Geräte zur Verfügung, die per Geräteregistrierung (Device Enrollment) verwaltet werden; für Geräte mit Benutzerregistrierung (User Enrollment/BYOD) ist sie nicht verfügbar.

Vergleichbare Siri-Schalter (Siri erlauben, Siri Schimpfwortfilter aktivieren) gibt es auch in der Konfiguration Restriktionen →. Sie sind dort als Veraltet gekennzeichnet und werden durch die Siri-Einstellungen abgelöst. Für Geräte vor macOS 26.4 lässt sich Siri weiterhin nur über die Restriktionen steuern.

Einstellungen für Siri

Für Version 26.4.0

- Siri aktivieren
  - Aktiviert oder deaktiviert Siri auf dem Gerät. Standardmäßig aktiviert.
- Obszönitätsfilter erzwingen
  - Erzwingt den Obszönitätsfilter von Siri. Standardmäßig deaktiviert.

Safari-Einstellungen

Mit der Konfiguration Safari-Einstellungen lässt sich das Verhalten des Safari-Browsers auf verwalteten macOS-Geräten zentral steuern. Dazu zählen das Löschen des Verlaufs, privates Surfen, die Zusammenfassung von Inhalten sowie die Startseite, die beim Öffnen eines neuen Tabs angezeigt wird. Auf iOS-Geräten stehen zusätzlich Optionen für Cookies, die Betrugswarnung, JavaScript und Pop-ups zur Verfügung; diese sind unter macOS nicht Bestandteil dieser Konfiguration.

> Hinweis: Die Konfiguration steht ausschließlich für Geräte mit einem Device-Enrollment-Profil zur Verfügung (kein User Enrollment/BYOD) und setzt mindestens macOS 26 voraus. Sie gilt je angemeldetem, verwaltetem Benutzerkonto und nicht geräteweit für alle lokalen Accounts.

Pro Richtlinie ist eine Konfiguration dieses Typs möglich.

Einstellungen für den Safari-Browser

- Löschen des Verlaufs zulassen
  - Wenn deaktiviert, kann der Browser-Verlauf in Safari nicht gelöscht werden. Standardmäßig aktiviert.
- Privates Surfen zulassen
  - Wenn deaktiviert, ist der private Surfmodus in Safari nicht verfügbar. Standardmäßig aktiviert.
- Zusammenfassung von Inhalten zulassen
  - Wenn deaktiviert, wird die automatische Zusammenfassung von Inhalten in Safari deaktiviert. Standardmäßig aktiviert.
- Startseite *(Pflichtfeld)*
  - Legt fest, welche Seite beim Öffnen eines neuen Tabs in Safari angezeigt wird.
    - Start – Safari verwendet die Standard-Startseite; die Homepage wird deaktiviert. *(Standardwert)*
    - Erweiterung – Safari verwendet die über den angegebenen Bezeichner referenzierte Safari-Erweiterung als Startseite; die Homepage wird deaktiviert. Erfordert die Angabe eines Erweiterungs-Bezeichners im gleichnamigen Feld Erweiterung im Format `Identifier (TeamIdentifier)`, z. B. `com.example.app (ABCD1234)`.
    - Homepage-URL – Safari verwendet die angegebene URL sowohl als Startseite für neue Tabs als auch als Homepage. Erfordert die Angabe einer URL im gleichnamigen Feld Homepage-URL, die mit `https://` oder `http://` beginnen muss.

In der Homepage-URL können Benutzer- und Geräteplatzhalter verwendet werden. Die verfügbaren Platzhalter werden unterhalb des Formulars angezeigt und beim Übertragen auf das Gerät ersetzt, siehe Erweiterte Platzhalter →.

Für Version 26.4.0

Mathematische Einstellungen

Ab Version 26.1.0 von Relution steht die Konfiguration Mathematische Einstellungen auch für macOS-Geräte ab macOS 15+ zur Verfügung.

Mit dieser Richtlinie lassen sich die Funktionen und Modi der Apple Taschenrechner App zentral steuern und an pädagogische oder organisatorische Anforderungen anpassen. Im Vergleich zu iOS bietet der macOS-Taschenrechner zusätzlich einen Programmierer-Modus sowie die Eingabe in umgekehrter polnischer Notation (RPN), die hier ebenfalls konfiguriert werden können.

> Hinweis: Die Richtlinie steht ausschließlich für Geräte zur Verfügung, die per Geräteregistrierung (Device Enrollment) verwaltet werden, nicht im User Enrollment (BYOD).

Konfiguration

Die Konfiguration ist im Portal in die Bereiche Taschenrechner und Systemverhalten gegliedert. Beim Anlegen sind alle Optionen aktiviert, mit Ausnahme von Quadratwurzel hinzufügen. Pro Richtlinie ist eine Konfiguration Mathematische Einstellungen möglich. Relution überträgt die Einstellungen über die Deklarative Geräteverwaltung (DDM) und nur an Geräte, die diesen Konfigurationstyp unterstützen; ältere Geräte erhalten sie nicht.

Für Version 26.4.0

Einstellungen für die Apple Taschenrechner App

Basis-Modus

- Quadratwurzel hinzufügen: Fügt dem Basisrechner eine Quadratwurzel-Taste hinzu, indem die Taste +/- ersetzt wird. Standardmäßig ist die Quadratwurzel-Funktion nur im wissenschaftlichen Modus verfügbar. Diese Option ermöglicht den Zugriff auf die Quadratwurzel auch dann, wenn der wissenschaftliche Modus eingeschränkt ist.

Mathematik-Notizen-Modus

- Aktiviert: Legt fest, ob der Mathematik-Notizen-Modus in der Taschenrechner App verwendet werden darf.

Programmierer-Modus

- Aktiviert: Legt fest, ob der Programmierer-Modus in der Taschenrechner App verwendet werden darf. Nur für macOS verfügbar.

Wissenschaftlicher Modus

- Aktiviert: Bestimmt, ob der wissenschaftliche Modus der Taschenrechner App verfügbar ist.

Globale Eingabeoptionen des Taschenrechners

- Aktivieren der umgekehrten polnischen Notation (RPN): Legt fest, ob die Eingabe in umgekehrter polnischer Notation verwendet werden darf. Nur für macOS verfügbar.
- Einheitenumrechnung aktivieren: Ermöglicht die Nutzung der integrierten Einheitenumrechnung innerhalb der App.

Systemverhalten

- Tastaturvorschläge aktivieren: Steuert, ob in Tastaturvorschlägen automatisch mathematische Lösungen angezeigt werden. Die Konfiguration Tastatur-Einstellungen → enthält mit Mathematische Tastaturvorschläge zulassen ebenfalls eine Option für mathematische Tastaturvorschläge.
- Mathe Notes für andere Apps aktivieren: Legt fest, ob die Funktion `Math Notes` auch in anderen Apps (z. B. Notizen) verwendet werden darf.

Für Version 26.4.0

Softwareupdates

Für macOS-Geräte ab Version 15 im überwachten Modus (Supervised) steht mit Relution die Apple-Konfiguration Softwareupdates-Einstellungen zur Verfügung. Sie basiert auf Apples Declarative Device Management und ersetzt die veralteten allgemeinen Einstellungen der Konfiguration System-Updates, die von Apple als veraltet eingestuft wurde. Das Erzwingen von Updates übernimmt die Konfiguration Verwaltete Softwareupdates (siehe unten).

Um Updates zuverlässig über den gesamten Gerätepool sicherzustellen, können die Konfigurationen Softwareupdates-Einstellungen und System-Updates parallel konfiguriert und auf alle macOS-Geräte verteilt werden.

Hinweis: Die veraltete Konfiguration System-Updates wird von Apple mittelfristig eingestellt.

Allgemein

Erlaubt Standardbenutzern, Betriebssystemupdates durchzuführen

- Aktivieren / Deaktivieren (Standard: aktiviert)

Alle Benachrichtigungen zur Durchsetzung von Softwareupdates anzeigen

- Aktivieren / Deaktivieren (Standard: aktiviert)

Ist die Option deaktiviert, zeigt das Gerät nur die Benachrichtigungen eine Stunde vor Ablauf der Frist sowie den Countdown für den Neustart.

Für Version 26.4.0

Einschreibungen in das Beta-Programm *(ab macOS 15.4)*

- Erlaubt (Standard) — der Benutzer kann sich für Beta-Programme anmelden, die mit seinem Apple Account verknüpft sind.
- Immer aus — das Gerät darf sich nicht für Beta-Programme registrieren und wird aus bereits gewählten Beta-Programmen entfernt.

Aktionen für automatische Softwareupdates *(nur im überwachten Modus)*

Für alle drei Einstellungen ist Wahl durch Benutzer voreingestellt.

Automatisches Herunterladen verfügbarer Betriebssystem-Updates

- Wahl durch Benutzer
- Immer aus
- Immer an

Verfügbare Betriebssystem-Updates automatisch installieren

- Wahl durch Benutzer
- Immer aus
- Immer an

Automatisches Installieren des verfügbaren Sicherheitsupdates

- Wahl durch Benutzer
- Immer aus
- Immer an

Aufschub von Betriebssystem-Updates *(nur im überwachten Modus)*

- Anzahl der Tage, um ein größeres Betriebssystem-Softwareupdate auf dem Gerät zu verschieben (1–90)
- Anzahl der Tage, um ein kleineres Betriebssystem-Softwareupdate auf dem Gerät zu verschieben (1–90)
- Anzahl der Tage, um System- oder Nicht-Betriebssystem-Updates zu verschieben (1–90)

Rapid Security Response

- Erlaubt dem Benutzer Sicherheitsverbesserungen im Hintergrund
- Ermöglicht dem Benutzer Rollbacks der Sicherheitsverbesserung im Hintergrund

Beide Schalter sind standardmäßig aktiviert.

Verwaltete Softwareupdates

Für Version 26.4.0

Neu in 26.4

Die Konfiguration Verwaltete Softwareupdates erzwingt Betriebssystemupdates und gibt dabei eine Zielversion bis zu einer Frist vor. Sie ist der Nachfolger der veralteten Konfiguration System-Updates und ergänzt die oben beschriebene Konfiguration Softwareupdates-Einstellungen: Während dort das Update-*Verhalten* gesteuert wird (automatisches Laden, Aufschub, Benachrichtigungen), legt Verwaltete Softwareupdates verbindlich fest, *welche* Version bis *wann* installiert sein muss.

Voraussetzung ist macOS 14 oder neuer im überwachten Modus (Supervised). Die Konfiguration steht außerdem für iOS ab 17, tvOS ab 18.4 und visionOS ab 26 zur Verfügung.

Zielversion

- Zu erzwingende Version (Standard: Neueste Nebenversion)
  - Neueste Hauptversion — das Gerät wird auf die aktuellste verfügbare Hauptversion gehoben.
  - Neueste Nebenversion — es wird innerhalb der installierten Hauptversion aktualisiert.
  - Bestimmte Mindestversion — eine konkrete Version wird als Mindeststand vorgegeben. Sie wird im Pflichtfeld Version aus den von Apple veröffentlichten Betriebssystemversionen ausgewählt. Eine bereits gespeicherte Version bleibt auswählbar, auch wenn sie nicht mehr in der Liste angeboten wird.

Durchsetzung

- Durchsetzungsplan (Standard: Relativ zum Veröffentlichungsdatum)
  - Relativ zum Veröffentlichungsdatum — die Frist ergibt sich aus Tage nach Veröffentlichung (Pflichtfeld, ab 0) und Uhrzeit (vorbelegt mit 00:00). Damit gilt für jede künftige Version automatisch dieselbe Regel.
  - Bestimmtes Datum und Uhrzeit — die Frist wird als fester Zeitpunkt gesetzt.
- Karenzzeit nach der Einschreibung — optional. Verschiebt die Frist auf so viele Tage nach der Einschreibung eines Geräts, damit neu eingeschriebene Geräte nicht sofort zum Update gezwungen werden. Die Angabe gilt für beide Durchsetzungspläne und verlängert eine Frist immer nur, verkürzt sie nie. Bleibt das Feld leer, ist die Funktion deaktiviert.

> Lassen sich die verfügbaren Betriebssystemversionen im Portal nicht laden, meldet die Konfiguration dies beim Öffnen. Die Auswahl einer bestimmten Mindestversion ist dann nicht möglich, die beiden anderen Modi bleiben nutzbar.

Eine bereits verstrichene Frist wird trotzdem an das Gerät übertragen; das Update wird dann beim nächsten Neustart erzwungen. Gibt es für ein Gerät kein passendes Update, z. B. keine neuere Nebenversion, wird keine Durchsetzung übertragen.

Details

- URL der Detailseite — optionaler Link, den macOS den Benutzern zur Update-Ankündigung anzeigt.

Update auslösen

Für Version 26.4.0

Es gibt zwei Möglichkeiten, macOS-Updates durchzuführen:

Richtlinien-Konfiguration Über die Konfiguration Verwaltete Softwareupdates wird eine Zielversion vorgegeben, die bis zu einer Frist installiert sein muss (siehe oben). Die veraltete Konfiguration System-Updates legt weiterhin Wochentage (Wiederholt sich am) und eine Startzeit für geplante Updates fest. Installiert wird dabei das neueste verfügbare Update, optional begrenzt durch Max. Version, auf die aktualisiert werden soll. Sind beide Konfigurationen auf einem Gerät aktiv, hat Verwaltete Softwareupdates Vorrang.

Geräte-Aktion Über die Geräteaktion Update Installieren im Geräte-Inventar wird eines der für das Gerät verfügbaren Updates ausgewählt. Zusätzlich wird festgelegt, wie das Update durchgeführt wird, z. B. Updates herunterladen und installieren, Updates nur herunterladen, ohne zu installieren, Updates herunterladen und später installieren (mit Maximale Verschiebungen durch den Benutzer) oder Herunterladen, installieren und anschließend einen Neustart erzwingen.

Damit macOS-Geräte ein Update erfolgreich durchführen können, gilt Folgendes:

- Die Geräte müssen ausreichend geladen oder an eine Stromquelle angeschlossen sein.
- Die Geräte müssen entsperrt sein; andernfalls müssen Benutzer ihr Gerätepasswort eingeben.
- Aktualisierungen können je nach Netzwerkinfrastruktur und Anzahl der Geräte sehr lange dauern.
- Unterstützte macOS-Geräte prüfen unabhängig von der Konfiguration System-Updates einmal täglich auf Updates.
- Die Konfiguration System-Updates überschreibt vorhandene Restriktionen zum Verzögern von Updates.

Desktop

Mit der Konfiguration Desktop für macOS-Geräte wird der Desktop-Hintergrund über die Angabe eines Pfads zu einer Bilddatei festgelegt. Im Unterschied zur vergleichbaren Konfiguration Hintergrundbild → für iOS-, Android- und Windows-Geräte wird im Rahmen dieser Richtlinie keine Bilddatei über Relution hochgeladen oder verteilt.

> Der im Feld „Pfadangabe zu dem zu verwendenden Desktop-Bild“ angegebene Pfad bezieht sich auf eine Datei, die bereits lokal auf dem macOS-Gerät vorhanden sein muss – nicht auf eine URL. Relution reicht diesen Pfad direkt an das native Desktop-Konfigurationsprofil von Apple weiter; dieses teilt dem Betriebssystem lediglich mit, wo nach einem vorhandenen Hintergrundbild gesucht werden soll, lädt die Datei jedoch nicht selbst herunter und installiert sie auch nicht.

Einstellungen

Die Konfiguration ist einmal pro Richtlinie möglich und enthält im Abschnitt Allgemein ein einziges Feld:

- Pfadangabe zu dem zu verwendenden Desktop-Bild: Pfad zur Bilddatei auf dem macOS-Gerät, z. B. `/Library/Desktop Pictures/Firma.jpg`. Relution übernimmt den Wert unverändert in das Konfigurationsprofil. Platzhalter werden in diesem Feld nicht ersetzt. Bleibt das Feld leer, wird ein Desktop-Profil ohne Bildvorgabe installiert.

Für Version 26.4.0

Bereitstellung der Bilddatei

Da die referenzierte Datei bereits vor Anwendung der Richtlinie auf dem Gerät vorhanden sein muss, erfolgt die Verteilung des Bildes getrennt von dieser Konfiguration – beispielsweise über eine Skript-Konfiguration (nur für Geräte mit Geräteregistrierung, nicht mit Benutzer-Einschreibung), ein Installationspaket oder einen anderen Mechanismus zur Dateiverteilung, der die Datei zuvor an dem konfigurierten Pfad ablegt.

FileVault

Mit der Konfiguration FileVault für macOS-Geräte wird die Festplattenverschlüsselung zentral auf verwalteten Macs aktiviert. Die Konfiguration ist einmal pro Richtlinie möglich und steht nur für Geräte mit Geräteregistrierung zur Verfügung, nicht für Geräte mit Benutzer-Einschreibung (User Enrollment) →.

> Die Installation der FileVault-Konfiguration startet die Festplattenverschlüsselung nicht sofort, da FileVault den Verschlüsselungsschlüssel aus dem Anmeldepasswort des Benutzers ableitet. Wann der Benutzer zur Aktivierung aufgefordert wird, hängt von den Optionen zum Verschieben der Aktivierung ab.

Zeitpunkt der Aktivierung

Mit den Standardeinstellungen gilt:

- Verschiebt die Aktivierung von FileVault, bis sich der angegebene Benutzer abmeldet. ist aktiv.
- Die Option, die Anforderung beim Abmelden zu unterdrücken, ist nicht aktiv.
- Die maximale Anzahl, wie oft Benutzer die Aktivierung von FileVault umgehen können ist `0`.

Der Benutzer wird dann beim nächsten Abmelden zur Aktivierung aufgefordert. Spätestens bei der nächsten Anmeldung wird die Aktivierung verlangt.

Ein Wert größer `0` (höchstens `9999`) erlaubt entsprechend viele Umgehungen. Mit `-1` wird die Aktivierung bei der Anmeldung nicht erzwungen. Ist die Option zum Unterdrücken der Anforderung beim Abmelden aktiv, entfällt die Abfrage beim Abmelden. Beide Unteroptionen sind nur verfügbar, solange das Verschieben aktiv ist. Ist das Verschieben deaktiviert, müssen Benutzername und Passwort eines Benutzers im Profil angegeben werden.

Für Version 26.4.0

Einstellungen

Im Abschnitt Allgemein stehen folgende Einstellungen zur Verfügung:

- FileVault Status: Ein aktiviert FileVault, Aus deaktiviert es (Pflichtfeld, Standardwert Ein).
- Typ des Wiederherstellungsschlüssels: institutioneller und persönlicher Wiederherstellungsschlüssel, nur institutioneller oder nur persönlicher Wiederherstellungsschlüssel. Für einen institutionellen Schlüssel ist ein Zertifikat erforderlich.
- Pfad des Wiederherstellungsschlüssels: Speicherort für den Wiederherstellungsschlüssel und die Computerinformationen, z. B. `/Library/Keychains/Recovery.plist`.
- Anzeige des persönlichen Wiederherstellungsschlüssels nach Aktivierung von FileVault auf dem Gerät zulassen: legt fest, ob der Benutzer den persönlichen Schlüssel nach der Aktivierung angezeigt bekommt.
- FileVault Open Directory-Benutzer und Passwort: Benutzer, der zu FileVault hinzugefügt wird. Alternativ lässt sich einstellen, dass fehlende Angaben zu Benutzername oder Passwort auf dem Gerät abgefragt werden.
- Optionen zum Verschieben der Aktivierung (siehe oben).

Im Abschnitt Handhabung von persönlichen Wiederherstellungsschlüsseln legt Erlaubt, dass Relution auf den persönlichen Wiederherstellungsschlüssel zugreifen kann fest, ob Relution den persönlichen Wiederherstellungsschlüssel speichert (Standardwert: aktiv). Der Schlüssel lässt sich anschließend in den Gerätedetails in der Karte Sicherheit unter FDE Persönlicher Wiederherstellungsschlüssel abrufen. Das ist nur möglich, wenn die Option bereits vor der Aktivierung von FileVault aktiv war; ist FileVault auf dem Mac schon aktiviert, hat die Option keine Wirkung.

Im Abschnitt Zusätzliche Optionen stehen Verbietet die Deaktivierung von FileVault, Verbietet die Aktivierung von FileVault und FileVault-Schlüssel im Standby-Modus löschen zur Verfügung.

Bereitstellung über die Automatische Geräteregistrierung (ADE)

Die FileVault-Konfiguration kann über die Automatische Geräteregistrierung (ADE, im Portal: DEP) bereits vor oder während des Setup-Assistenten bereitgestellt werden, sodass sie beim ersten Start des Geräts bereits vorliegt. Da die Ableitung des Verschlüsselungsschlüssels ein Benutzerkonto samt Anmeldepasswort voraussetzt, kann die eigentliche Verschlüsselung erst beginnen, nachdem ein Benutzerkonto angelegt und dieser Benutzer erstmals angemeldet wurde.

Soll Relution den persönlichen Wiederherstellungsschlüssel speichern, muss die Konfiguration mit aktivierter Option Erlaubt, dass Relution auf den persönlichen Wiederherstellungsschlüssel zugreifen kann auf dem Gerät sein, bevor FileVault aktiviert wird. Im DEP-Profil lässt sich der Schritt FileVault des Setup-Assistenten überspringen. Eine erzwungene Aktivierung von FileVault im Setup-Assistenten unterstützt Relution nicht.

Für Version 26.4.0

Kernel-Erweiterungen

KEXTs (Kernel Extensions) sind Module, die tief in das macOS-Betriebssystem integriert werden, um dessen Funktionalität zu erweitern oder spezielle Hardware- und Systemanforderungen zu unterstützen. Sie agieren auf Kernel-Ebene – dem „Nervensystem“ des Betriebssystems – und ermöglichen dadurch den Zugriff auf Ressourcen und Funktionen, die auf Benutzerebene (Userspace) nicht direkt erreichbar sind.

Wofür benötigt man KEXTs?

- Unterstützung für nicht-native Hardware, z. B. spezielle Grafikkarten, Netzwerkkarten oder externe Speichergeräte.
- Implementierung von Dateisystemen (z. B. NTFS, FUSE), die standardmäßig in macOS nicht verfügbar sind.
- Erweiterung der Netzwerkfunktionen, etwa für VPN-Protokolle oder virtuelle Netzwerkschnittstellen.
- Integration von Sicherheitslösungen und -prüfungen auf Kernel-Ebene.
- Entwicklung von Virtualisierungsplattformen und deren Interaktion mit dem Kernel.

Vorteile von KEXTs

- Tiefer Systemzugriff: Ermöglicht Funktionen, die ohne direkten Kernel-Zugriff nicht realisierbar wären.
- Hardware-Kompatibilität: Geräte und Funktionen, die von macOS nicht standardmäßig unterstützt werden, können durch KEXTs vollständig integriert werden.
- Flexible Erweiterbarkeit: Entwickler können maßgeschneiderte Lösungen für spezifische Anforderungen erstellen.

Für Version 26.4.0

Allgemein

Die Konfiguration Kernel-Erweiterungen wird unter `Geräte` → `Richtlinien` in einer macOS-Richtlinie über Hinzufügen angelegt. Pro Richtlinie ist eine Konfiguration dieses Typs möglich. Sie steht nur für Geräte zur Verfügung, die über eine Geräteregistrierung eingeschrieben sind, nicht für Benutzerregistrierungen.

Folgende Konfigurationsoptionen stehen im Abschnitt Allgemein zur Verfügung:

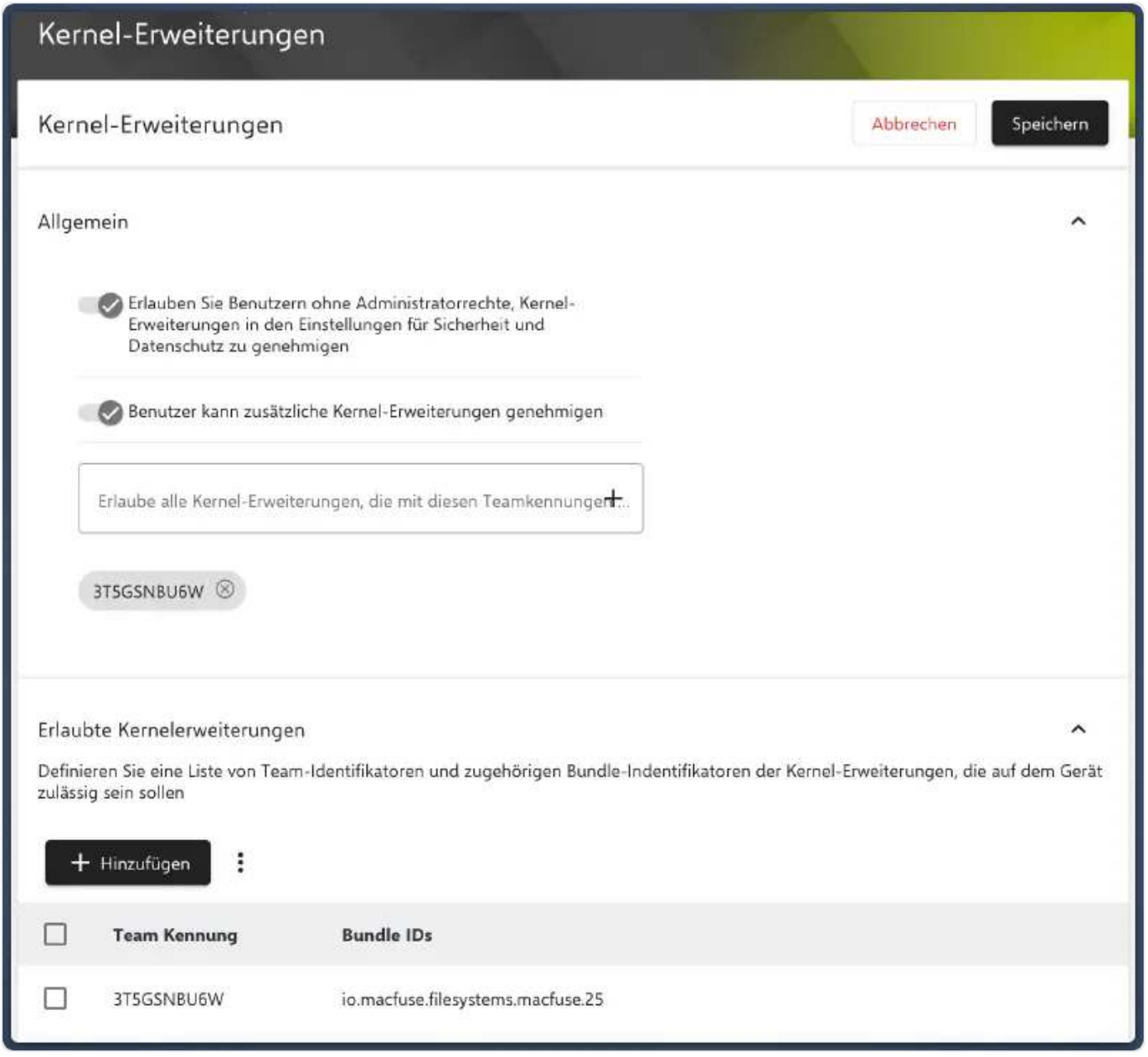
- Benutzern ohne Administratorrechte erlauben, Kernel-Erweiterungen in den Einstellungen für Sicherheit und Datenschutz zu genehmigen: Schalter, standardmäßig deaktiviert. Ist er aktiviert, können auch Benutzer ohne Administratorrechte zusätzliche Kernel-Erweiterungen genehmigen. Wirksam ab macOS 11.
- Benutzer kann zusätzliche Kernel-Erweiterungen genehmigen: Schalter, standardmäßig deaktiviert. Ist er aktiviert, können Benutzer Kernel-Erweiterungen genehmigen, die nicht ausdrücklich über die Konfiguration erlaubt sind.
- Alle Kernel-Erweiterungen erlauben, die mit diesen Teamkennungen signiert sind: Listenfeld für Teamkennungen. Gültig signierte Kernel-Erweiterungen dieser Teamkennungen dürfen geladen werden. Bleibt die Liste leer, wird keine Teamkennung übertragen.

Grundsätzlich können alle KEXTs mit derselben Teamkennung erlaubt werden. Alternativ können im nächsten Abschnitt einzelne Erweiterungen explizit mit einer bestimmten Teamkennung freigegeben werden.

Erlaubte Kernelerweiterungen

Über Hinzufügen öffnet sich der Dialog Neue Zuordnung der Team-Kennung hinzufügen. Darin wird die Team Kennung (Pflichtfeld) eingetragen und unter Bundle IDs eine Liste der zugehörigen Bundle-IDs erfasst.

Team Kennung	Bundle IDs
3T5GSNBU6W	io.macfuse.filesystems.macfuse.25



Teamkennung und Bundle-ID auslesen

Die Teamkennung kann im folgenden Beispiel aus der heruntergeladenen Datei macfuse-5.1.1.dmg ausgelesen werden:

```
codesign -d --verbose=2 macfuse-5.1.1.dmg 2>&1 | grep -i teamidentifier
```

Ausgabe:

```
TeamIdentifier=3T5GSNBU6W
```

Die Bundle-ID kann bei einer manuell installierten KEXT (z. B. macFUSE) wie folgt ermittelt werden:

```
kextstat | grep -i fuse
```

Ausgabe:

Für Version

```
Executing: /usr/bin/kmutil showloaded
No variant specified, falling back to release
  265    0 0                  0x1830     0x1830     io.macfuse.filesystems.macfuse.25
(5.1.1) 67A4F7E1-82FE-30A4-A3B3-B6E8722C287A <9 7 6 5 3>
```

Damit ist io.macfuse.filesystems.macfuse.25 die benötigte Bundle-ID.

Hinweis

Unter Erlaubte Kernelerweiterungen können einer Teamkennung mehrere Bundle-IDs zugeordnet werden – entweder beim Anlegen eines neuen Eintrags über Hinzufügen oder beim Bearbeiten eines bestehenden Eintrags über das Dreipunkte-Menü und Bearbeiten.

Jede Teamkennung kann nur einmal angelegt werden. Ein zweiter Eintrag mit derselben Teamkennung wird mit dem Hinweis Die Team-Kennung existiert bereits abgelehnt; weitere Bundle-IDs werden deshalb im bestehenden Eintrag ergänzt.

Apple KEXT →

Migrationsassistent

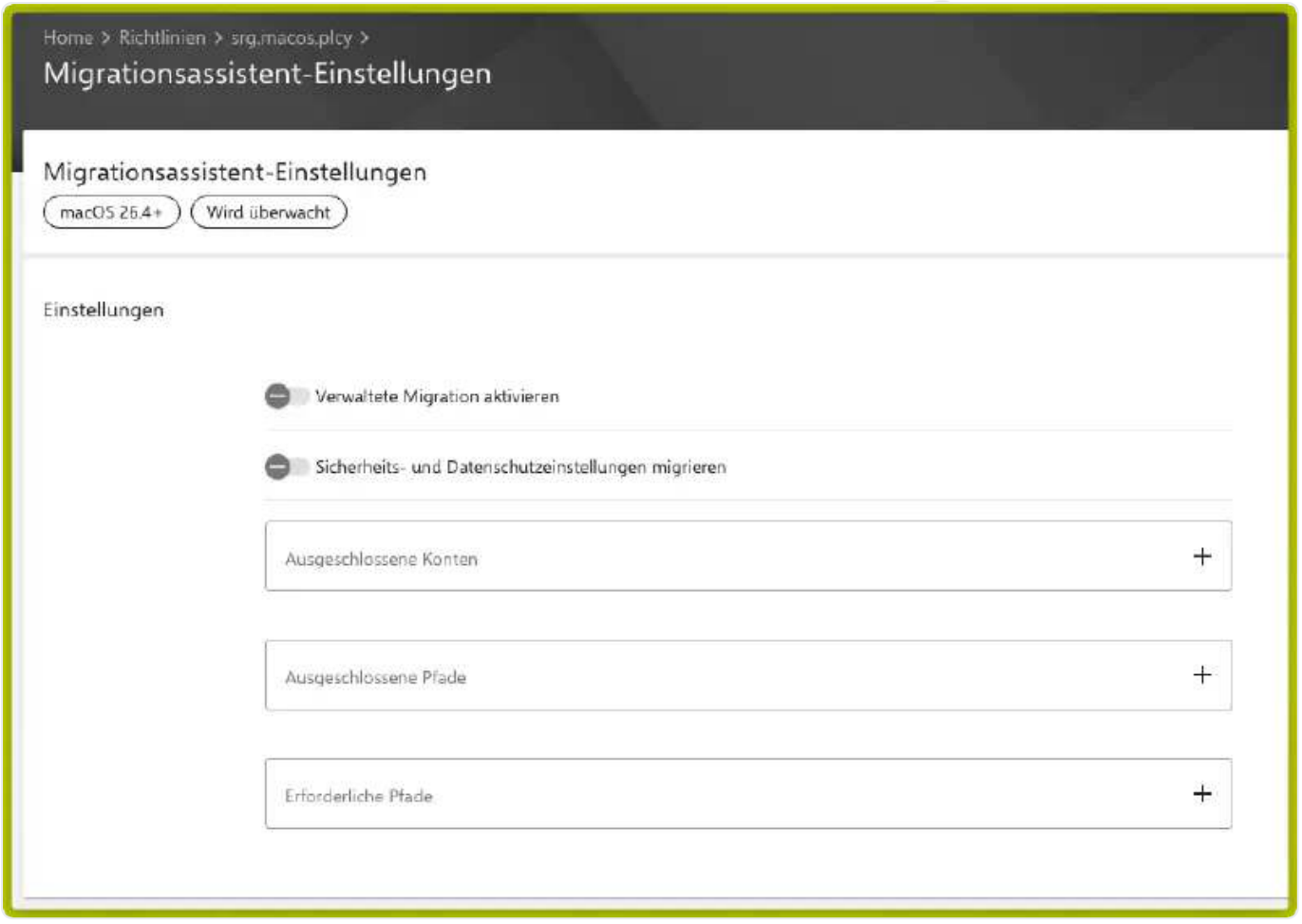
Der Migrationsassistent ist ein macOS-Bordwerkzeug, das beim Einrichten eines neuen Macs hilft. Er überträgt Benutzerdaten, Apps, Einstellungen und Dateien vom alten auf das neue Gerät — damit man nicht alles neu einrichten muss.

Ab macOS 26.4 unterstützt Apple die Verwaltung des Migrationsassistenten über die Deklarative Geräteverwaltung (DDM). Relution 26.3 implementiert diese Unterstützung vollständig: Einstellungen können per Richtlinie auf Geräte gepusht werden, und der aktuelle Migrationsstatus wird als Statusbericht an Relution zurückgemeldet.

Die Konfiguration erfordert macOS 26.4 oder neuer und ein überwachtes Gerät (Supervised).

Einstellungsdeklaration

Neu in 26.3



Verwaltete Migration aktivieren

Aktiviert die verwaltete Migration auf dem Gerät. Solange dieser Schalter deaktiviert ist, gelten keine weiteren Einschränkungen. Der Schalter ist standardmäßig deaktiviert.

Sicherheits- und Datenschutzeinstellungen migrieren

Legt fest, ob Sicherheits- und Datenschutzeinstellungen aus der Quelle auf das neue Gerät übertragen werden. Ist die Option deaktiviert, werden nur Benutzerdaten migriert; systemweite Sicherheitseinstellungen verbleiben im Ausgangszustand. Die Option ist standardmäßig deaktiviert.

Ausgeschlossene Konten

Liste der Benutzerkonten, die vom Migrationsprozess ausgenommen werden. Angegeben wird jeweils der Kurzname des Benutzerkontos. Über die +-Schaltfläche lassen sich Kontonamen einzeln hinzufügen.

Beispiele:

Kontoname	Anwendungsfall
`administrator`	Lokales Admin-Konto soll nicht übertragen werden
`gastbenutzer`	Temporäres Gastkonto ausschließen

Ausgeschlossene Pfade

Liste der Dateien und Verzeichnisse, die nicht migriert werden. Über die +-Schaltfläche lassen sich Pfade einzeln hinzufügen.

Pfade werden relativ zum Home-Verzeichnis des Benutzers angegeben und dürfen nicht mit `/` oder `~` beginnen; Verzeichnispfade enden mit `/`. Ungültige Einträge werden beim Hinzufügen abgelehnt. Systemweite Pfade außerhalb des Home-Verzeichnisses lassen sich nicht angeben.

Beispiele:

Pfad	Anwendungsfall
`Library/Caches/`	Cache-Daten werden auf dem Zielgerät neu aufgebaut
`Downloads/`	Temporäre Downloads werden nicht übertragen
`Documents/Excluded/`	Ein bestimmter Dokumentenordner bleibt zurück

Erforderliche Pfade

Liste der Dateien und Verzeichnisse, die zwingend migriert werden müssen. Fehlt ein erforderlicher Pfad auf dem Quellgerät, wird die Migration abgebrochen. Über die +-Schaltfläche lassen sich Pfade hinzufügen. Es gelten dieselben Formatregeln wie bei Ausgeschlossene Pfade.

Beispiele:

26.4.0

Pfad	Anwendungsfall
`Documents/`	Arbeitsdokumente müssen vollständig übertragen werden
`Library/Keychains/`	Schlüsselbunde sind für den Betrieb notwendig

Statusberichte

Relution liest automatisch zwei Statusberichte vom Gerät aus. Die Werte erscheinen nach Auswahl des Geräts unter `Geräte` → `Inventar` im Reiter Informationen in der Karte Details zum Gerät. Die Einträge werden erst angezeigt, wenn das Gerät die jeweiligen Werte gemeldet hat.

Migrationsstatus

Der Eintrag Migrationsassistent gibt den aktuellen Zustand des Migrationsassistenten auf dem Gerät an:

Status	Bedeutung
Wartend	Der Migrationsassistent wurde noch nicht gestartet oder es fand keine Migration statt
Migriert	Die Migration läuft gerade
Abgeschlossen	Die Migration wurde erfolgreich abgeschlossen
Fehlgeschlagen	Die Migration ist fehlgeschlagen
Abgebrochen	Die Migration wurde vom Benutzer abgebrochen
Unbekannt	Das Gerät meldet einen Status, den Relution nicht zuordnen kann

Migrationsbericht

Enthält detaillierte Informationen über die durchgeführte Migration:

- Quellbenutzer: Benutzerkonto auf dem Quell-Mac
- Zielbenutzer: Benutzerkonto auf dem neuen Mac
- Startzeit und Abschlusszeit: Beginn und Ende der Migration
- Übertragene Dateien: übertragene Dateien im Verhältnis zur Gesamtzahl
- Übertragene Daten: übertragene Datenmenge im Verhältnis zur Gesamtgröße
- Fehler: während der Migration gemeldete Fehler

Für Version 26.4.0

Konfiguration in Relution

1. Unter `Geräte` → `Richtlinien` über Hinzufügen eine macOS-Richtlinie anlegen oder eine bestehende macOS-Richtlinie öffnen.
2. Über Hinzufügen die Konfiguration Migrationsassistent-Einstellungen auswählen.
3. Die Option Verwaltete Migration aktivieren einschalten.
4. Die gewünschten Konten und Pfade konfigurieren.
5. Die Konfiguration speichern, die Richtlinie veröffentlichen und den Zielgeräten zuweisen.

Pro Richtlinie ist eine Konfiguration Migrationsassistent-Einstellungen möglich. Erhält ein Gerät über mehrere Richtlinien mehrere dieser Konfigurationen, wird nur eine davon an das Gerät übertragen.

Gerätename

Mit Relution ist es möglich, bei iOS, iPadOS, tvOS und macOS den Gerätenamen zu setzen. Hierfür kann eine Richtlinie mit der Konfiguration Gerätename erstellt und an Gerätegruppen verteilt werden. Die Konfiguration ist einmal pro Richtlinie möglich; das Feld Gerätename ist ein Pflichtfeld mit höchstens 255 Zeichen.

Die Konfiguration ist für überwachte Geräte vorgesehen (Kennzeichnung Wird überwacht) und steht für Geräte mit Benutzer-Einschreibung (User Enrollment) → nicht zur Verfügung.

Der Gerätename kann statisch vergeben werden, z. B. `Koffer iPad`. Somit erhalten alle Geräte in der Gerätegruppe denselben Namen.

Für mehrere Geräte in einer Gruppe kann es jedoch sinnvoller sein, Platzhalter in der Konfiguration zu verwenden. Die verfügbaren Benutzer- und Geräteplatzhalter zeigt das Portal unter dem Formular in der Karte Verfügbare Platzhalter.

Ein Beispiel: Der Gerätename wird wie folgt zusammengesetzt: `Koffer ${device.model} ${user.name}` Dies führt zu einer Darstellung wie: `Koffer iPad12,1 Max.Mustermann` Dies erleichtert die Übersicht im Inventar erheblich.

Weitere Funktionen wie Teilzeichenfolgen, Standardwerte für nicht gesetzte Felder oder das Ersetzen von Umlauten sind im Artikel Erweiterte Platzhalter → beschrieben.

Ist die Konfiguration auf einem Gerät aktiv, übernimmt Relution den vom Gerät gemeldeten Namen bei jeder Geräteabfrage ins Inventar. Ohne diese Konfiguration wird der gemeldete Name nur übernommen, solange im Inventar noch kein Name gesetzt ist.

Für Version 26.4.0

Active Directory

Mit Relution ist es möglich, macOS Geräte so zu konfigurieren, dass ein Login mit Accounts aus einer Windows Domäne möglich ist. Hierzu muss der Domain Controller erreichbar sein.

Voraussetzung

Es gelten die üblichen Anforderungen an den Domänen Controller. Die folgende Anleitung bezieht sich auf Tests und Erfahrungen mit einem Windows Server 2019 Standard Edition.

- Domänen Controller
- Administrative Berechtigung in der Domäne
- macOS Gerät muss FQDN vom Domänen Controller auflösen können. (Eintrag in der hosts Datei reicht nicht aus).
- macOS Gerät muss den Domänen Controller erreichen können
- Computerkonto in der Domäne

Konfiguration der Richtlinie Active-Directory

Die hier gezeigte Konfiguration stellt lediglich ein Beispiel dar und wurde mit macOS 13 und höher getestet.

Für Version 26.4.0

1. In einer Richtlinie für macOS die Konfiguration Active Directory hinzufügen.

2. Mindestens die folgenden Parameter konfigurieren:

Parameter	Wert
Name (optional)	Name der Konfiguration; ohne Angabe wird der Wert aus Active Directory-Domäne, der beizutreten ist übernommen
Active Directory-Domäne, der beizutreten ist	Name der Windows Domäne (z.B. relution.loc)
Benutzername des Kontos für die Domäne	Username eines Domänen Adminaccounts
Passwort des Kontos für die Domäne	Passwort für den Domänen Admin
Bei der Anmeldung ein mobiles Konto erstellen	ON
Active Directory-Gruppen mit Admin-Zugriff (optional)	DOMÄNE\Gruppenname

Für Version 26.4.

Pflichtfeld ist nur Active Directory-Domäne, der beizutreten ist; der Wert muss ein gültiger Hostname sein. Benutzername und Passwort erzwingt das Portal nicht, sie werden für den Domänenbeitritt aber benötigt.

3. Wurde die Richtlinie mit der Konfiguration auf dem Mac angewendet, diesen in jedem Fall neu starten, um Loginprobleme zu reduzieren.

Beim Entfernen der Richtlinie wird im AD das Computerkonto ebenfalls entfernt.

Optionale Einstellungen

Neben den oben genannten Parametern bietet die Konfiguration weitere Einstellungen, die nur bei Bedarf gesetzt werden:

- Allgemein: ClientID legt den Namen des Computerobjekts in der Domäne fest. Authentifizierung von jeder Domäne im Namensraum erlauben lässt Anmeldungen aus allen Domänen der Gesamtstruktur zu.
- Konten: Organisationseinheit, zu der das beitretende Computerobjekt hinzugefügt werden soll gibt die OU für das Computerkonto vor. Rund um das mobile Konto stehen Warnung vor der Erstellung des mobilen Kontos anzeigen, Erzwingt ein lokales Home-Verzeichnis, Netzwerk-Home-Protokoll (AFP oder SMB), UNC-Pfad aus dem Active Directory verwenden, um die Netzwerk Home Location abzuleiten, Standard-Benutzer-Shell und Namenskonvention für primäre Benutzerkonten (Domain oder Forest) zur Verfügung.
- Erweiterte Optionen: Bevorzugter Domänenserver, Für dynamische DNS-Updates zugelassene Schnittstellen, Richtlinie zum Signieren von Paketen, Richtlinie zur Paketverschlüsselung, die Zuordnung von UID, GID und Gruppen-GID zu AD-Attributen sowie Anzahl der Tage, bis das Passwort für das Computer-Konto geändert werden muss (0 bis 3650; `0` deaktiviert den Wechsel, Standardwert).

Weitere Konfiguration

Um ein Login am Mac zu ermöglichen, muss zusätzlich die Konfiguration Anmeldefenster hinzugefügt werden. Dort müssen folgende Parameter aktiviert werden:

- Anzeige der Felder für Name und Passwort anstelle der Benutzerliste
- Netzwerkbenutzer anzeigen
- ‘Andere…’ in der Benutzerliste anzeigen

Die Konfiguration Anmeldefenster steht nur für Geräte mit Geräteregistrierung zur Verfügung, nicht für Geräte mit Benutzer-Einschreibung (User Enrollment) →.

Für Version 26.4.0

Mögliche Fehler

1. `(1) The 'Directory Binding Account' payload could not be installed. Attempts to bind to the server 'rltn.mway' returned an unspecified problem. (-319)`
    - Überprüfen, ob ein Computerkonto mit dem Namen des Geräts auf dem DC vorhanden ist.
2. `(1) Das Account für das Einbinden in Verzeichnisse-Payload konnte nicht installiert werden. Der Server rltn.mway wurde nicht gefunden oder antwortet nicht.`
    - Überprüfen, ob der Domänen Controller vom Mac aus erreichbar ist. Der FQDN muss auflösbar sein.

App zu VPN Zuordnung

Bei der Einrichtung eines geräteübergreifenden VPNs werden alle Daten der Geräte durch das private Netzwerk geleitet. Manchmal möchte ein Unternehmen ein VPN nur für seine Unternehmensanwendungen einrichten. Apple ermöglicht die Einrichtung von VPN-Verbindungen für iPhones, iPads und Macs auf App-Basis. Hier können Administratoren genau steuern, welche Daten durch das VPN fließen. Die Richtlinien-Konfiguration einer App-zu-VPN-Zuordnung hilft Unternehmen, den Datenverkehr auf App-Ebene auseinander zu halten und ermöglicht so die Trennung von persönlichen und unternehmensbezogenen Daten.

Voraussetzung

Eine App-zu-VPN-Zuordnung kann direkt über Relution eingerichtet werden. Dies funktioniert nur für Apps, die vom MDM auf den Geräten installiert und verwaltet werden.

Relution unterstützt die folgenden Verbindungstypen für den Aufbau einer VPN-Verbindung pro App auf iOS- und macOS-Geräten:

- IPSec
- JuniperSSL
- SonicWALL
- AnyConnect Legacy
- AnyConnect
- IKEv2
- Benutzerdefiniertes SSL

Bei anderen VPN-Typen weist die VPN-Konfiguration auf die unterstützten Typen hin; beim Typ IKEv2 Always On steht die Option nicht zur Verfügung.

Für Version 26.4.0

App-zu-VPN-Zuordnung für iOS- und macOS-Geräte konfigurieren

1. Für ein VPN pro App werden zwei Konfigurationen in derselben Richtlinie benötigt:
    - VPN
    - App zu VPN Zuordnung
2. Innerhalb der VPN-Konfiguration muss die Option VPN-Verbindung für Apps und Konten aktiviert und je nach VPN-Typ alle notwendigen Felder ausgefüllt werden.
3. In der Konfiguration App zu VPN Zuordnung werden Apps einer VPN-Konfiguration derselben Richtlinie zugeordnet. Die Konfiguration ist einmal pro Richtlinie möglich. Über Hinzufügen wird zuerst die VPN-Konfiguration (Konfiguration) gewählt, anschließend die Quelle der App: Relution App Store App, Apple App Store App, iOS System-App / mitgelieferte App, App Konformität oder App manuell hinzufügen.
4. Nach dem Aktivieren von VPN-Verbindung für Apps und Konten erscheint in der VPN-Konfiguration der Bereich Per Account VPN. Dort lässt sich mit Automatisch mit dem VPN verbinden, wenn eine zugehörige App eine Netzwerkverbindung anfordert festlegen, dass die Verbindung bei Bedarf automatisch aufgebaut wird. Außerdem lassen sich Zugehörige Domänen, Ausgeschlossene Domänen, Safari Domänen und SMB Domänen angeben. Unter Konfigurationen auswählen lassen sich Konto-Konfigurationen derselben Richtlinie dem VPN zuordnen; auf macOS sind das E-Mail-, CalDAV- und CardDAV-Konfigurationen.

Die Liste der Zuordnungen zeigt in den Spalten Aktiviert und Per App VPN aktiv, ob die zugeordnete VPN-Konfiguration aktiv ist und ob dort VPN-Verbindung für Apps und Konten eingeschaltet ist. Nur wenn beides zutrifft, wird die Zuordnung wirksam.

Für Version 26.4.0

Besonderheiten bei macOS

In macOS-Richtlinien sind für jede zugeordnete App zusätzlich die Pflichtfelder Signierungsindentität und Vorgesehene Anforderung vorhanden. Beim Hinzufügen übernimmt Relution für beide Felder zunächst die Bundle-ID der App; über Bearbeiten lassen sich die Werte anpassen. Die Signierungsidentität zeigt `codesign -dv /Applications/Safari.app` in der Zeile `Identifier`, die vorgesehene Anforderung (Designated Requirement) zeigt `codesign -d --requirements - /Applications/Safari.app`.

Kalender (CalDAV)

Mit der Konfiguration Kalender wird ein CalDAV-Konto auch auf macOS-Geräten per Konfigurationsprofil an die native Kalender-App übergeben. Die Konfigurationsfelder sowie die serverseitige Voraussetzung – die automatische Erkennung nach RFC 6764 über eine Umleitung unter `/.well-known/caldav` – sind mit iOS identisch.

Konfiguration und serverseitige Voraussetzung

Die vollständige Beschreibung der Konfigurationsfelder, der automatischen Erkennung über `/.well-known` sowie der serverseitigen Einrichtung der Umleitung inklusive Fehlerbehebung ist im iOS-Artikel dokumentiert und gilt für macOS unverändert:

- Kalender (CalDAV) für iOS →

Zu beachten ist insbesondere, dass die Umleitung zwingend auf eine `https://`-Adresse ohne internen Port verweisen muss und die Vorrangige URL (Principal-URL) – sofern gesetzt – als reiner Pfad anzugeben ist.

Besonderheiten bei macOS

Auf macOS stellt Relution die Konfiguration über den Benutzerkanal zu. Das CalDAV-Konto wird damit im Profil des angemeldeten Benutzers installiert und nicht geräteweit. Unterstützt das Gerät keinen Benutzerkanal, erfolgt die Zustellung über den Gerätekanal.

Die Konfiguration steht auch für Macs mit Benutzer-Einschreibung (User Enrollment) → zur Verfügung.

Für Version 26.4.0

Apple Configurator 2 Konfiguration

Mit dieser Richtlinien-Konfiguration können `.mobileconfig`-Dateien auf Apple-Geräte übertragen werden. Eine solche Datei kann beispielsweise eine WLAN-Verbindung samt zugehörigem Identitätszertifikat (PKCS#12, `.p12`) enthalten.

Konfiguration

Die Konfiguration heißt im Portal Apple Configurator 2 Konfiguration. Im Feld Name wird eine Bezeichnung für die Konfiguration vergeben. Über .mobileconfig Datei auswählen wird die Datei hochgeladen. Danach erscheint ihr Inhalt anstelle der Dateiauswahl im Feld Payload Inhalt und kann dort bearbeitet werden. Der Inhalt muss gültiges XML sein. Signierte Profile sind kein lesbares XML und lassen sich daher nicht verwenden. In Apple Configurator 2 wird die Datei deshalb ohne Signatur gesichert. Wird das Feld Payload Inhalt geleert, kann erneut eine Datei ausgewählt werden.

Im Feld Payload Inhalt können Benutzer-, Geräte- und Zertifikatsplatzhalter verwendet werden. Die verfügbaren Platzhalter werden unterhalb des Formulars angezeigt und beim Übertragen auf das Gerät ersetzt, siehe Erweiterte Platzhalter →.

Pro Richtlinie können mehrere Apple-Configurator-2-Konfigurationen angelegt werden. Auf diese Weise lassen sich mehrere Konfigurationstypen auf getrennte Konfigurationen verteilen.

> Unter macOS weist das Portal darauf hin, dass diese Konfiguration nur verwendet werden sollte, wenn die Datei keinen der folgenden Konfigurationstypen enthält: CardDAV, CalDAV, LDAP, Exchange, E-Mail und Web Clip. Für diese Typen stehen in Relution eigene Konfigurationen zur Verfügung.

Für Version 26.4.0

Anforderungen an die Datei

Beim Speichern wird der Inhalt geprüft. Die Datei muss folgende Bedingungen erfüllen:

- Auf der obersten Ebene sind die Schlüssel `PayloadType`, `PayloadVersion` (als Zahl), `PayloadIdentifier`, `PayloadUUID` und `PayloadDisplayName` vorhanden.
- `PayloadContent` enthält genau einen Konfigurationstyp. Zusätzlich dürfen Zertifikat-Payloads enthalten sein.

Dateien, die sich nicht auslesen lassen, denen einer dieser Schlüssel fehlt, die keinen Payload oder mehrere Konfigurationstypen enthalten, werden beim Speichern abgelehnt.

> Mit übertragen werden nur Zertifikate im Format PKCS#12 (`com.apple.security.pkcs12`). PKCS#1-Zertifikate (`com.apple.security.pkcs1`) werden bei der Prüfung zwar akzeptiert, aber nicht an das Gerät übertragen. Andere Zertifikate wie Root-Zertifikate (`com.apple.security.root`) zählen als eigener Konfigurationstyp. Zusammen mit einer weiteren Konfiguration führen sie zu einem Fehler beim Speichern und werden daher in einer eigenen Konfiguration hinterlegt.
>
> Die eigentliche Konfiguration muss in `PayloadContent` an erster Stelle stehen. Enthält die Datei mehrere Payloads desselben Typs, wird nur der erste auf das Gerät übertragen.

Enthält die Datei einen Konfigurationstyp, den Relution auch als eigene, nur einmal pro Richtlinie zulässige Konfiguration anbietet, lässt sich diese Konfiguration in derselben Richtlinie nicht mehr hinzufügen. Umgekehrt wird eine solche Datei beim Speichern abgelehnt, wenn die Richtlinie die entsprechende Konfiguration oder eine weitere aktive Apple-Configurator-2-Konfiguration mit demselben Payload-Typ bereits enthält.

> Betroffene Payload-Typen unter macOS

Beispiel

Die folgende Datei überträgt eine WLAN-Verbindung (`com.apple.wifi.managed`). SSID, Passwort, Bezeichner und UUIDs sind Beispielwerte und werden durch eigene Werte ersetzt. Jede `PayloadUUID` muss eindeutig sein.

Für Version 26.4.0

```xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
 <key>PayloadContent</key>
 <array>
  <dict>
   <key>AutoJoin</key>
   <true/>
   <key>EncryptionType</key>
   <string>WPA2</string>
   <key>HIDDEN_NETWORK</key>
   <false/>
   <key>Password</key>
   <string>WLAN-Passwort</string>
   <key>PayloadDisplayName</key>
   <string>WLAN</string>
   <key>PayloadIdentifier</key>
   <string>com.example.wifi.payload</string>
   <key>PayloadType</key>
   <string>com.apple.wifi.managed</string>
   <key>PayloadUUID</key>
   <string>8D2E4C1A-3B5F-4A7E-9C6D-1F0B2A3C4D5E</string>
   <key>PayloadVersion</key>
   <integer>1</integer>
   <key>SSID_STR</key>
   <string>Firmen-WLAN</string>
  </dict>
 </array>
 <key>PayloadDescription</key>
 <string>WLAN-Konfiguration für Apple-Geräte</string>
 <key>PayloadDisplayName</key>
 <string>WLAN</string>
 <key>PayloadIdentifier</key>
 <string>com.example.wifi</string>
 <key>PayloadOrganization</key>
 <string>Beispiel GmbH</string>
 <key>PayloadType</key>
 <string>Configuration</string>
 <key>PayloadUUID</key>
 <string>4A7B1C2D-5E6F-4890-A1B2-C3D4E5F60718</string>
 <key>PayloadVersion</key>
 <integer>1</integer>
</dict>
</plist>
```

Managed App Konfiguration

Es ist möglich, einige Apps mit der Richtlinien-Konfiguration Managed App vorzukonfigurieren. Diese Konfiguration ist nur für iOS-Geräte ab Version 7 und macOS-Geräte ab Version 11+ verfügbar.

Konfiguration

In der Konfiguration werden die Bundle-ID der zu konfigurierenden App im Feld Bundle Identifier und eine gültige App-Konfigurations-Payload im Feld Payload hinterlegt. Die Bundle-ID wird über einen Auswahldialog übernommen: aus den in Relution hinterlegten Apps, aus dem Apple App Store oder per manueller Eingabe. Das Feld Payload ist mit einem leeren plist-Grundgerüst vorbelegt. Ungültiges XML wird als Fehler markiert, die Konfiguration lässt sich dann nicht speichern. Eine Richtlinie kann mehrere Managed-App-Konfigurationen enthalten, etwa für verschiedene Apps.

In der Payload lassen sich die Platzhalter verwenden, die unten auf der Seite angezeigt werden. Zum Beispiel lässt sich eine E-Mail-Client-App konfigurieren, indem der Platzhalter `${user.email}` verwendet wird. So lässt sich die Konfiguration für verschiedene Benutzer nutzbar machen. Die Platzhalter werden ausgefüllt, wenn die Konfiguration auf die Geräte übertragen wird. Unbekannte oder falsch geschriebene Platzhalter werden ohne Fehlermeldung durch einen leeren Wert ersetzt.

> Die zu konfigurierende App muss auf den Geräten installiert sein, damit die App-Konfiguration angewendet wird. Installiert Relution die App – aus dem App Store, über Apps und Bücher (im Portal: VPP) oder als Unternehmens-App – und ist auf dem Gerät bereits eine Richtlinie mit einer Managed-App-Konfiguration für dieselbe Bundle-ID angewendet, überträgt Relution die Konfiguration zusammen mit dem Installationsbefehl. Die Reihenfolge der Konfigurationen in der Richtlinie hat darauf keinen Einfluss.

Für Version 26.4.0

Grundsätzlich ist der Hersteller der jeweiligen App für die Konfigurationsmöglichkeiten verantwortlich. Die folgenden Beispiele haben zum Zeitpunkt der Erstellung dieses Dokuments mit den jeweiligen Apps funktioniert. Eine Gewähr, dass dies weiterhin gilt, besteht nicht.

Microsoft Outlook für Office365

```
com.microsoft.Office.Outlook
```

```xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
 <key>com.microsoft.outlook.EmailProfile.AccountType</key>
 <string>ModernAuth</string>
 <key>com.microsoft.outlook.EmailProfile.EmailAccountName</key>
 <string>${user.fullname}</string>
 <key>com.microsoft.outlook.EmailProfile.ServerHostName</key>
 <string>outlook.office365.com</string>
 <key>com.microsoft.outlook.EmailProfile.EmailAddress</key>
 <string>${user.email}</string>
 <key>com.microsoft.outlook.EmailProfile.EmailUPN</key>
 <string>${user.email}</string>
 <key>com.microsoft.outlook.EmailProfile.AccountDomain</key>
 <string></string>
 <key>com.microsoft.outlook.EmailProfile.ServerAuthentication</key>
 <string>Username and Password</string>
 <key>IntuneMAMAllowedAccountsOnly</key>
 <string>Enabled</string>
 <key>IntuneMAMUPN</key>
 <string>${user.email}</string>
</dict>
</plist>
```

Für Versi

Microsoft Outlook für einen on premise Exchange Server

```
com.microsoft.Office.Outlook
```

```xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
 <key>com.microsoft.outlook.EmailProfile.AccountType</key>
 <string>BasicAuth</string>
 <key>com.microsoft.outlook.EmailProfile.EmailAccountName</key>
 <string>${user.fullname}</string>
 <key>com.microsoft.outlook.EmailProfile.ServerHostName</key>
 <string>exchange.server.name</string>
 <key>com.microsoft.outlook.EmailProfile.AccountDomain</key>
 <string>domainname</string>
 <key>com.microsoft.outlook.EmailProfile.EmailAddress</key>
 <string>${user.email}</string>
 <key>com.microsoft.outlook.EmailProfile.EmailUPN</key>
 <string>${user.email}</string>
 <key>com.microsoft.outlook.EmailProfile.ServerAuthentication</key>
 <string>Username and Password</string>
 <key>IntuneMAMAllowedAccountsOnly</key>
 <string>Disabled</string>
 <key>IntuneMAMUPN</key>
 <string>${user.email}</string>
</dict>
</plist>
```

Für Versi

SecurePIM für Office365

```
com.virtual-solution.securepim-enterprise
```

```xml
<?xml version="1.0" ?>
<!DOCTYPE plist PUBLIC "-//Apple Inc//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
 <dict>
  <key>license</key>
    <string>your-license-key</string>
    <key>activeSyncServer</key>
    <string>outlook.office365.com</string>
    <key>userEmail</key>
    <string>${user.email}</string>
    <key>activeSyncUser</key>
    <string>${user.email}</string>
    <key>deviceSerialNumber</key>
    <string>${device.serialnumber}</string>
    <key>recipientCertificateEmail</key>
    <string>${user.email}</string>
    <key>allowTouchIDAuthentication</key>
    <string>true</string>
    <key>callKitEnabled</key>
    <string>true</string>
  </dict>
 </plist>
```

Konfiguration unvollständig

Beim Export einer bestehenden Konfiguration aus einem anderen MDM-System als XML und der anschließenden Umwandlung in eine `plist`-Datei kann aus einem als optional markierten, leeren Wert ein leerer `<string></string>`-Wert in der `plist` werden. Betroffen ist unter anderem der Key `subscriptionWebServiceEndPointURL`.

SecurePIM meldet in diesem Fall beim App-Start dauerhaft die Meldung „Konfiguration unvollständig", obwohl der Key im ursprünglichen System ohne Wert funktioniert hat. Abhilfe schafft das Eintragen eines beliebigen, nicht-leeren Werts in den betroffenen Key oder das vollständige Entfernen des Keys aus der `plist`.

FileBrowser for Education

```
com.stratospherix.filebrowsereducation
```

Konfiguration eines SMB-Share

```xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>mdm-enforce</key>
  <integer>1</integer>
  <key>lockdown</key>
  <integer>1</integer>
  <key>1displayname</key>
  <string>My NAS</string>
  <key>1domain</key>
  <string>office.mwaysolutions.com</string>
  <key>1flags</key>
  <integer>1746</integer>
  <key>1machinename</key>
  <string>smb://yoursmbservershare/</string>
  <key>1username</key>
  <string>${user.email}</string>
  <key>1vpntype</key>
  <integer>0</integer>
  <key>waitForSearchButton</key>
  <integer>0</integer>
</dict>
</plist>
```

Für Versi

IBM Verse client

```
com.ibm.lotus.traveler
```

Vollständiges Konfigurationsbeispiel anzeigen

Filter für Inhalte

Die Konfiguration Filter für Inhalte bindet auf macOS-Geräten den Inhaltsfilter einer Drittanbieter-App ein (Filtertyp Plugin), z. B. einer Filter-App mit Network Extension. Die Filterung selbst übernimmt diese App.

> Relution hat keinen Einfluss auf die gefilterten Inhalte. Welche Inhalte gefiltert werden, bestimmt der Anbieter der Filter-App.

In macOS-Richtlinien gibt es keine Auswahl Filter-Typ: Der Filtertyp ist fest auf Plugin gesetzt. Der integrierte Filter (Built In) mit Auto-Filter aktivieren, Gesperrte URLs, Erlaubte URLs und Bestimmte Lesezeichen steht nur in iOS-Richtlinien zur Verfügung, siehe Filter für Inhalte unter iOS →. Einen in macOS integrierten Webfilter mit Sperr- und Zulassungslisten bietet die macOS-Konfiguration Bildschirmzeit im Abschnitt Filter für Webinhalte.

Voraussetzungen

- Das Gerät ist überwacht (Badge Wird überwacht) und über eine Geräteregistrierung eingeschrieben; für Benutzerregistrierungen steht die Konfiguration nicht zur Verfügung.
- Die Filter-App des Anbieters ist auf dem Gerät installiert.

Für Version 26.4.0

Konfiguration

Unter `Geräte` → `Richtlinien` wird die Konfiguration Filter für Inhalte in einer macOS-Richtlinie über Hinzufügen angelegt. Eine Richtlinie kann mehrere dieser Konfigurationen enthalten; sie werden über den Filternamen unterschieden.

Feld	Beschreibung
Filtername	Pflichtfeld. Name des Filters
ID	Pflichtfeld. Bundle-ID der App, die den Filteranbieter enthält
Dienstaddresse	Optional. Adresse des Filterdienstes, z. B. Hostname oder URL
Benutzername	Optional. Benutzername für die Anmeldung beim Filterdienst
Passwort	Optional. Passwort für die Anmeldung beim Filterdienst; nur zusammen mit einem Benutzernamen zulässig
Payload Zertifikat	Optional. Zertifikat (PKCS#1 oder PKCS#12) aus der Zertifikatsverwaltung für die Anmeldung beim Filterdienst
Verkehr-Filter Typ	Socket-basiert (Standard) filtert den Netzwerkverkehr auf Socket-Ebene, WebKit den Verkehr von WebKit-Browsern; es ist genau eine Option aktiv

Aufbewahrung der Safari-Historie erzwingen

Der Schalter Aufbewahrung der Safari-Historie erzwingen gilt ab macOS 26 und ist standardmäßig aktiviert. Ist er aktiviert, kann der Safari-Verlauf auf dem Gerät nicht gelöscht werden und das private Surfen ist deaktiviert. Ist er deaktiviert, bleibt das Löschen des Verlaufs möglich.

Für Version 26.4.0

Relution Decon (Inhaltsfilter)

Ab Version 26.5 ermöglicht Relution die Einrichtung eines DNS-basierten Inhaltsfilters für macOS-Geräte. Diese Funktion sorgt für einen sicheren und fokussierten Internetzugang, indem der Zugriff auf ausgewählte Webseiten und Apps eingeschränkt wird. Dank der KI-gestützten Kategorisierung von Inhalten bietet Relution Decon einen umfassenden Jugendschutzfilter mit erweiterten Einstellungsmöglichkeiten.

Was ist Relution Decon?

Relution Decon ist ein KI-gestütztes Add-on für macOS, das Inhalte in Echtzeit filtert und ein sicheres digitales Umfeld schafft. Mithilfe der DNS-basierten Inhaltskontrolle blockiert Decon unerwünschte Webseiten und Apps, sodass Benutzer in einem geschützten, ablenkungsfreien Raum arbeiten und lernen können.

Relution Decon nutzt einen DNS-Proxy, um alle Anfragen an den Decon-Server weiterzuleiten. Dort werden Webseiten klassifiziert und gemäß den Richtlinien entweder erlaubt oder blockiert. Dank SSL-Verschlüsselung bleiben alle Datenübertragungen sicher, und die Nutzeraktivitäten geschützt.

Decon App

Für Version 26.4.0

Die Decon-App wird bei der Richtlinieninstallation automatisch auf den macOS-Geräten bereitgestellt. Sie überwacht die DNS-Anfragen des Geräts und stellt sicher, dass nur zugelassene Inhalte aufgerufen werden können.

Funktionen der App:

- Aktiviert einen systemweiten DNS-Proxy, der vom Benutzer nicht deaktiviert werden kann
- Zeigt den aktuellen Status von Relution Decon an
- Gibt Einsicht in blockierte Webseiten und die angewendeten Filterkategorien

> Empfehlenswert: Vor der Verteilung ausreichend Lizenzen für die App über Apps und Bücher (im Portal: VPP) bereitstellen.

Apps und Bücher (VPP) in Relution einrichten →
Relution Decon im Apple App Store →

Decon Richtlinie

Die Konfiguration wird in der Geräte-Richtlinie über `Hinzufügen` → `Relution Decon` angelegt. Mit dieser Richtlinie wird die Decon-App automatisch auf den Geräten installiert und fungiert als Proxy für alle DNS-Anfragen. Anders als unter iOS werden auf macOS zusätzlich eine Managed App Konfiguration → und die Freigabe der Systemerweiterung benötigt — beides richtet Relution automatisch ein.

Die Konfiguration wird mit der Veröffentlichung der Richtlinie abgeschlossen.

Auf macOS steht Relution Decon ausschließlich für Geräte mit Geräteeinschreibung zur Verfügung. Bei der Benutzer Einschreibung → kann die Konfiguration nicht hinzugefügt werden.

Voraussetzung ist eine Lizenz, die Relution Decon umfasst. Ohne diese Lizenz zeigt die Konfiguration einen Hinweis an und kann nicht gespeichert werden.

> Enthalten die auf einem Gerät angewendeten Richtlinien bereits eine Konfiguration **DNS Proxy**, setzt Relution den DNS-Proxy für Decon nicht. Das Gerät erhält dann den Compliance-Hinweis **DNS-Proxy für Decon kann nicht gesetzt werden, da der Konfigurationstyp bereits existiert**.

Hierarchie der Richtlinienkonfiguration (höchste zu niedrigste Priorität)

1. Apps auf der Positivliste
2. Apps auf der Sperrliste
3. Erlaubte Domains
4. Gesperrte Domains
5. Blockierte Kategorien

Decon in Relution Teacher

Auf macOS-Geräten kann Decon ab Relution Server 26.5 in Unterrichtsprofilen ausgewählt und gesteuert werden. Voraussetzung: Die Schülergeräte sind mit einer Decon-Richtlinie versehen. Einen Hinweis auf eine fehlende Decon-Konfiguration zeigt Relution Teacher nur für iOS-Geräte an, nicht für macOS-Geräte.

Für Version 26.4.0

Mehr zu Relution Teacher →

Hinweis: Ist Decon im Unterrichtsprofil aktiviert, wird für die Dauer der Unterrichtsstunde die sonst gültige Decon-Konfiguration vollständig überschrieben. Freigegebene oder gesperrte Domains aus den Relution Decon Anfragen gelten in dieser Zeit nicht.

Filtern

Im Abschnitt Filtern der Decon-Richtlinie wird über Filter-Typ festgelegt, wonach Webseiten gefiltert werden:

- Aus: Es wird weder nach Kategorien noch nach Altersstufe gefiltert.
- Kategorien (Standard): Die zu blockierenden Kategorien werden einzeln per Schalter gewählt. Die Schalter erscheinen nur bei diesem Filter-Typ. Standardmäßig blockiert sind Erwachseneninhalte, Werbung und Phishing.
- Altersstufe: Gefiltert wird nach einer Altersstufe (0+, 6+, 12+ oder 16+, Standard 12+).

Unabhängig vom Filter-Typ stehen zwei weitere Schalter zur Verfügung:

- BPJM-Liste: Filtert zusätzlich Inhalte, die von der BPjM als unzulässig eingestuft wurden. Einträge unter Erlaubte Domains können den Zugriff auf solche Inhalte dennoch ermöglichen.
- Sichere Suche: Wird unabhängig von den blockierten Kategorien und der Altersstufe geschaltet. Das Blockieren der Kategorie Erwachseneninhalte aktiviert die sichere Suche nicht.

Werden auf einem Gerät mehrere Decon-Konfigurationen verwendet, kommt automatisch die stärkste Filterung zum Tragen: Filter nach Altersstufe gehen Filtern nach Kategorien vor. Konfigurationen ohne Filterung werden ignoriert.

Klassifizierung nach Kategorien

Relution Decon ordnet Webseiten automatisch einer Kategorie zu. Beim Filter-Typ Kategorien legen Administratoren fest, welche Kategorien blockiert werden:

Kategorie	Beschreibung	Beispiele
Erwachseneninhalte	Nicht für Jugendliche geeignete Seiten	Pornografie, Gewalt, Waffen, Drogen, Gambling, Adult Entertainment, Adult Shopping, Dating
Werbung	Werbeseiten	Ad Providers
Soziale Medien	Social-Media-Inhalte	Facebook, Instagram, TikTok, etc.
Unterhaltung	Unterhaltung, z. B. Streaming oder Spiele	Movies, Games, Videos
Musik	Musik-Streaming-Anbieter	Spotify, Tidal, etc.
Nachrichten	Nachrichten und Magazine	News, Wetter
Einkaufen	Online-Shops (außer adult content)	Amazon, eBay, etc.
Bildung	Lerninhalte	Wikipedia, Google Scholar
Generative KI	KI-spezifische Webseiten	ChatGPT, Perplexity.ai, etc.
Phishing	Potenzielle Phishing-Webseiten	Potential scams, Data theft
Sonstiges	Alles Andere	Rest

Erlaubte und gesperrte Apps und Domains

- Apps auf der Positivliste / Apps auf der Sperrliste (Abschnitt Apps): Der Internetzugang einzelner Apps wird gezielt freigegeben oder gesperrt, Basisfunktionen bleiben erhalten.
- Erlaubte Domains / Gesperrte Domains (Abschnitt Domains): Einzelne Domains werden gezielt freigegeben oder gesperrt (keine Pfadunterscheidung). Erlaubte Domains sind auch dann erreichbar, wenn der Filter sie als unpassend einstuft. Die Anzahl gesperrter Domains sollte auf etwa 500 begrenzt werden.

Unabhängig von diesen Listen sind die URL des Relution Servers, der Decon-Server sowie die Relution-Apps (Relution Agent, Teacher, Files, Assets und Decon) immer freigegeben. Zusätzlich übernimmt Relution die organisationsweit unter `Einstellungen` → `Relution Decon Anfragen` erlaubten und gesperrten Domains in jede Decon-Konfiguration.

Erweiterte DNS-Konfiguration

DNS-Server auf dem Gerät: Alternative DNS-Server können hinterlegt werden, falls Relution Decon DNS nicht erreichbar ist. Fallback: Cloudflare Families DNS (1.1.1.3).

DNS-Server auf dem Relution Decon Server: Ersetzt den Standard-DNS für den Decon-Server. IP-Adressen (UDP) oder DNS-over-HTTPS (DoH) wie Zero oder Quad9 sind möglich.

Limitierungen

- Zwischenspeicherung: Blockierungen und Richtlinienänderungen können bis zu 1 Minute verzögert umgesetzt werden.
- Pfadunabhängigkeit: DNS arbeitet auf Domain-Ebene, keine Unterscheidung von Unterseiten.
- App-Blockierung: Nur Internetzugang wird gesperrt, Basisfunktionen und zwischengespeicherte Inhalte bleiben verfügbar.

AirPrint

Für Version 26.4.0

Mit der Richtlinienkonfiguration AirPrint werden AirPrint-fähige Drucker auch auf macOS-Geräten per Konfigurationsprofil bereitgestellt. Die hinterlegten Drucker stehen anschließend im Druckdialog zur Verfügung, ohne dass sie im lokalen Netzwerk über Bonjour gefunden werden müssen — etwa wenn Mac und Drucker in unterschiedlichen Subnetzen bzw. VLANs liegen.

Konfiguration

Die Konfiguration wird unter `Geräte` → `Richtlinien` in einer macOS-Richtlinie über Konfiguration hinzufügen → AirPrint angelegt. Die Felder Hostname oder IP-Adresse, Port, Pfad der Ressource und TLS verwenden sowie die Voraussetzungen und die Ermittlung des Ressourcenpfads sind mit iOS identisch und im iOS-Artikel beschrieben:

- AirPrint für iOS →

Setup-Assistent

Mit der Konfiguration Setup-Assistent lassen sich Einrichtungsschritte ausblenden, die macOS auf einem bereits eingerichteten Mac anzeigt, z. B. bei der ersten Anmeldung eines weiteren Benutzers oder nach einem Softwareupdate. Für Geräte mit Benutzerregistrierung (User Enrollment/BYOD) ist die Konfiguration nicht verfügbar.

Unterschied zum DEP-Profil

Die im Konfigurationsprofil → der Automatischen Geräteregistrierung (ADE, im Portal: DEP) gewählten Setup-Schritte gelten nur für die Ersteinrichtung des Macs. Die Konfiguration Setup-Assistent wird dagegen per Richtlinie auf dem eingeschriebenen Gerät installiert und wirkt auf Einrichtungsschritte, die macOS danach anzeigt.

Die Konfiguration ist damit keine Voraussetzung für die Einschreibung. Sie wird nur benötigt, wenn auch nach der Ersteinrichtung keine zusätzlichen Einrichtungsschritte angezeigt werden sollen.

Einstellungen

Für Version 26.4.0

Im Bereich Allgemein wird pro Einrichtungsschritt festgelegt, ob er übersprungen wird:

- Barrierefreiheit überspringen
- Darstellung überspringen
- Cloud-Einrichtung überspringen (Anmeldung mit dem Apple Account)
- iCloud-Einrichtung überspringen (iCloud-Speicher)
- Datenschutz-Einrichtung überspringen
- Siri-Einrichtung überspringen
- True Tone Einrichtung überspringen
- Bildschirmzeit-Einrichtung überspringen
- Touch ID-Einrichtung überspringen
- Entriegelung mit Apple Watch überspringen
- Hintergrundbild überspringen

Apple hat diese einzelnen Einstellungen ab macOS 15 als veraltet gekennzeichnet. Für neuere macOS-Versionen sieht Apple stattdessen eine Liste der zu überspringenden Setup-Schritte vor. Diese Liste bietet Relution derzeit nur in der iOS-Konfiguration an.

Apple erlaubt pro Gerät nur eine Konfiguration Setup-Assistent. Einem Gerät sollten daher nicht mehrere Richtlinien mit dieser Konfiguration gleichzeitig zugewiesen werden.

Restriktionen

Mit der Richtlinien-Konfiguration Restriktionen werden Funktionen auf verwalteten macOS-Geräten eingeschränkt oder freigegeben. Die Konfiguration entspricht dem Apple-Payload für Einschränkungen; welche Einstellungen ein Gerät tatsächlich übernimmt, hängt von der macOS-Version und davon ab, ob das Gerät im überwachten Modus (Supervised) verwaltet wird.

Die folgende Übersicht folgt dem Aufbau des Formulars im Portal. Viele Restriktionen setzen eine bestimmte macOS-Version voraus; die Mindestversion steht im Formular als Hinweis an der Restriktion (z. B. macOS 14+) und ist in der Übersicht angegeben. Restriktionen mit dem Hinweis Wird überwacht wirken nur auf überwachten Geräten, Restriktionen mit dem Hinweis Unterstützt Benutzerregistrierung auch auf Geräten mit Benutzerregistrierung. Restriktionen mit dem Hinweis Veraltet hat Apple als veraltet eingestuft, Restriktionen mit dem Hinweis Veraltet auf nicht überwachten Geräten gelten nur auf nicht überwachten Geräten als veraltet.

> Relution überträgt alle Schalter mit ihrem aktuellen Wert an das Gerät. Ist eine Funktion deaktiviert, wird sie in der Regel auf dem Gerät gesperrt; Optionen, die ein Verhalten erzwingen (etwa „⋯ erzwingen“), wirken erst, wenn sie aktiviert sind.

Standardmäßig sind alle Optionen aktiviert, ausgenommen Diktat nur auf dem Gerät erzwingen, die drei Schalter Verzögerung der Sichtbarkeit von ⋯ erzwingen, Siri Schimpfwortfilter aktivieren, Darstellung einer Bildschirmaufnahme-Warnung erlauben und die vier Classroom-Einschränkungen. Die Altersbeschränkungen stehen auf Alle, die Liste Zulässige Workspace-IDs für die externe Integration ist leer. Eine neue Konfiguration schränkt ohne Anpassungen somit keine Funktion ein.

Über das Download-Symbol oben im Formular (Restriktionen als CSV-Datei exportieren) lassen sich die eingestellten Werte einschließlich noch nicht gespeicherter Änderungen als CSV-Datei herunterladen.

Von den Empfohlenen Restriktionen für iOS/iPadOS → betreffen nur die Hinweise zu Alle Inhalte & Einstellungen löschen und zur Verzögerung von Betriebssystem-Updates auch macOS.

Für Version 26.4.0

Gerät

Die Restriktionen für das Gerät sind in drei Bereiche gegliedert.

Geräterestriktionen

Alle Restriktionen anzeigen

Restriktionen bei der Authentifizierung

Alle Restriktionen anzeigen

Aktualisierungs-Restriktionen

Dieser Bereich ist im Portal als Veraltet gekennzeichnet, da Apple die Einstellungen als veraltet eingestuft hat. Für neue Richtlinien ist stattdessen die Konfiguration Softwareupdates → vorgesehen.

Die Felder für die Verzögerung in Tagen lassen sich erst bearbeiten und werden erst an das Gerät übertragen, wenn der zugehörige Schalter ··· erzwingen aktiviert ist. Erlaubt sind Werte von 1 bis 90 Tagen.

Alle Restriktionen anzeigen

Apps

Die folgenden Einschränkungen betreffen einzelne Apps und Dienste.

App-Restriktionen

Alle Restriktionen anzeigen

Safari-Optionen für JavaScript, Pop-ups oder die Betrugswarnung bietet Relution für macOS nicht an. Das Löschen des Verlaufs, privates Surfen, die Zusammenfassung von Inhalten und die Startseite für neue Tabs lassen sich ab macOS 26 zusätzlich über die Konfiguration Safari-Einstellungen → steuern.

Für Version 26.4.0

Einstellungen

Die folgenden Einschränkungen betreffen die Systemeinstellungen des Geräts und die App Classroom.

Einschränkungen der Einstellungen

Alle Restriktionen anzeigen

Classroom Einschränkungen

Alle Restriktionen anzeigen

Medien

Die folgenden Einschränkungen betreffen Medieninhalte. Alle Optionen dieses Bereichs setzen macOS 15 voraus (macOS 15+).

Einschränkungen für die Medien

Alle Restriktionen anzeigen

Änderungen

Diese Einschränkungen legen fest, welche Einstellungen am Gerät geändert werden dürfen.

Einschränkungen für Änderungen

Alle Restriktionen anzeigen

iCloud

Die folgenden Einschränkungen betreffen die iCloud-Dienste auf dem Gerät.

iCloud-Einschränkungen

Alle Restriktionen anzeigen

Für Version 26.4.0

Restriktionen für AI-Funktionen

Diese Einschränkungen steuern die Apple-Intelligence-Funktionen.

Alle Restriktionen dieses Abschnitts sind im Portal als Veraltet gekennzeichnet. Für Geräte ab macOS 26.4 stehen dafür die Konfigurationen Intelligence-Einstellungen → (Apple-Intelligence-Bericht, Genmoji, Image Playground, Schreibwerkzeuge) und Externe Intelligenz-Einstellungen → (externe Intelligence-Integrationen, Anmeldung, Workspace-ID) zur Verfügung. Für Geräte mit älteren macOS-Versionen gelten weiterhin die hier beschriebenen Restriktionen.

Allgemein

Alle Restriktionen anzeigen

Verwandte Themen

- Restriktionen für iOS und iPadOS → — Die Einstellungen für iOS und iPadOS im Überblick.
- Softwareupdates → — Nachfolger der Aktualisierungs-Restriktionen.
- Safari-Einstellungen → — Weitere Safari-Optionen ab macOS 26.
- Intelligence-Einstellungen → — Nachfolger der Restriktionen für AI-Funktionen ab macOS 26.4.
- Externe Intelligenz-Einstellungen → — Externe Intelligence-Dienste ab macOS 26.4.

Für Version 26.4.0

MS Office Volumenlizenz 2024

Lizenzierung von Microsoft Office LTSC 2024 auf macOS-Geräten mithilfe des VL Serializers in Relution.

Damit Microsoft Office Apps auf macOS verwendet werden können, müssen diese mit dem Paket `Microsoft_Office_LTSC_2024_VL_Serializer.pkg` lizenziert werden.

Die Herausforderung hierbei ist, dass die PKG während der Installation ihren internen Paketnamen ändert. Da es sich nicht um eine klassische App handelt, scheitert die übliche Vorgehensweise für native Apps in Relution.

Daher sind zusätzliche Schritte notwendig, um:

- Die Geräte korrekt mit der PKG auszustatten.
- Die Office Apps erfolgreich zu lizenzieren.
- Die Geräte konform zu halten.

VL Serializer vorbereiten

Die benötigte PKG kann im Microsoft Admin Center → heruntergeladen werden.

Relution-Konfiguration

Für Version 26.4.0

1. Die PKG in den Relution App Store hochladen.
2. Im Abschnitt Erkennungsregeln der App über Hinzufügen eine Regel vom Typ Package Name anlegen (ohne Erkennungsregel lässt sich die App nicht speichern) und im Feld Package Name folgenden Wert eintragen, damit Relution den Installationsstatus korrekt interpretieren kann:

```
com.microsoft.office.licensingV2.helper
```

Bereitstellung der PKG

Die PKG muss auf die Endgeräte übertragen werden. Hierfür stehen zwei Wege zur Verfügung:

Manuelle Installation

Die PKG wird händisch auf das jeweilige Gerät kopiert und lokal ausgeführt. Dies ist für größere Rollouts jedoch nicht effizient.

Automatisierte Installation (empfohlen)

- Bereitstellung über ein Relution-Skript, das unter `Skripte` → `Skripte` angelegt und vom macOS Companion ausgeführt wird: einmalig über die Aktion Shell-Skript ausführen bzw. Auf Gerät ausführen oder zeitgesteuert über die Konfiguration Script einer macOS-Richtlinie.
- Download der Datei nach `/Users/Shared/`.
- Anschließende stille Installation über das Terminal.

Download & Installation

Dieses Skript lädt den Serializer von einer externen Quelle (z.B. dem eigenen Fileserver) und installiert ihn direkt.

```
#!/bin/bash

# Konfiguration
URL="https://ihr-share.com/link/zur/datei"
PKG="/Users/Shared/Microsoft_Office_LTSC_2024_VL_Serializer.pkg"

echo "Download startet..."
if ! curl -fL "$URL" -o "$PKG"; then
    echo "Fehler: Download fehlgeschlagen."
    exit 1
fi

echo "Serializer gefunden – Installation startet..."
/usr/sbin/installer -pkg "$PKG" -target /

if [ $? -eq 0 ]; then
    echo "Installation erfolgreich abgeschlossen."
    rm "$PKG" # Optional: Installer nach Erfolg löschen
    exit 0
else
    echo "Fehler: Installation fehlgeschlagen."
    exit 1
fi
```

Installation einer lokal vorhandenen PKG

Falls die Datei bereits im Shared-Ordner abgelegt wurde, nutzt man dieses Skript:

```bash
#!/bin/bash

PKG="/Users/Shared/Microsoft_Office_LTSC_2024_VL_Serializer.pkg"

if [ -f "$PKG" ]; then
    echo "Serializer gefunden – Installation startet..."

    sudo /usr/sbin/installer -pkg "$PKG" -target /

    if [ $? -eq 0 ]; then
        echo "Installation erfolgreich abgeschlossen."
        exit 0
    else
        echo "Fehler: Installation fehlgeschlagen."
        exit 1
    fi
else
    echo "Fehler: PKG Datei nicht unter $PKG gefunden."
    exit 1
fi
```

Verteilung über App-Konformität

Für Version 26.4.0

Sobald die PKG in Relution hochgeladen und die Erkennungsregel hinterlegt ist, kann sie über die Konfiguration App Konformität einer macOS-Richtlinie verwaltet werden:

1. In der Konfiguration die App unter Erforderliche Apps hinzufügen und die Richtlinie veröffentlichen. Ist für die App Auto Installation aktiviert, installiert Relution die hochgeladene PKG selbst auf Geräten, auf denen der Identifier fehlt; die Erkennungsregel verhindert dabei erneute Installationen.
2. Relution prüft anhand der Erkennungsregel, ob der Identifier `com.microsoft.office.licensingV2.helper` in der Liste der installierten Apps des Geräts enthalten ist (bei aktiviertem Versionscheck zusätzlich die Version). Ob Office tatsächlich lizenziert ist, prüft Relution nicht.
3. Geräte ohne diesen Identifier werden als Nicht konform markiert, sofern unter `Einstellungen` → `Geräteverwaltung` → `Geräteverwaltung` die Option Konformitätsverletzungen anlegen, falls erforderliche Apps fehlen aktiv ist (Standard). Auf diesen Geräten kann das Skript erneut ausgeführt werden.

Adobe Creative Cloud Apps

Bereitstellung von Adobe-Apps (Creative Cloud, Acrobat, Photoshop) auf macOS-Geräten über Relution sowie deren Aktualisierung mit dem Remote Update Manager.

Adobe Apps lassen sich nicht wie eine klassische native App über Relution installieren. Der Grund: Adobe Pakete sind keine einfachen stillen Installer, sondern starten während der Installation eigene Hintergrundprozesse (Creative Cloud Desktop / HyperDrive). Diese laufen im eingeschränkten Kontext des nativen MDM-Befehls nicht zuverlässig durch – der Upload der PKG gelingt, die Installation bleibt jedoch hängen oder scheitert.

Daher wird die Installation über ein Skript ausgeführt (macOS Companion). Updates werden zentral über den Remote Update Manager gesteuert.

Warum ein Skript nötig ist

- Installation: `installer -pkg … -target /` läuft im vollen Root-Kontext, so wie Adobe es dokumentiert. Der angemeldete Benutzer benötigt dafür keine Administratorrechte.
- Kein Datei-Push: Der macOS Companion liefert keine Datei mit. Die PKG muss daher per Netzwerk bezogen (heruntergeladen) werden.
- Updates: Im Managed-Paket ist das Auto-Update für Endnutzer deaktiviert. Aktualisierungen erfolgen über ein wiederkehrend ausgeführtes Update-Skript, das den Remote Update Manager (RUM) aufruft.

Für Version 26.4.0

Paket in der Admin Console erstellen

1. In der Adobe Admin Console → anmelden und zu Pakete navigieren.
2. Ein Managed Package erstellen. Dabei alle Apps auswählen, die auf den Geräten installiert werden sollen – mehrere Apps (z. B. Photoshop, Illustrator, Acrobat) werden in einer PKG gebündelt.
3. In den Management-Optionen Remote Update Manager (RUM) aktivieren. Damit wird das RUM-Binary mit der PKG auf die Geräte ausgeliefert und steht später für Updates zur Verfügung.
4. Das fertige Paket herunterladen. Der Installer liegt im Paketordner unter `Build/<Paketname>_Install.pkg`.

Hinweis zur Aufteilung: Erhalten alle Nutzer denselben App-Satz, genügt ein kombiniertes Paket. Sollen verschiedene Gruppen unterschiedliche Apps erhalten, wird pro App bzw. Bündel ein eigenes Paket erstellt und der jeweiligen Gerätegruppe zugewiesen. Das Update-Skript (siehe unten) bleibt in beiden Fällen dasselbe.

Bereitstellung der PKG

Da der Companion keine Datei mitliefert, muss die PKG an einem per Netzwerk erreichbaren Ort liegen, von dem das Skript sie herunterlädt – z. B. ein interner Webserver oder Cloud-Storage.

Wichtig: Einen dauerhaften Speicherort verwenden. Der Download-Link aus der Adobe Admin Console ist temporär und session-gebunden und eignet sich nicht als feste Bezugsquelle. Das Paket einmalig herunterladen und selbst bereitstellen. Außerdem auf einen Dateinamen ohne Leerzeichen achten.

Skripte zur Automatisierung

Voraussetzung: Der macOS Companion ist unter `Einstellungen` → `Relution Client Apps` über macOS Companion aktivieren eingeschaltet. Auf Geräten mit einer macOS-Version kleiner als 12 und auf benutzerseitig eingeschriebenen Geräten wird der Companion nicht bereitgestellt; dort lässt sich dieses Verfahren nicht anwenden.

Der Rollout besteht aus einer einmaligen Erstinstallation und einer wiederkehrenden Aktualisierung. Beide Skripte werden unter `Skripte` → `Skripte` über Skript hinzufügen als Shell-Skript für macOS angelegt und vom macOS Companion auf dem Gerät ausgeführt:

- Erstinstallation: Das Skript wird einmalig über die Aktion Shell-Skript ausführen auf dem Gerät bzw. der Gerätegruppe gestartet, alternativ über Auf Gerät ausführen in der Skriptliste (siehe Verfügbare Aktionen →).
- Aktualisierung: In einer macOS-Richtlinie wird die Konfiguration Script hinzugefügt und das Update-Skript ausgewählt. Im Abschnitt Zeitbasierte Ausführung werden die Wochentage (Wiederholt sich am) und die Startzeit festgelegt (siehe Verfügbare Konfigurationen →).

Ausführungsstatus sowie Ergebnis- und Fehlerausgabe jeder Ausführung sind zusätzlich zur Logdatei auf dem Gerät in der Historie des jeweiligen Skripts unter `Skripte` → `Skripte` einsehbar.

Erstinstallation (empfohlen)

Adobe-Pakete sind oft mehrere Gigabyte groß. Ein direkter Download innerhalb eines Relution-Skripts kann das Skript-Timeout überschreiten und wird dann abgebrochen. Das Timeout wird am Skript im Feld Zeitüberschreitung (in Minuten) festgelegt (Standard 5, höchstens 30 Minuten). Das folgende Skript umgeht das: Es installiert einen LaunchDaemon, der Download, Installation und den ersten Update-Lauf entkoppelt im Hintergrund ausführt. Das Relution-Skript selbst ist in Sekunden fertig.

Pro Paket wird lediglich `PKG_URL` und `APP_LABEL` gesetzt.

> Vollständiges Konfigurationsbeispiel anzeigen

Das Ergebnis wird protokolliert unter `/var/log/relution_adobe_deploy.log`.

Laufende Updates

Dieses Skript wird als Konfiguration Script in einer macOS-Richtlinie zugewiesen und damit wiederkehrend ausgeführt (z. B. einmal pro Woche). Es benötigt keinen Download – der Remote Update Manager bezieht die Updates direkt von Adobe. Ohne Angabe von Produkten werden alle installierten Adobe-Apps gemeinsam aktualisiert; ein separates Skript pro App ist nicht nötig.

Für Version 26.4.0

```bash
#!/bin/bash
RUM_BIN="/usr/local/bin/RemoteUpdateManager"
RUM_PRODUCTS=""   # leer = alle Apps; sonst SAP-Codes, z. B. "APRO,PHSP"
LOG="/var/log/relution_adobe_update.log"

log() { echo "$(date '+%Y-%m-%d %H:%M:%S') $1" | tee -a "$LOG"; }

if [ ! -x "$RUM_BIN" ]; then
    log "FEHLER: RUM nicht gefunden – ist eine Adobe-App installiert?"
    exit 2
fi

log "=== RUM-Update gestartet ==="
if [ -n "$RUM_PRODUCTS" ]; then
    "$RUM_BIN" --action=install --productVersions="$RUM_PRODUCTS" >>"$LOG" 2>&1
else
    "$RUM_BIN" --action=install >>"$LOG" 2>&1
fi
log "RUM beendet (RC $?)."
```

SAP-Codes für die gezielte Aktualisierung einzelner Apps: `APRO` (Acrobat), `PHSP` (Photoshop), `ILST` (Illustrator), `IDSN` (InDesign), `PPRO` (Premiere Pro), `AEFT` (After Effects).

Für Version 26.4.0

Alternative: Self-Service

Sollen die Nutzer ihre Adobe Apps selbst installieren, statt sie zentral auszurollen, wird in der Admin Console stattdessen ein Self-Service-Paket erstellt (bzw. im Paket die Optionen Enable self-service install und Allow non-admins to update and install apps aktiviert). Das Skript installiert dann nur die Creative Cloud Desktop App; die eigentlichen Apps wählt und installiert der Nutzer anschließend selbst. Voraussetzung ist eine Named-User-Lizenzierung mit passenden Produktprofilen. Ein zentrales Update-Skript entfällt, da Updates über die Desktop App laufen.

> Vollständiges Konfigurationsbeispiel anzeigen

Hinweis: Ist das Paket sehr groß und läuft der direkte Download ins Skript-Timeout, wird die entkoppelte LaunchDaemon-Variante aus Erstinstallation verwendet – dort einfach `PKG_URL` auf das Creative-Cloud-Desktop-App-Paket setzen und den RUM-Schritt weglassen.

Statusüberwachung über App-Konformität

In diesem Setup erfolgt die Installation über das Skript – es wird keine PKG in Relution hochgeladen. Die Konfiguration App Konformität einer macOS-Richtlinie dient daher nicht der Verteilung, sondern der Statusüberwachung: Die App wird über App manuell hinzufügen angelegt, im Feld Interner Name wird die Bundle-ID eingetragen.

1. In der Konfiguration App Konformität unter Erforderliche Apps über Hinzufügen die Quelle App manuell hinzufügen wählen (ohne PKG-Upload).
2. Einen Name vergeben und im Feld Interner Name die Bundle-ID eintragen, z. B. `com.adobe.acc.AdobeCreativeCloud`.
3. Relution prüft regelmäßig, ob diese Bundle-ID in der Liste der installierten Apps des Geräts enthalten ist.
4. Geräte ohne die App werden als Nicht konform markiert, sofern unter `Einstellungen` → `Geräteverwaltung` → `Geräteverwaltung` die Option Konformitätsverletzungen anlegen, falls erforderliche Apps fehlen aktiv ist (Standard). Dort kann anschließend das Installations-Skript (erneut) ausgeführt werden.

App-spezifische Erkennung (z. B. nur Photoshop): Relution prüft jede hinterlegte Bundle-ID gegen die Liste der installierten Apps des Geräts. Für eine app-spezifische Prüfung wird daher statt `com.adobe.acc.AdobeCreativeCloud` die Bundle-ID der einzelnen App hinterlegt (über App manuell hinzufügen). Die Bundle-ID lässt sich in der Liste der installierten Apps eines Geräts nachschlagen, auf dem die App bereits installiert ist. Voraussetzung ist, dass macOS die App in dieser Liste meldet.

Hinweise

- Lizenzierung (Named User Licensing): Nach der Installation meldet sich der Benutzer beim ersten Start mit seiner Adobe-ID an. Jede App benötigt ein passendes Produktprofil in der Admin Console – ohne Berechtigung ist die App zwar installiert, aber nicht nutzbar.
- Major-Upgrades: Der Remote Update Manager aktualisiert nur innerhalb der installierten Hauptversion (Basis- und Sicherheitsupdates). Der Wechsel auf eine neue Jahresgeneration erfordert ein neues Paket.
- Bildungsumgebungen: Für Adobe-Bildungskunden ist das automatische Update für Endnutzer nicht verfügbar; die Steuerung über den Remote Update Manager ist hier der vorgesehene Weg.
- Spotlight: Das Erstinstallations-Skript indexiert installierte Apps per `mdimport`, damit sie sofort über die Spotlight-Suche auffindbar sind – nicht nur im Finder.

Für Version 26.4.0

Platform SSO (PSSO)

Mit Relution ist es möglich, macOS Geräte so zu konfigurieren, dass sich Nutzer mit ihrem Microsoft Entra ID Konto direkt am Anmeldefenster anmelden können (Platform Single Sign-On). Dabei wird bei der ersten Anmeldung ein lokales Benutzerkonto erstellt, das mit der Entra ID Identität verknüpft ist.

Voraussetzung

- macOS 13 (Ventura) oder höher für Extensible SSO, macOS 15 (Sequoia) oder höher für Login-, Entsperr- und FileVault-Richtlinie, die Karenzzeiten und SSO-Konten außerhalb der Plattform, macOS 26 (Tahoe) für Setup-Assistent-Registrierung und authentifizierten Gastmodus. Microsoft empfiehlt mindestens macOS 14 (Sonoma).
- Mac mit Apple Silicon, wenn die empfohlene Methode *Secure-Enclave-Schlüssel* verwendet wird (siehe Authentifizierungsmethode wählen →). Auf Intel-Macs ist nur die Methode *Passwort* möglich.
- Microsoft Entra ID Tenant
- Berechtigung zur Geräte-Registrierung in Microsoft Entra ID für die Nutzer
- Microsoft Company Portal für Mac muss als App verfügbar sein und installiert werden, *bevor* die Nutzer für PSSO adressiert werden. Für die Registrierung während des Setup-Assistenten (macOS 26+) wird 5.2604.0 (April 2026) benötigt. Empfohlen wird immer die aktuelle Version – sie erfüllt beide Anforderungen.
- Netzwerkzugriff auf die Microsoft-/Apple-Anmelde-URLs (siehe Bereich Allgemein →). Diese URLs müssen erreichbar und von einer eventuellen TLS-Inspection ausgenommen sein, sonst schlägt die Registrierung fehl.

Für Platform SSO selbst muss Relution nicht mit Microsoft Entra ID verknüpft sein; die Konfiguration kommt ohne diese Anbindung aus. Die Verknüpfung wird nur benötigt, wenn zusätzlich Benutzer aus Entra ID synchronisiert oder Conditional Access → genutzt werden sollen: Relution mit Entra ID verknüpfen →. Für Conditional Access ist außerdem OIDC → erforderlich.

Für Version 26.4.0

Vorbereitung in Microsoft Entra ID

Bevor die Konfiguration in Relution ausgerollt wird, sollten folgende Punkte im Microsoft Entra Admin Center geprüft werden:

- Geräteeinstellungen: Unter `Identität` → `Geräte` → `Geräteeinstellungen` muss Benutzer dürfen Geräte mit Microsoft Entra ID verknüpfen auf Alle (oder auf die betroffene Zielgruppe) gesetzt sein.
- Multifaktor-Authentifizierung: Ist auf dem Konto klassische Per-User-MFA aktiviert, kann die PSSO-Registrierung fehlschlagen. Für die MFA-Anforderung wird stattdessen Conditional Access verwendet.
- Passwortkomplexität: Bei der Methode *Passwort* müssen die Komplexitätsanforderungen von lokalem Konto und Entra ID übereinstimmen, damit die Synchronisierung funktioniert.

Company Portal App hochladen

1. Die aktuelle Version von Microsoft Company Portal für Mac (.pkg) wird bei Microsoft heruntergeladen → und anschließend unter `Apps` → `App Store` über Hinzufügen als Native App in Relution hochgeladen (siehe Native Apps für macOS →).
2. Die App muss für die Zielgruppe bzw. Organisation freigegeben sein.

Die Company Portal App enthält die SSO-Extension `com.microsoft.CompanyPortalMac.ssoextension`, die für Platform SSO benötigt wird. Sie muss mindestens in Version 5.2404.0 vorliegen (für die Setup-Assistent-Registrierung unter macOS 26+: 5.2604.0).

Hinweis zu den Versionsnummern: Company Portal führt zwei Versionsangaben. Die `Über diese App`-Version folgt dem Schema `5.JJMM.x` (z. B. `5.2604.0` = April 2026), während die im Paket bzw. per `pkgutil` sichtbare Build-Nummer anders aussieht – z. B. `4.83.26040910`, wobei `260409` das Build-Datum (2026-04-09) ist. Beide bezeichnen dieselbe Version; ein Build aus 2026 erfüllt die PSSO-Anforderung problemlos.

Gerätegruppe und Richtlinien zuweisen

1. Für die Mac-Geräte, auf denen PSSO ausgerollt werden soll, wird eine Gerätegruppe angelegt.
2. Der Gerätegruppe wird im Bereich Richtlinien über Hinzufügen eine macOS-Richtlinie zugewiesen, die die beiden folgenden Konfigurationen enthält (eine gemeinsame Richtlinie oder zwei getrennte):
   - Erweiterbares Single Sign On (siehe Konfiguration der Richtlinie Erweiterbares Single Sign On →)
   - App Konformität: Unter Erforderliche Apps wird die hochgeladene Company Portal App über Hinzufügen eingetragen. Ist in der Spalte Auto Installation das Häkchen gesetzt (beim Hinzufügen Standard), installiert Relution die App automatisch. Ohne Auto Installation gilt das Gerät bei fehlender App lediglich als nicht konform.
3. Die Konfigurationen gelangen erst auf die Geräte, wenn die Richtlinie veröffentlicht ist.

Ohne installierte Company Portal App kann sich die SSO-Extension nicht registrieren. Relution verteilt das SSO-Profil unabhängig von der App-Installation; eine Reihenfolge zwischen beiden wird nicht erzwungen.

Für Version 26.4.0

Authentifizierungsmethode wählen

Die Authentifizierungsmethode bestimmt, wie sich die Nutzer am Gerät und an den Apps anmelden. Sie ist die wichtigste Entscheidung bei der Einrichtung und wird im Bereich Plattform SSO → der Konfiguration gesetzt.

Methode	Passwortlos	Lokales Passwort	Min. macOS	Geeignet für
Secure-Enclave-Schlüssel *(empfohlen)*	Ja, phishing-resistent	bleibt unverändert	13 / 14	Personalisierte Geräte, nur Apple Silicon
Passwort	Nein	wird mit Entra ID synchronisiert	13 / 14	Intel-Macs, geteilte/Lab-Geräte
Smartcard	Ja (über CBA)	bleibt unverändert	14+	Organisationen mit physischen Smartcards

Empfehlung: Für personalisierte Firmen-Macs (Apple Silicon) wird die Methode Secure-Enclave-Schlüssel empfohlen – sie ist passwortlos, hardwaregebunden und erfüllt phishing-resistente MFA. Für Intel-Geräte oder geteilte Geräte bietet sich Passwort an.

Wichtig: *Smartcard* wird während des Setup-Assistenten nicht unterstützt.

Registrierung im Setup-Assistenten (macOS 26+): Wird PSSO bereits im Einrichtungsassistenten registriert (Registrierung während des Einrichtungsassistenten aktivieren auf AN), muss auch Erstellen des ersten Benutzers während des Einrichtungsassistenten aktivieren auf AN stehen – unabhängig von der gewählten Methode. Andernfalls wird beim Setup kein lokales Konto angelegt und die Registrierung schlägt fehl (praktisch bestätigt):

- Methode Secure-Enclave-Schlüssel: die Anmeldung landet in einem Login-Loop.
- Methode Passwort: es erscheint `Anmelden nicht möglich – Registrierung fehlgeschlagen`.

Steht der Schalter auf AN, wird das erste lokale Konto über PSSO erstellt und die Anmeldung läuft in beiden Fällen durch.

Konfiguration der Richtlinie Erweiterbares Single Sign On

In einer Richtlinie für macOS wird die Konfiguration Erweiterbares Single Sign On hinzugefügt.

Für Version 26.4.0

Bereich Allgemein

Parameter	Wert
Kennung der Erweiterung	`com.microsoft.CompanyPortalMac.ssoextension`
Verweigerte Bündelkennungen	leer lassen (Standard)
Daten zur Erweiterung → `AppPrefixAllowList`	`com.microsoft.,com.apple.`
Daten zur Erweiterung → `browser_sso_interaction_enabled`	`1`
Daten zur Erweiterung → `disable_explicit_app_prompt`	`1`
Realm	leer lassen
Registrierungs-Token	leer lassen (für Entra ID nicht erforderlich – siehe Hinweis)
Verhalten bei gesperrtem Bildschirm	Nicht handhaben (Standard: Abbrechen)
Team Kennung	`UBF8T346G9` (Microsoft Team ID)
Typ	Umleitung (Standard: Anmeldedaten)
URLs	`https://login.microsoftonline.com` `https://login.microsoft.com` `https://sts.windows.net`

Pflichtfelder sind Kennung der Erweiterung, Team Kennung und beim Typ Umleitung die URLs. Beim Typ Anmeldedaten erscheint statt URLs das Feld Hosts.

Registrierungs-Token: Für Microsoft Entra ID wird im Extensible-SSO-Payload kein Registrierungs-Token benötigt; das Feld bleibt leer. (Das Feld ist für andere IdP-/Kerberos-Szenarien vorgesehen.)

URLs / TLS: Die drei Anmelde-URLs müssen im Netzwerk erreichbar und von einer TLS-Inspection ausgenommen sein.

Bereich Plattform SSO

Parameter	Wert	Hinweis
Name der Kontoanzeige	leer lassen	optional
Methode der Authentifizierung	Secure-Enclave-Schlüssel (im Portal: Benutzersicherer Enclave-Schlüssel)	Empfohlen; für Intel/geteilte Geräte: *Passwort* (Standard bei neuen Konfigurationen)
├── Login-Richtlinie	– (entfällt)	nur bei Methode *Passwort* sichtbar; macOS 15+
├── Richtlinie entsperren	– (entfällt)	nur bei Methode *Passwort* sichtbar; macOS 15+
├── FileVault Richtlinie	– (entfällt)	nur bei Methode *Passwort* sichtbar; macOS 15+
├── Offline Karenzzeit	– (entfällt)	nur bei Methode *Passwort* sichtbar; macOS 15+
└── Karenzzeit für die Authentifizierung	– (entfällt)	nur bei Methode *Passwort* sichtbar; macOS 15+
SSO-Konten außerhalb der Plattform	nicht gesetzt	macOS 15+
Häufigkeit der Anmeldung	`64800` (Sekunden, entspricht 18 Std.)	Re-Auth-Intervall; Standard `64800`, mindestens `3600`
Shared Device-Schlüssel verwenden	AN	Für die JIT-Kontoerstellung erforderlich, siehe Shared Device-Schlüssel und Kontoerstellung →; Standard: AUS
├── Autorisierung einschalten	AN	
└── Benutzer bei der Anmeldung erstellen aktivieren	AN	Just-in-Time-Provisioning des lokalen Kontos
Zusätzliche Gruppen	nicht gesetzt	optional
Administrator-Gruppen	nicht gesetzt	optional
Berechtigungsgruppen	nicht gesetzt	optional
Neuer Benutzerautorisierungsmodus	Standard	
Modus der Benutzerautorisierung	Standard	
Gerätekennungen in Attestierung zulassen	AUS	macOS 15.4+
Erstellen des ersten Benutzers während des Einrichtungsassistenten aktivieren	AN (Standard)	macOS 26+ — bei Registrierung im Setup-Assistenten erforderlich (sonst schlägt die Registrierung fehl)

Parameter	Wert	Hinweis
Authentifizierungsmethoden für neue Benutzer	nicht gesetzt	macOS 26+; Auswahl aus Passwort, Smartcard und Access Key. Bei Access Key erscheinen zusätzliche Felder für Lesegerät-Gruppenkennung, Terminalidentität, Ausstellerzertifikat und Expressmodus
Profilbild synchronisieren	AUS	macOS 26+
Schnellanmeldung für den authentifizierten Gastmodus aktivieren	AUS	macOS 26+
Registrierung während des Einrichtungsassistenten aktivieren	AN	macOS 26+
Kontoname	`com.apple.PlatformSSO.AccountShortName`	Platzhalter für den lokalen Kurznamen
Vollständiger Name	`name`	Platzhalter für den vollständigen Namen

Bei der Methode Passwort blendet das Portal zusätzlich Login-Richtlinie, Richtlinie entsperren und FileVault Richtlinie ein. Jede dieser Richtlinien bietet die Optionen Authentifizierung versuchen, Authentifizierung erforderlich, Offline-Karenzzeit zulassen und Karenzzeit für die Authentifizierung zulassen; Richtlinie entsperren zusätzlich Touch ID oder Uhr zum Entsperren zulassen. Die Felder Offline Karenzzeit und Karenzzeit für die Authentifizierung (vorbelegt mit `0`) sind erst bearbeitbar, wenn in mindestens einer der drei Richtlinien die zugehörige Option Offline-Karenzzeit zulassen bzw. Karenzzeit für die Authentifizierung zulassen gewählt ist. Bei den Methoden Smartcard und Benutzersicherer Enclave-Schlüssel werden diese Felder weder angezeigt noch übertragen.

Für Version 26.4.0

> Die mit macOS 26+ markierten Felder wirken nur auf Geräten mit macOS Tahoe 26 oder neuer und setzen voraus, dass die Registrierung bereits während des Einrichtungsassistenten (Setup Assistant) erfolgt.

Home > Richtlinien > PSSO >

Erweiterbares Single Sign On

Erweiterbares Single Sign On

Unterstützt Benutzerregistrierung

Abbrechen | Speichern

Allgemein

com.microsoft.CompanyPortalMac.ssoextension

Verweigerte Bündelkennungen

+ Hinzufügen

Name	Package-Name

Es sind keine Ergebnisse verfügbar

Daten zur Erweiterung

+ Hinzufügen

Schlüssel	Wert
AppPrefixAllowList	com.microsoft.,com.apple.
browser_sso_interaction_enabled	1
disable_explicit_app_prompt	1

Realm

{{DEVICEREGISTRATION}}

Nicht handhaben

UBF8T346G9

Umleitung

URLs *

https://login.microsoftonline.com | https://login.microsoft.com | https://sts.windows.net

Plattform SSO

Name der Kontoanzeige

Methode der Authentifizierung
Passwort

Login-Richtlinie macOS 15+

Richtlinie entsperren macOS 15+

FileVault Richtlinie macOS 15+

Offline Kennwort?
0 macOS 15+

Kennwort für die Authentifizierung?
0 macOS 15+

SSO-Konten außerhalb der Plattform + macOS 15+

Ablaufzeit der Anmeldung
64800

Shared Device-Schlüssel verwenden

Autorisierung einschalten

Benutzer bei der Anmeldung erstellen aktivieren

Zusätzliche Gruppen +

Administrator-Gruppen +

Berechtigungsgruppen

+ Hinzufügen

Schlüssel	Wert
Es sind keine Ergebnisse verfügbar	

Neue Benutzerautorisierungsmodus
Standard

Modus der Benutzerautorisierung
Standard

Gerätekennungen in Attestierung zulassen macOS 15.4+

Erstellen des ersten Benutzers während des Einrichtungsassistenten aktivieren macOS 26+

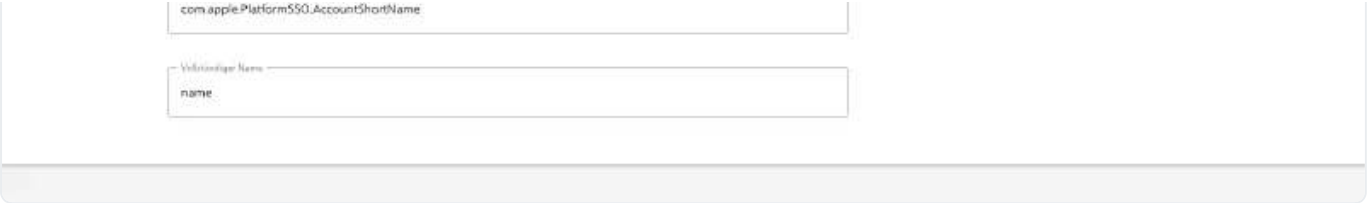
Authentifizierungsmethoden für neue Benutzer macOS 26+

Profilbild synchronisieren macOS 26+

Schnellanmeldung für den authentifizierten Gastmodus aktivieren macOS 26+

Registrierung während des Einrichtungsassistenten aktivieren macOS 26+

Homepage



Der Screenshot zeigt beispielhaft die Methode Passwort. Bei Secure-Enclave-Schlüssel (empfohlen, siehe Tabelle) blendet das Portal Login-Richtlinie, Richtlinie entsperren, FileVault Richtlinie sowie die beiden Karenzzeiten aus; die übrige Konfiguration ist identisch.

Weitere Konfiguration

- Eine der Gerätegruppe zugewiesene Richtlinie muss zusätzlich die Konfiguration App Konformität für Company Portal enthalten, damit die Extension zum Registrierungszeitpunkt bereits verfügbar ist.
- Für die Automatische Geräteregistrierung (ADE, im Portal: DEP) empfiehlt es sich, die Gerätegruppe mit den PSSO-Konfigurationen bereits in der Auto-Einschreibung zuzuweisen (`Geräte` → `Auto-Einschreibungen`, im Eintrag des Geräts Bereich Gerätegruppen → Statische Gerätegruppen), damit die Registrierung im Einrichtungsassistenten greifen kann (macOS 26+).

Shared Device-Schlüssel und Kontoerstellung

Für Version 26.4.0

Shared Device-Schlüssel verwenden muss AN sein, weil in diesem Ablauf die lokalen Konten per Just-in-Time-Provisioning angelegt werden (Schalter Autorisierung einschalten und Benutzer bei der Anmeldung erstellen aktivieren). Ohne Shared Device-Schlüssel würden benutzergebundene Schlüssel benötigt – die sich aber nicht erzeugen lassen, solange das Benutzerkonto noch gar nicht existiert (Henne-Ei-Problem).

> Autorisierung einschalten und Benutzer bei der Anmeldung erstellen aktivieren sind nur bei eingeschaltetem Shared Device-Schlüssel verwenden bedienbar. Ist der Schalter AUS, sind beide ausgegraut und werden nicht übernommen, auch wenn sie noch als AN angezeigt werden. Eine Kontoerstellung bei der Anmeldung findet dann nicht statt.

Methodenwahl je Gerätetyp:

- Personalisiertes Gerät (empfohlen): Methode Secure-Enclave-Schlüssel – passwortlos, hardwaregebunden, Touch ID.
- Geteiltes / Multi-User-Gerät (z. B. Klassenraum, Schichtbetrieb): Methode Passwort, da wechselnde Nutzer ohne vorab eingerichtete passwortlose Anmeldedaten auskommen. Solche Geräte werden ohne Benutzeraffinität registriert; Conditional Access wird auf geteilten Macs nicht unterstützt.

Hintergrundobjekte für Microsoft AutoUpdate freigeben

Ab macOS Ventura werden Hintergrundprozesse wie Microsoft AutoUpdate (MAU) standardmäßig blockiert bzw. Nutzer erhalten eine Benachrichtigung `Hintergrundobjekt hinzugefügt` und müssen das manuell bestätigen. Ohne diese Freigabe kann MAU nicht automatisch im Hintergrund aktualisieren – das betrifft auch Company Portal, da dessen Updates über MAU laufen.

Vorab freigeben lassen sich Hintergrundobjekte über ein Profil mit dem Payload `com.apple.servicemanagement` (verwaltete Anmeldeobjekte), z. B. mit einer Regel für die Team-ID von Microsoft (`UBF8T346G9`). Eine eigene Relution-Konfiguration für diesen Payload gibt es nicht; ein solches Profil lässt sich aber als `.mobileconfig`-Datei über die Konfiguration Apple Configurator 2 Konfiguration verteilen (siehe Apple Configurator 2 Konfiguration →).

Die Relution-Konfiguration Login-Elemente eignet sich dafür nicht: Sie legt fest, welche Apps bei der Anmeldung automatisch gestartet werden, genehmigt aber keine Hintergrundobjekte.

> Ohne diese Freigabe erscheinen bei den Nutzern wiederholt Systembenachrichtigungen zu neuen Hintergrundobjekten, und MAU aktualisiert die SSO-relevanten Komponenten ggf. nicht zuverlässig automatisch.

Registrierung durch die Endnutzer

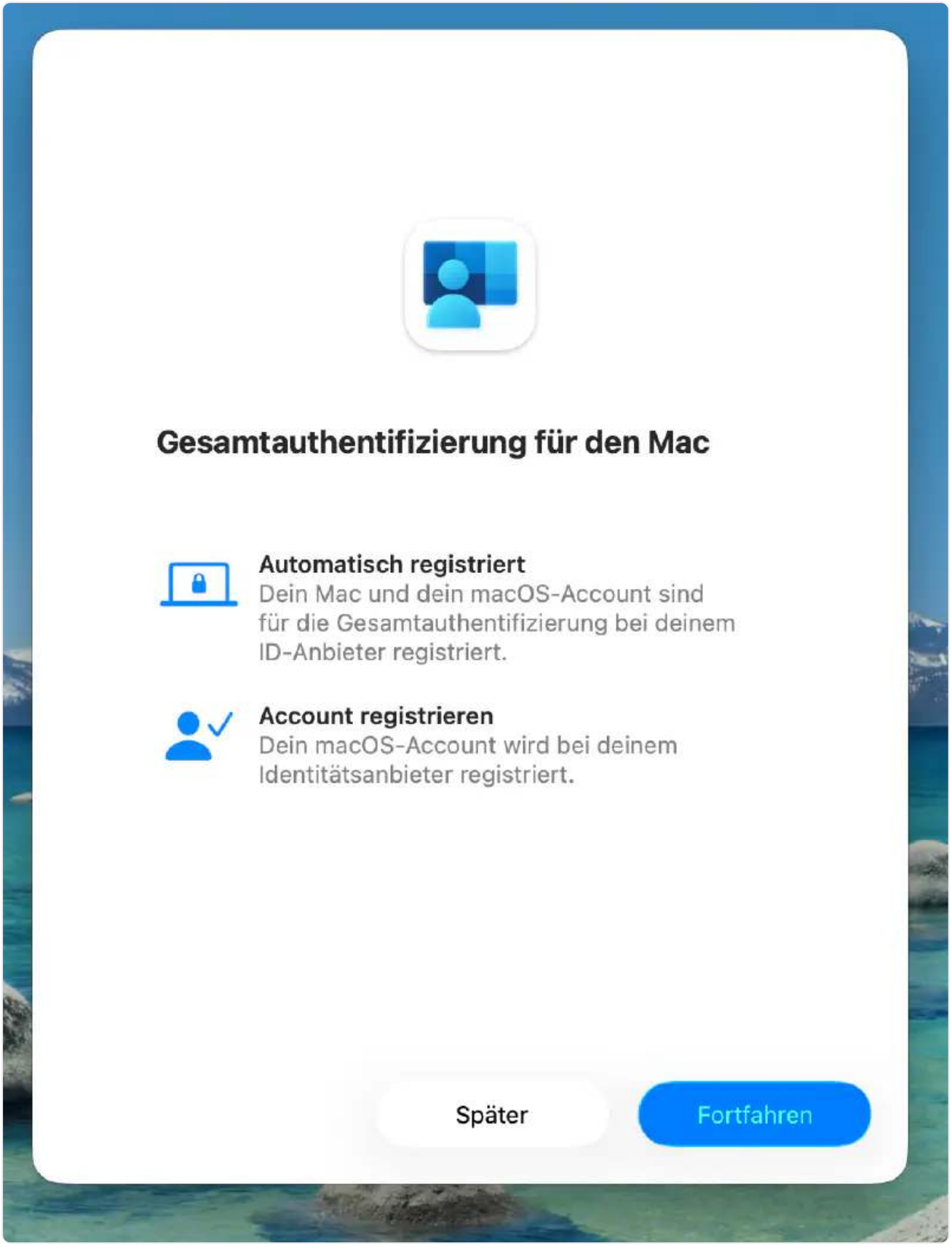
Nachdem die Konfiguration auf dem Gerät angekommen und die Company Portal App installiert ist, läuft die Erstregistrierung so ab:

Für Version 26.4.0

1. Am Gerät erscheint die Benachrichtigung `Registrierung erforderlich` (*Registration Required*). Alternativ kann sie über die Systemeinstellungen ausgelöst werden.

Für Version 26.4.0

2. Direkt nach der ersten Anmeldung öffnet sich der Dialog `Gesamtauthentifizierung für den Mac` mit dem Punkt `Account registrieren`. Die Registrierung wird über Fortfahren fortgesetzt (sie erscheint bei den Methoden Passwort und Secure-Enclave-Schlüssel gleichermaßen).



3. Die Nutzer melden sich mit ihrem Microsoft Entra ID Konto an und bestätigen bei Bedarf die MFA (z. B. über Microsoft Authenticator).

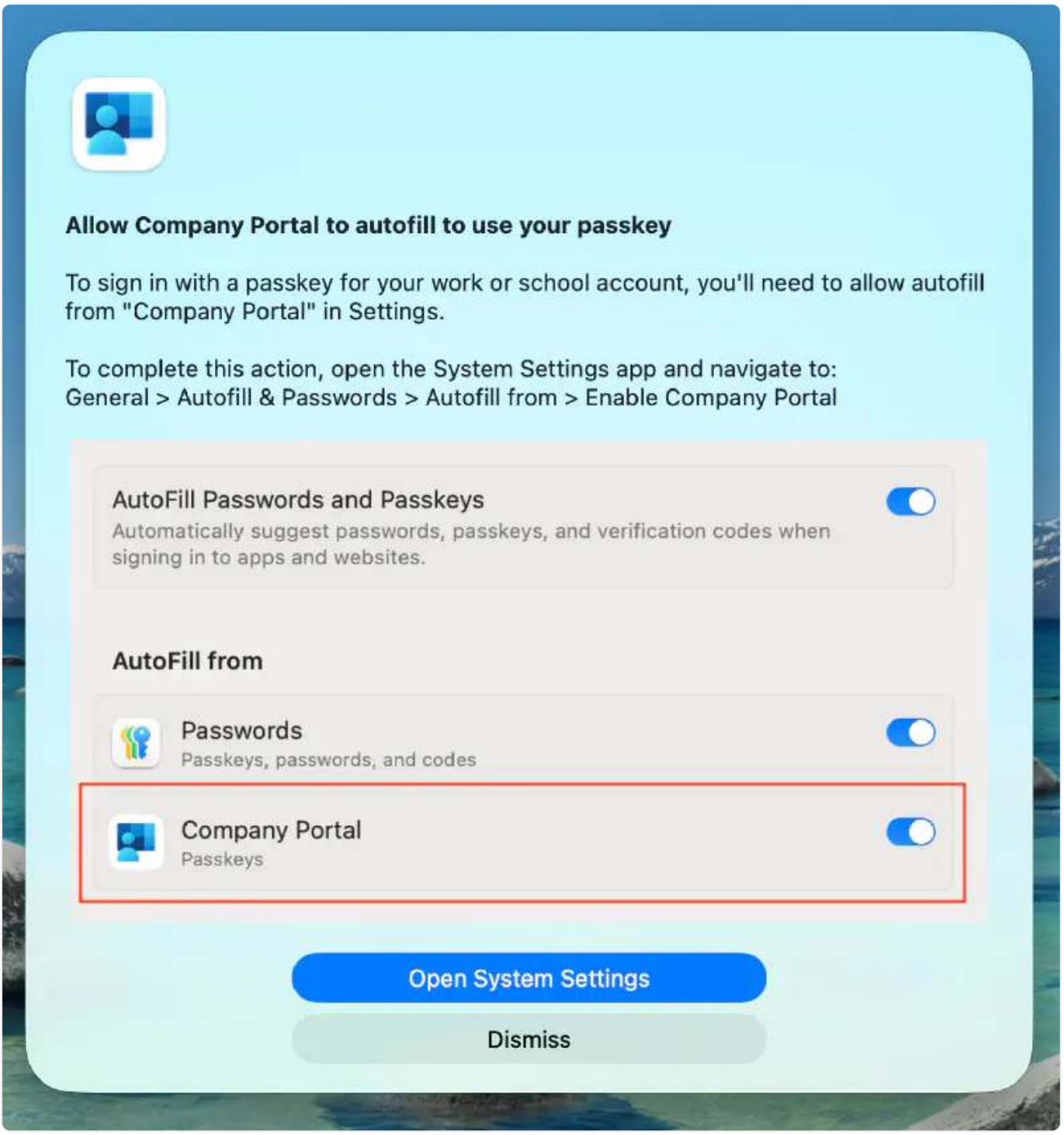
4. Das lokale Benutzerkonto wird mit der Entra ID Identität verknüpft. Ab jetzt greift Single Sign-On für Apps und Browser, die Entra ID nutzen.

Passkey-Autofill für Company Portal freigeben

Nach der ersten Anmeldung erscheint ein Hinweis `Allow Company Portal to autofill to use your passkey`. Damit die Anmeldung per Passkey (Platform Credential, insbesondere bei Methode Secure-Enclave-Schlüssel) funktioniert, müssen die Nutzer das automatische Ausfüllen für Company Portal einmalig aktivieren:

1. Über Open System Settings (oder manuell) werden die Systemeinstellungen geöffnet.
2. Dort wird `Allgemein` → `AutoFill & Passwörter` aufgerufen.
3. Unter AutoFill von wird der Schalter für Company Portal aktiviert.

Für Version 26.4.0



Ohne diese Freigabe kann Company Portal den Passkey nicht zum Anmelden anbieten; die passwortlose Anmeldung schlägt dann fehl bzw. der Hinweis erscheint wiederholt.

Bei der Methode *Secure-Enclave-Schlüssel* bleibt das lokale Passwort unverändert; nach einem Neustart ist zunächst das lokale Passwort für die FileVault-Entsperrung nötig, danach kann Touch ID verwendet werden.

Verifizierung

So lässt sich prüfen, ob die Registrierung erfolgreich war:

- Auf dem Gerät (Terminal): `app-sso platform -s` zeigt den Registrierungsstatus der Platform-SSO-Extension.
- In Microsoft Entra: Unter *Geräte* erscheint das Gerät als registriert/verknüpft.
- Company Portal: Der Gerätestatus wird als konform/registriert angezeigt.

Mögliche Fehler

- Registrierungsprompt erscheint nicht → zu prüfen ist, ob Company Portal (Version 5.2404.0+) installiert ist und die App-Konformität bereits ausgewertet wurde.
- Anmeldung schlägt fehl → Team Kennung, Kennung der Erweiterung und URLs sind auf Tippfehler zu prüfen; die URLs müssen von der TLS-Inspection ausgenommen sein.
- Registrierung bricht bei der MFA ab → Per-User-MFA wird auf dem Konto deaktiviert und stattdessen Conditional Access verwendet.
- Secure Enclave nicht verfügbar → betrifft Intel-Macs; dort wird die Methode Passwort verwendet.
- Login-Loop bzw. **`Anmelden nicht möglich – Registrierung fehlgeschlagen`** → bei Registrierung im Setup-Assistenten (macOS 26+) muss Erstellen des ersten Benutzers während des Einrichtungsassistenten aktivieren auf AN stehen – unabhängig von der Methode. Steht der Schalter auf AUS, wird kein lokales Konto angelegt: mit Secure Enclave entsteht ein Login-Loop, mit Passwort die Meldung `Registrierung fehlgeschlagen`.

Weitere bekannte Probleme und Diagnosehinweise siehe: Microsoft Dokumentation →

Für Version 26.4.0

SFTP-Upload

Relution kann genutzt werden, um verwaltete Apple Accounts (im Portal: Managed Apple ID) in großer Stückzahl anzulegen. Dies ist über das Relution Portal in den Einstellungen möglich und erleichtert Schulen und Schulbehörden die automatisierte Konfiguration dieser Accounts, um sie für Schüler und Lehrer bereitstellen zu können.
Über diesen Prozess werden auch automatisch die Klassen, die in Relution angelegt wurden, zu Klassen im Apple School Manager migriert.

Voraussetzungen

- Port 22 Ausgehend zu den Apple Servern zulassen vor allem für die URL: `upload.appleschoolcontent.com`
- Einen Apple School Manager
- Eine Education- oder Free-Lizenz in Relution
- Lese- und Bearbeitungsrecht für Apple School Manager SFTP-Upload in der Rolle des Administrators (ohne Bearbeitungsrecht lässt sich der Setup-Assistent nicht abschließen)
- Mindestens eine bestätigte Domain im Apple School Manager (Reserve Adressen von Apple sind nicht möglich)
- Eine Klasse in Relution mit mindestens einem Lehrer und einem Schüler Benutzer
- Die Lehrer müssen Teil der Systemgruppe `Teacher` und die Schüler Teil der Systemgruppe `Student` sein

Für Version 26.4.0

Konfiguration

- Relution Portal und Apple School Manager öffnen.
- Zum folgenden Punkt in Relution navigieren: `Einstellungen` → `Bildung` → `Apple School Manager SFTP-Upload`
- Im Setup-Assistenten weiter bis zur Eingabe von Server-URL, Benutzer und Passwort.
- Im School Manager zu folgendem Punkt navigieren: links unten in der Ecke auf den eigenen `Benutzer` → `Einstellungen` → `verwaltete Apple Accounts` → `Starten Sie die ersten Schritte der Verknüpfung der Verzeichnissynchronisierung`.
- Klick auf Neue Accounts erstellen
- Klick auf CSV-Datei im Apple Format verwenden
- Bei Punkt 1. SFTP Einrichten
- Die Werte kopieren und in Relution in die Felder eintragen, dann Weiter klicken.
- Die bestätigte Domain aus dem Apple School Manager im Feld Domain der verwalteten Apple Accounts eintragen.
- Klick auf Save Settings. Die Einstellungen werden gespeichert und ein erster SFTP-Upload startet automatisch.
- Klick auf weiter im Apple School Manager und auf den Import warten.

Die Accounts werden jetzt angezeigt und können hier auf Fehler überprüft werden.

Im Apple School Manager wird unter Accounts und Klassen erstellen für Lehrkräfte und für Schüler dieselbe bestätigte Domain und als Benutzernamen-Format `Vorname.Nachname` eingestellt (z. B. `Max.Mustermann@schule.de`). Relution legt für Benutzer, die noch keinen verwalteten Apple Account haben, die Adresse in genau diesem Format (`Vorname.Nachname@<Domain>`) am Benutzer ab. Weicht das Format im Apple School Manager davon ab, stimmen die Accounts im Apple School Manager und die in Relution gespeicherten Adressen nicht überein.

Upload und Umfang

Nach der Einrichtung lädt Relution die Daten standardmäßig einmal täglich automatisch in den Apple School Manager hoch. Zusätzlich lässt sich ein Upload unter `Einstellungen` → `Bildung` → `Apple School Manager SFTP-Upload` über Upload starten manuell auslösen. Nach Abschluss des Imports sendet der Apple School Manager eine E-Mail.

Übertragen werden:

- alle Mitglieder der Systemgruppe `Teacher` als Lehrkräfte und alle Mitglieder der Systemgruppe `Student` als Schüler, auch wenn sie der Gruppe nur über eine Untergruppe angehören; ein Benutzer in beiden Gruppen wird nur als Lehrkraft übertragen
- die Klassen der Organisation mit den direkt oder über Gruppen zugewiesenen Lehrkräften und Schülern

Auf derselben Seite wird über Passwort-Richtlinie für Schüler festgelegt, welche Passwortrichtlinie die verwalteten Apple Accounts der Schüler erhalten:

- Standardeinstellung des Standorts verwenden: Neue Accounts verwenden die Standard-Passwortrichtlinie des Standorts im Apple School Manager, bestehende Accounts behalten ihre aktuelle Richtlinie.
- Passwörter mit acht Ziffern (Standard), Passwörter mit sechs Ziffern oder Passwörter mit vier Ziffern: Neue und bereits bestehende Accounts werden auf die jeweilige Richtlinie umgestellt.

Standort

Für Version 26.4.0

Der SFTP-Upload erstellt für jede Relution Organisation, die den SFTP-Upload nutzt einen neuen Standort im Apple School Manager. Der Name dieses Standortes wird genauso benannt, wie der eindeutige Name der Organisation der jeweiligen Relution Organisation.

Als Beispiel:

- Organisationsname: `User-Import-Test`
- Eindeutiger Name der Organisation: `UIT`
- Neuer Standort im ASM: `UIT`

Wenn der Standort im Apple School Manager, der für den Einkauf von Apps genutzt wird und schon existiert genauso heißt, kann es zu Problemen führen.
Dies vorher mit dem jeweiligen Betreiber des eigenen Servers oder dem eigenen Partner absprechen.

Trennen der Verbindung

Niemals die Verbindung des SFTP-Uploads trennen, wenn die Accounts noch aktiv genutzt werden und in Zukunft auch weitere Accounts erstellt werden sollen. Wird die Verbindung aufgetrennt, werden alle Accounts, die über den SFTP-Upload angelegt wurden, auf die Quelle Manuell von SFTP geändert.
Wird jetzt erneut eine Verbindung hergestellt, kann es zu einer Vervielfältigung von verwalteten Apple Accounts kommen. Da mit der Relution Version 5.26 auch der Import von Benutzern dazu gekommen ist, kann dadurch ein Kreislauf entstehen.

In Relution werden die Einstellungen über SFTP-Server-Einstellungen entfernen → Löschen zurückgesetzt. Dabei werden nur die Einstellungen in Relution entfernt: Die SFTP-Zugangsdaten bleiben gültig, bis die Verzeichnissynchronisation in den Einstellungen des Apple School Manager getrennt wird.

Native macOS-Apps installieren

Mit Relution lassen sich native macOS-Anwendungen zentral in den App Store hochladen und auf verwaltete Macs verteilen. Als Dateiformate werden `.pkg` (Installer-Paket) und `.dmg` (Disk Image) unterstützt. Für eine zuverlässige, unbeaufsichtigte Verteilung ist das Zusammenspiel aus passendem Paketformat, korrekter Erkennungsregel sowie gültiger Signierung entscheidend. Die nachfolgenden Abschnitte beschreiben diese Bestandteile im Detail.

> Native macOS-Apps werden über den Relution App Store bzw. eine Verteilaktion installiert. Voraussetzung ist ein in Relution verwalteter (enrolled) Mac.

PKG und DMG im Vergleich

Die Wahl des Paketformats bestimmt, wie eine App installiert wird und ob sich der Vorgang automatisieren lässt.

Merkmal	**`.pkg`** (Installer-Paket)	**`.dmg`** (Disk Image)
Aufbau	Installer mit optionalen Skripten (`preinstall` / `postinstall`)	Container/Archiv, enthält meist eine `.app`
Installationsort	flexibel, an mehreren Zielorten möglich	in der Regel Kopie nach `/Applications` (im Finder: Programme)
Installationslogik	eigene Installationsroutine des Pakets	Kopiervorgang der enthaltenen `.app`
Automatisierte Installation	im Hintergrund ohne Interaktion möglich	nur verwertbar, wenn genau eine `.app` enthalten ist
Empfehlung	bevorzugt für die MDM-Verteilung	geeignet, sofern kein PKG angeboten wird

Ein `.pkg` ist für die automatisierte Verteilung das robustere Format, da die Installationsroutine im Paket selbst hinterlegt ist und still im Hintergrund ausgeführt werden kann. Skripte innerhalb des Pakets können zusätzliche Schritte übernehmen, etwa das Anlegen von Konfigurationsdateien. Beim Hochladen liest Relution die Distribution-Datei des Pakets aus und übernimmt daraus Produkt-ID und Version. Pakete ohne Distribution-Datei (reine Komponentenpakete) werden als nicht unterstützte Datei abgelehnt.

Ein `.dmg` ist ein Datenträger-Abbild. Für die Verteilung ist es nur dann geeignet, wenn es eine einzelne Programmdatei (`.app`) enthält, die nach `/Applications` (im Finder: Programme) kopiert wird. Abbilder mit einem interaktiven Installations-Assistenten oder mehreren Elementen lassen sich nicht unbeaufsichtigt installieren.

Ein wesentlicher Unterschied betrifft den Verteilkanal: `.pkg`-Apps werden direkt über das MDM-Protokoll installiert, während `.dmg`-Apps über den macOS Companion ausgebracht werden. Voraussetzung ist, dass der macOS Companion unter `Einstellungen` → `Relution Client Apps` über macOS Companion aktivieren eingeschaltet ist. Auf Macs mit einer macOS-Version vor 12 sowie auf Macs mit Benutzer-Einschreibung steht der macOS Companion nicht zur Verfügung; DMG-Apps lassen sich dort nicht verteilen.

Hinweis: Steht eine App sowohl als `.pkg` als auch als `.dmg` zur Verfügung, ist für die zentrale Verteilung das `.pkg` vorzuziehen.

Native App in Relution anlegen

Native macOS-Apps werden im Menü unter `Apps` → `App Store` angelegt. Die Schaltfläche Hinzufügen öffnet den Dialog Neue Apps hinzufügen. Unter Quelle wird Native App gewählt.

Nach einem Klick auf Weiter wird über Datei wählen die `.pkg`- oder `.dmg`-Datei hochgeladen. Details hinzufügen öffnet anschließend das Formular App hinzufügen.

> Bei großen Paketen kann die Dateigröße durch Datenbank oder Reverse Proxy begrenzt sein. In diesem Fall ist die serverseitige Konfiguration entsprechend anzupassen.

Im Formular sind folgende Angaben erforderlich:

- Interner Name: Bei `.pkg`-Dateien wird die Produkt-ID aus der Distribution-Datei übernommen. Bei `.dmg`-Dateien ist der Dateiname als Platzhalter vorbelegt und wird durch einen eindeutigen Namen ersetzt. Existiert bereits eine App mit demselben internen Namen, wird beim Speichern eine neue Version dieser App angelegt.
- Versions-Name: Bei `.pkg`-Dateien wird die Version aus der Distribution-Datei übernommen, bei `.dmg`-Dateien wird sie von Hand eingetragen.
- Erkennungsregeln: Im gleichnamigen Abschnitt wird mindestens eine Erkennungsregel eingetragen – ohne Erkennungsregel lässt sich die App nicht speichern (siehe Abschnitt zur Erkennungsregel weiter unten).

Für Version 26.4.0

Nach Angabe des gewünschten Freigabestatus wird die App über Speichern angelegt.

Versionsverwaltung und Freigabestatus

Für native macOS-Apps lässt sich zusätzlich ein Release-Management betreiben: Verschiedene Versionen einer App können parallel für unterschiedliche Personengruppen bereitgestellt werden. So kann etwa eine Version im produktiven Einsatz sein, während eine neue Version durch eine ausgewählte Gruppe getestet wird, ohne dass die übrigen Anwender davon betroffen sind.

Jede Version durchläuft dabei einen der folgenden Status:

- Produktiv: Version, die regulär über den Relution Agent verteilt und installiert wird.
- Entwicklung bzw. Prüfung: Status für Versionen, die vor der Produktivsetzung getestet werden.
- Archiv: Status einer früheren Version, die durch eine neuere Produktiv-Version abgelöst wurde.

Mit Ausnahme des Status Archiv kann sich in jedem Freigabestatus nur eine Version der App befinden.

Neue Version parallel testen

Soll eine neue Version parallel zur bestehenden produktiven Version getestet werden, wird diese über die Schaltfläche Neue Version hochgeladen und zunächst in den Status Entwicklung oder Prüfung versetzt. Bei `.pkg`-Dateien muss der interne Name der neuen Version mit dem der bestehenden App übereinstimmen. Bei `.dmg`-Dateien kann eine Abweichung über Nicht übereinstimmende interne App-Namen ignorieren zugelassen werden.

Für die neue Version lässt sich im Feld Go-Live Datum ein Termin hinterlegen. Automatisch in den Status Produktiv wechselt die Version an diesem Tag nur, wenn ein App-Freigabeprozess → aktiv ist und die Version im Status Prüfung alle Freigabeschritte durchlaufen hat. Ohne aktiven Freigabeprozess dient das Datum nur als Wunschtermin, und die Version wird manuell in den Status Produktiv versetzt (siehe unten).

Beide Versionen sind währenddessen in den App-Eigenschaften einsehbar; Anwender mit entsprechender Berechtigung können die neue Version bereits auf Endgeräten sehen, installieren und testen.

Manuelle Produktivnahme

Liegt die neue Version im Status Prüfung, wird sie auf der App-Detailseite über die Schaltfläche Produktiv in diesen Status versetzt. Liegt sie noch in Entwicklung, erfolgt der Wechsel über `Verschieben` → `Produktiv`. Eine bereits produktive Version wird dabei automatisch in den Status Archiv verschoben. Veröffentlichte Versionen globaler Apps lassen sich nicht in einen anderen Status verschieben.

> Die App wird auf den Endgeräten nicht automatisch aktualisiert. Ein Update wird durch die Benutzer im Relution Agent ausgelöst oder durch Administratoren über die Geräteaktion Relution Store App bereitstellen bzw. in der App-Ansicht unter Geräte mit dieser App über die Schaltfläche App aktualisieren.

Für Version 26.4.0

Erkennungsregel über den Bundle-Identifier

Die Erkennungsregel teilt Relution mit, woran der installierte Zustand einer App erkannt wird. Für native macOS-Apps steht dafür der Regeltyp Package Name zur Verfügung. Eingetragen wird der Bundle-Identifier der installierten App (z. B. `com.hersteller.appname`); zulässig sind Buchstaben, Ziffern, Punkte und Bindestriche. Anhand dieses Werts wird in der Liste der installierten Apps des Geräts geprüft, ob die App bereits vorhanden ist und ob eine Installation als erfolgreich gilt.

Erkennungsregeln werden im Abschnitt Erkennungsregeln über Neue Erkennungsregel hinzufügen angelegt – beim Hochladen im Formular App hinzufügen, bei bestehenden Apps auf der App-Detailseite im Reiter Einstellungen. Optional vergleicht ein Versionscheck zusätzlich die installierte Version: Unter Operator wird Version ist gleich (=) oder Version ist nicht gleich (≠) gewählt und unter Wert die Version eingetragen. Eine App kann mehrere Erkennungsregeln haben, etwa wenn ein Paket mehrere Apps installiert. Als installiert gilt die App nur, wenn alle Regeln zutreffen.

Der zuverlässigste Weg, den korrekten Bundle-Identifier zu ermitteln, führt über einen bereits verwalteten Mac:

1. Die App wird auf einem in Relution verwalteten Mac einmalig manuell installiert.
2. Im Relution-Portal wird das Gerät unter `Geräte` → `Inventar` geöffnet.
3. Auf dem Reiter Installierte Apps wird die App gesucht. Der Bundle-Identifier steht in der Spalte Interner Name.
4. Dieser Wert wird in der Erkennungsregel im Feld Package Name eingetragen.

> Nach einer manuellen Installation kann es einen Moment dauern, bis der nächste Inventar-Abgleich die App im Portal anzeigt. Die Aktion Geräteinformationen aktualisieren beschleunigt die Darstellung.

Alternativ lässt sich der Bundle-Identifier direkt auf dem Mac über das Terminal auslesen:

```
osascript -e 'id of app "App-Name"'
```

Ist der Pfad der Programmdatei bekannt, kann der Wert auch aus dem Paket-Metadatum gelesen werden:

```
mdls -name kMDItemCFBundleIdentifier -raw /Applications/App-Name.app
```

Soll die Erkennungsregel bereits vor einer Installation ermittelt werden, kann der Inhalt eines `.pkg` mit einem Drittanbieter-Werkzeug wie Suspicious Package inspiziert werden. Ein solches Werkzeug zeigt neben den Installationspfaden und enthaltenen Skripten auch den Bundle-Identifier an, ohne dass das Paket ausgeführt werden muss.

Hinweis: Drittanbieter-Werkzeuge dienen ausschließlich der Analyse. Der maßgebliche Bundle-Identifier bleibt der Wert, der nach einer Installation im Relution-Inventar ausgewiesen wird.

Für Version 26.4.0

Alternative Wege ohne funktionierende Erkennung

Bei manchen nativen Apps kann Relution den installierten Zustand nicht zuverlässig prüfen – etwa weil kein eindeutiger Bundle-Identifier vorliegt oder das Paket die App an einen untypischen Ort ablegt. Eine automatische Installation über die App Konformität eignet sich in diesen Fällen nicht: Relution erkennt eine PKG- oder DMG-App nur dann als installiert, wenn alle Erkennungsregeln erfüllt sind. Andernfalls wird die Installation bei jeder Konformitätsprüfung erneut eingeplant.

Zwei Wege kommen ohne belastbare Erkennungsregel aus:

- Bereitstellung über den Relution App Store: Die App wird den Benutzern im Relution Agent bereitgestellt und dort manuell installiert. Da die Installation aktiv angestoßen wird, ist keine automatische Zustandsprüfung nötig.
- Verteilung per Aktion: Über die Aktion Relution Store App bereitstellen auf ausgewählten Geräten oder Gruppen wird die Installation gezielt ausgelöst. Der Installationsbefehl wird an das Gerät übertragen und dort ausgeführt, unabhängig von einer Erkennungsregel.

> Ohne zutreffende Erkennungsregel kann Relution den Erfolg der Installation nur eingeschränkt bewerten. Der tatsächliche Installationszustand ist in diesem Fall am Gerät zu verifizieren.

Signierung und Notarisierung

macOS prüft über Gatekeeper, ob Software aus einer vertrauenswürdigen Quelle stammt. Pakete, die weder signiert noch von Apple notarisiert sind, können blockiert werden oder eine Nutzerinteraktion erfordern – was eine unbeaufsichtigte Verteilung verhindert.

- Signierung: Das Paket ist mit einer gültigen Developer ID signiert. Dadurch ist die Herkunft nachvollziehbar und Manipulation ausgeschlossen.
- Notarisierung: Das Paket wurde zusätzlich von Apple geprüft (notarisiert). Erst dadurch wird es auf aktuellen macOS-Versionen ohne Warnhinweis akzeptiert.

Ob ein Paket korrekt signiert und notarisiert ist, kann auf dem Mac im Terminal überprüft werden:

```
spctl --assess --type install -vv /Pfad/zur/App.pkg
pkgutil --check-signature /Pfad/zur/App.pkg
```

Hinweis: Schlägt eine Installation nur bei einzelnen Paketen still fehl, ist eine fehlende Signierung oder Notarisierung eine der häufigsten Ursachen.

Fehleranalyse per Logs und Geräteprotokollierung

Für Version 26.4.0

Bleibt eine Installation ohne Erfolg, lassen sich die Ursachen über die Protokollierung eingrenzen.

Geräteprotokollierung in Relution

Die Geräteprotokollierung wird in der globalen Organisation für ein einzelnes Gerät eingeschaltet: Im Geräte-Inventar wird das Gerät ausgewählt und über Geräteprotokollierung verwalten die Option Gerätebasierte Protokollierung aktivieren für die unter Dauer (in Minuten) angegebene Zeit gesetzt. In diesem Zeitraum werden Befehle wie die App-Installation samt Rückmeldung des Geräts protokolliert. Die erfassten Geräteprotokolle werden im selben Dialog als Datei heruntergeladen. Auf diese Weise wird sichtbar, ob ein Installationsbefehl das Gerät erreicht hat und mit welchem Status er quittiert wurde.

> Die Protokollierung endet automatisch nach der eingestellten Dauer. Die Protokolldatei wird einen Tag nach dem Ende der Protokollierung gelöscht und übersteht keinen Neustart des Relution-Servers.

Installationslogs am Mac

Ergänzend geben die Systemprotokolle des Macs Aufschluss über den Installationsvorgang. Der Verlauf einer PKG-Installation wird lokal protokolliert und kann im Terminal ausgewertet werden:

```
tail -n 100 /var/log/install.log
```

Für die laufende Beobachtung während einer Installation eignet sich der Live-Datenstrom des Systemprotokolls:

```
log stream --predicate 'process == "installer"' --info
```

Aus diesen Ausgaben lässt sich ablesen, ob das Paket entpackt, ein Skript ausgeführt oder der Vorgang durch Gatekeeper abgebrochen wurde.

Deinstallation

Native macOS-Apps, die über Relution installiert wurden, lassen sich über Relution auch wieder deinstallieren – sowohl `.pkg`- als auch `.dmg`-Apps. Voraussetzung ist ein Bundle-Identifier (Erkennungsregel), über den die App auf dem Gerät eindeutig adressiert wird. Ohne gültigen Bundle-Identifier wird keine Deinstallation ausgelöst. Wie schon bei der Installation läuft die Entfernung je nach Format über unterschiedliche Kanäle – `.pkg` über MDM, `.dmg` über den macOS Companion –, das Vorgehen im Portal ist jedoch identisch.

Für Version 26.4.0

Für die Deinstallation bestehen zwei Wege:

- Gezielt über eine Aktion: Über die Aktion App entfernen auf ausgewählten Geräten oder Gruppen wird die App deinstalliert. In der Befehlshistorie des Geräts erscheint der Vorgang als `<Bundle-Identifier> deinstallieren`.
- Automatisch beim Wegfall der Zuweisung: Wird eine App, die über die App Konformität automatisch installiert wurde (Häkchen in der Spalte Auto Installation), nach einer Änderung oder Entfernung der Richtlinie nicht mehr gefordert, deinstalliert Relution sie automatisch. Anders als unter iOS bietet die macOS-Konfiguration App Konformität keine Option, diese Deinstallation abzuschalten.

> Ausschlaggebend für die Deinstallation ist der Bundle-Identifier, nicht das Paketformat. Ohne gültige Erkennungsregel kann Relution die App auf dem Gerät nicht auflösen und daher nicht gezielt entfernen.

Nicht über Relution entfernen lassen sich Apps ohne Bundle-Identifier sowie manuell – außerhalb von Relution – installierte Apps. Bei `.dmg`-Apps ist zusätzlich der macOS Companion erforderlich; ist dieser deaktiviert oder auf dem Gerät nicht einsetzbar (macOS vor Version 12, Benutzer-Einschreibung), ist keine Deinstallation über Relution möglich. In diesen Fällen wird die Entfernung über ein Skript umgesetzt, das die App beendet und die zugehörigen Verzeichnisse entfernt und gezielt über eine Aktion verteilt wird.

App-Store-Apps verwalten

Mit Relution ist es möglich, Apps aus dem Apple App Store auf Geräten zu verteilen. Hierzu muss immer eine App-Lizenz erworben werden – unabhängig davon, ob die App kostenpflichtig ist oder nicht. Eine App-Lizenz kann entweder über Apps und Bücher (im Portal: VPP) erworben oder über eine auf dem Gerät angemeldete Apple-ID bezogen werden. Je nach Anwendungsfall ist das eine oder andere Szenario die sinnvollere Vorgehensweise. Soll auf Geräten ohne Apple-ID gearbeitet werden, führt an einer Lizenz aus Apps und Bücher kein Weg vorbei. Wie Apps und Bücher eingerichtet wird, ist dem entsprechenden Kapitel → zu entnehmen.

Apps, die im Apple School/Business Manager erworben werden, werden automatisch nach Relution synchronisiert (ab Version 5.10). Die Apps werden in Relution im Status Produktiv veröffentlicht und können im Anschluss auf Geräte verteilt werden. Apps, die nicht allen Benutzern zugänglich gemacht werden sollen, können auch manuell einem anderen Freigabestatus zugewiesen werden. Es kann jederzeit auch eine App manuell zum Relution App Store hinzugefügt werden. Für diese Apps sind jedoch keine Lizenzen aus Apps und Bücher automatisch verfügbar und eine Installation ist nur möglich, wenn auf den entsprechenden Endgeräten Benutzer mit einer Apple-ID angemeldet sind. Es ist möglich, nachträglich Lizenzen aus Apps und Bücher für diese Apps zu beschaffen.

Sind für eine App Lizenzen aus Apps und Bücher vorhanden, weist Relution bei der Installation automatisch eine Lizenz zu – auch bei manuell hinzugefügten Apps, sobald die Lizenzen nachträglich synchronisiert wurden. Auf Macs mit Benutzer-Einschreibung wird dafür eine benutzerbasierte Lizenz verwendet.

Apps verteilen

Für Version 26.4.0

Regulär werden Apps aus dem App Store über die Richtlinien-Konfiguration App Konformität als erforderliche Apps auf Macs verteilt.

Für einzelne Geräte stehen zwei Geräteaktionen zur Verfügung:

- Relution Store App bereitstellen: Zur Auswahl stehen die Apps aus dem Relution App Store, neben nativen Apps also auch die dort angelegten Apps aus dem App Store.
- App vom Apple App Store installieren: Die App wird direkt im Apple App Store gesucht und installiert, ohne dass sie zuvor im Relution App Store angelegt sein muss.

Apps managen

Apps aus dem App Store werden vom Betriebssystem selbständig aktualisiert. In seltenen Fällen funktioniert dies jedoch nicht. Für diesen Fall gibt es zwei Wege, ein Update anzustoßen:

- In der Detailansicht der App werden im Reiter Geräte mit dieser App die betroffenen Geräte ausgewählt und über App aktualisieren aktualisiert. Die Schaltfläche ist deaktiviert, sobald auf einem der ausgewählten Geräte bereits die Version im Status Produktiv installiert ist.
- Alternativ wird auf den betroffenen Geräten die Aktion Relution Store App bereitstellen (bzw. App vom Apple App Store installieren) mit der betreffenden App erneut ausgeführt.

In beiden Fällen wird eine erneute Installation angestoßen und die Geräte validieren die App-Version mit dem App Store von Apple. Ist die verfügbare Version aktueller als die installierte Version, wird die vorhandene App aktualisiert.

Managed App Konfiguration für native Apps

Native macOS-Apps – also selbst als `.pkg` oder `.dmg` hochgeladene Anwendungen – lassen sich in Relution vorkonfigurieren. Der dafür vorgesehene Weg unterscheidet sich jedoch von dem für Apps aus dem App Store. Entscheidend ist die Quelle der App, denn sie bestimmt, welche Methode zur Verfügung steht.

App-Quelle bestimmt die Konfigurationsmethode

Die Richtlinien-Konfiguration Managed App → setzt voraus, dass die App über einen von Apple verwalteten Kanal installiert wurde. Sie wird von macOS nur auf Apps angewendet, die aus dem App Store bzw. über Apps und Bücher (im Portal: VPP) installiert wurden. Bei diesen Apps übernimmt das Betriebssystem die Zuordnung der Konfiguration zur App anhand der Bundle-ID.

Für native Apps greift dieser Mechanismus nicht, da sie nicht über den verwalteten App-Store-Kanal installiert wurden. Im Portal lassen sie sich in der Konfiguration Managed App zwar auswählen, die Konfiguration wird für sie jedoch nicht wirksam. Die Konfiguration einer nativen App muss daher als Payload über die Richtlinien-Konfiguration Apple Configurator 2 Konfiguration → übertragen werden.

App-Quelle	Konfigurationsmethode
App Store / Apps und Bücher	Managed App
Native App (`.pkg` / `.dmg`)	Payload über Apple Configurator 2 Konfiguration

Konfiguration nativer Apps über Apple Configurator 2

Welche Schlüssel und Werte in der Payload (Property-List) unterstützt werden, gibt der jeweilige App-Hersteller vor. Die Einrichtung erfolgt in wenigen Schritten:

1. Die native App wird zunächst wie gewohnt bereitgestellt, sodass sie auf den Zielgeräten installiert ist (siehe Native macOS-Apps installieren →).
2. Die gewünschte App-Konfiguration wird als `.mobileconfig`-Datei zusammengestellt (siehe Empfehlung unten).
3. In der Richtlinie wird eine Apple Configurator 2 Konfiguration hinzugefügt, ein Name vergeben und die `.mobileconfig`-Datei vollständig über .mobileconfig Datei auswählen hochgeladen. Der Inhalt erscheint anschließend im Feld Payload Inhalt und kann dort bei Bedarf angepasst werden.
4. Die Richtlinie wird veröffentlicht und den betroffenen Gerätegruppen zugewiesen.

> Die App muss auf dem Gerät bereits installiert sein, bevor die Konfiguration greift. Die Reihenfolge der Konfigurationen innerhalb einer Richtlinie lässt sich nicht festlegen. Wird die App über dieselbe Richtlinie installiert, kann die Apple Configurator 2 Konfiguration daher vor der App auf dem Gerät ankommen.

Eine `.mobileconfig`-Datei darf in `PayloadContent` nur einen Konfigurationstyp (Payload-Typ) enthalten; zusätzliche Zertifikat-Payloads sind erlaubt. Enthält die Datei mehrere Typen, etwa Einstellungen für mehrere Apps, lässt sich die Konfiguration nicht speichern. Für jede App wird daher eine eigene Apple Configurator 2 Konfiguration angelegt. Enthält die Datei mehrere Payloads desselben Typs, wird nur der erste übertragen. Weitere Anforderungen an die Datei beschreibt der Artikel Apple Configurator 2 Konfiguration →.

Empfehlung: Payload mit dem iMazing Profile Editor erstellen

Das manuelle Schreiben einer Payload ist fehleranfällig. Zur komfortablen Erstellung empfiehlt sich das Drittanbieter-Werkzeug iMazing Profile Editor. Darin lässt sich die Konfiguration über eine grafische Oberfläche zusammenklicken, ohne die zugrunde liegende Property-List von Hand zu schreiben.

Der Ablauf gestaltet sich wie folgt:

1. Im iMazing Profile Editor werden die gewünschten Einstellungen für die App über die Oberfläche gesetzt.
2. Das Ergebnis wird unsigniert als `.mobileconfig` exportiert. Relution liest die Datei als XML ein; signierte Profile lassen sich nicht speichern.
3. Die vollständige `.mobileconfig`-Datei wird in der Apple Configurator 2 Konfiguration in Relution hochgeladen.

Für Version 26.4.0

> Der iMazing Profile Editor ist ein Werkzeug eines Drittanbieters und nicht Bestandteil von Relution. Er dient ausschließlich der Erstellung der Payload.

In der Payload lassen sich zusätzlich die von Relution bereitgestellten Platzhalter verwenden (z. B. `${user.email}`), um die Konfiguration benutzerabhängig auszufüllen. Die verfügbaren Platzhalter werden unterhalb des Konfigurationsformulars angezeigt und beim Übertragen der Konfiguration auf die Geräte ersetzt, siehe Erweiterte Platzhalter →.

Übersicht Einschreibungen

Die Vision Pro wird zu einem zentralen Bestandteil moderner Organisationen und eröffnet vollkommen neue Möglichkeiten. Relution sorgt mit unterschiedlichen Einschreibeverfahren dafür, dass die Vision Pro nahtlos integriert und optimal genutzt werden kann. Neben der Automatischen Geräteregistrierung (ADE, im Portal: DEP) steht zusätzlich die Option der Apple Benutzer-Einschreibung (User Enrollment) zur Verfügung.

Automatische Geräteregistrierung (ADE) mit DEP-Profil

Der Apple School- oder Business Manager wurde von Apple eingeführt, um Organisationen und Bildungseinrichtungen bei der Bereitstellung von Apple-Geräten aus der Ferne zu unterstützen. Mithilfe von ASM/ABM können brandneue Apple-Geräte in Relution registriert werden, ohne dass ein Techniker sie jemals in die Hand nehmen muss.

Konfigurationsprofil für ADE →
DEP konfigurieren →

Voraussetzungen

- visionOS 1.1 oder höher.
- Die Organisation sollte im Apple School/ Apple Business Manager angemeldet sein.
- Wenn Geräte direkt bei Apple gekauft wurden, ist die Apple-Kundennummer, die der eigenen Organisation zugewiesen ist, erforderlich, um berechtigte Bestellungen und Geräte mit dem Apple School/ Business Manager zu verbinden.
- Wurden Geräte direkt von einem autorisierten Wiederverkäufer oder Netzbetreiber beschafft, müssen die Geräte mit der Reseller-ID dieses Händlers verknüpft sein. Das tatsächliche Datum der Berechtigung wird durch die Verkaufshistorie des autorisierten Wiederverkäufers oder Netzbetreibers bestimmt.
- Ein in Relution hinterlegtes APNs-Zertifikat (APNS Push Zertifikate →).
- Ein in Relution eingebundenes DEP-Konto und ein DEP-Profil, das den Geräten zugewiesen ist. Über das Feld Mindestversion visionOS im DEP-Profil lässt sich zusätzlich eine minimale visionOS-Version für die Einschreibung festlegen.

Für Version 26.4.0

Kontogesteuerte Benutzer-Einschreibung

Hierbei handelt es sich um die typische Einschreibung für Bring Your Own Device-Geräte (BYOD). Die Benutzer können die Einschreibung selbst durchführen und die Geräte müssen nicht auf Werkseinstellungen zurückgesetzt werden.

Relution unterstützt die kontobasierte Benutzer-Registrierung von visionOS-Geräten, die sich nicht im `Überwachter Modus` (Supervised Mode) befinden.

Die Anmeldung erfolgt auf der Vision Pro in den Geräteeinstellungen mit einem verwalteten Apple Account (im Portal: Managed Apple ID). Über die Service Discovery ermittelt das Gerät den zuständigen MDM-Server und leitet auf die Anmeldeseite von Relution weiter, auf der die Anmeldung mit dem Relution-Benutzerkonto erfolgt. Relution legt dabei automatisch eine Benutzer-Einschreibung mit der Eigentümerschaft Gerät in Mitarbeiterbesitz (BYOD) an. Für visionOS lässt sich im Portal keine Benutzer-Einschreibung manuell anlegen.

Voraussetzungen

- Ein in Relution hinterlegtes APNs-Zertifikat (APNS Push Zertifikate →).
- Ein verwalteter Apple Account und ein Relution-Benutzerkonto für den jeweiligen Benutzer.
- Die aktivierte Einstellung Kontobasierte Apple-Benutzerregistrierung in der Organisation.
- Eine Service Discovery für die Domain der verwalteten Apple Accounts, entweder automatisch über den Apple School/Business Manager oder über eine Well-Known-Datei.

Kontobasierte Apple-Benutzerregistrierung aktivieren

Die Einstellung befindet sich unter `Einstellungen` → `Geräteverwaltung` im Bereich Kontobasierte Apple-Benutzerregistrierung. Sie gilt je Organisation; in der globalen Organisation wird der Bereich nicht angezeigt.

Ist der Schieberegler Kontobasierte Apple-Benutzerregistrierung aktiviert, legt Relution bei der Anmeldung eines Benutzers automatisch eine Benutzer-Einschreibung an. Standardmäßig ist der Schieberegler deaktiviert; in diesem Fall schlägt die Einschreibung von visionOS-Geräten fehl.

Service Discovery einrichten

Eine Service Discovery muss konfiguriert werden, damit Apple die Geräte an den richtigen MDM Server übertragen kann. Dafür stehen zwei Wege zur Verfügung.

Für Version 26.4.0

Automatisch über den Apple School/Business Manager

Ab visionOS 2.2 ist keine eigene Datei erforderlich, wenn der Apple School/Business Manager über ein DEP-Konto in Relution eingebunden ist. Relution hinterlegt die Service-Discovery-URL bei jeder Synchronisation der ADE-Geräte automatisch im Apple School/Business Manager. Voraussetzung ist, dass dort unter `Preferences` → `Your MDM Servers` → `MDM Server Assignment` → `Default MDM Server Assignment` Relution als Standard-MDM-Server für Apple Vision Pro festgelegt ist.

Über eine Well-Known-Datei

Für Geräte mit einer älteren visionOS-Version als 2.2 oder ohne eingebundenen Apple School/Business Manager muss eine HTTP Well-Known-Ressourcen-Datei an der Domain hinterlegt werden, mit der sich die Benutzer anmelden. Für den eigenen Hostnamen beantwortet Relution diese Anfrage bereits selbst; eine eigene Datei ist daher nur erforderlich, wenn die Domain der verwalteten Apple Accounts davon abweicht. Apple muss diese Datei über einen HTTP GET unter folgender URL abrufen können:

```
https://yourdomain.com/.well-known/com.apple.remotemanagement
```

Unter dem Punkt `yourdomain.com` muss die Domain hinterlegt werden, die auch für die verwalteten Apple Accounts verwendet wird. Die Datei muss auf einer Domain hinterlegt werden, die mit HTTP-GET-Anfragen umgehen kann.

Die Datei im JSON-Format mit dem Content-Type `application/json` anlegen. Um die richtigen Informationen in die Datei einzutragen, lassen sich die benötigten Informationen direkt aus dem Relution Portal kopieren:

1. `Einstellungen` → `Geräteverwaltung` öffnen.
2. Im Bereich Kontobasierte Apple-Benutzerregistrierung den unter Antwort angezeigten JSON-Text vollständig, einschließlich der äußeren geschweiften Klammern, kopieren (Schaltfläche In Zwischenablage kopieren) und in die Datei einfügen. Der JSON-Text wird unabhängig vom Schieberegler angezeigt.

> Damit die Datei richtig funktioniert, darf sie keine Dateiendung haben.

Beispiel: maxmustermann@musterhausen.de

In diesem Beispiel wäre die Domain `musterhausen.de`. Dort müsste die Service Discovery hinterlegt werden.

Nachträgliche Einschreibung über den Apple Configurator 2

Apple Configurator 2 ist eine kostenlose App, die im Mac App Store verfügbar ist. Mit der Anwendung lassen sich über USB verbundene Apple-Geräte manuell mit einem macOS-Gerät konfigurieren, bevor die Geräte an Benutzer ausgehändigt werden. Hierzu können sogenannte Profile erstellt und auf den Geräten angewendet werden. Zudem ermöglicht es der Apple Configurator 2, Apple-Geräte, die nicht bereits von einem autorisierten Wiederverkäufer für die ADE registriert wurden, nachträglich hinzuzufügen. Insgesamt empfiehlt es sich, direkt ADE-fähige Geräte zu beschaffen, da ein nachträgliches Hinzufügen mit manuellen Aufwänden verbunden ist.

Voraussetzungen

Für Version 26.4.0

- visionOS 1.1 oder höher.
- macOS-Gerät mit Apple Configurator 2.5 oder höher.
- Sicherstellen, dass das macOS-Gerät und die Vision Pro mit derselben WLAN- oder Ethernet-Verbindung verbunden sind.

Für visionOS-Geräte muss folgender Pfad als MDM-Server-URL angegeben werden, sofern die Geräte auf dem Relution-Livesystem verwaltet werden sollen. Bei einer eigenen Relution-Instanz `live.relution.io` durch den Hostnamen des eigenen Servers ersetzen.

```
https://live.relution.io/api/enrollment/v1/appleMdm/depenroll
```

Apple-Geräte, die nachträglich über Apple Configurator 2 im Apple School/Business Manager registriert sind, funktionieren in den ersten 30 Tagen nach der Bereitstellung nicht wie direkt über ADE registrierte Geräte beim Kauf über einen autorisierten Wiederverkäufer. Selbst wenn die manuelle Entfernung der MDM-Verwaltung auf den Geräten über das zugehörige DEP-Profil im MDM-System blockiert wurde, können Benutzer die MDM-Verwaltung unter `Einstellungen` → `Allgemein` → `Profile` entfernen.

> Mit Ablauf der 30-Tage-Frist ab Registrierung werden Benutzer daran gehindert, die MDM-Verwaltung auf den Geräten zu entfernen.

Nachträgliches Hinzufügen von Apple-Geräten zur ADE →

Verfügbare Aktionen

Relution stellt eine Auswahl an Aktionen bereit, um die Vision Pro direkt zu kontrollieren. Die Aktionen lassen sich gezielt auf einzelne Geräte anwenden, per Mehrfachauswahl in der Geräteliste auf mehrere Geräte gleichzeitig oder automatisiert über Aktionen mit Gerätegruppen →.

Aktionsübersicht

Aktion	Beschreibung
Geräteinformationen aktualisieren	Aktualisiert alle verfügbaren Informationen zu dem Gerät, die unter Details aufgelistet sind.
Relution Store App bereitstellen	Installiert eine App aus dem Relution Store auf den Geräten. Neben visionOS-Apps stehen auch iOS-Apps zur Auswahl.
MDM Profil aktualisieren	Installiert das MDM-Profil auf dem Gerät neu. Dabei werden das Identitätszertifikat erneuert und aktuelle Einstellungen wie das Certificate Pinning übernommen. Die MDM-Server-URL bleibt unverändert; eine geänderte externe URL wird so nicht auf das Gerät übertragen. Relution erneuert das MDM-Profil automatisch, bevor das Identitätszertifikat abläuft. Die manuelle Aktion ist daher nur in Sonderfällen erforderlich.
Im Geräte-Setup-Assistenten fortfahren	Informiert das Gerät, dass die Vorkonfiguration abgeschlossen ist und es im Setup-Assistenten fortfahren kann. Wirkt nur bei Geräten, die über die Automatische Geräteregistrierung (ADE, im Portal: DEP) registriert wurden und in deren DEP-Profil die Option Konfiguration abwarten aktiviert ist. Für Geräte mit Benutzerregistrierung ist die Aktion nicht verfügbar.

Die Aktionen Gerät neu starten, Gerät vollständig sperren, Gerät herunterfahren und Gerät auf Werkszustand zurücksetzen werden für visionOS-Geräte nicht angeboten.

Verfügbare Konfigurationen

Eine Richtlinie ist eine Sammlung einer oder mehrerer Konfigurationen. Jede Richtlinie kann auf einem oder mehreren Geräten gleichzeitig angewendet werden. Zudem können mit jedem Gerät eine oder mehrere Richtlinien verknüpft sein.

Konfigurationen im Überblick

Konfiguration	Beschreibung
App Konformität →	Verwaltung appspezifischer Einschränkungen
Apple Configurator 2 Konfiguration →	Wendet ein mit Apple Configurator 2 erstelltes Konfigurationsprofil (`.mobileconfig`) auf Geräte an
Externe Intelligenz-Einstellungen →	Externe, cloudbasierte KI-Integrationen über Siri und Apple Intelligence steuern (ab visionOS 26.4)
Intelligence-Einstellungen →	Apple-Intelligence-Funktionen wie Genmoji, Image Playground und Schreibwerkzeuge zentral steuern (ab visionOS 26.4)
Passwort →	Passwortrichtlinie für Apple-Geräte
Restriktionen →	Verwaltung von Geräterestriktionen
Siri-Einstellungen →	Verhalten von Siri zentral steuern, u. a. Obszönitätsfilter und Zugriff im gesperrten Zustand
Softwareupdates-Einstellungen →	Update-Verhalten der Geräte steuern, z. B. automatisches Laden, Aufschub und Benachrichtigungen (ab visionOS 26)
Verwaltete Softwareupdates →	Betriebssystemupdates erzwingen und eine Zielversion bis zu einer Frist vorgeben (ab visionOS 26, nur überwachte Geräte)
WLAN	Verwaltung der WLAN-Einstellungen
Zertifikat	Zertifikat auswählen, das standardmäßig auf dem Gerät installiert werden soll

Passwort

Die Apple Passwort-Policy definiert Sicherheitsvorgaben für Gerätepasswörter (Codes) auf visionOS-Geräten. Die Konfiguration ist unter visionOS für die Geräteregistrierung vorgesehen.

Die Richtlinie bietet eine Vielzahl an Optionen, um Anforderungen an die Passwortsicherheit weiter anzupassen. Dazu zählen unter anderem Vorgaben zur Komplexität, Länge, Gültigkeitsdauer und Anzahl zulässiger Fehlversuche.

Sobald die Richtlinie auf ein Gerät angewendet wird, ist dort grundsätzlich ein Gerätecode erforderlich. Felder, die leer bleiben, werden nicht an das Gerät übertragen; für diese Einstellungen macht die Richtlinie keine Vorgabe.

Als Voraussetzung wird mindestens visionOS 2.x benötigt.

Konfigurationsmöglichkeiten

- Einfache Passwörter erlauben (standardmäßig aktiviert): Erlaubt Codes mit sich wiederholenden oder auf- bzw. absteigenden Zeichenfolgen wie `aaa`, `abc` oder `123`.
- Zahlen und Buchstaben erzwingen (standardmäßig deaktiviert): Legt fest, ob der Code Buchstaben enthalten muss oder ob Ziffern ausreichen.
- Minimale Passwortlänge: Werte von 0 bis 25 Zeichen.
- Benötigte Anzahl von Sonderzeichen: Werte von 0 bis 4.
- Maximales Passwortalter (in Tagen): Anzahl der Tage, nach denen ein neuer Code gesetzt werden muss; Werte von 0 bis 730.
- Inaktivität (in Minuten): Höchstwert für die automatische Sperre nach Inaktivität, der dem Benutzer am Gerät zur Auswahl steht.
- Passwortverlauf: Anzahl zuvor verwendeter Codes, die nicht erneut gesetzt werden dürfen; Werte von 1 bis 50.
- Maximale Zeitgrenze für Gerätesperrung (in Minuten): Zeitraum nach dem Sperren, in dem das Gerät noch ohne Eingabe des Codes entsperrt werden kann. Bei Sofort wird der Code bei jedem Entsperren abgefragt. Die Einstellung legt nicht fest, wann das Gerät gesperrt wird – das regelt Inaktivität (in Minuten).
    - Sofort
    - 1 Minute
    - 5 Minuten
    - 15 Minuten
    - 60 Minuten
    - 4 Stunden
- Maximale Anzahl von Fehlversuchen: Werte von 2 bis 11.

    Wird die Anzahl überschritten, wird eine Wipe-Aktion ausgelöst.

Für Version 26.4.0

Apple Configurator 2 Konfiguration

Mit dieser Richtlinien-Konfiguration können `.mobileconfig`-Dateien auf Apple-Geräte übertragen werden. Eine solche Datei kann beispielsweise eine WLAN-Verbindung samt zugehörigem Identitätszertifikat (PKCS#12, `.p12`) enthalten.

Konfiguration

Im Feld Name wird eine Bezeichnung für die Konfiguration vergeben. Über .mobileconfig Datei auswählen wird die Datei hochgeladen. Danach erscheint ihr Inhalt anstelle der Dateiauswahl im Feld Payload Inhalt und kann dort bearbeitet werden. Der Inhalt muss gültiges XML sein. Signierte Profile sind kein lesbares XML und lassen sich daher nicht verwenden. In Apple Configurator 2 wird die Datei deshalb ohne Signatur gesichert. Wird das Feld Payload Inhalt geleert, kann erneut eine Datei ausgewählt werden.

Im Feld Payload Inhalt können Benutzer-, Geräte- und Zertifikatsplatzhalter verwendet werden. Die verfügbaren Platzhalter werden unterhalb des Formulars angezeigt und beim Übertragen auf das Gerät ersetzt, siehe Erweiterte Platzhalter →.

Pro Richtlinie können mehrere Apple-Configurator-2-Konfigurationen angelegt werden. Auf diese Weise lassen sich mehrere Konfigurationstypen auf getrennte Konfigurationen verteilen.

Anforderungen an die Datei

Für Version 26.4.0

Beim Speichern wird der Inhalt geprüft. Die Datei muss folgende Bedingungen erfüllen:

- Auf der obersten Ebene sind die Schlüssel `PayloadType`, `PayloadVersion` (als Zahl), `PayloadIdentifier`, `PayloadUUID` und `PayloadDisplayName` vorhanden.
- `PayloadContent` enthält genau einen Konfigurationstyp. Zusätzlich dürfen Zertifikat-Payloads enthalten sein.

Dateien, die sich nicht auslesen lassen, denen einer dieser Schlüssel fehlt, die keinen Payload oder mehrere Konfigurationstypen enthalten, werden beim Speichern abgelehnt.

> Mit übertragen werden nur Zertifikate im Format PKCS#12 (`com.apple.security.pkcs12`). PKCS#1-Zertifikate (`com.apple.security.pkcs1`) werden bei der Prüfung zwar akzeptiert, aber nicht an das Gerät übertragen. Andere Zertifikate wie Root-Zertifikate (`com.apple.security.root`) zählen als eigener Konfigurationstyp. Zusammen mit einer weiteren Konfiguration führen sie zu einem Fehler beim Speichern und werden daher in einer eigenen Konfiguration hinterlegt.
>
> Die eigentliche Konfiguration muss in `PayloadContent` an erster Stelle stehen. Enthält die Datei mehrere Payloads desselben Typs, wird nur der erste auf das Gerät übertragen.

Enthält die Datei einen Konfigurationstyp, den Relution auch als eigene, nur einmal pro Richtlinie zulässige Konfiguration anbietet, lässt sich diese Konfiguration in derselben Richtlinie nicht mehr hinzufügen. Unter visionOS betrifft das Passwort → (`com.apple.mobiledevice.passwordpolicy`) und Restriktionen → (`com.apple.applicationaccess`).

Umgekehrt wird eine solche Datei beim Speichern abgelehnt, wenn die Richtlinie die entsprechende Konfiguration oder eine weitere aktive Apple-Configurator-2-Konfiguration mit demselben Payload-Typ bereits enthält.

Beispiel

Die folgende Datei überträgt eine WLAN-Verbindung (`com.apple.wifi.managed`). SSID, Passwort, Bezeichner und UUIDs sind Beispielwerte und werden durch eigene Werte ersetzt. Jede `PayloadUUID` muss eindeutig sein.

Für Version 26.4.0

```xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
 <key>PayloadContent</key>
 <array>
  <dict>
   <key>AutoJoin</key>
   <true/>
   <key>EncryptionType</key>
   <string>WPA2</string>
   <key>HIDDEN_NETWORK</key>
   <false/>
   <key>Password</key>
   <string>WLAN-Passwort</string>
   <key>PayloadDisplayName</key>
   <string>WLAN</string>
   <key>PayloadIdentifier</key>
   <string>com.example.wifi.payload</string>
   <key>PayloadType</key>
   <string>com.apple.wifi.managed</string>
   <key>PayloadUUID</key>
   <string>8D2E4C1A-3B5F-4A7E-9C6D-1F0B2A3C4D5E</string>
   <key>PayloadVersion</key>
   <integer>1</integer>
   <key>SSID_STR</key>
   <string>Firmen-WLAN</string>
  </dict>
 </array>
 <key>PayloadDescription</key>
 <string>WLAN-Konfiguration für Apple-Geräte</string>
 <key>PayloadDisplayName</key>
 <string>WLAN</string>
 <key>PayloadIdentifier</key>
 <string>com.example.wifi</string>
 <key>PayloadOrganization</key>
 <string>Beispiel GmbH</string>
 <key>PayloadType</key>
 <string>Configuration</string>
 <key>PayloadUUID</key>
 <string>4A7B1C2D-5E6F-4890-A1B2-C3D4E5F60718</string>
 <key>PayloadVersion</key>
 <integer>1</integer>
</dict>
</plist>
```

Intelligence-Einstellungen

Mit Relution lässt sich die Konfiguration Intelligence-Einstellungen zentral verwalten, um die Funktionen von Apple Intelligence auf verwalteten visionOS-Geräten zu steuern. Über die Richtlinie lassen sich einzelne KI-gestützte Funktionen wie der Apple-Intelligence-Bericht, Genmoji, Image Playground, Image Wand und die Schreibwerkzeuge erlauben oder unterbinden. Zusätzlich lassen sich die Intelligence-Funktionen in Mail und Safari steuern und das Diktieren ausschließlich lokal auf dem Gerät erzwingen, ohne Verbindung zu Apple-Servern.

Die Konfiguration steht für visionOS-Geräte ab Version 26.4 zur Verfügung.

> Das Formular ist für iOS, macOS und visionOS gleich aufgebaut. Die Optionen Personalisierte Handschriftergebnisse erlauben, Visual-Intelligence-Zusammenfassung erlauben, Übersetzung nur auf dem Gerät erzwingen sowie Transkription erlauben und Transkriptionszusammenfassung erlauben im Abschnitt Notizen werden auch für visionOS angezeigt, von visionOS aber nicht unterstützt. Sie sind deshalb hier nicht beschrieben, siehe Intelligence-Einstellungen für iOS →.

Einstellungen

Für Version 26.4.0

- Apple-Intelligence-Bericht erlauben
  - Wenn deaktiviert, wird der Apple-Intelligence-Bericht auf dem Gerät deaktiviert. Standardmäßig aktiviert.
- Genmoji erlauben
  - Wenn deaktiviert, wird die Genmoji-Funktion deaktiviert. Standardmäßig aktiviert.
- Image Playground erlauben
  - Wenn deaktiviert, wird Image Playground deaktiviert. Standardmäßig aktiviert.
- Image Wand erlauben
  - Wenn deaktiviert, wird Image Wand deaktiviert. Standardmäßig aktiviert.
- Schreibwerkzeuge erlauben
  - Wenn deaktiviert, werden die Schreibwerkzeuge (Writing Tools) deaktiviert. Standardmäßig aktiviert.
- Diktat nur auf dem Gerät erzwingen
  - Wenn aktiviert, wird Diktieren ausschließlich lokal auf dem Gerät verarbeitet, ohne Verbindung zu Apple-Servern. Standardmäßig deaktiviert.

Mail

- Intelligente Antworten erlauben
  - Wenn deaktiviert, werden intelligente Antworten (Smart Replies) in Mail deaktiviert. Standardmäßig aktiviert.
- Zusammenfassung erlauben
  - Wenn deaktiviert, wird die Zusammenfassungsfunktion in Mail deaktiviert. Standardmäßig aktiviert.

Safari

- Zusammenfassung erlauben
  - Wenn deaktiviert, wird die Zusammenfassungsfunktion in Safari deaktiviert. Standardmäßig aktiviert.

Für Version 26.4.0

Restriktionen

Folgend eine Übersicht der verfügbaren visionOS Restriktionen.

Die meisten Restriktionen setzen visionOS 2 voraus (Hinweis visionOS 2+ im Formular); abweichende Mindestversionen wie visionOS 1.1+, visionOS 2.4+ oder visionOS 26+ sind in der Übersicht unten angegeben. Restriktionen mit dem Hinweis Wird überwacht wirken nur auf überwachten Geräten, Restriktionen mit dem Hinweis Unterstützt Benutzerregistrierung auch auf Geräten mit Benutzerregistrierung; beides ist in der Übersicht entsprechend markiert. Die Restriktionen für AI-Funktionen sind im Portal als Veraltet gekennzeichnet.

Standardmäßig sind alle Optionen aktiviert, ausgenommen das Diktieren nur auf dem Gerät, die beiden Kontakt-Optionen unter Verwaltete Apps und Dokumente, die Anwendung der Einstellungen für Öffnen von ··· auf Copy and Paste, AirDrop-Ziele immer als nicht verwaltet betrachten, Automatische Datums- und Zeiteinstellungen erzwingen und WLAN-Whitelisting erzwingen. Die Liste Zulässige Workspace-IDs für die externe Integration ist leer. Mit den Standardwerten sind somit alle Funktionen erlaubt; einzig Authentifizierung vor automatischer Ausfüllung erzwingen ist standardmäßig aktiviert, vor dem automatischen Ausfüllen ist also eine Authentifizierung erforderlich.

Über das Download-Symbol oben im Formular (Restriktionen als CSV-Datei exportieren) lassen sich die eingestellten Werte einschließlich noch nicht gespeicherter Änderungen als CSV-Datei herunterladen.

Von den Empfohlenen Restriktionen für iOS/iPadOS → betreffen nur die Hinweise zu Alle Inhalte & Einstellungen löschen, Automatische Datums- und Zeiteinstellungen erzwingen und WLAN-Whitelisting erzwingen auch visionOS.

Für Version 26.4.0

Gerät

> Alle Restriktionen anzeigen

Apps

Die Einschränkungen für Apps sind nach Anwendungsbereich gruppiert.

Allgemein

> Alle Restriktionen anzeigen

Safari

> Alle Restriktionen anzeigen

Siri

Alle Restriktionen anzeigen

Andere Apps

Alle Restriktionen anzeigen

Verwaltete Apps und Dokumente

Diese Einstellungen steuern den Datenaustausch zwischen verwalteten und nicht verwalteten Apps.

Einschränkungen für verwaltete Apps und Dokumente

Alle Restriktionen anzeigen

Für Version 26.4.0

Einstellungen

Die folgenden Einschränkungen betreffen die Systemeinstellungen des Geräts.

Einschränkungen der Einstellungen

Alle Restriktionen anzeigen

Medien

Die folgenden Einschränkungen betreffen Medieninhalte und deren Wiedergabe.

Einschränkungen für die Medien

Alle Restriktionen anzeigen

Änderungen

Diese Einschränkungen legen fest, welche Einstellungen am Gerät geändert werden dürfen.

Einschränkungen bei Änderungen

Alle Restriktionen anzeigen

iCloud

Die folgenden Einschränkungen betreffen die iCloud-Dienste auf dem Gerät.

iCloud-Einschränkungen

Alle Restriktionen anzeigen

Restriktionen für AI-Funktionen

Für Version 26.4.0

Diese Einschränkungen steuern die Apple-Intelligence-Funktionen.

Alle Restriktionen dieses Abschnitts sind im Portal als Veraltet gekennzeichnet. Für Geräte ab visionOS 26.4 stehen dafür die Konfigurationen Intelligence-Einstellungen → (Genmoji, Image Playground, Schreibwerkzeuge, Image Wand) und Externe Intelligenz-Einstellungen → (externe Intelligence-Integrationen, Anmeldung, Workspace-ID) zur Verfügung; der Artikel zu den externen Intelligenz-Einstellungen beschreibt die Konfiguration am Beispiel von iOS. Für Geräte mit älteren visionOS-Versionen gelten weiterhin die hier beschriebenen Restriktionen.

Allgemein

Alle Restriktionen anzeigen

App Konformität

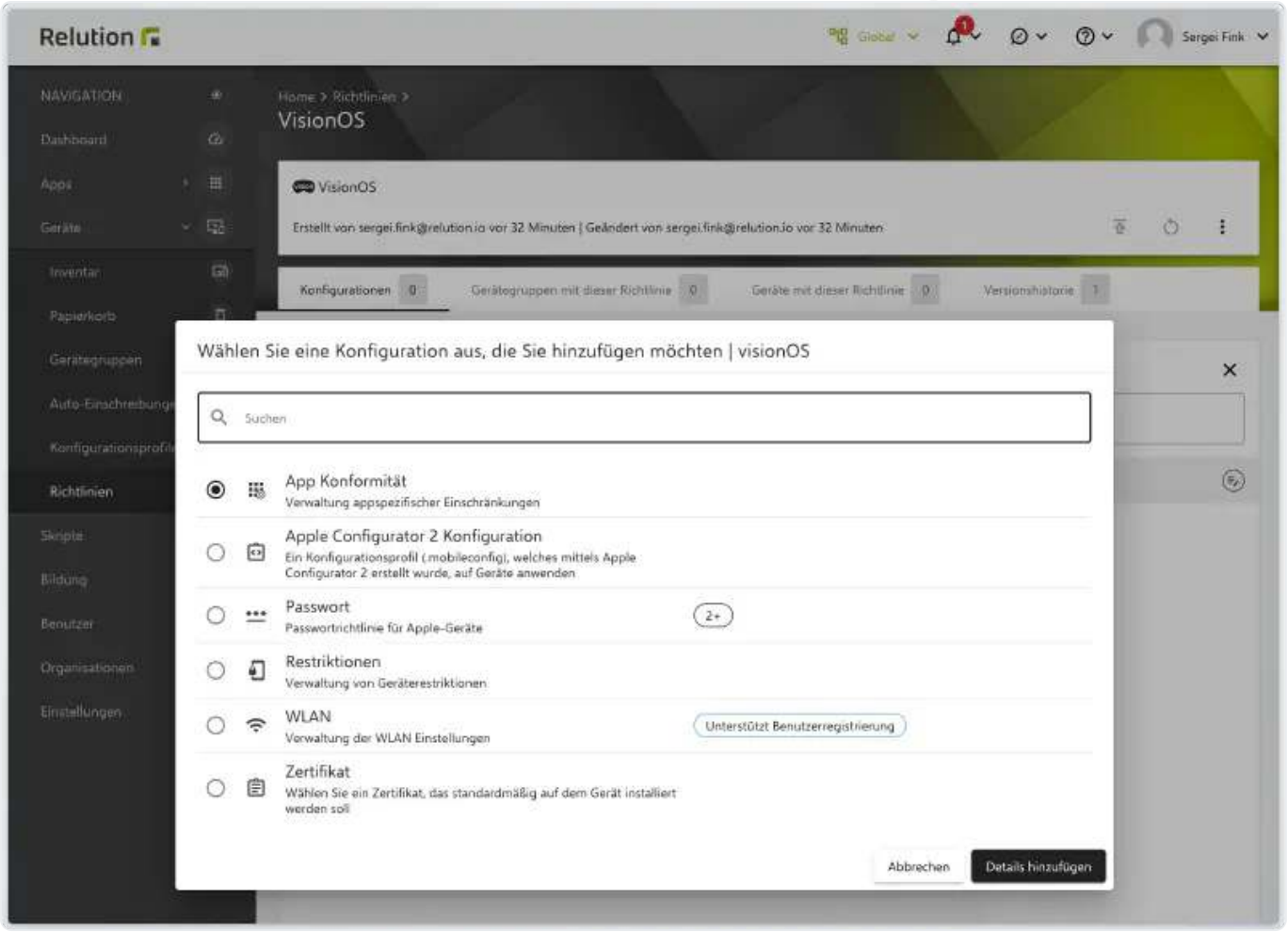
Die Installation von Apps aus Apps und Bücher (im Portal: VPP) auf Apple Vision Geräten gestaltet sich dank der App Konformität-Richtlinie von Relution besonders unkompliziert. Diese Konfiguration ermöglicht eine einfache und zentrale Verteilung von Anwendungen auf eine Vielzahl von Geräten.

Um mit der Verteilung zu beginnen, ist lediglich Folgendes erforderlich:

- Ein Apple School- oder Apple Business-Konto.
- Die Einbindung des eigenen Tokens für Apps und Bücher → in Relution.
- Erworbene Lizenzen für die gewünschten Apps aus dem Apple School Manager (ASM) oder Apple Business Manager (ABM).

Konfiguration der App Konformität

Die Verteilung von Apps auf Apple Vision Geräten (analog zu iOS-Geräten) erfolgt über die Richtlinien-Konfiguration App Konformität. Sie wird unter `Geräte` → `Richtlinien` in einer visionOS-Richtlinie über Konfiguration hinzufügen ausgewählt und mit Details hinzufügen angelegt.



Ähnlich wie bei iOS-Geräten wird die Verfügbarkeit von Apps im Abschnitt Allgemein unter Listenart gesteuert: entweder als Sperrliste (Alle Apps in der folgenden Liste sind nicht erlaubt, Standard bei neuen Konfigurationen) oder als Positivliste (Alle Apps in der folgenden Liste sind erlaubt). Die Apps werden im darunterliegenden Abschnitt Apps auf der Sperrliste bzw. Apps auf der Positivliste über Hinzufügen eingetragen.

Positiv- und Sperrliste werden nur auf betreuten (supervised) Geräten angewendet.

Positivliste (erlaubte Apps)

Mit der Positivliste wird explizit definiert, welche Apps auf den Geräten verfügbar sein dürfen. Zusätzlich stehen zwei Optionen zur Verfügung:

- Alle Auto-Deployments hinzufügen: Apps, die über Auto-Deployments an die Benutzer der Geräte verteilt werden, werden automatisch in die Positivliste aufgenommen.
- Lokale Sicherheitsabfrage-Dialoge erlauben (z.B. iCloud- oder Google-Login): Der Systemdialog für lokale Sicherheitsabfragen wird in die Positivliste aufgenommen, damit solche Abfragen nicht blockiert werden.

Sperrliste (blockierte Apps)

Die Sperrliste wird verwendet, um bestimmte Apps auf den visionOS-Geräten auszublenden oder zu sperren.

Erforderliche Apps

Für Version 26.4.0

Im Abschnitt Erforderliche Apps wird festgelegt, welche Anwendungen verpflichtend auf den Geräten installiert werden sollen. Über Hinzufügen stehen folgende Quellen zur Verfügung (dieselben gelten auch für Positiv- und Sperrliste):

- Relution App Store App: Auswahl von Apps aus dem Relution App Store. Angeboten werden Apps der Plattformen visionOS und iOS, also öffentliche Apps (z. B. mit Lizenzen aus Apps und Bücher) und native, selbst hochgeladene Apps. iOS-Apps lassen sich nur auf Apple Vision Geräten nutzen, wenn sie mit visionOS kompatibel sind.
- Apple App Store App: Suche einer App im öffentlichen Apple App Store.
- App manuell hinzufügen: Eintrag einer App über Name und Interner Name (Bundle-ID).

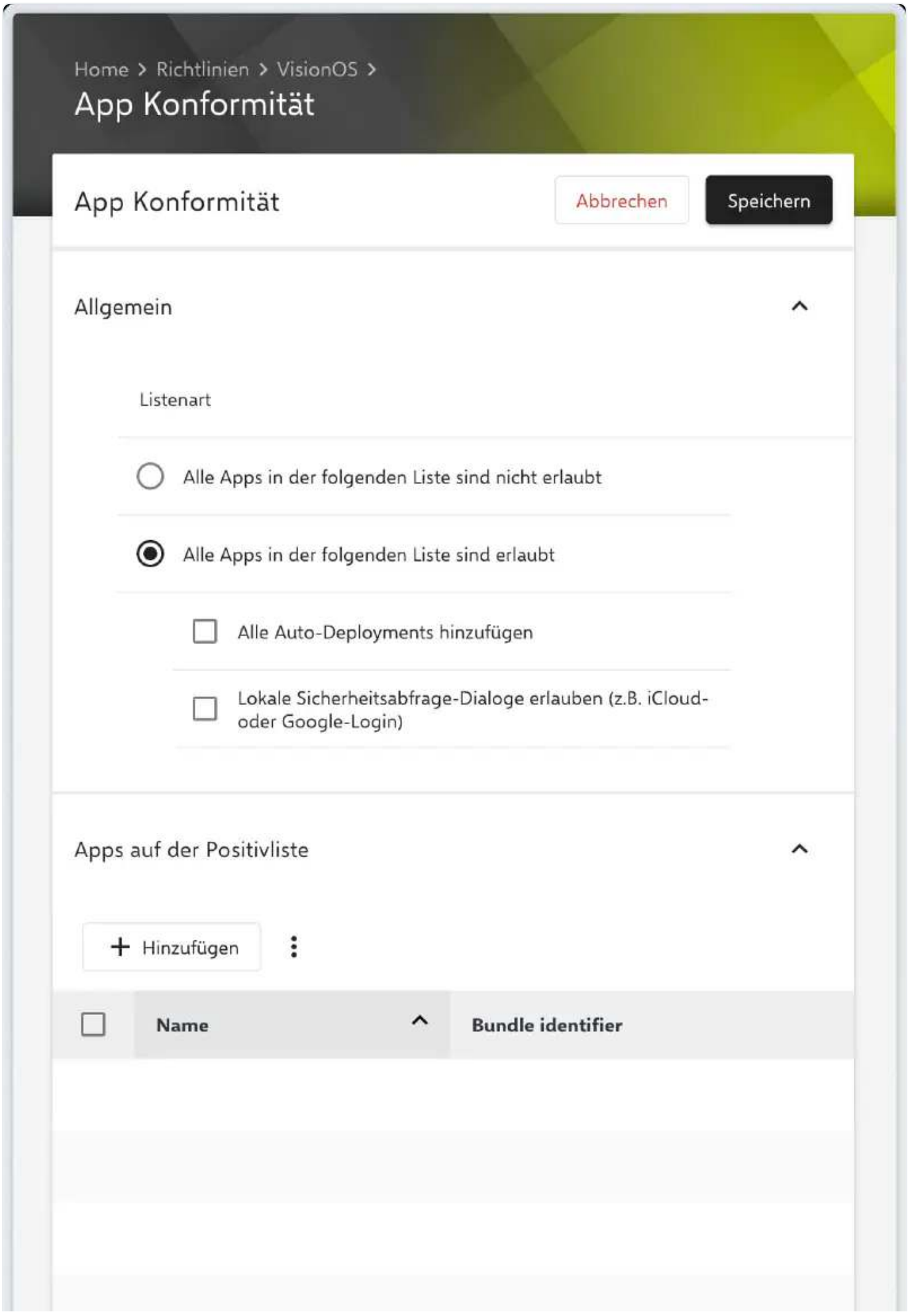
Ist eine erforderliche App nicht auf dem Gerät installiert, gilt das Gerät als nicht konform. Aktiv installiert wird die App nur, wenn in der Spalte Auto Installation das Häkchen gesetzt ist; beim Hinzufügen einer App ist es standardmäßig gesetzt. Automatisch installieren lassen sich native Apps aus dem Relution App Store sowie App-Store-Apps, deren Lizenzen aus Apps und Bücher den Geräten zugewiesen sind. Die Spalten VPP Lizenzen und Verfügbare VPP Lizenzen zeigen die vorhandenen und die noch freien Lizenzen je App.

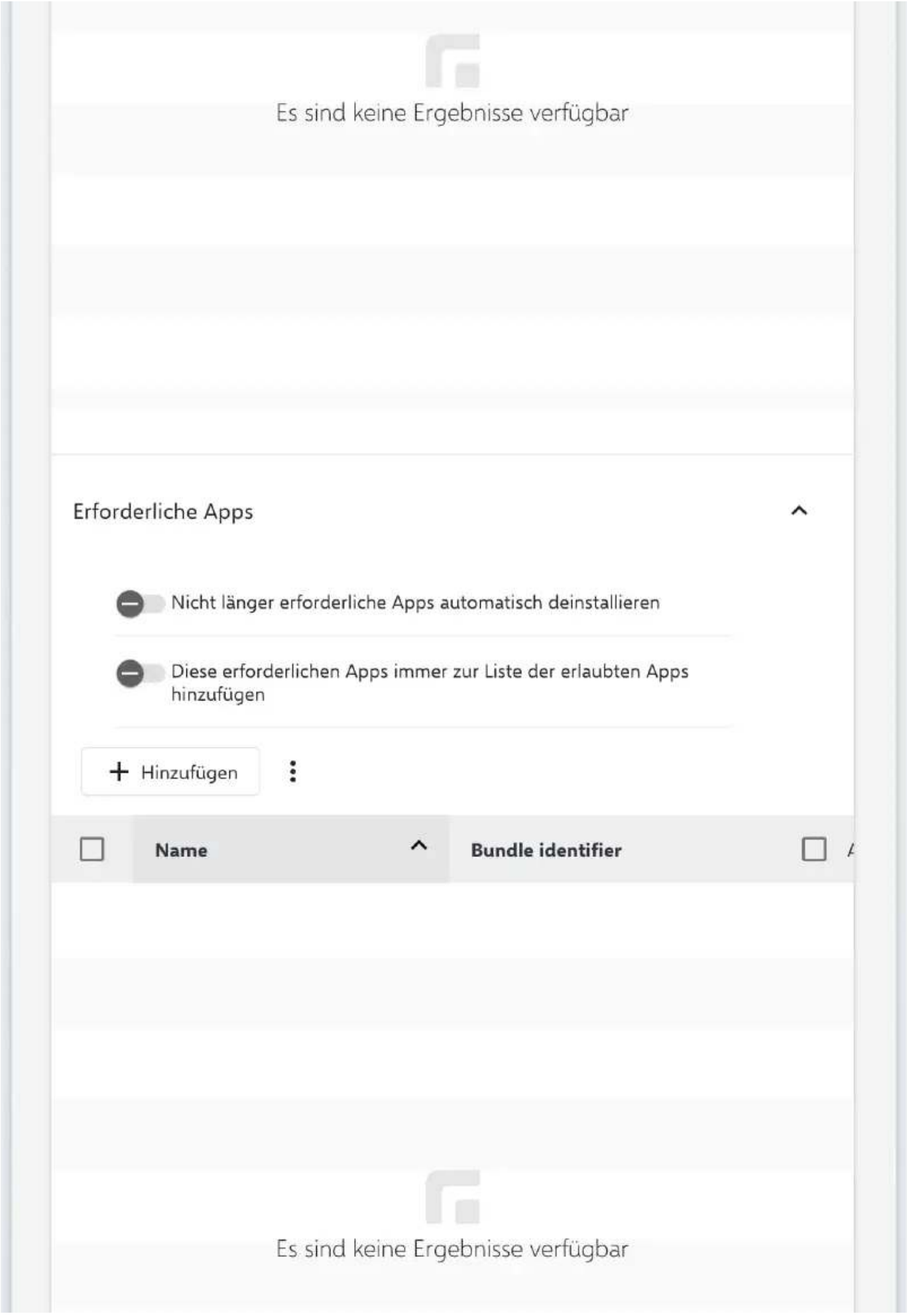
Oberhalb der Liste stehen zwei Schalter zur Verfügung:

- Nicht länger erforderliche Apps automatisch deinstallieren: Wird eine automatisch installierte erforderliche App aus der Konfiguration entfernt oder die Konfiguration vom Gerät entfernt, wird die App deinstalliert. Bei neuen Konfigurationen ist der Schalter ausgeschaltet.
- Diese erforderlichen Apps immer zur Liste der erlaubten Apps hinzufügen: Wird durch diese oder eine andere Richtlinie eine Positivliste für das Gerät konfiguriert, werden die erforderlichen Apps dort ergänzt.

Beim Speichern wird geprüft, ob sich die Listen widersprechen: Eine erforderliche App darf nicht auf der Sperrliste stehen. Ist bei einer Positivliste der zweite Schalter ausgeschaltet, müssen alle erforderlichen Apps auch auf der Positivliste eingetragen sein.

Sobald die Konfiguration abgeschlossen ist, kann sie gespeichert, veröffentlicht und den entsprechenden Geräten zugewiesen werden.


Home > Richtlinien > VisionOS >
App Konformität
App Konformität
Abbrechen
Speichern
Allgemein
Listenart
Alle Apps in der folgenden Liste sind nicht erlaubt
Alle Apps in der folgenden Liste sind erlaubt
Alle Auto-Deployments hinzufügen
Lokale Sicherheitsabfrage-Dialoge erlauben (z.B. iCloud- oder Google-Login)
Apps auf der Positivliste
+ Hinzufügen
Name
Bundle identifier


Es sind keine Ergebnisse verfügbar
Erforderliche Apps
Nicht länger erforderliche Apps automatisch deinstallieren
Diese erforderlichen Apps immer zur Liste der erlaubten Apps hinzufügen
+ Hinzufügen
Name
Bundle identifier
Es sind keine Ergebnisse verfügbar

Für Version 26.4.0

Einschreibung unter watchOS

Mit der iOS Konfiguration Einschreibungen für die Apple Watch können Apple Watch Geräte (watchOS) über ein verwaltetes iPhone in Relution eingeschrieben und verwaltet werden. Die Apple Watch selbst kann nicht direkt in Relution aufgenommen werden, sondern wird über ein gekoppeltes, in Relution verwaltetes iPhone registriert.

Voraussetzungen

- Ein iPhone mit iOS 17 oder neuer, das bereits in Relution eingeschrieben und verwaltet wird. Die Konfiguration wird über Apples deklarative Geräteverwaltung (Declarative Device Management) ausgeliefert und erreicht nur Geräte, die sie unterstützen. Ältere iPhones erhalten sie nicht, ohne dass ein Hinweis erscheint.
- Eine Apple Watch, die mit diesem iPhone gekoppelt werden kann.
- Eine aktive Internetverbindung auf dem iPhone.
- Die Kopplung mit einer Apple Watch ist auf dem iPhone erlaubt. Ist in den Restriktionen → die Option Kopplung mit Watch erlauben deaktiviert, ist keine Kopplung möglich; bereits gekoppelte Apple Watches werden sofort entkoppelt und gelöscht.

Vorgehensweise

Für Version 26.4.0

1. Konfiguration erstellen
   - Unter `Geräte` → `Richtlinien` wird in einer iOS-Richtlinie über Konfiguration hinzufügen die Konfiguration Einschreibungen für die Apple Watch angelegt.
2. Konfiguration anwenden
   - Die Richtlinie wird dem verwalteten iPhone zugewiesen.
   - Die Kopplung sollte erst beginnen, wenn das iPhone die Konfiguration erhalten hat.
   - Die Konfiguration wird über die deklarative Geräteverwaltung übertragen. Im Reiter Aktionen des iPhones zeigt die Aktion Synchronisierung der deklarativen Verwaltung, ob das iPhone die Synchronisierung angenommen hat. Ob die Konfiguration selbst angewendet wurde, zeigt Relution nicht gesondert an.
3. Apple Watch koppeln
   - Die Apple Watch wird in die Nähe des konfigurierten iPhones gehalten.
   - Der Kopplungsprozess wird auf dem iPhone gestartet.
   - Während der Kopplung erscheint eine Aufforderung, der Einschreibung in Relution zuzustimmen.

Nach Bestätigung dieser Aufforderung wird die Apple Watch in Relution registriert. Nach erfolgreicher Kopplung erscheint die Apple Watch als eigenständiges Gerät (watchOS) im Geräte-Inventar. Sie übernimmt Organisation und Benutzer des iPhones und wird als Gerät in Firmenbesitz (COD) geführt. In den Gerätedetails des iPhones ist sie zusätzlich im Reiter Gekoppelte Geräte aufgeführt. Über die Richtlinien können anschließend bestimmte Einschränkungen oder Profile angewendet werden, die für watchOS unterstützt werden.

Hinweise

- Wenn die Apple Watch von einem iPhone entkoppelt wird, verliert sie automatisch ihre MDM-Zuordnung.
- Wird das iPhone in Relution gelöscht oder zurückgezogen, wird die gekoppelte Apple Watch ebenfalls aus der Verwaltung entfernt.
- Nur kompatible watchOS-Versionen können über diese Methode eingeschrieben werden.

Verfügbare Aktionen

Relution stellt eine Auswahl an Aktionen bereit, um die Apple Watch direkt zu kontrollieren und zu lenken. Die Aktionen lassen sich gezielt auf ein einzelnes Gerät oder über die Mehrfachauswahl in der Geräteliste auf mehrere Geräte gleichzeitig anwenden. Zusätzlich können sie über die Mitgliedschaft in Gerätegruppen ereignis- oder zeitgesteuert ausgelöst werden: Aktionen mit Gerätegruppen →

Aktionsübersicht

Aktion	Beschreibung
Geräteinformationen aktualisieren	Aktualisiert alle verfügbaren Informationen zu dem Gerät, die unter Details aufgelistet sind.
Relution Store App bereitstellen	Nach einer App im Relution Store suchen und diese auf den Geräten installieren.
MDM Profil aktualisieren	Erneuert die MDM-Registrierungsdaten auf dem Gerät, um sicherzustellen, dass es mit den aktuellen Server- und Profileinstellungen übereinstimmt.

Verfügbare Konfigurationen

Eine Richtlinie ist eine Sammlung einer oder mehrerer Konfigurationen. Jede Richtlinie kann auf einem oder mehreren Geräten gleichzeitig angewendet werden. Zudem können mit jedem Gerät eine oder mehrere Richtlinien verknüpft sein.

Konfigurationen im Überblick

Konfiguration	Beschreibung
App Konformität →	Verwaltung appspezifischer Einschränkungen
Apple Configurator 2 Konfiguration →	Wendet ein mit Apple Configurator 2 erstelltes Konfigurationsprofil (`.mobileconfig`) auf Geräte an
Passwort →	Passwortrichtlinie für Apple-Geräte
Restriktionen →	Verwaltung von Geräterestriktionen
Siri-Einstellungen	Verwaltung der Siri-Einstellungen
WLAN	Verwaltung der WLAN-Einstellungen
Zertifikat	Zertifikat auswählen, das standardmäßig auf dem Gerät installiert werden soll

Die Konfigurationen WLAN, Zertifikat und Apple Configurator 2 Konfiguration können mehrfach in einer Richtlinie angelegt werden, alle übrigen jeweils nur einmal.

Passwort

Die Apple Passwort-Policy definiert Sicherheitsvorgaben für Gerätepasswörter (Codes) auf watchOS-Geräten.

Die Richtlinie bietet eine Vielzahl an Optionen, um Anforderungen an die Passwortsicherheit weiter anzupassen. Dazu zählen unter anderem Vorgaben zur Komplexität, Länge, Gültigkeitsdauer und Anzahl zulässiger Fehlversuche.

Sobald die Richtlinie auf ein Gerät angewendet wird, ist dort grundsätzlich ein Gerätecode erforderlich. Felder, die leer bleiben, werden nicht an das Gerät übertragen; für diese Einstellungen macht die Richtlinie keine Vorgabe.

Als Voraussetzung wird mindestens watchOS 10.x benötigt.

Konfigurationsmöglichkeiten

- Einfache Passwörter erlauben (standardmäßig aktiviert): Erlaubt Codes mit sich wiederholenden oder auf- bzw. absteigenden Zeichenfolgen wie `aaa`, `abc` oder `123`.
- Zahlen und Buchstaben erzwingen (standardmäßig deaktiviert): Legt fest, ob der Code Buchstaben enthalten muss oder ob Ziffern ausreichen.
- Minimale Passwortlänge: Werte von 0 bis 25 Zeichen.
- Benötigte Anzahl von Sonderzeichen: Werte von 0 bis 4.
- Maximales Passwortalter (in Tagen): Anzahl der Tage, nach denen ein neuer Code gesetzt werden muss; Werte von 0 bis 730.
- Inaktivität (in Minuten): Höchstwert für die automatische Sperre nach Inaktivität, der dem Benutzer am Gerät zur Auswahl steht.
- Passwortverlauf: Anzahl zuvor verwendeter Codes, die nicht erneut gesetzt werden dürfen; Werte von 1 bis 50.
- Maximale Zeitgrenze für Gerätesperrung (in Minuten): Zeitraum nach dem Sperren, in dem das Gerät noch ohne Eingabe des Codes entsperrt werden kann. Bei Sofort wird der Code bei jedem Entsperren abgefragt. Die Einstellung legt nicht fest, wann das Gerät gesperrt wird – das regelt Inaktivität (in Minuten).
    - Sofort
    - 1 Minute
    - 5 Minuten
    - 15 Minuten
    - 60 Minuten
    - 4 Stunden
- Maximale Anzahl von Fehlversuchen: Werte von 2 bis 11.

Wird die Anzahl überschritten, wird eine Wipe-Aktion ausgelöst.

Für Version 26.4.0

Apple Configurator 2 Konfiguration

Mit dieser Richtlinien-Konfiguration können `.mobileconfig`-Dateien auf Apple-Geräte übertragen werden. Eine solche Datei kann beispielsweise eine WLAN-Verbindung samt zugehörigem Identitätszertifikat (PKCS#12, `.p12`) enthalten.

Konfiguration

Im Feld Name wird eine Bezeichnung für die Konfiguration vergeben. Über .mobileconfig Datei auswählen wird die Datei hochgeladen. Danach erscheint ihr Inhalt anstelle der Dateiauswahl im Feld Payload Inhalt und kann dort bearbeitet werden. Der Inhalt muss gültiges XML sein. Signierte Profile sind kein lesbares XML und lassen sich daher nicht verwenden. In Apple Configurator 2 wird die Datei deshalb ohne Signatur gesichert. Wird das Feld Payload Inhalt geleert, kann erneut eine Datei ausgewählt werden.

Im Feld Payload Inhalt können Benutzer-, Geräte- und Zertifikatsplatzhalter verwendet werden. Die verfügbaren Platzhalter werden unterhalb des Formulars angezeigt und beim Übertragen auf das Gerät ersetzt, siehe Erweiterte Platzhalter →.

Pro Richtlinie können mehrere Apple-Configurator-2-Konfigurationen angelegt werden. Auf diese Weise lassen sich mehrere Konfigurationstypen auf getrennte Konfigurationen verteilen.

Anforderungen an die Datei

Für Version 26.4.0

Beim Speichern wird der Inhalt geprüft. Die Datei muss folgende Bedingungen erfüllen:

- Auf der obersten Ebene sind die Schlüssel `PayloadType`, `PayloadVersion` (als Zahl), `PayloadIdentifier`, `PayloadUUID` und `PayloadDisplayName` vorhanden.
- `PayloadContent` enthält genau einen Konfigurationstyp. Zusätzlich dürfen Zertifikat-Payloads enthalten sein.

Dateien, die sich nicht auslesen lassen, denen einer dieser Schlüssel fehlt, die keinen Payload oder mehrere Konfigurationstypen enthalten, werden beim Speichern abgelehnt.

> Mit übertragen werden nur Zertifikate im Format PKCS#12 (`com.apple.security.pkcs12`). PKCS#1-Zertifikate (`com.apple.security.pkcs1`) werden bei der Prüfung zwar akzeptiert, aber nicht an das Gerät übertragen. Andere Zertifikate wie Root-Zertifikate (`com.apple.security.root`) zählen als eigener Konfigurationstyp. Zusammen mit einer weiteren Konfiguration führen sie zu einem Fehler beim Speichern und werden daher in einer eigenen Konfiguration hinterlegt.
>
> Die eigentliche Konfiguration muss in `PayloadContent` an erster Stelle stehen. Enthält die Datei mehrere Payloads desselben Typs, wird nur der erste auf das Gerät übertragen.

Enthält die Datei einen Konfigurationstyp, den Relution auch als eigene, nur einmal pro Richtlinie zulässige Konfiguration anbietet, lässt sich diese Konfiguration in derselben Richtlinie nicht mehr hinzufügen. Unter watchOS betrifft das Passwort → (`com.apple.mobiledevice.passwordpolicy`) und Restriktionen → (`com.apple.applicationaccess`).

Umgekehrt wird eine solche Datei beim Speichern abgelehnt, wenn die Richtlinie die entsprechende Konfiguration oder eine weitere aktive Apple-Configurator-2-Konfiguration mit demselben Payload-Typ bereits enthält.

Beispiel

Die folgende Datei überträgt eine WLAN-Verbindung (`com.apple.wifi.managed`). SSID, Passwort, Bezeichner und UUIDs sind Beispielwerte und werden durch eigene Werte ersetzt. Jede `PayloadUUID` muss eindeutig sein.

Für Version 26.4.0

```xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
 <key>PayloadContent</key>
 <array>
  <dict>
   <key>AutoJoin</key>
   <true/>
   <key>EncryptionType</key>
   <string>WPA2</string>
   <key>HIDDEN_NETWORK</key>
   <false/>
   <key>Password</key>
   <string>WLAN-Passwort</string>
   <key>PayloadDisplayName</key>
   <string>WLAN</string>
   <key>PayloadIdentifier</key>
   <string>com.example.wifi.payload</string>
   <key>PayloadType</key>
   <string>com.apple.wifi.managed</string>
   <key>PayloadUUID</key>
   <string>8D2E4C1A-3B5F-4A7E-9C6D-1F0B2A3C4D5E</string>
   <key>PayloadVersion</key>
   <integer>1</integer>
   <key>SSID_STR</key>
   <string>Firmen-WLAN</string>
  </dict>
 </array>
 <key>PayloadDescription</key>
 <string>WLAN-Konfiguration für Apple-Geräte</string>
 <key>PayloadDisplayName</key>
 <string>WLAN</string>
 <key>PayloadIdentifier</key>
 <string>com.example.wifi</string>
 <key>PayloadOrganization</key>
 <string>Beispiel GmbH</string>
 <key>PayloadType</key>
 <string>Configuration</string>
 <key>PayloadUUID</key>
 <string>4A7B1C2D-5E6F-4890-A1B2-C3D4E5F60718</string>
 <key>PayloadVersion</key>
 <integer>1</integer>
</dict>
</plist>
```

Restriktionen

Folgend eine Übersicht der verfügbaren watchOS Restriktionen.

Die Konfiguration Restriktionen steht für watchOS-Geräte ab watchOS 10 zur Verfügung (Hinweis watchOS 10+ im Formular). Einzelne Restriktionen sind im Portal mit Wird überwacht gekennzeichnet und wirken nur auf überwachten Geräten; sie sind in der Übersicht unten entsprechend markiert.

Im Portal sind die Restriktionen in die Bereiche Gerät, Apps (mit den Abschnitten Allgemein und Siri), Einstellungen, Änderungen und Sperrbildschirm gegliedert. Standardmäßig sind alle Schalter aktiviert, ausgenommen Apple Watch Handgelenkerkennung erzwingen und die beiden Optionen zum Diktieren und Übersetzen nur auf dem Gerät. Mit den Standardwerten wird das Gerät somit nicht eingeschränkt.

Über das Download-Symbol oben im Formular (Restriktionen als CSV-Datei exportieren) lassen sich die eingestellten Werte einschließlich noch nicht gespeicherter Änderungen als CSV-Datei herunterladen.

Gerät

Alle Restriktionen anzeigen

Für Version 26.4.0

Apps

Der Bereich Apps ist in die Abschnitte Allgemein und Siri unterteilt.

Allgemein

Alle Restriktionen anzeigen

Siri

Alle Restriktionen anzeigen

Einschränkungen der Einstellungen

Alle Restriktionen anzeigen

Einschränkungen bei Änderungen

Alle Restriktionen anzeigen

Lockscreen-Einschränkungen

Alle Restriktionen anzeigen

Für Version 26.4.0

App Konformität

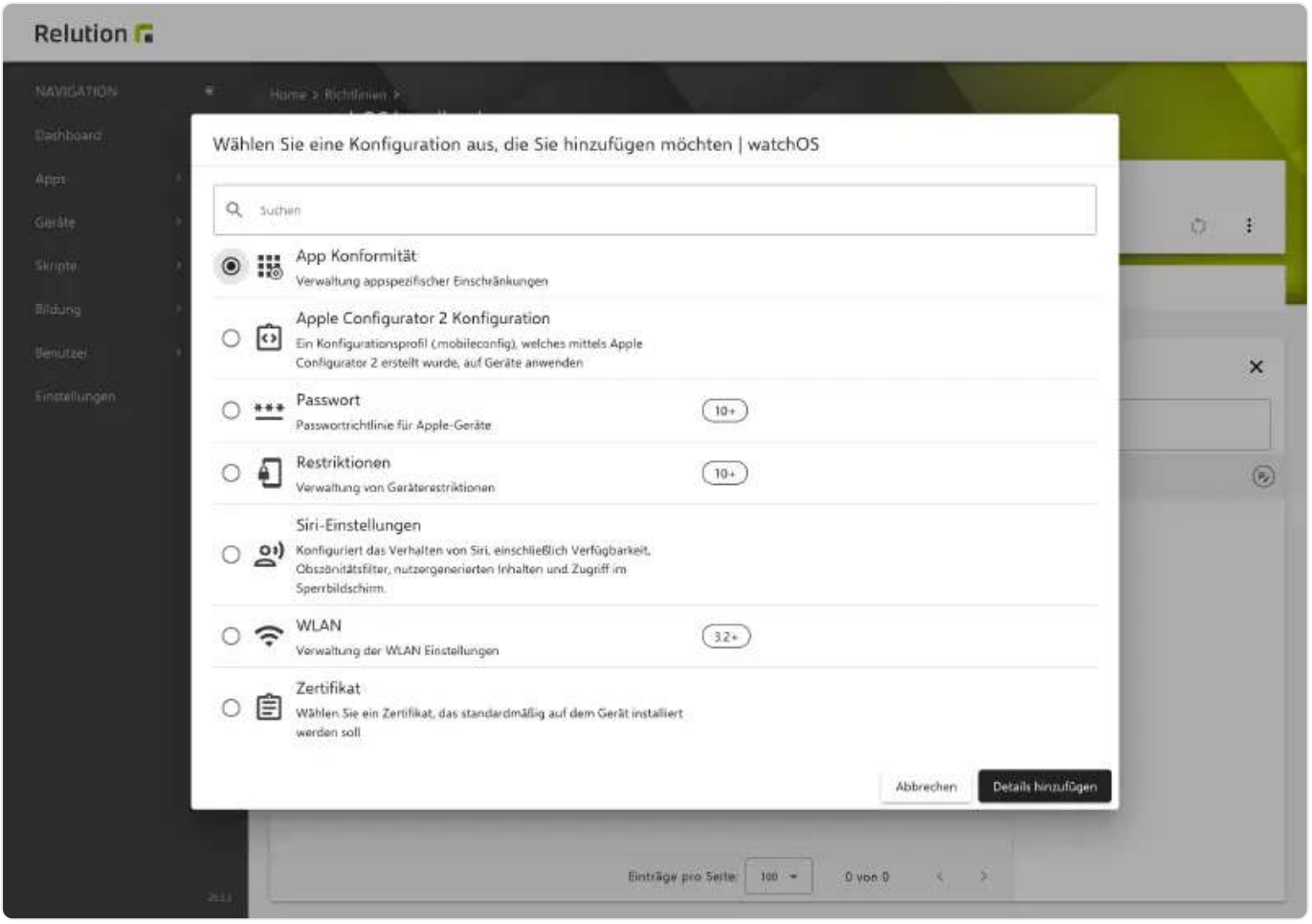
Die Installation von Apps aus Apps und Bücher (im Portal: VPP) auf Apple Watch Geräten gestaltet sich dank der App Konformität-Richtlinie von Relution besonders unkompliziert. Diese Konfiguration ermöglicht eine einfache und zentrale Verteilung von Anwendungen auf eine Vielzahl von Geräten.

Um mit der Verteilung zu beginnen, ist lediglich Folgendes erforderlich:

- Ein Apple School- oder Apple Business-Konto.
- Die Einbindung des eigenen Tokens für Apps und Bücher → in Relution.
- Erworbene Lizenzen für die gewünschten Apps aus dem Apple School Manager (ASM) oder Apple Business Manager (ABM).

Konfiguration der App Konformität

Die Verteilung von Apps auf Apple Watch Geräten (analog zu iOS-Geräten) erfolgt über die Richtlinien-Konfiguration App Konformität. Sie wird unter `Geräte` → `Richtlinien` in einer watchOS-Richtlinie über Konfiguration hinzufügen ausgewählt und mit Details hinzufügen angelegt.



Ähnlich wie bei iOS-Geräten wird die Verfügbarkeit von Apps im Abschnitt Allgemein unter Listenart gesteuert: entweder als Sperrliste (Alle Apps in der folgenden Liste sind nicht erlaubt, Standard bei neuen Konfigurationen) oder als Positivliste (Alle Apps in der folgenden Liste sind erlaubt). Die Apps werden im darunterliegenden Abschnitt Apps auf der Sperrliste bzw. Apps auf der Positivliste über Hinzufügen eingetragen.

Positiv- und Sperrliste werden nur auf betreuten (supervised) Geräten angewendet.

Positivliste (erlaubte Apps)

Mit der Positivliste wird explizit definiert, welche Apps auf den Geräten verfügbar sein dürfen. Zusätzlich stehen zwei Optionen zur Verfügung:

- Alle Auto-Deployments hinzufügen: Apps, die über Auto-Deployments an die Benutzer der Geräte verteilt werden, werden automatisch in die Positivliste aufgenommen.
- Lokale Sicherheitsabfrage-Dialoge erlauben (z.B. iCloud- oder Google-Login): Der Systemdialog für lokale Sicherheitsabfragen wird in die Positivliste aufgenommen, damit solche Abfragen nicht blockiert werden.

Sperrliste (blockierte Apps)

Die Sperrliste wird verwendet, um bestimmte Apps auf den watchOS-Geräten auszublenden oder zu sperren.

Erforderliche Apps

Für Version 26.4.0

Im Abschnitt Erforderliche Apps wird festgelegt, welche Anwendungen verpflichtend auf den Geräten installiert werden sollen. Über Hinzufügen stehen folgende Quellen zur Verfügung (dieselben gelten auch für Positiv- und Sperrliste):

- Relution App Store App: Auswahl öffentlicher Apps mit watchOS-Unterstützung aus dem Relution App Store, z. B. Apps mit Lizenzen aus Apps und Bücher. Eine direkte Suche im öffentlichen Apple App Store gibt es für watchOS nicht; die Apps müssen zuvor in den Relution App Store übernommen worden sein.
- App manuell hinzufügen: Eintrag einer App über Name und Interner Name (Bundle-ID).

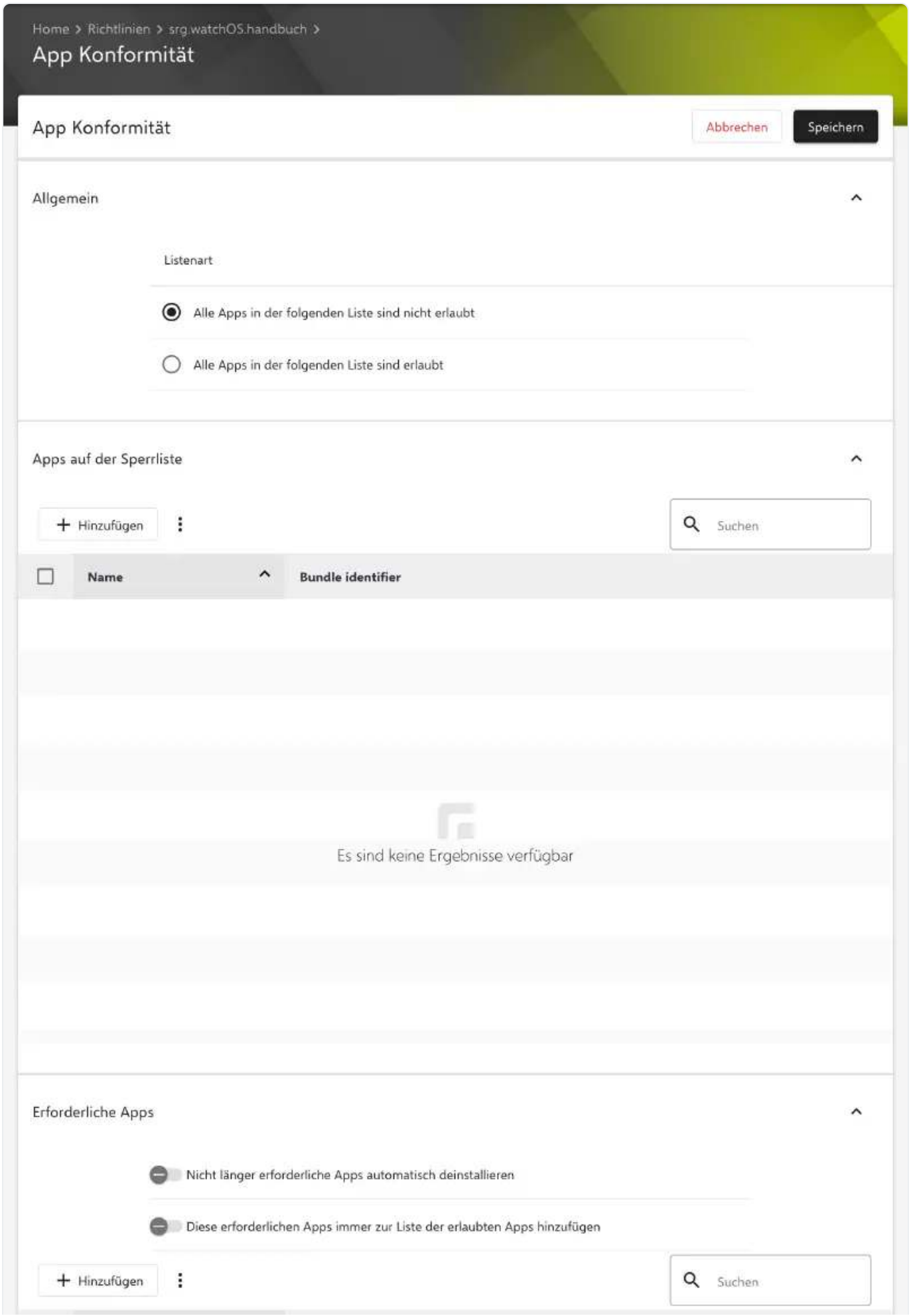
Native (selbst hochgeladene) Apps stehen in watchOS-Richtlinien nicht zur Auswahl, da Relution ihnen die Plattform iOS zuweist.

Ist eine erforderliche App nicht auf dem Gerät installiert, gilt das Gerät als nicht konform. Aktiv installiert wird die App nur, wenn in der Spalte Auto Installation das Häkchen gesetzt ist; beim Hinzufügen einer App ist es standardmäßig gesetzt. Die Spalten VPP Lizenzen und Verfügbare VPP Lizenzen zeigen die vorhandenen und die noch freien Lizenzen je App.

Oberhalb der Liste stehen zwei Schalter zur Verfügung:

- Nicht länger erforderliche Apps automatisch deinstallieren: Wird eine automatisch installierte erforderliche App aus der Konfiguration entfernt oder die Konfiguration vom Gerät entfernt, wird die App deinstalliert. Bei neuen Konfigurationen ist der Schalter ausgeschaltet.
- Diese erforderlichen Apps immer zur Liste der erlaubten Apps hinzufügen: Wird durch diese oder eine andere Richtlinie eine Positivliste für das Gerät konfiguriert, werden die erforderlichen Apps dort ergänzt.

Sobald die Konfiguration abgeschlossen ist, kann sie gespeichert, veröffentlicht und den entsprechenden Geräten zugewiesen werden.


Home > Richtlinien > srg.watchOS.handbuch >
App Konformität
App Konformität
Abbrechen
Speichern
Allgemein
Listenart
Alle Apps in der folgenden Liste sind nicht erlaubt
Alle Apps in der folgenden Liste sind erlaubt
Apps auf der Sperrliste
+ Hinzufügen
Suchen
Name
Bundle identifier
Es sind keine Ergebnisse verfügbar
Erforderliche Apps
Nicht länger erforderliche Apps automatisch deinstallieren
Diese erforderlichen Apps immer zur Liste der erlaubten Apps hinzufügen
+ Hinzufügen
Suchen

Für Version 26.4.0

Bildungsgruppen

Bildungsgruppen sind Gerätegruppen vom Typ Bildung. Sie bündeln Richtlinien, die für die Dauer einer Unterrichtsstunde automatisch auf die Geräte der teilnehmenden Schüler angewendet werden. Die Gruppe und ihre Richtlinien werden im Portal vorbereitet; in Relution Teacher werden sie als Konfigurationen in der Unterrichtsvorlage ausgewählt. So lassen sich auch umfangreichere MDM-Einstellungen gezielt nur während des Unterrichts ausrollen.

Funktionsweise

Bei einer Bildungsgruppe werden ausschließlich die Richtlinien konfiguriert. Welche Geräte Mitglied sind, steuert Relution automatisch über den Unterricht: Die Geräte der teilnehmenden Schüler werden beim Start eines Unterrichts, der diese Gruppe als Konfiguration verwendet, hinzugefügt und beim Beenden wieder entfernt. Geräte lassen sich bei diesem Gruppentyp nicht manuell zuweisen; ein Filter wird nicht ausgewertet. Die Geräte der Lehrkraft werden nicht Mitglied der Gruppe.

- Beim Start des Unterrichts werden die Schülergeräte der Gruppe hinzugefügt und erhalten die verknüpften Richtlinien.
- Während des Unterrichts wird die Zuordnung angepasst, sobald Schüler hinzukommen oder entfernt werden. Werden die Konfigurationen des laufenden Unterrichts geändert, werden die Schülergeräte den neu gewählten Bildungsgruppen hinzugefügt und aus den abgewählten entfernt.
- Beim Beenden des Unterrichts werden die Geräte wieder aus der Gruppe entfernt, die Richtlinien entfallen.

> Infrastruktur-Richtlinien wie WLAN sollten nicht über eine Bildungsgruppe verteilt werden: Sie würden den Geräten beim Beenden des Unterrichts wieder entzogen.

Für Version 26.4.0

Bildungsgruppe anlegen

Bildungsgruppen werden wie andere Gerätegruppen unter `Geräte` → `Gerätegruppen` über Hinzufügen angelegt. Als Art der Gruppe wird Bildung gewählt. Anschließend werden der Gruppe die gewünschten Richtlinien zugewiesen. Die Art Bildung ist nur mit einer Education- oder Free-Lizenz verfügbar.

> Wird eine bestehende statische oder dynamische Gerätegruppe nachträglich auf Bildung umgestellt, entfernt Relution beim Speichern alle bisherigen Geräte aus der Gruppe. Die verknüpften Richtlinien entfallen damit auf diesen Geräten.

Name, Beschreibung und die verknüpften Richtlinien werden in Relution Teacher angezeigt. Aussagekräftige Namen und Beschreibungen erleichtern daher die Auswahl im Unterricht.

Allgemeine Informationen zu Gerätegruppen: Gerätegruppen →.

Berechtigung für Lehrkräfte

Welche Lehrkräfte Konfigurationen sehen und auswählen können, steuert die Leseberechtigung `Bildung` → `Unterrichts-Gerätegruppen` im Rollen-Editor. Sie ergänzt die Berechtigung `Bildung` → `Teacher App verwenden`; für die Auswahl von Konfigurationen sind beide erforderlich. Ohne diese Berechtigung werden in Relution Teacher keine Konfigurationen angezeigt. In den vordefinierten Rollen, die die Nutzung der Teacher App erlauben, ist sie bereits enthalten. Benutzerdefinierte Rollen erhalten sie nicht automatisch; dort wird `Bildung` → `Unterrichts-Gerätegruppen` bei Bedarf manuell ergänzt.

Mehr zu Rollen und Rechten: Berechtigungen →.

Verwendung in Relution Teacher

In der Unterrichtsvorlage listet der Bereich Konfigurationen die Bildungsgruppen der Organisation mit Name, Beschreibung und den verknüpften Richtlinien. Eine oder mehrere Konfigurationen können ausgewählt werden. Ist keine Bildungsgruppe vorhanden, erscheint der Hinweis Keine Konfigurationen verfügbar; die Vorlage lässt sich trotzdem wie gewohnt verwenden.

Details zur Unterrichtsvorlage: Relution Teacher →.

Apple Classroom

Relution ermöglicht es, an Apple-Geräten, die über Relution verwaltet werden (iPadOS / macOS), die Konfiguration für die Nutzung der Classroom-App zu verteilen. Apple Classroom ist eine App, die im Bildungssektor dafür genutzt wird, Lehrenden die Möglichkeit zu geben, Schülergeräte während des Unterrichts zu steuern bzw. zu kontrollieren.

Voraussetzungen

1. Zwei eingeschriebene Geräte in Relution (Supervised / Überwacht).
2. Mindestens zwei Benutzer.
3. Auf einem Gerät muss die Apple Classroom App installiert sein (Lehrer).
4. Eine gültige Education- oder Free-Lizenz für Relution.

Netzwerkvorbereitung

1. Die Geräte müssen sich im gleichen Netzwerk befinden, wenn Classroom genutzt werden soll.
2. Im WLAN muss eine Client-to-Client-Kommunikation möglich sein.
3. Port 3284: Für das Teilen von Dokumenten über Classroom.
4. Port 3285: Für die Kommunikation der Classroom-App.

Für Version 26.4.0

Benutzervorbereitung

1. Mindestens zwei Benutzer werden benötigt (ein Lehrender und ein Schüler).
2. Die Klassen müssen unter dem Punkt `Bildung` → `Klassen` angelegt werden. Dieser Schritt kann durch Import über eine Schnittstelle (z. B. LDAP oder Apple School Manager) automatisiert werden, alternativ können Benutzer und Klassen über eine CSV-Datei importiert werden. Relevante Handbuchartikel:
   - CSV-Import: Benutzer per CSV importieren →
   - LDAP-Integration: LDAP Konfiguration →
   - ASM-Import: Apple School Manager Import →
   - SchulConnex-Import: SchulConnex Import →
   - OneRoster: OneRoster Schnittstelle →
3. Lehrende und Schüler werden in der Klasse entweder einzeln oder über Benutzergruppen eingetragen, z. B. über die Gruppen `UIT - Teacher` / `UIT - Student`. Eine bestimmte Gruppenmitgliedschaft ist für Apple Classroom nicht erforderlich; maßgeblich ist allein die Eintragung als Lehrender bzw. Schüler in einer Klasse. Zu den Standardgruppen `Teacher` / `Student` und deren Rechten in Relution siehe Bildungsfunktion →.

Konfiguration

Relution verteilt an die Geräte sogenannte `Education-Konfigurationen`. In diesen Konfigurationen sind die Informationen enthalten, welche Klassen und Schüler von welchen Lehrenden gesteuert werden können.

Klassen, die nicht mindestens einen Lehrenden und einen Schüler enthalten, werden nicht in die Education-Konfiguration übernommen und erscheinen daher nicht in Apple Classroom. Zusätzlich zu den Klassen wird ein laufender Ad-hoc-Unterricht aus Relution Teacher als eigene Gruppe in die Education-Konfiguration aufgenommen, siehe Relution Teacher →.

Damit die Verteilung der Education-Konfiguration gelingt, müssen die Benutzer den Geräten zugewiesen werden. Die Zuweisung kann entweder manuell oder per CSV-Datei erfolgen. Alternativ erfolgt die Zuweisung bei der Automatischen Geräteregistrierung (ADE, im Portal: DEP): Im DEP-Profil unter `Geräte` → `Konfigurationsprofile` wird bei Benutzerauthentifizierung die Option Benutzername + Passwort gewählt. Das Gerät wird dann dem Benutzer zugewiesen, der sich bei der Einschreibung anmeldet. Details: Konfigurationsprofil für ADE →. Es sollte beachtet werden, dass bereits eingeschriebene Geräte zurückgesetzt (`gelöscht`) und anschließend erneut eingeschrieben werden müssen, wenn die Benutzer auf diesem Weg zugewiesen werden.

Geteilte iPads ohne zugewiesenen Benutzer erhalten die Education-Konfiguration über die Klassen, die in der Konfiguration Einstellungen geteiltes iPad einer Richtlinie hinterlegt sind, siehe Klassenlisten (Geteiltes iPad) →.

Fehlerbehebung

Gelegentlich kann es vorkommen, dass einzelne oder mehrere Benutzer als `offline` für den Lehrenden angezeigt werden. Mögliche Ursachen und Lösungen:

1. Ungültige oder abgelaufene Education-Konfiguration:
    - Bei einer ungültigen Konfiguration muss diese neu installiert werden. Hierzu muss der Benutzer aus der Klasse entfernt und neu zugewiesen werden.
    - Sollten Klassen automatisch über LDAP angelegt worden sein, muss der Benutzer dem Gerät entzogen und neu zugewiesen werden. Hinweis: Beim Einsatz dynamischer Gerätegruppen auf Benutzerbasis kann es hierbei zu Problemen kommen.
2. Fehlerhafte Netzwerkkonfiguration (Ports oder WLAN-Netzwerke):
    - Sind die benötigten Ports geschlossen oder befinden sich die Geräte in unterschiedlichen WLAN-Netzwerken, können Verbindungsprobleme auftreten.
    - Zur Überprüfung kann ein mobiler Hotspot genutzt werden, um die Geräte miteinander zu verbinden. Wenn die Geräte in dieser Umgebung als `online` angezeigt werden, ist eine entsprechende Anpassung der Netzwerkkonfiguration erforderlich.

Für Version 26.4.0

Apple School Manager Import

Die ASM Import Konfiguration ermöglicht es Relution, neue Benutzer basierend auf den Daten aus dem Apple School Manager (ASM) zu erstellen oder bestehende Benutzer mit den verwalteten Apple Accounts (im Portal: Managed Apple ID) aus dem ASM zu synchronisieren. Zusätzlich lassen sich die Klassen aus dem ASM übernehmen.

Der umgekehrte Weg, also das Anlegen verwalteter Apple Accounts im ASM aus den Daten in Relution, ist unter SFTP-Upload → beschrieben.

Voraussetzungen

- Ein gültiger ADE-Token (Automatische Geräteregistrierung, im Portal: DEP-Token) in der Organisation, in der die Konfiguration angelegt werden soll.
- Verwaltete Apple Accounts, die im ASM mindestens in einer Klasse zusammengefasst sind (mindestens ein Schüler und mindestens ein Lehrer).

Konfiguration

Für Version 26.4.0

1. Navigieren zu den Einstellungen: `Einstellungen` → `Bildung` → `Apple School Manager Import Konfiguration`

2. Neue Konfiguration hinzufügen: Über Hinzufügen wird eine neue Konfiguration angelegt.

3. Name des Anbieters eintragen: Unter Name des Anbieters wird ein eindeutiger Name eingetragen. Der Name kann nach dem Speichern nicht mehr geändert werden, da Relution darüber die bereits synchronisierten Objekte zuordnet.

4. DEP-Konto auswählen: Unter DEP-Konto wird über Auswählen das DEP-Konto festgelegt, über das auf den Apple School Manager zugegriffen wird. Ohne DEP-Konto sind Verbindung prüfen, Standorte und Vorschau nicht verfügbar, und die Konfiguration lässt sich nicht speichern.

5. Verbindung prüfen: Über Verbindung prüfen kann überprüft werden, ob mit dem DEP-Konto eine Verbindung zum Apple School Manager möglich ist.

6. Standorte auswählen: Unter Standorte werden über Auswählen ein oder mehrere ASM-Standorte für den Import festgelegt. Importiert werden nur die Klassen dieser Standorte sowie die Lehrkräfte und Schüler, die Mitglied einer dieser Klassen sind.

7. Vorschau der Klassen: Unter Vorschau werden über Anzeigen die Klassen angezeigt, die schlussendlich importiert werden.

In der Global-Organisation und in Meta-Organisationen gibt es den Punkt Standorte nicht. Dort wird die Konfiguration zunächst mit dem DEP-Konto gespeichert. Anschließend wird im Bereich Objekte zu Organisationen zuordnen unter Standorte zu Organisationen zuordnen festgelegt, welche ASM-Standorte in welche Organisation importiert werden. Ohne zugeordnete Standorte findet keine Synchronisation statt.

Synchronisationseinstellungen

Im Bereich Synchronisationseinstellungen wird festgelegt, welche Objekte Relution aus dem ASM anlegt und was mit Objekten geschieht, die nicht mehr aus dem ASM geliefert werden.

Neue Relution-Benutzer erstellen

- Standardmäßig aktiviert.
- Relution legt für jeden ASM-Benutzer, zu dem kein passender Relution-Benutzer gefunden wird, einen neuen Benutzer an. Gesucht wird über die Verknüpfung aus früheren Synchronisationen, den verwalteten Apple Account und die unter Erweitert aktivierten Abgleichsregeln.
- Gefundene Benutzer ohne Quellsystem (z.B. manuell angelegt) oder aus derselben ASM-Konfiguration werden stattdessen verknüpft und übernommen. Sie erhalten die ASM-Konfiguration als Quellsystem.
- Benutzer anderer Quellsysteme (z.B. LDAP) werden nicht verknüpft. Haben sie dieselbe E-Mail-Adresse oder denselben Benutzernamen wie der anzulegende Benutzer, schlägt das Anlegen fehl (Synchronisierungsfehler Doppelte E-Mail bzw. Doppelter Benutzername).
- Ist die Option deaktiviert, werden nur vorhandene Benutzer verknüpft. ASM-Benutzer ohne passenden Relution-Benutzer werden nicht importiert.

Verwaltete Apple ID für den zugehörigen Benutzer eines beliebigen Quellsystems aktualisieren

Für Version 26.4.0

- Standardmäßig deaktiviert.
- Überschreibt das Feld Managed Apple ID eines Benutzers aus einem anderen Quellsystem (z.B. LDAP), wenn der ASM-Benutzer diesem Benutzer über eine der unter Erweitert aktivierten Abgleichsregeln zugeordnet werden kann. Weitere Daten des Benutzers und sein Quellsystem bleiben unverändert.
- Die Option greift nur für ASM-Benutzer, die weder verknüpft noch neu angelegt wurden, in der Praxis also nur, wenn Neue Relution-Benutzer erstellen deaktiviert ist.

Klassen synchronisieren

- Standardmäßig aktiviert.
- Importiert die Klassen der ausgewählten Standorte aus dem ASM und legt sie in Relution an bzw. aktualisiert sie.
- Klassen, für die in Relution keine synchronisierte Lehrkraft oder kein synchronisierter Schüler vorhanden ist, werden übersprungen (Synchronisierungsfehler Unterrichtsteilnehmer fehlen).
- Nur zu empfehlen, wenn:
  - Noch keine Daten (Klassen) in Relution vorliegen.
  - Klassen nicht manuell in Relution erstellt werden.
  - Kein LDAP-System genutzt wird.
- Wichtig: Sollten Klassen bereits über LDAP synchronisiert werden, ist von diesem Punkt abzuraten.

Aktion, wenn ein Benutzer in ASM entfernt wird

- Legt fest, was mit Benutzern dieser Konfiguration geschieht, die bei einer Synchronisation nicht mehr geliefert werden:
  - Keine (Standard): Die Benutzer bleiben unverändert.
  - Deaktivieren: Die Benutzer werden in Relution deaktiviert.
  - Löschen: Die Benutzer werden in Relution gelöscht.
- Betroffen sind alle Benutzer, die die ASM-Konfiguration als Quellsystem haben, also neu angelegte Benutzer ebenso wie verknüpfte Benutzer ohne vorheriges Quellsystem (z.B. manuell angelegt).
- Benutzer anderer Quellsysteme (z.B. LDAP), bei denen nur der verwaltete Apple Account aktualisiert wurde, bleiben unverändert. Ihr verwalteter Apple Account wird nicht entfernt.
- Liefert eine Synchronisation keinen einzigen Benutzer, etwa wegen eines Verbindungsproblems oder einer Fehlkonfiguration, werden keine Benutzer deaktiviert oder gelöscht.

Aktion, wenn eine Klasse in ASM entfernt wird

- Legt fest, ob Klassen in Relution bei Entfernung im ASM gelöscht werden: Keine (Standard) oder Löschen.
- Wenn keine Klassen synchronisiert wurden, hat diese Option keine Auswirkung.

Automatische Synchronisation über Cron-Syntax

- Definiert die Häufigkeit, mit der Relution automatisiert Informationen aus dem ASM importiert.
- Standardmäßig läuft die Synchronisation täglich um 6 und 21 Uhr (`0 0 6,21 * * ?`).

Erweitert

Für Version 26.4.0

Im Bereich Erweitert wird festgelegt, wie ASM-Benutzer vorhandenen Relution-Benutzern zugeordnet werden und welcher ASM-Wert als Benutzername dient.

Zuordnung zwischen ASM-Benutzer und Relution-Benutzer

- Legt fest, nach welchen Regeln ein ASM-Benutzer einem vorhandenen Relution-Benutzer zugeordnet wird. Mehrere Regeln können gleichzeitig aktiv sein.
- Vor diesen Regeln sucht die Synchronisation immer zuerst einen Relution-Benutzer, der bereits mit dem ASM-Benutzer verknüpft ist oder denselben verwalteten Apple Account hat.
- Danach werden die aktivierten Regeln in dieser Reihenfolge geprüft. Die erste zutreffende Regel gilt:
  1. Abgleich der verwalteten Apple-ID des ASM-Benutzers mit der E-Mail des Relution-Benutzers (Standard: aktiviert)
  2. Abgleich der E-Mail des ASM-Benutzers mit der E-Mail des Relution-Benutzers (Standard: deaktiviert)
  3. Abgleich des ASM-Benutzernamens mit dem Relution-Benutzername (Standard: deaktiviert)
  4. Abgleich von Vor- und Nachname des ASM-Benutzers mit Vor- und Nachname des Relution-Benutzers (Standard: deaktiviert)
- Berücksichtigt werden nur Relution-Benutzer derselben Organisation, die keinem Quellsystem zugeordnet sind oder aus dieser ASM-Konfiguration stammen. Benutzer anderer Quellsysteme (z.B. LDAP) werden nicht übernommen. Ist Verwaltete Apple ID für den zugehörigen Benutzer eines beliebigen Quellsystems aktualisieren aktiviert, bestimmen dieselben Regeln (ohne die vorgeschaltete Prüfung), bei welchem Benutzer eines anderen Quellsystems nur der verwaltete Apple Account aktualisiert wird.
- Hinweis: Wenn Neue Relution-Benutzer erstellen nicht ausgewählt wurde und keine der Regeln eine Zuordnung zulässt, passiert keine Verknüpfung zwischen den beiden Systemen.

Zuordnung ASM-Benutzer zu Relution-Benutzer

- Über Als Benutzername zu verwendende ASM-Eigenschaft wird festgelegt, welcher Wert aus dem ASM als Benutzername in Relution genutzt wird. Zur Auswahl stehen Name (Standard), Managed Apple ID und E-Mail.
- Hinweis: Bei jeder Synchronisation werden für zugeordnete Benutzer der Benutzername sowie Vor- und Nachname aus dem ASM übernommen. Die E-Mail-Adresse in Relution wird durch den verwalteten Apple Account ersetzt, und der Benutzer wird aktiviert.

Synchronisation

Die Synchronisation läuft automatisch nach dem eingestellten Zeitplan. Manuell wird sie in der Liste der Konfigurationen über das Kontextmenü mit Synchronisieren oder in der Detailansicht einer Konfiguration über das Symbol Synchronisieren gestartet.

Synchronisierte Lehrkräfte und Schüler werden der jeweiligen Standardgruppe `Teacher` bzw. `Student` ihrer Organisation hinzugefügt. Zu diesen Gruppen siehe Bildungsfunktion →.

Die Detailansicht zeigt die Ergebnisse der Synchronisationen getrennt nach Benutzer und Klassen, unter anderem mit Nächste geplante Synchronisierung, Zuletzt abgeschlossen und Erfolgreich. Über die Spalte Synchronisierungsfehler lassen sich die einzelnen Fehler anzeigen, z.B. Doppelte E-Mail, Doppelter Benutzername, Unterrichtsteilnehmer fehlen oder Die Synchronisation des Roster-Objekts ist fehlgeschlagen.

Für Version 26.4.0

Organisation verknüpfen

Bevor Android-Geräte über Android Enterprise eingeschrieben werden können, muss die Relution-Organisation zunächst mit einer Google-Organisation verknüpft werden. Diese Verknüpfung ermöglicht es Unternehmen, die volle Kontrolle über ihre Android-Geräte zu haben und sie effektiv zu verwalten; einschließlich Konfiguration, App-Verwaltung und Sicherheitsrichtlinien.

Registrierung der Relution-Organisation für Android Enterprise

Hierzu im Relution-Portal unter `Einstellungen` → `Geräteplattformspezifisch` → `Android Enterprise` ein entsprechendes Google-Konto hinterlegen:

- Auf Jetzt registrieren klicken und ein bestehendes Google-Konto auswählen oder ein neues erstellen.
- Bei der Erstellung eines neuen Google-Kontos zwischen Für mich selbst oder Für mein Unternehmen wählen und die verlinkte Vereinbarung zu Google Managed Play Store lesen.
- Nachdem die Vereinbarung akzeptiert wurde, das Feld Ich habe die Google Play-Vereinbarung gelesen und stimme ihr zu bestätigen und auf Bestätigen klicken.
- Mit Klick auf Registrierung abschließen geht es zurück zum Relution-Portal.

Mit dem Rücksprung ist die Verknüpfung automatisch gespeichert, ein weiterer Speicherschritt ist nicht erforderlich. Der Tab Allgemein zeigt anschließend die Organisations-ID und den Unternehmenstyp an. Anzeigename, Primärfarbe und Logo lassen sich optional im Tab Kontoinformationen anpassen, siehe Kontoinformationen →.

Für Version 26.4.0

Für die Verknüpfung mit dem Google Managed Play Store sind ausschließlich nicht-verwaltete Google-Konten nutzbar. Managed Accounts von Organisationen für Mitarbeiter sind nicht möglich.

Die neue Multi EMM-Funktion ist jetzt verfügbar. Diese Funktion ermöglicht es einem IT-Administrator, mehrere EMMs an sein verwaltetes Google-Domänenkonto zu binden. Google Multiple EMM Providers →

Zum Entfernen einer bestehenden Verknüpfung inklusive der Konsequenzen siehe Einrichtung löschen →.

Organisations-ID

In Relution sollte jeder Mandant / Organisation mit einem eigenen Google-Konto verknüpft werden. So ist sichergestellt, dass jeder Mandant eine einzigartige Organisations-ID von Google erhält und entsprechend für sich verwaltet werden kann.

Bei Relution-Organisationen, die vor mehreren Jahren mit Google Enterprise verknüpft wurden, steht als Unternehmenstyp häufig noch GooglePlay Enterprise-Konto. Für neu verknüpfte Organisationen wird von Google inzwischen automatisch eine Verwaltete Google-Domain mit einer eigenen, einmaligen Organisations-ID angelegt. Für ältere Organisationen bietet Google ein Upgrade von GooglePlay Enterprise-Konto auf Verwaltete Google-Domain an. Relution zeigt dafür unter `Einstellungen` → `Geräteplattformspezifisch` → `Android Enterprise` im Tab Allgemein einen Hinweis und die Schaltfläche Upgrade an (Berechtigung zum Bearbeiten der Android-Enterprise-Einstellungen erforderlich). Die Schaltfläche öffnet den von Google bereitgestellten Upgrade-Assistenten in einem neuen Tab; nach Abschluss aktualisiert Relution den Unternehmenstyp automatisch (siehe auch Abschnitt Enterprise upgraden →).

Upgrade von GooglePlay Enterprise-Konto auf verwaltete Google-Domain

Getestet und von Google bestätigt (Stand 08/2026): Das Upgrade lässt sich ohne Risiko durchführen – auch dann, wenn mehrere Relution-Organisationen mit demselben Google Play Enterprise-Konto und derselben Organisations-ID verknüpft sind.

- Risiko beim Upgrade: Es sind keine Risiken bekannt. Der Vorgang wurde erfolgreich getestet und läuft ohne Fehler durch.
- Auswirkung auf bereits eingeschriebene Android-Geräte: Diese werden durch das Upgrade weder zurückgesetzt noch anderweitig verändert.
- Mehrfach verknüpftes Google Play Enterprise-Konto: Auch wenn ein Google Play Enterprise-Konto mit mehreren Relution-Organisationen verknüpft ist und diese dieselbe Organisations-ID teilen, ist das Upgrade problemlos möglich. Ein getrenntes Upgrade einzelner Relution-Organisationen gibt es dabei nicht, das Upgrade gilt automatisch für alle verknüpften Relution-Organisationen (siehe Umfang des Upgrades).
- Empfehlung: Das Upgrade auf eine verwaltete Google-Domain sollte vorgenommen werden.
- Umfang des Upgrades: Das Upgrade gilt für die gesamte Google Organisations-ID und damit für alle daran verknüpften Relution-Organisationen gemeinsam. Es genügt daher, das Upgrade einmalig über eine der verknüpften Relution-Organisationen anzustoßen.

Google Organisations-ID nicht durch Trennen einzelner Relution-Organisationen aufteilen

Für Version 26.4.0

Sind mehrere Relution-Organisationen mit derselben Google Organisations-ID verknüpft, darf keine dieser Verbindungen im Tab Konto Einstellungen über Android Enterprise entfernen aufgehoben werden, um die Organisations-ID nachträglich aufzuteilen. Wie im Artikel Einrichtung löschen → beschrieben, verliert die betroffene Relution-Organisation dabei unabhängig von der gewählten Option die Kontrolle über ihre Android Enterprise-Geräte. Bei den Optionen Enterprise und in Relution bekannte Geräte entfernen und Enterprise und Geräte entfernen gehen zudem sämtliche bestehenden Einschreibungen der betroffenen Relution-Organisation unwiderruflich verloren und die Geräte werden zurückgesetzt. Die Option Enterprise und Geräte entfernen löscht darüber hinaus auch Geräte, die Relution in dieser Organisation nicht kennt, also auch Geräte der anderen Relution-Organisationen mit derselben Organisations-ID. Ein nachträgliches Wiederherstellen der Verbindung zur Wiedererlangung der Kontrolle über die Geräte ist nicht möglich.

Für eine dauerhaft eindeutige Zuordnung zwischen Relution-Organisation und Google Organisations-ID sollten stattdessen ausschließlich neue Relution-Organisationen jeweils mit einem eigenen, neuen Google-Konto verknüpft werden.

Einstellungen der verknüpften Organisation

Nach der Verknüpfung gliedert sich die Seite `Einstellungen` → `Geräteplattformspezifisch` → `Android Enterprise` in die Tabs Allgemein, Managed Google Play, Kontoinformationen, Einschreibungen und Konto Einstellungen. Änderungen setzen die Berechtigung zum Bearbeiten der Android-Enterprise-Einstellungen voraus.

Kontoinformationen

Der Tab Kontoinformationen enthält zwei Bereiche:

- Erscheinungsbild: Anzeigename des Unternehmens und Primärfarbe (Hex-Farbcode, z. B. `#ffffff`) sind Pflichtfelder und werden mit Speichern übernommen. Ein Logo der Organisation im Format JPEG oder PNG wird direkt nach dem Hochladen übernommen. Relution überträgt diese Angaben an das Android Enterprise bei Google.
- Kontaktinformationen: zeigt die bei Google hinterlegten Angaben schreibgeschützt an, gegliedert in Kontakt für die Benachrichtigung (E-Mail), Datenschutzbeauftragter und EU-Vertreter (jeweils Name, E-Mail und Telefonnummer). Bearbeitet werden sie laut Hinweis im Portal unter play.google.com/work/adminsettings →. Der Bereich erscheint nur, wenn Google Kontaktinformationen liefert.

Bedingungen und Konditionen

Im Tab Einschreibungen werden im Bereich Bedingungen und Konditionen Texte gepflegt, die Relution an das Android Enterprise bei Google überträgt. Jeder Eintrag besteht aus Kopfzeile und Inhalt. Beim Hinzufügen oder Bearbeiten steht für jede Sprache ein eigener Reiter zur Verfügung, in dem beide Felder Pflichtfelder sind; der Text der Standardsprache dient als Standardtext. Die Reihenfolge der Einträge lässt sich per Drag-and-drop ändern. Änderungen werden mit Speichern übernommen.

Zero-Touch

Ebenfalls im Tab Einschreibungen bettet Relution im Bereich Android Enterprise Zero Touch die Zero-Touch-Ansicht von Google ein, siehe Zero Touch Enrollment →.

Für Version 26.4.0

Registrierung reparieren

Neu in 26.5

Im Tab Konto Einstellungen steht oberhalb von Android Enterprise entfernen der Bereich Registrierung reparieren zur Verfügung. Laut Hinweis im Portal dient er dazu, die Kontrolle über die Geräte zurückzuerlangen, falls Google die Bindung an das Android Enterprise entfernt hat. Dabei wird die Registrierung bei Google erneut durchlaufen, ohne die bestehende Verknüpfung zuvor zu entfernen.

Vor dem Start ist zu prüfen, ob die angezeigte Organisations-ID mit der bei Google übereinstimmt:

- GooglePlay Enterprise-Konto: unter play.google.com/work →
- Verwaltete Google-Domain: unter admin.google.com → in `Geräte` → `Mobilgeräte & Endpunkte` → `Einstellungen` → `Integrationen von Drittanbietern`

Starten leitet zur Registrierung bei Google weiter. Bei einer verwalteten Google-Domain ist die Anmeldung dabei auf diese Domain beschränkt. Nach Abschluss prüft Relution, ob das angemeldete Enterprise dem bisher verbundenen entspricht; weicht die Organisations-ID ab, wird die Reparatur mit einer Fehlermeldung abgebrochen.

Einschreibungsarten

Für Android Enterprise stehen drei unterschiedliche Arten der Einschreibung zur Verfügung. Jede verfügt über spezielle Funktionalitäten, die für spezifische Anwendungsfälle geeignet sind.

Einschreibungsart	Werksreset zur Einrichtung	Private Nutzung	Zugriff der Administratoren
Verwaltetes Gerät →	erforderlich	nicht möglich	Vollzugriff auf das gesamte Gerät
Persönliches Profil (COPE) →	erforderlich	im privaten Profil möglich	Vollzugriff auf das Gerät, kein Einblick ins private Profil
Arbeitsprofil / BYOD →	nicht erforderlich	auf dem restlichen Gerät möglich	kein Zugriff auf private Bereiche des Geräts

Für Version 26.4.0

Verwaltetes Gerät (Managed Device)

Die Einschreibungsart Verwaltetes Gerät eignet sich beispielsweise für Organisationen oder Schulen, um Geräte an Benutzer auszuhändigen, die ausschließlich für dienstliche oder schulische Tätigkeiten genutzt werden.

- Zugriff der Administratoren: voller Zugriff auf das Gerät, u. a. Einsicht in die Liste installierter Apps sowie Zurücksetzen auf Werkseinstellungen.
- Voraussetzung: Zurücksetzen des Geräts auf Werkseinstellungen vor der Inbetriebnahme.
- Einschränkung: kein privates Profil, das Gerät ist ausschließlich für die dienstliche Nutzung vorgesehen. Das Hinzufügen weiterer Konten, etwa einer privaten Google-ID, unterbindet Relution nicht automatisch. Dafür steht in der Konfiguration Restriktionen → die Option Verbieten, Konten hinzuzufügen und zu entfernen zur Verfügung.

Details zur Einrichtung: Verwaltetes Gerät →

Verwaltetes Gerät mit persönlichem Profil (Company Owned, Personally Enabled COPE)

Die Einschreibungsart bildet das Gegenstück zum Arbeitsprofil und ermöglicht es, Geräte einer Organisation an Benutzer auszuhändigen, die diese auch privat nutzen dürfen.

- Privates Profil: Benutzer melden dort ihre private GoogleID an und installieren eigene Apps; private und dienstliche Daten sind strikt voneinander getrennt.
- Zugriff der Administratoren: voller Zugriff auf das Gerät, jedoch kein Einblick ins private Profil (z. B. keine Sicht auf installierte Apps oder aktivierte Einstellungen).
- Zurücksetzen auf Werkseinstellungen: vor der Inbetriebnahme erforderlich; ein späterer Werksreset durch Administratoren löscht sowohl private als auch dienstliche Daten vollständig.

Details zur Einrichtung: Persönliches Profil →

Arbeitsprofil / BYOD

Die Einschreibungsart Arbeitsprofil ist die richtige Wahl für den Bring Your Own Device-Ansatz (BYOD): Benutzer stellen ihr privates Gerät zur Verfügung, auf dem die Organisation ein Arbeitsprofil einrichtet.

- Voraussetzung: kein Zurücksetzen des Geräts notwendig.
- Nutzung: Innerhalb des Arbeitsprofils werden beispielsweise die Mail-App oder weitere Apps der Organisation bereitgestellt; private und organisationsbezogene Daten sind strikt getrennt.
- Zugriff der Administratoren: kein Einblick auf installierte private Apps, keine Zugriffsrechte auf Funktionen oder Einstellungen des privaten Geräts.
- Löschung: Wird das Arbeitsprofil entfernt, werden nur die organisationsbezogenen Daten gelöscht – private Daten bleiben erhalten.

Details zur Einrichtung: Arbeitsprofil / BYOD →

Für Version 26.4.0

Optionen der Einschreibung

Beim Anlegen einer Einschreibung unter `Geräte` → `Einschreibungen` zeigt das Formular für die Plattform Android Enterprise neben Typ und Eigentümerschaft weitere Optionen an. Sie stehen für alle drei Einschreibungsarten zur Auswahl; Einschränkungen sind jeweils genannt.

> Sprache, Mobilfunkregistrierung zulassen, System-Apps aktiviert lassen und die Angaben im Bereich WLAN übernimmt Relution ausschließlich in den QR-Code, der bei Verwaltetes Gerät und Persönliches Profil unter `Einschreibungs-Information` → `Mittels QR-Code` angezeigt wird. Der DPC-Identifier, das KME Custom JSON und das Android Enterprise Zero Touch benutzerdefiniertes JSON enthalten sie nicht. Beim Arbeitsprofil enthält der QR-Code lediglich den Link zur Einschreibung.

Authentifizierung, Mehrfach-Einschreibung und Mobilfunkregistrierung zulassen lassen sich nach dem Speichern nicht mehr ändern. Laut Hinweis im Formular erzeugt jede Änderung einer bestehenden Android-Enterprise-Einschreibung die Registrierung bei Google neu; der bisherige QR-Code und der DPC-Identifier werden dadurch ungültig.

Authentifizierung

Das Auswahlfeld Authentifizierung im Abschnitt Zuweisung legt fest, ob sich ein Benutzer während der Einschreibung anmelden muss:

- Nicht erforderlich (Standard): Die Einschreibung erfolgt ohne Anmeldung.
- Mit Relution Companion-App (unterstützt Einmalnutzung & Ablaufdatum): Die Relution Companion-App verlangt während der Einschreibung die Anmeldung des Benutzers. Mehrfach-Einschreibung und Gültig bis bleiben verfügbar.
- Mit integrierter Android-App (erzwingt Mehrfachnutzung): Die Anmeldung erfolgt ohne Companion-App während der Geräteeinrichtung über die Anmeldeseite von Relution. Gibt es genau einen Relution-Benutzer mit der E-Mail-Adresse des bei Google angemeldeten Kontos, wird dieser automatisch angemeldet; andernfalls erscheint die Anmeldeseite. Ist der Einschreibung ein Benutzer mit E-Mail-Adresse zugewiesen, ist sie mit dessen E-Mail-Adresse vorbelegt, sonst mit der des Google-Kontos. Die Einschreibung wird dem angemeldeten Benutzer zugeordnet, wobei Relution für jedes Gerät eine eigene, einmalig nutzbare Kopie der Einschreibung anlegt. Das Formular blendet Mehrfach-Einschreibung und Gültig bis aus.

Der Anmeldeablauf über die integrierte Android-App wird nur genutzt, wenn zusätzlich die Option Google Arbeitskonto-Anmeldung anzeigen aktiviert ist. Diese wird ausschließlich beim Typ Verwaltetes Gerät angeboten und setzt eine verwaltete Google-Domain voraus, siehe Google Work-Account-Einrichtung →. Einschreibungen mit dieser Option sind immer für mehrere Geräte nutzbar und laufen nicht ab.

Ablauf

Im Abschnitt Ablauf legt Mehrfach-Einschreibung fest, ob die Einschreibung für mehrere Geräte verwendet werden kann. Nach dem Datum unter Gültig bis lässt sich die Einschreibung nicht mehr verwenden; vorbelegt ist ein Datum sieben Tage nach dem Anlegen. Bei der Authentifizierung Mit integrierter Android-App (erzwingt Mehrfachnutzung) wird der Abschnitt nicht angezeigt.

Compliance

Für Version 26.4.0

Der Abschnitt Compliance enthält folgende Optionen:

- Immer ein Gerätekennwort erfordern (standardmäßig aktiv): Auch ohne explizite Kennwort-Richtlinie ist ein Gerätekennwort erforderlich. Relution hinterlegt dazu in der Standardrichtlinie der Einschreibung eine Kennwortanforderung für das Gerät sowie eine Compliance-Regel, die Apps deaktiviert, solange kein Kennwort gesetzt ist.
- Mobilfunkregistrierung zulassen: Die Einrichtung darf über mobile Daten erfolgen. Relution ergänzt dazu eine entsprechende Angabe im QR-Code.
- Sprache: Die gewählte Sprache wird als Sprache für die Geräteeinrichtung in den QR-Code übernommen. Ohne Auswahl entfällt die Angabe.
- System-Apps aktiviert lassen: Nicht wesentliche System-Apps bleiben nach der Einschreibung aktiviert, siehe Verwaltetes Gerät →.

WLAN

Im Bereich WLAN lässt sich ein Netzwerk für die Geräteeinrichtung hinterlegen:

- Abschnitt Verbindung: Netzwerk SSID, Verstecktes Netzwerk, Sicherheitstyp (Keiner / Offen für alle, WEP oder WPA/WPA2 PSK) sowie bei WEP und WPA das Passwort.
- Abschnitt Proxy Typ: Keine, Manuell mit Host, Portnummer und Proxy umgehen für (Liste von Adressen, die nicht über den Proxy geleitet werden) oder Automatisch konfigurieren mit PAC URL (Adresse der PAC-Datei).

Relution übernimmt WLAN und Proxy nur in den QR-Code, wenn Netzwerk SSID ausgefüllt ist. Für die Einschreibung per NFC gilt eine Einschränkung, siehe Geräte mit NFC einschreiben →.

Vereinbarungen

Im Abschnitt Konfiguration lassen sich unter Vereinbarungen Vereinbarungen auswählen, die unter `Einstellungen` → `Allgemein` → `Vereinbarungen` angelegt wurden. Relution stellt deren Texte dem Gerät während der Einschreibung bereit. Die Auswahl erscheint nur für Benutzer mit Leserecht auf Vereinbarungen.

Für Version 26.4.0

Verwaltetes Gerät

Die Einschreibungsart Verwaltetes Gerät (Managed Device) eignet sich beispielsweise für Organisationen oder Schulen, um Geräte an Benutzer auszuhändigen. Administratoren haben vollen Zugriff auf die Geräte und können beispielsweise die Liste der installierten Apps einsehen sowie die Geräte auf Werkseinstellungen zurücksetzen. Für die Inbetriebnahme ist ein Zurücksetzen auf Werkseinstellungen notwendig. Das Hinzufügen weiterer Konten, etwa einer privaten Google-ID, unterbindet Relution nicht automatisch. Dafür steht in der Konfiguration Restriktionen → die Option Verbieten, Konten hinzuzufügen und zu entfernen zur Verfügung. In der Regel kommt diese Einschreibungsart für organisationseigene Geräte in Frage, die Mitarbeiter oder Schüler bereitgestellt werden, um damit ausschließlich dienstliche oder schulische Tätigkeiten auszuüben (keine private Nutzung).

> Die Relution-Organisation muss mit einer Google-Organisation verknüpft sein, um Android-Geräte über Android Enterprise einschreiben zu können.

Einschreibung in Relution erstellen

- Zu `Geräte` → `Einschreibungen` gehen und anschließend auf Hinzufügen klicken.
- Als Plattform Android Enterprise und unter Typ das Symbol Verwaltetes Gerät wählen (die Bezeichnung erscheint als Tooltip; standardmäßig vorausgewählt).
- Eigentümerschaft wäre in diesem Fall `COD` (Company Owned Device).
- Einen Gerätenamen vergeben und die Einschreibung speichern.

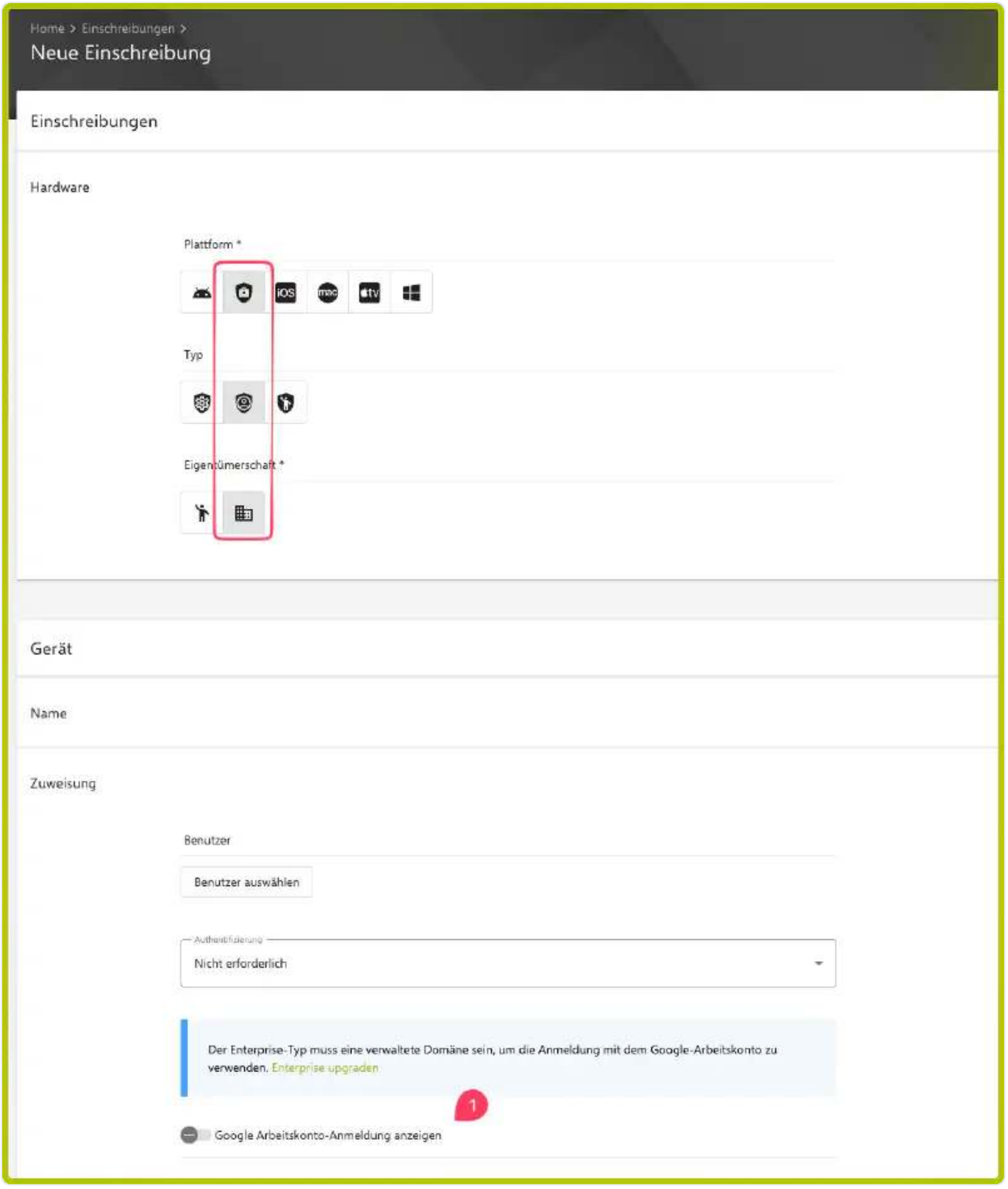
Für Version 26.4.0

> Ab Relution 5.33 ist es möglich, vorinstallierte System Apps wie Samsung Internet oder sonstige Drittanbieter zu behalten. Hierfür gibt es bei der Einschreibung den Schalter System-Apps aktiviert lassen. Im Umkehrschluss müssen die unerwünschten Apps in der Apps verwalten Konfiguration blockiert werden.

Die Eigentümerschaft ist ein Pflichtfeld und wird bei der Einschreibung auf das Gerät übernommen. Zusammen mit den Einstellungen unter `Einstellungen` → `Geräteverwaltung` → `Einschreibungen` legt sie fest, welche Geräteaktionen erlaubt sind (Gerät auf Werkszustand zurücksetzen, Gerät vollständig sperren, Gerät orten, Passwort zurücksetzen) und ob sich die Eigentümerschaft nach der Einschreibung noch ändern lässt. Bei COD sind alle diese Aktionen standardmäßig erlaubt, und die Eigentümerschaft lässt sich nachträglich ändern.

Google Work-Account-Einrichtung

Bei der Einschreibung steht die Option Google Arbeitskonto-Anmeldung anzeigen zur Verfügung. Ist diese aktiviert, wird das Gerät weiterhin über den QR-Code der Einschreibung eingerichtet. Nach dem Scan erfolgt die Anmeldung mit dem Google-Arbeitskonto (Google Workspace). Ist unter Authentifizierung zusätzlich Mit integrierter Android-App (erzwingt Mehrfachnutzung) gewählt, meldet Relution den Benutzer anhand der E-Mail-Adresse des Google-Kontos automatisch an; gelingt das nicht, erscheint die Anmeldeseite von Relution. Das Gerät wird so einem benannten Relution-Benutzer zugeordnet, siehe Optionen der Einschreibung →. Einschreibungen mit dieser Option sind immer für mehrere Geräte nutzbar und laufen nicht ab.



Weitere Details zur Richtlinienkonfiguration des Work Accounts sind im Artikel Work-Account-Einrichtung → zu finden.

Voraussetzung: verwaltete Domäne

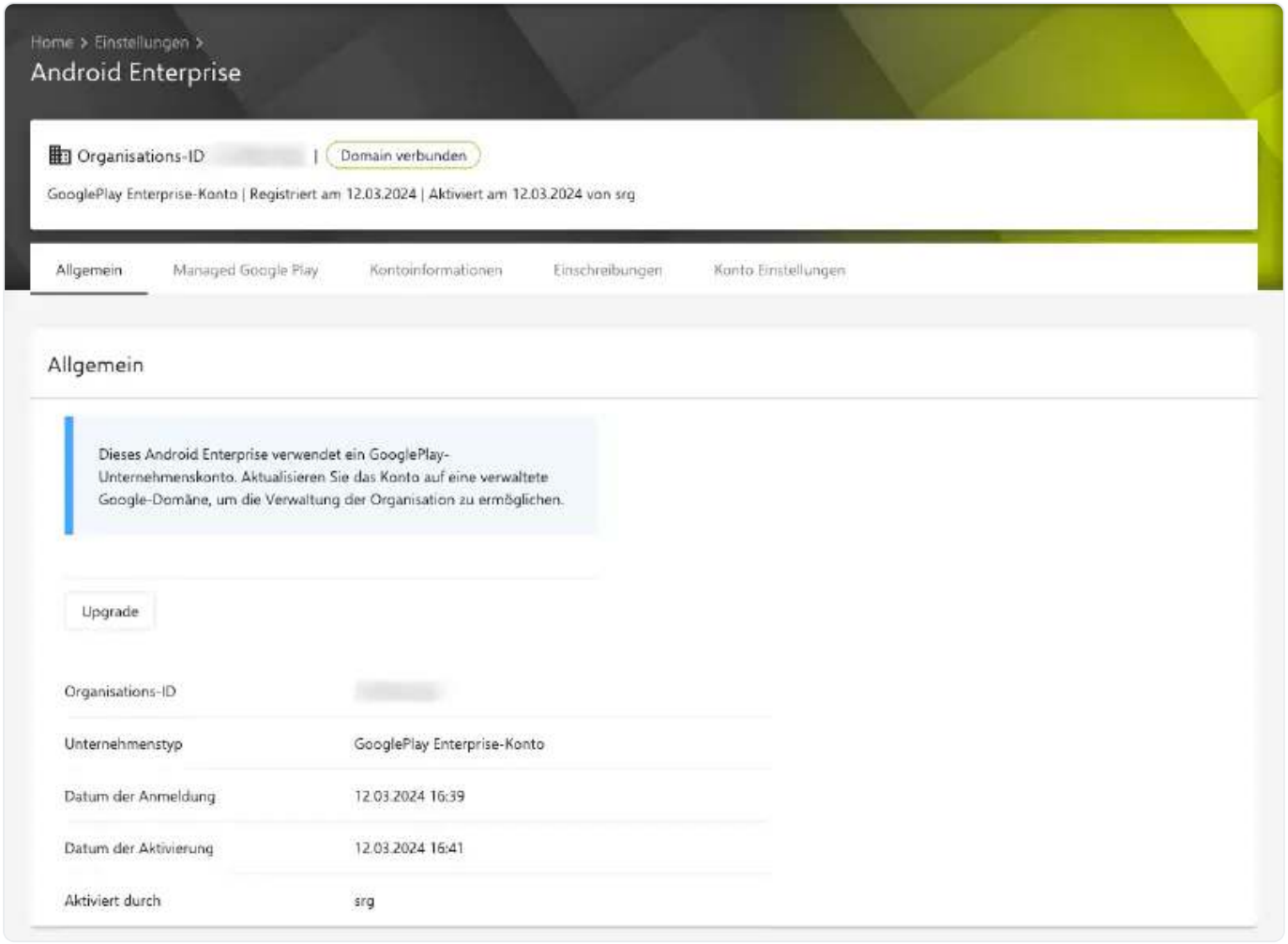
Android Enterprise unterscheidet zwei Enterprise-Typen:

Enterprise-Typ	Einrichtung	Google Work-Account-Einrichtung
Managed Google Play Accounts	Standard – mit beliebigem Google-Konto registriert. Nutzer erhalten automatisch ein verwaltetes Google-Konto.	Nicht verfügbar
Verwaltete Domäne	Erfordert eine aktive Google Workspace-Lizenz mit verifizierter Unternehmensdomäne. Nutzer melden sich mit ihrem bestehenden `@firma.de`-Konto an.	Verfügbar

Wurde die Relution-Organisation initial mit einem persönlichen Google-Konto verknüpft (Managed Google Play Accounts), zeigt das Formular beim Typ Verwaltetes Gerät oberhalb des Schalters Google Arbeitskonto-Anmeldung anzeigen folgenden Hinweis an:

„Der Enterprise-Typ muss eine verwaltete Domäne sein, um die Anmeldung mit dem Google-Arbeitskonto zu verwenden."

Enterprise upgraden



Der Link Enterprise upgraden öffnet die Seite `Einstellungen` → `Android Enterprise`. Dort startet im Reiter Allgemein die Schaltfläche Upgrade in einem neuen Browser-Tab einen von Google bereitgestellten Assistenten, der das bestehende Android Enterprise mit der eigenen Google Workspace-Organisation verknüpft. Der Link erscheint nur für Benutzer mit Leserecht auf die Android-Enterprise-Einstellungen; alle anderen sehen stattdessen den Hinweis, sich für das Upgrade an einen Administrator zu wenden. Folgende Voraussetzungen müssen erfüllt sein:

- Aktive Google Workspace-Lizenz (Business, Enterprise, Education o. ä.)
- Administratorenzugang zur Google Workspace Admin-Konsole
- In Google Workspace verifizierte Unternehmensdomäne

Nach erfolgreichem Upgrade steht die Option Google Arbeitskonto-Anmeldung anzeigen in der Einschreibung zur Verfügung. Zusätzlich muss für das verbundene Enterprise im Google Admin-Dashboard (admin.google.com) die Benutzerauthentifizierung aktiviert sein. Ist sie nicht aktiv, zeigt das Einschreibungsformular folgenden Hinweis:

„Das verbundene Enterprise-Konto muss die Benutzerauthentifizierung aktivieren. Dies kann nur im Admin-Dashboard unter admin.google.com durchgeführt werden.“

Sind beide Voraussetzungen erfüllt, können sich Benutzer mit ihren bestehenden `@firma.de`-Konten einschreiben.

Notwendige Informationen zur Durchführung der Einschreibung

In der angelegten Einschreibung wird unter Einschreibungs-Information ein QR-Code angezeigt, mit dem Android-Geräte eingeschrieben werden können. Dieser ist auch über die Spalte QR-Code in der Übersicht Einschreibungen aufrufbar. Alternativ ist die Einschreibung über den Reiter Mittels DPC-Identifier möglich, siehe Geräte ohne Kamera einschreiben →.

Für Version 26.4.0

Android-Geräte zurücksetzen

Um die Einschreibung für Verwaltetes Gerät zu starten, müssen Android-Geräte zuerst auf Werkseinstellungen zurückgesetzt werden.

Begrüßungsbildschirm auf den Geräten

Auf dem Begrüßungsbildschirm 6 Mal schnell auf eine Stelle tippen.

Relution QR-Code scannen

Die Geräte fordern anschließend dazu auf, den QR-Code aus der angelegten Einschreibung zu scannen.

Einschreibung abschließen

Den weiteren Anweisungen folgen, um die Geräte einzurichten. Nach der erfolgreichen Einschreibung haben Administratoren vollen Zugriff auf die verwalteten Geräte.

Aktionen

- App aus dem Google Play Store installieren
- App entfernen
- App aus dem Relution Store installieren
- App-Daten löschen (ab Android 9)
- Datei an Gerät senden
- eSIM entfernen
- eSIM hinzufügen
- Gerät auf Werkszustand zurücksetzen
- Gerät herunterfahren
- Gerät neu starten
- Gerät orten →
- Gerät vollständig sperren
- Geräteinformationen aktualisieren
- Lost Mode aktivieren (ab Android 11)
- Lost Mode deaktivieren
- Nachricht senden
- Passwort zurücksetzen

Für Version 26.4.0

Richtlinienkonfiguration

Unter anderem stehen folgende Konfigurationen zur Verfügung:

- Work-Account-Einrichtung →
- Apps verwalten →
- Erweiterte Keyguard-Verwaltung →
- Erweiterte Sicherheitsüberschreibungen →
- Gerätekennwort →
- Globaler Proxy →
- Kiosk-Modus →
- Laufzeitberechtigungen verwalten →
- Play Store Verwaltung →
- Restriktionen →
- Samsung Classroom Management →
- Standort-Modus →
- System-Updates →
- WLAN →

Alle Konfigurationen sind im Artikel Verfügbare Konfigurationen → beschrieben.

Persönliches Profil

Die Einschreibungsart Verwaltetes Gerät mit persönlichem Profil (Company Owned, Personally Enabled – COPE) ermöglicht es, Geräte einer Organisation an Benutzer auszuhändigen, die diese auch für private Zwecke nutzen dürfen. Benutzer haben die Möglichkeit, ihre private GoogleID in einem privaten Profil anzumelden und eigene Apps zu installieren. Private und organisationsbezogene Daten werden strikt auf den Geräten getrennt. Administratoren haben keinen Einblick oder Zugriff auf das private Profil und können beispielsweise nicht sehen, welche Apps im privaten Profil installiert und welche Einstellungen aktiviert sind. Administratoren haben aber vollen Zugriff auf die Geräte und können beispielsweise ein Zurücksetzen auf Werkseinstellungen durchführen, wodurch alle Daten, privat wie dienstlich, gelöscht werden. Für die Inbetriebnahme der Betriebsart ist ein Zurücksetzen auf Werkseinstellungen notwendig.

Die Relution-Organisation muss mit einer Google-Organisation verknüpft sein, um Android-Geräte über Android Enterprise einschreiben zu können.

Einschreibung in Relution erstellen

- Zu `Geräte` → `Einschreibungen` gehen und anschließend auf Hinzufügen klicken.
- Als Plattform Android Enterprise und unter Typ das Symbol Persönliches Profil wählen (die Bezeichnung erscheint als Tooltip; standardmäßig ist Verwaltetes Gerät vorausgewählt).
- Eigentümerschaft wäre in diesem Fall COD (Company Owned Device).
- Einen Gerätenamen vergeben und die Einschreibung speichern.

Für Version 26.4.0

Die Eigentümerschaft ist ein Pflichtfeld und wird bei der Einschreibung auf das Gerät übernommen. Zusammen mit den Einstellungen unter `Einstellungen` → `Geräteverwaltung` → `Einschreibungen` legt sie fest, welche Geräteaktionen erlaubt sind und ob sich die Eigentümerschaft nach der Einschreibung noch ändern lässt. Bei BYOD sind Gerät auf Werkszustand zurücksetzen, Gerät orten und Passwort zurücksetzen standardmäßig deaktiviert, und die Eigentümerschaft lässt sich nachträglich nicht mehr ändern. Für Geräte mit persönlichem Profil ist daher COD die passende Wahl.

Notwendige Informationen zur Durchführung der Einschreibung

In der angelegten Einschreibung wird unter Einschreibungs-Information ein QR-Code angezeigt, mit dem Android-Geräte eingeschrieben werden können. Dieser ist auch über die Spalte QR-Code in der Übersicht Einschreibungen aufrufbar. Alternativ ist die Einschreibung über den Reiter Mittels DPC-Identifier möglich, siehe Geräte ohne Kamera einschreiben →.

Android-Geräte zurücksetzen

Um die Einschreibung für Verwaltetes Gerät mit persönlichem Profil zu starten, müssen Android-Geräte zuerst auf Werkseinstellungen zurückgesetzt werden.

Begrüßungsbildschirm auf den Geräten

Auf dem Begrüßungsbildschirm 6 Mal schnell auf eine Stelle tippen.

Relution-QR Code scannen

Die Geräte fordern anschließend dazu auf, den QR-Code aus der angelegten Einschreibung zu scannen. Den weiteren Anweisungen folgen, um die verwalteten Geräte einzurichten.

Container Persönliches Profil auf den COD-Geräten

Nach der erfolgreichen Einschreibung sind auf der Bedienoberfläche der Android-Geräte die zwei getrennten Bereiche Persönlich und Arbeit verfügbar, zwischen denen jederzeit gewechselt werden kann.

Aktionen

Unter anderem stehen folgende Aktionen zur Verfügung:

- Enterprise Wipe (ab Android 8): entfernt das Arbeitsprofil und alle Richtlinien, Apps und Daten des persönlichen Profils bleiben erhalten
- Gerät auf Werkszustand zurücksetzen
- Geräteinformationen aktualisieren

Alle Aktionen sind im Artikel Verfügbare Aktionen → beschrieben.

Für Version 26.4.0

Richtlinienkonfiguration

Unter anderem stehen folgende Konfigurationen zur Verfügung:

- Apps verwalten →
- Arbeitsprofil-Passwort →
- Benutzer-Meldungen →
- Bildschirm →
- Erweiterte Keyguard-Verwaltung →
- Erweiterte Sicherheitsüberschreibungen →
- Gerätekennwort →
- Globaler Proxy →
- Hintergrundbild →
- Kiosk-Modus →
- Laufzeitberechtigungen verwalten →
- Persönliche Nutzung →: Einstellungen für das persönliche Profil
- Play Store Verwaltung →
- Restriktionen →
- Samsung Classroom Management →
- Standort-Modus →
- System-Updates →
- WLAN →

Alle Konfigurationen sind im Artikel Verfügbare Konfigurationen → beschrieben.

Mit der Option Aktivieren Sie den Factory Reset-Schutz (FRP) in der Konfiguration Restriktionen lässt sich das Zurücksetzen auf Werkseinstellungen über die Android-Geräteeinstellungen blockieren. Das Zurücksetzen über das Wiederherstellungsmenü bleibt möglich. Hat das Gerät keine Netzwerkverbindung, kann Relution keine Aktion zum Zurücksetzen an das Gerät senden. Weitere Details enthält der Artikel Restriktionen →.

Für Version 26.4.0

Arbeitsprofil / BYOD

Die Einschreibungsart Arbeitsprofil (Work Profile) ist die richtige Wahl für den Bring Your Own Device-Ansatz (BYOD). Benutzer können ihre privaten Geräte zur Verfügung stellen, um darauf von der Organisation ein Arbeitsprofil installieren zu lassen. Für die Inbetriebnahme eines Arbeitsprofils ist kein Zurücksetzen der Geräte notwendig. Innerhalb eines Arbeitsprofils können anschließend die Mail-App oder andere Apps der Organisation bereitgestellt werden. Private und organisationsbezogene Daten werden auf den Geräten strikt getrennt. Zudem haben Administratoren keinen Einblick auf installierte Apps und keine Zugriffsrechte auf Funktionen oder Einstellungen der privaten Geräte. Mit Löschung eines Arbeitsprofils werden alle organisationsbezogenen Daten von den Geräten entfernt, wohingegen alle privaten Daten erhalten bleiben.

> Die Relution-Organisation muss mit einer Google-Organisation verknüpft sein, um Android-Geräte über Android Enterprise einschreiben zu können.

Einschreibung in Relution erstellen

- Zu `Geräte` → `Einschreibungen` gehen und anschließend auf Hinzufügen klicken.
- Als Plattform Android Enterprise und unter Typ das Symbol Arbeitsprofil wählen (die Bezeichnung erscheint als Tooltip; standardmäßig ist Verwaltetes Gerät vorausgewählt).
- Eigentümerschaft wäre in diesem Fall BYOD (Bring Your Own Device).
- Einen Gerätenamen vergeben und die Einschreibung speichern.

Für Version 26.4.0

Die Eigentümerschaft ist ein Pflichtfeld und wird bei der Einschreibung auf das Gerät übernommen. Auf die Einrichtung des Arbeitsprofils hat sie keinen Einfluss. Zusammen mit den Einstellungen unter `Einstellungen` → `Geräteverwaltung` → `Einschreibungen` legt sie aber fest, welche Geräteaktionen erlaubt sind (Gerät auf Werkszustand zurücksetzen, Gerät vollständig sperren, Gerät orten, Passwort zurücksetzen) und ob sich die Eigentümerschaft nach der Einschreibung noch ändern lässt. Bei BYOD sind Zurücksetzen auf Werkszustand, Orten und Passwort zurücksetzen standardmäßig deaktiviert, und die Eigentümerschaft lässt sich nachträglich nicht mehr ändern. Vollständiges Sperren ist standardmäßig erlaubt.

Notwendige Informationen zur Durchführung der Einschreibung

In der angelegten Einschreibung wird unter Einschreibungs-Information ein QR-Code angezeigt, mit dem Android-Geräte eingeschrieben werden können. Dieser ist auch über die Spalte QR-Code in der Übersicht Einschreibungen aufrufbar.

> Der Link muss mit Google Chrome geöffnet werden, andere Browser wie Samsung Browser zeigen nur eine weiße Seite an.

Einschreibung abschließen

Die Kamera-App nutzen, um den frisch erstellten QR-Code zu scannen. Anschließend den angezeigten Schritten folgen, um den Einschreibungsprozess abzuschließen.

Container Arbeitsprofil auf den privaten Geräten

Nach der erfolgreichen Einschreibung sind auf der Bedienoberfläche der Android-Geräte zwei getrennte Bereiche Persönlich und Arbeit verfügbar, zwischen denen jederzeit gewechselt werden kann.

Während der Erstellung des Arbeitsprofils keine anderen Arbeiten am Gerät vornehmen.

Aktionen

- Apps aus dem Google Play Store installieren
- Apps entfernen
- App-Daten löschen (ab Android 9)
- Datei an Gerät senden
- eSIM entfernen
- eSIM hinzufügen
- Gerät herunterfahren
- Gerät orten (bei Eigentümerschaft BYOD standardmäßig deaktiviert)
- Gerät vollständig sperren
- Geräteinformationen aktualisieren
- Geräteinformationen anfordern (ab Android 13)
- Nachricht senden
- Passwort zurücksetzen (bei Eigentümerschaft BYOD standardmäßig deaktiviert)
- Play Store-App aus dem Relution Store auswählen

Für Version 26.4.0

Richtlinienkonfiguration

Unter anderem stehen folgende Konfigurationen zur Verfügung:

- Always-On VPN →
- Apps verwalten →
- Arbeitsprofil-Passwort →
- Durchsetzung der Konformität →
- Erweiterte Sicherheitsüberschreibungen →
- Gerätekennwort →
- Laufzeitberechtigungen verwalten →
- Play Store Verwaltung →
- Restriktionen →
- Samsung Classroom Management →
- Standard-Anwendungen → (ab Android 16)
- StrongSwan Restriktionen →
- StrongSwan VPN Profil →
- Work-Account-Einrichtung →
- Zertifikat →

Alle Konfigurationen sind im Artikel Verfügbare Konfigurationen → beschrieben.

Nicht verfügbare Konfigurationen

- Benutzer-Meldungen →
- Bildschirm →
- Erweiterte Keyguard-Verwaltung →
- Globaler Proxy →
- Hintergrundbild →
- Kiosk-Modus →
- Persönliche Nutzung →
- Standort-Modus →
- System-Updates →
- WLAN →

Für Version 26.4.0

Knox Mobile Enrollment

Knox ist eine Sicherheitsplattform für Samsung-Geräte, die Unternehmen eine sichere und zentrale Verwaltung mobiler Endgeräte ermöglicht. Die Plattform unterstützt die effiziente Bereitstellung, Konfiguration und Absicherung von Geräten im Unternehmensumfeld.

Samsung Knox Mobile Enrollment (KME)

Samsung Knox Mobile Enrollment (KME) ermöglicht die automatisierte Vorbereitung von Samsung-Geräten für die Verwaltung in einem Mobile Device Management (MDM)-System wie Relution.

Nach dem ersten Start eines Geräts und bestehender Internetverbindung beginnt die Einrichtung automatisch. Auch nach einem Zurücksetzen auf Werkseinstellungen erfolgt die erneute Einschreibung in das hinterlegte MDM-System automatisch.

Das KME-Programm bietet damit vergleichbare Funktionen wie das Device Enrollment Program (DEP) von Apple.

Voraussetzungen

1. Das Samsung-Gerät muss Knox-fähig sein. Eine Übersicht unterstützter Geräte bietet die Samsung Knox Support-Seite →.
2. Samsung-Geräte können durch autorisierte Händler anhand der Seriennummer direkt im KME-Programm registriert werden.
3. Geräte, die nicht über autorisierte Händler bezogen wurden, können nachträglich manuell hinzugefügt werden:
    - durch Scannen eines speziellen QR-Codes während der Geräteeinrichtung
    - oder mithilfe der Knox Mobile Deployment App auf einem zusätzlichen Samsung-Gerät

Das KME-Programm wird nach der Registrierung kostenfrei im Samsung Knox Portal bereitgestellt. Samsung Knox Portal →

> Die in Relution angebotene Konfiguration Knox Mobile Enrollment in den Einstellungen darf nicht verwendet werden. Diese Konfiguration ist veraltet, ausschließlich für Android Legacy vorgesehen und nur bis einschließlich Android Version 10 nutzbar.
>
> Stattdessen ist folgende Anleitung zu verwenden: Organisation verknüpfen →

Kombination von KME und Android Enterprise

Samsung Knox Mobile Enrollment lässt sich mit den Android-Enterprise-Einschreibungsarten kombinieren:

- Verwaltetes Gerät (Managed Device)
- Verwaltetes Gerät mit persönlichem Profil (COPE – Company Owned, Personally Enabled)

Für Version 26.4.0

Einschreibung in Relution vorbereiten

1. Navigation zu `Geräte` → `Einschreibungen`.
2. Auswahl von Hinzufügen.
3. Einstellungen:
   - Plattform: Android Enterprise
   - Typ: Verwaltetes Gerät oder Persönliches Profil (Symbol-Schaltflächen; die Bezeichnung erscheint als Tooltip)
   - Eigentümerschaft: COD (Gerät in Firmenbesitz); ohne Auswahl lässt sich die Einschreibung nicht speichern
4. Aktivierung der Option Mehrfach-Einschreibung im Abschnitt Ablauf.
5. Auswahl eines langfristigen Datums unter Gültig bis (z. B. 100 Jahre).
6. Speichern der Einschreibung.

Da diese Schritte Mehrfach-Einschreibung und Gültig bis voraussetzen, bleibt die Authentifizierung auf Nicht erforderlich oder Mit Relution Companion-App (unterstützt Einmalnutzung & Ablaufdatum). Bei Mit integrierter Android-App (erzwingt Mehrfachnutzung) blendet das Formular beide Felder aus. Angaben zu WLAN, Sprache und Mobilfunkregistrierung zulassen sind im KME Custom JSON nicht enthalten. Wird die Einschreibung später geändert, erzeugt Relution die Registrierung bei Google neu; das im Knox-Portal hinterlegte JSON ist dann zu ersetzen. Details: Optionen der Einschreibung →

Nach dem Speichern:

- Öffnen der erstellten Einschreibung.
- Wechsel zu `Einschreibungs-Information` → `Mittels DPC-Identifier`.
- Kopieren des bereitgestellten KME Custom JSON zur späteren Verwendung im Knox-Portal.

Für Version 26.4.0

KME-Profil im Samsung Knox Portal erstellen

1. Anmeldung im Samsung Knox Portal →.
2. Navigation zu Profiles.
3. Auswahl von CREATE PROFILE.

Profileinstellungen

- Vergabe eines Profilnamens und einer Beschreibung.
- Aktivierung von EMM.
- Deaktivierung von Knox Service Plugin.
- Fortfahren mit Weiter.
- Ausfüllen der Kontaktinformationen.

EMM-Informationen

- Bei Select your EMM (required) Auswahl von: Other
- Eintrag bei Link to agent APK (required):

```
https://play.google.com/managed/downloadManagingApp?identifier=setup
```

- Fortfahren mit Weiter.
- Einfügen des in Relution unter `Einschreibungs-Information` → `Mittels DPC-Identifier` angezeigten DPC-Identifier bei DPC Extras. Das KME Custom JSON enthält den DPC-Identifier bereits.
- Einfügen des zuvor kopierten JSON bei Custom JSON Data.
- Abschluss mit Create.

Optional: QR-Code erstellen

Ein QR-Code kann zur Einschreibung oder zur Aufnahme neuer Geräte in KME erstellt werden.

Vorgehen:

1. Auswahl von ADD A QR CODE.
2. Aktivierung von Also allow QR Code enrollment for devices not uploaded by a reseller, sofern Geräte nicht durch einen Händler vorregistriert wurden.
3. Optionales Hinterlegen einer WLAN-Konfiguration zur Vereinfachung der Masseneinrichtung.
4. Abschluss mit ADD.

Zur Nutzung des QR-Codes wird im Samsung-Willkommensbildschirm ein Plus-Zeichen (+) auf dem Display gezeichnet. Dadurch öffnet sich der QR-Code-Scanner.

Geräte mit dem Profil verknüpfen

Für Version 26.4.0

Sofern kein QR-Code verwendet wird:

1. Navigation im Knox-Portal zu Devices.
2. Markierung der gewünschten Geräte.
3. Auswahl von `Actions` → `Configure Devices`.
4. Inbetriebnahme der Geräte.

Zero Touch Enrollment

Android Zero-Touch Enrollment ist ein Dienst, der Unternehmen die automatisierte Bereitstellung großer Mengen an Android-Geräten ermöglicht – ohne zusätzliche manuelle Konfiguration durch Administratoren oder Endanwender.

Sobald ein Gerät ausgepackt, eingeschaltet und mit dem Internet verbunden wird, erfolgt die automatische Konfiguration mit den definierten Unternehmensrichtlinien, Apps und Einstellungen. Dies ermöglicht eine schnelle, standardisierte und sichere Inbetriebnahme von Android-Geräten im Unternehmensumfeld.

Android Zero-Touch Enrollment

Die Funktionsweise von Android Zero-Touch Enrollment ist vergleichbar mit Knox Mobile Enrollment (KME) →.

Im Zero-Touch-Portal wird zunächst eine Konfiguration erstellt, die anschließend den gewünschten Geräten aus der Geräteliste zugewiesen wird.

> Geräte für Android Zero-Touch Enrollment (ZTE) können nicht manuell durch Endkunden hinzugefügt werden. Das Hinzufügen von Geräten in das Zero-Touch-Portal erfolgt ausschließlich durch autorisierte Reseller oder OEMs.

Für Version 26.4.0

Vorbereitung der Einschreibung in Relution

1. Navigation zu `Geräte` → `Einschreibungen`.
2. Auswahl von Hinzufügen.
3. Konfiguration:
   - Plattform: Android Enterprise
   - Typ: Verwaltetes Gerät oder Persönliches Profil (Symbol-Schaltflächen; die Bezeichnung erscheint als Tooltip)
   - Eigentümerschaft: COD (Gerät in Firmenbesitz); ohne Auswahl lässt sich die Einschreibung nicht speichern
4. Aktivierung der Option Mehrfach-Einschreibung im Abschnitt Ablauf.
5. Auswahl eines ausreichend späten Datums unter Gültig bis.
6. Speichern der Einschreibung.

Da diese Schritte Mehrfach-Einschreibung und Gültig bis voraussetzen, bleibt die Authentifizierung auf Nicht erforderlich oder Mit Relution Companion-App (unterstützt Einmalnutzung & Ablaufdatum). Bei Mit integrierter Android-App (erzwingt Mehrfachnutzung) blendet das Formular beide Felder aus. Angaben zu WLAN, Sprache und Mobilfunkregistrierung zulassen sind im Zero-Touch-JSON nicht enthalten. Wird die Einschreibung später geändert, erzeugt Relution die Registrierung bei Google neu; das in der Zero-Touch-Konfiguration hinterlegte JSON ist dann zu ersetzen. Details: Optionen der Einschreibung →

Nach dem Speichern:

- Öffnen der erstellten Einschreibung.
- Wechsel zu `Einschreibungs-Information` → `Mittels DPC-Identifier`.
- Kopieren des bereitgestellten Android Enterprise Zero-Touch benutzerdefinierten JSON in die Zwischenablage.

Zero-Touch in Relution

Neben dem Zero-Touch-Portal → bettet Relution unter `Einstellungen` → `Geräteplattformspezifisch` → `Android Enterprise` im Tab Einschreibungen im Bereich Android Enterprise Zero Touch die Zero-Touch-Ansicht von Google ein. Die Ansicht wird in der Sprache des Portals geladen und ist mit Android Device Policy als DPC vorbelegt. Welche Funktionen sie bietet, legt Google fest.

Zero-Touch-Profil erstellen

1. Anmeldung im Zero-Touch-Portal →
2. Wechsel in den Bereich Configurations.
3. Auswahl des Plus-Symbols + im oberen Bereich.
4. Vergabe eines Namens für die Konfiguration.
5. Auswahl von Android Device Policy unter EMM DPC. (Falls mehrere Einträge vorhanden sind, kann ein beliebiger verwendet werden.)
6. Einfügen des zuvor kopierten JSON in das Feld DPC extras.
7. Ausfüllen der weiteren Felder gemäß Anforderungen.
8. Abschluss mit ADD.

Verknüpfung von Geräten und Konfiguration

Für Version 26.4.0

1. Wechsel in den Bereich Devices im Zero-Touch-Portal.
2. Zuweisung der gewünschten Konfiguration zu den jeweiligen Geräten.
3. Inbetriebnahme der Geräte.

Ein Scan eines QR-Codes ist nicht erforderlich. Android-Geräte melden sich beim ersten Start automatisch beim Zero-Touch-Dienst, der die Anfrage an Android Enterprise und anschließend an Relution weiterleitet.

Geräte mit NFC einschreiben

Mit dem Relution Agent können Android Enterprise Geräte einfach und schnell per NFC (Near Field Communication) in Relution eingeschrieben werden. Voraussetzung ist, dass beide Geräte NFC-fähig sind und das Träger-Gerät bereits in Relution registriert ist. Das Zielgerät kann wahlweise als Fully Managed Device oder mit Persönlichem Profil eingeschrieben werden. Android Work Profile oder eine Legacy Einschreibung sind nicht möglich.

Einrichtungsschritte

1. In Relution unter `Geräte` → `Einschreibungen` eine Einschreibung für die Plattform Android Enterprise mit dem Typ Verwaltetes Gerät oder Persönliches Profil erstellen (nicht Arbeitsprofil).

   Tipp: Sollen mehrere Geräte nacheinander eingeschrieben werden, im Abschnitt Ablauf die Option Mehrfach-Einschreibung aktivieren und unter Gültig bis ein spätes Datum wählen. Der Abschnitt Ablauf fehlt, wenn unter Authentifizierung die Auswahl Mit integrierter Android-App (erzwingt Mehrfachnutzung) getroffen wurde, siehe Optionen der Einschreibung →.

   > Aktuell darf kein WLAN-Profil bei der NFC-Einschreibung mitgegeben werden.

2. Auf dem Träger-Gerät die Relution Agent App öffnen.
3. Navigieren zu `Hamburger-Menü` → `Geräteinformationen` → `Teilen der NFC-Einschreibung`
4. Auf Einschreibung scannen klicken.
5. Den QR-Code aus der angelegten Einschreibung scannen.

   Danach kann das Trägergerät verwendet werden, um beliebig viele weitere Geräte einzuschreiben. Alternativ lässt sich ein NFC-Tag beschreiben.

6. Das Zielgerät vollständig zurücksetzen und den Ersten Einrichtungsbildschirm aufrufen.
7. Nun das Trägergerät oder den vorbereiteten NFC-Tag an das Zielgerät halten und den Anweisungen auf dem Bildschirm folgen.

Für Version 26.4.0

Geräte ohne Kamera einschreiben

Nicht alle Android-Geräte verfügen über eine Kamera oder einen funktionsfähigen QR-Code-Scanner. Trotzdem ist es möglich, diese Geräte als verwaltete Geräte in Relution einzuschreiben – mithilfe eines sogenannten DPC-Identifier-Codes (Device Policy Controller Identifier).

Geräte ohne Kamera/ QR-Code einschreiben

In einer angelegten Einschreibung wird unter Einschreibungs-Information im Reiter Mittels DPC-Identifier der DPC-Identifier angezeigt (der hervorgehobene Code oberhalb von Einschreibungsprozess). Er ist nicht mit dem Feld Einschreibungscode unter Details zu verwechseln. Derselbe Reiter steht auch im QR-Code-Dialog der Einschreibung zur Verfügung. Mit dem DPC-Identifier wird folgendermaßen vorgegangen:

- Das Zielgerät auf Werkseinstellungen zurücksetzen.
- Die Einrichtung des Geräts starten und den Anweisungen auf dem Bildschirm folgen.
- Fordern die Geräte zur Eingabe der Zugangsdaten für das Google-Konto auf, den Code `afw#setup` als Benutzernamen eingeben.
- Fordern die Geräte zur Eingabe des DPC-Identifier auf, den entsprechenden Code eingeben.
- Den Anweisungen folgen, um die verwalteten Geräte einzurichten. Die Geräte sind nun identisch dem alternativen QR-Code-Prozess eingeschrieben.

Für Version 26.4.0

Einschreibung aufheben

Mit dem Aufheben der Einschreibung endet die Verwaltung eines Geräts durch Relution. Die Einschreibung wird aufgehoben, indem das Gerät gelöscht wird: Die Aktion Löschen steht im Geräteinventar sowie in den Gerätedetails zur Verfügung. Nach Bestätigung des Löschdialogs werden die Unternehmensdaten vom Gerät entfernt und das Gerät wird aus dem Inventar gelöscht. Der Vorgang wird im Audit-Protokoll aufgezeichnet; eine erneute Einschreibung des Geräts ist jederzeit möglich.

Enthält die Auswahl ein verwaltetes Gerät, bietet der Löschdialog unter Verwaltetes Gerät zusätzlich die Optionen Factory Reset Protection (FRP) aktiviert lassen und Den externen Speicher des Geräts ebenfalls löschen (z.B. SD-Karten); beide sind standardmäßig deaktiviert (siehe Factory Reset Protection →). Das ebenfalls angezeigte Feld Nachricht hat auf firmeneigenen Geräten keine Auswirkung.

> Bei Geräten, die über Samsung Knox Mobile Enrollment (KME) eingeschrieben wurden, muss vor dem Löschen die Profilzuweisung des Geräts im Samsung Knox Portal entfernt werden. Andernfalls wird das Gerät automatisch neu eingeschrieben.

Auswirkung je Einschreibungsart

Was auf dem Gerät geschieht, hängt von der Art der Einschreibung ab:

Für Version 26.4.0

Einschreibungsart	Auswirkung des Löschens
Verwaltetes Gerät →	Das Gerät wird gelöscht und auf die Werkseinstellungen zurückgesetzt.
Arbeitsprofil / BYOD →	Es wird ausschließlich das Arbeitsprofil einschließlich aller geschäftlichen Apps und Daten entfernt. Private Daten bleiben auf dem Gerät erhalten.
Persönliches Profil →	Es wird ausschließlich das Arbeitsprofil einschließlich aller geschäftlichen Apps und Daten entfernt. Private Daten bleiben auf dem Gerät erhalten.

Papierkorb

Gelöschte Geräte werden zunächst in den Papierkorb verschoben (`Geräte` → `Papierkorb`). Erst durch erneutes Löschen im Papierkorb wird ein Gerät endgültig aus Relution entfernt.

Endgültig entfernt werden dabei nur Geräte im Status Gelöscht. Ein Gerät im Status Wird gelöscht··· hat die Löschung noch nicht bestätigt, etwa weil es offline ist. Wird es im Papierkorb gelöscht, wird es zunächst nur auf Gelöscht gesetzt und bleibt im Papierkorb; erst ein weiteres Löschen entfernt es endgültig.

Einrichtung löschen

Es ist möglich, eine bestehende Verbindung zwischen Relution und Android Enterprise aufzuheben.

Hinweis

Bei Android Enterprise-Einschreibungen kommunizieren die Android-Geräte direkt über die Android Enterprise-API und nicht, wie bei Android Classic/Legacy-Einschreibungen, über Relution mit Android Enterprise. Wird die Verbindung zu Android Enterprise aufgehoben, indem das verknüpfte Google-Konto entfernt wird, gehen alle bestehenden Einschreibungen verloren und Bestandsgeräte können in Relution nicht mehr verwaltet und keine neuen Geräte über Android Enterprise eingeschrieben werden. Richtlinienkonfigurationen, die sich zu dieser Zeit auf eingeschriebenen Geräten befinden, können nicht mehr zurückgezogen oder entfernt werden. Ein nachträgliches Wiederherstellen der Verbindung zur Wiedererlangung der Kontrolle über die Geräte ist nicht möglich. Welche Folgen das Aufheben der Verbindung in Relution für die Geräte hat, hängt dagegen von der dort gewählten Option ab (siehe nächster Abschnitt).

Relution-seitiges Aufheben einer bestehenden Verbindung

Für Version 26.4.0

Die Verbindung wird unter `Einstellungen` → `Geräteplattformspezifisch` → `Android Enterprise` im Tab Konto Einstellungen aufgehoben:

- In der Karte Android Enterprise entfernen unter Optionen zum Entfernen des Enterprise die gewünschte Option auswählen. Vorausgewählt ist Enterprise und in Relution bekannte Geräte entfernen.
- Auf Starten klicken.
- Den Dialog Organisationen trennen mit Entfernen bestätigen.

Die Schaltfläche Starten ist nur mit der Berechtigung zum Bearbeiten der Android Enterprise-Einstellungen sichtbar.

Die Optionen wirken sich unterschiedlich auf die Geräte aus:

- Enterprise und in Relution bekannte Geräte entfernen: Die von Relution verwalteten Geräte werden auf Werkseinstellungen zurückgesetzt bzw. ihr Arbeitsprofil wird entfernt, und sie werden in Relution gelöscht. Geräte, die Relution nicht kennt, bleiben im Android Enterprise.
- Enterprise und Geräte entfernen: Zusätzlich zu den von Relution verwalteten Geräten werden alle übrigen Geräte des Android Enterprise gelöscht, auch solche, die Relution nicht kennt.

Bereits mit der vorausgewählten Option werden alle von Relution verwalteten Geräte zurückgesetzt bzw. ihre Arbeitsprofile entfernt. Zuvor eingeschriebene Geräte werden auch beim Wiederherstellen der Verbindung nicht wiederhergestellt.

Google-seitiges Aufheben einer bestehenden Verbindung

Das Aufheben der Verbindung in Relution löscht die Google-Organisation nicht. Nach dem Trennen zeigt Relution unter `Einstellungen` → `Geräteplattformspezifisch` → `Android Enterprise` die passenden Schritte zum Löschen an. Welche das sind, hängt vom Unternehmenstyp der Organisation ab.

Verwaltete Google-Domain

- admin.google.com → aufrufen und sich mit dem Konto anmelden, mit dem die Organisation erstellt bzw. aktualisiert wurde.
- Zu `Geräte` → `Mobile und Endpunkte` → `Einstellungen` → `Integrationen von Drittanbietern` wechseln.
- Die Drittanbieter-Integration auswählen und auf EMM-Anbieter verwalten klicken.
- In der Liste der Anbieter die Organisation mit der Organisations-ID aus Relution entfernen.

Laut Hinweis in Relution ist eine Reaktivierung des Unternehmens innerhalb von 30 Tagen möglich, und zwar durch Anmeldung mit dem Konto, mit dem die Verbindung hergestellt wurde.

GooglePlay Enterprise-Konto

- play.google.com/work → aufrufen und sich mit dem Konto anmelden, mit dem die Organisation erstellt wurde.
- Im linken Menü auf Admin-Einstellungen wechseln.
- Die ID, welche im oberen Bereich der Seite zu sehen ist, mit der im Relution Portal vergleichen.
- Auf die drei Punkte rechts in der Kachel und dann auf Organisation löschen klicken.

Ein Gmail-Konto kann nur mit einer einzigen Google-Organisation verbunden sein und lässt sich erst nach deren Löschung für eine neue Organisation verwenden. Solange die Google-Organisation nicht gelöscht ist, kann die Verbindung in Relution mit demselben Gmail-Konto wiederhergestellt werden; zuvor eingeschriebene Geräte werden dabei nicht wiederhergestellt.

Für Version 26.4.0

Verfügbare Aktionen

Relution stellt eine Auswahl an Aktionen bereit, um Android Enterprise-Geräte direkt zu kontrollieren und zu lenken. Ein herausragender Vorteil liegt darin, dass diese Aktionen gezielt auf einzelnen Geräten angewendet werden können.

Aktionsübersicht

Nicht jede Aktion steht für jede Einschreibungsart zur Verfügung. Einschränkungen und Mindestversionen sind in der Beschreibung vermerkt; Aktionen ohne Vermerk stehen für verwaltete Geräte, Arbeitsprofile und Geräte mit persönlichem Profil zur Verfügung.

Für Version 26.4.0

Aktion	Beschreibung
App aus dem Google Play Store installieren	Installiert eine ausgewählte App aus dem Google Play Store auf dem Gerät. Nur für als verwaltetes Gerät oder als Arbeitsprofil eingeschriebene Geräte verfügbar.
App aus dem Relution Store installieren	Installiert eine im Relution Store hinterlegte App auf dem Gerät: Play Store Apps sowie native Apps (APK), sofern Relution deren Signaturzertifikate ermittelt hat. Native Apps stehen nur zur Auswahl, wenn ausschließlich vollständig verwaltete Geräte ausgewählt sind. Nur für vollständig verwaltete Geräte, auch mit persönlichem Profil, verfügbar. Details: APK-Apps verwalten →
App entfernen	Deinstalliert eine ausgewählte App vom Gerät. Nur für als verwaltetes Gerät oder als Arbeitsprofil eingeschriebene Geräte verfügbar.
App-Daten löschen	Löscht alle mit einer App verbundenen Daten vom Gerät. Ab Android 9 verfügbar.
Datei an Gerät senden	Überträgt eine Datei (z. B. PDF, Dokument, Bild) sicher auf das Gerät.
Enterprise Wipe	Entfernt das Arbeitsprofil und alle zugehörigen Richtlinien und überlässt das Gerät der persönlichen Nutzung; Apps und Daten des persönlichen Profils bleiben erhalten. Nur für Geräte mit aktiviertem persönlichem Profil ab Android 8 verfügbar.
eSIM entfernen	Entfernt ein eSIM-Profil vom Gerät anhand der ICCID.
eSIM hinzufügen	Fügt dem Gerät über den angegebenen Aktivierungscode ein eSIM-Profil hinzu.
Gerät auf Werkszustand zurücksetzen	Setzt das Gerät auf die Werkseinstellungen zurück und löscht alle Daten. Nur für als verwaltetes Gerät oder mit persönlichem Profil eingeschriebene Geräte verfügbar. Hinweis: Seit Relution 5.34.0 kann bei Geräten mit Arbeits- oder persönlichem Profil auch nur das Management-Profil entfernt werden (Gerätedetails über das Papierkorb-Symbol oder im Geräteinventar über Löschen).
Gerät herunterfahren	Fährt das Gerät vollständig herunter.
Gerät neu starten	Startet das Gerät neu. Nur für als verwaltetes Gerät eingeschriebene Geräte verfügbar.
Gerät orten	Ermittelt den aktuellen Standort des Geräts.
Gerät vollständig sperren	Nur für als verwaltetes Gerät oder als Arbeitsprofil eingeschriebene Geräte verfügbar. Sperrt das Gerät mit dem aktuell gesetzten Passwort. Ist kein Passwort gesetzt, kann das Gerät ohne Passwort entsperrt werden. Eine Aktion zum Entsperren gibt es nicht; ist das Passwort nicht bekannt, kann über Passwort zurücksetzen ein neues Passwort vergeben werden (bei als Arbeitsprofil eingeschriebenen Geräten betrifft das nur das Passwort des Arbeitsprofils).
Geräteinformationen aktualisieren	Aktualisiert die Geräteinformationen in der Relution-Konsole.
Geräteinformationen anfordern	Fragt die eSIM-Kennung (EID) des Geräts ab. Der Benutzer muss der Weitergabe auf dem Gerät zustimmen. Nur für als Arbeitsprofil eingeschriebene Geräte ab Android 13 verfügbar.
Lost Mode aktivieren	Aktiviert den Lost Mode bei Verlust oder Diebstahl des Geräts: Sperrbildschirm, Standortverfolgung und Nachricht auf dem Sperrbildschirm. Nur für als verwaltetes Gerät (ab Android 11) oder mit persönlichem Profil (ab Android 13) eingeschriebene Geräte verfügbar.

Aktion	Beschreibung
Lost Mode deaktivieren	Entsperrt das Gerät und beendet den Lost Mode wieder. Verfügbarkeit wie bei Lost Mode aktivieren.
Nachricht senden	Zeigt eine Textnachricht auf dem Gerät an.
Passwort zurücksetzen	Setzt auf verwalteten Geräten das Gerätepasswort zurück. Auf Geräten mit Arbeitsprofil oder persönlichem Profil wird nur das Passwort des Arbeitsprofils zurückgesetzt; bei Geräten mit persönlichem Profil lässt sich das Gerät nicht mit dem neuen Passwort entsperren.
Play Store App aus dem Relution Store auswählen	Installiert eine im Relution Store hinterlegte Play Store App auf dem Gerät. Nur für als Arbeitsprofil eingeschriebene Geräte verfügbar.

Für Version 26.4.0

Android Gerät orten

Mit Relution ist es möglich, Android Enterprise Geräte zu orten.
Die Aktion kann im Inventar auf dem zu ortenden Gerät im Reiter `Standort` → `Gerät orten` ausgelöst werden. Liegt bereits ein Standort vor, heißt die Schaltfläche Aktuelle Position anfordern. Nach dem Anfordern ist die Schaltfläche deaktiviert, bis die so angeforderte Ortung abgeschlossen ist, höchstens jedoch etwa 20 Sekunden. Fehlen dem Relution Companion die nötigen Berechtigungen, ist sie ebenfalls deaktiviert; im aktiven Lost Mode wird sie nicht angezeigt. Alternativ im Reiter `Aktionen` → `Aktion anwenden` → `Gerät orten`.

Bei jeder Ortung erfolgt eine Benachrichtigung auf dem Endgerät im Benachrichtigungsmenü, zusätzlich wird der Verlauf im Relution Companion angezeigt

Das erfolgreich geortete Gerät wird im Reiter Standort unter `Geräte` → `Inventar` → `ihr Gerät` → `Standort` auf einer Karte dargestellt

Voraussetzung

Das Gerät muss über ein GPS-Modul und eine Internetverbindung verfügen sowie eingeschaltet sein und grundsätzlich ortbar sein.

In Relution muss die Ortung unter `Einstellungen` → `Geräteverwaltung` → `Einschreibungen` in der Zeile Gerät orten für die Eigentümerschaft des Geräts (COD oder BYOD) aktiviert sein. Standardmäßig ist sie für COD aktiviert, für BYOD deaktiviert. Geräte mit unbekannter Eigentümerschaft sind standardmäßig ortbar; diese Einstellung ist im Portal nicht änderbar. Ist die Ortung deaktiviert, bietet Relution die Aktion Gerät orten nicht an und blendet den Reiter Standort aus. Bei Android Enterprise-Geräten im Lost Mode bleibt der Reiter Standort sichtbar und aktualisiert die Position etwa jede Minute; die Aktion Gerät orten steht auch dann nicht zur Verfügung.

Für Version 26.4.0

Weitere Voraussetzungen sind aktivierte Standortdienste am Gerät in den Einstellungen bzw. in den Schnelleinstellungen.
Die Standortberechtigung des Companions vergibt Relution per Richtlinie: Ist Gerät orten für COD aktiviert, wird sie automatisch erteilt, andernfalls verweigert. Das gilt unabhängig von der Eigentümerschaft des Geräts. Über die Konfiguration Apps verwalten lässt sich diese Vorgabe überschreiben.
Weitere Einstellungen →

Sind diese deaktiviert, zeigt Relution in den Aktionen folgende Meldung:

```
Unable to determine location; No location available; GPS is disabled; Network location
is disabled.
```

Sind die Dienste aktiviert, sieht eine erfolgreiche Meldung wie folgt aus:

```
Determined current location, using fused provider, accuracy 13,37 meter, age <1m.
```

Standort im Self-Service Portal anzeigen

Neu in 26.4

Berechtigte Benutzer können den zuletzt ermittelten Standort ihres eigenen Geräts auch direkt im Self-Service Portal auf einer Karte anzeigen, ohne dafür einen Administrator-Zugang zu benötigen: Standort auf einer Karte anzeigen →

Hinweise

- Ausstehende Aktionen
  Es kann zu Problemen bei der Positionsbestimmung kommen, wenn noch Aktionen zur Ortung in Relution ausstehen. Diese müssen abgebrochen und die Aktion neu versendet werden.
- Standortgenauigkeit
  Die Option Standortgenauigkeit in den Geräteeinstellungen hat einen großen Einfluss auf die Ortungsgenauigkeit. Ist diese Einstellung deaktiviert, kann die Abweichung der Ortung mehrere Hundert Meter betragen.
  Bei Samsung Geräten mit Android 13 ist die Einstellung unter `Einstellungen` → `Standort` → `Standortdienste` → `Standortgenauigkeit`
- Berechtigung zur Ortung
  Um möglichen Missbrauch einzuschränken, bietet Relution ab Version 5.31.0 die Möglichkeit, eine Berechtigung zur Ortung anzupassen. Details: Standortdienste →

Für Version 26.4.0

Verfügbare Konfigurationen

Eine Richtlinie ist eine Sammlung einer oder mehrerer Konfigurationen. Jede Richtlinie kann auf einem oder auf mehreren Geräten gleichzeitig angewendet werden. Zudem können mit jedem Gerät eine oder mehrere Richtlinien verknüpft sein.

Für Version 26.4.0

Konfigurationsübersicht

Konfiguration	Beschreibung
Always-On VPN →	Always-On-VPN-Einstellungen verwalten
Apps verwalten →	Apps auf verwalteten Geräten installieren, aktualisieren und deinstallieren
Arbeitsprofil-Passwort →	Verwaltung der Passwortrichtlinie für das Arbeitsprofil
Bedingter Zugriff →	Erfordert die Einrichtung des Bedingten Zugriffs auf dem Gerät über den Relution Agent, um geschützte Ressourcen nutzen zu können
Benutzer-Meldungen →	Benutzerdefinierte Meldungen festlegen
Bevorzugte Aktivitäten →	Verwaltet, welche App standardmäßig für einen bestimmten Vorgang verwendet werden soll
Bildschirm →	Die Anzeigeeinstellungen für das Gerät verwalten
CVTE OEM-Konfiguration →	CVTE OEMConfig-App konfigurieren
Durchsetzung der Konformität →	Definition von Sperr- und Löschaktionen, wenn ein Gerät nicht konform ist
Erweiterte Keyguard-Verwaltung →	IT-Administratoren können erweiterte Funktionen für die Tastensperre des Geräts (Sperrbildschirm) steuern
Erweiterte Sicherheitsüberschreibungen →	Sicherheitsrichtlinien standardmäßig auf sichere Werte eingestellt
Gerätefunk-Status →	Status der Funk-Einstellungen auf dem Gerät verwalten
Gerätekennwort →	Verwaltung der Passwortrichtlinie für das Gerät
Gerätekonnektivität →	Verwalten der Gerätekonnektivitätseinstellungen
Globaler Proxy →	Konfiguriert einen netzwerkunabhängigen globalen HTTP-Proxy
Hintergrundbild →	Hintergrundbild verwalten
Kiosk-Modus →	Kiosk-Modus-Einstellungen
Knox →	Knox Service Plugin (KSP) von Samsung konfigurieren
Laufzeitberechtigungen verwalten →	Standardantworten auf Berechtigungsanforderungen von verwalteten Apps definieren
Newline OEMConfig →	Newline OEMConfig-Anwendung konfigurieren
Persönliche Nutzung →	Persönliche Nutzung für ein vollständig verwaltetes Gerät konfigurieren
Play Store Verwaltung →	Konfiguration von Google Play Store Funktionen

Konfiguration	Beschreibung
Relution Dateifreigaben →	Freigabekonfiguration für die Relution Files App
Relution Decon →	Konfiguration für die Relution Decon App
Relution Homescreen Layout →	Relution Home Screen Layout App konfigurieren
Restriktionen →	Verwaltung der Restriktionen
Samsung Classroom Management →	Samsung Classroom Management App vorkonfigurieren
Standard-Anwendungen →	Festlegen, welche Anwendungen als Standard-Anwendungen auf dem Gerät verwendet werden sollen
Standort-Modus →	Einstellungsoptionen der verfügbaren Standorterkennung konfigurieren
StrongSwan Restriktionen →	StrongSwan App konfigurieren und Standardprofil festlegen
StrongSwan VPN Profil →	VPN-Profil für die StrongSwan App konfigurieren
System-Updates →	System-Updates verwalten
WLAN →	Verwaltung der WLAN Einstellungen
Work-Account-Einrichtung →	Upgrade eines Benutzerkontos auf eine verwaltete Google-Domain konfigurieren
Zertifikat →	CA-Zertifikat oder Zertifikat und einen privaten Schlüssel zur Installation auf dem Gerät definieren

Arbeitsprofil-Passwort

Über diese Konfiguration werden die Passwortanforderungen für das Arbeitsprofil von Android Enterprise Geräten festgelegt. Anforderungen an die Gerätesperre werden über die Konfiguration Gerätekennwort → definiert.

Unterstützte Einschreibungsarten

Die Badges Arbeitsprofil und Persönliches Profil im Formular zeigen, für welche Einschreibungsarten die Konfiguration unterstützt wird:

- Geräte mit Arbeitsprofil →
- Verwaltete Geräte mit persönlichem Profil →

Eine Auswahl des Profils gibt es nicht. Die Passwortvorgaben gelten in beiden Fällen für das Arbeitsprofil.

Mindestqualität

Definiert die erforderliche Qualität beziehungsweise Art der Bildschirmsperre oder des Passworts. Die gewählte Stufe ist eine Mindestanforderung, Passwörter einer höheren Qualitätsstufe werden ebenfalls akzeptiert.

Folgende Optionen stehen zur Verfügung:

Für Version 26.4.0

- Komplex (stark)
  Das Passwort muss mindestens einen Buchstaben, eine Ziffer und ein Sonderzeichen enthalten. Bei dieser Auswahl erscheinen zusätzlich folgende Pflichtfelder (kleinster zulässiger Wert in Klammern):
  - Minimale Anzahl von Buchstaben (1)
  - Minimale Anzahl von Kleinbuchstaben (0)
  - Minimale Anzahl von Großbuchstaben (0)
  - Minimale Anzahl von Nicht-Buchstaben (0)
  - Minimale Anzahl numerischer Zahlen (1)
  - Minimale Anzahl von Symbolen (1)

  Die Felder sind bei einer neuen Konfiguration nicht vorbelegt. Gespeichert werden kann die Konfiguration erst, wenn alle Felder ausgefüllt sind.

- Alphanumerisch
  Das Passwort muss aus Buchstaben und Zahlen bestehen.

- Alphabetisch
  Das Passwort muss mindestens Buchstaben (oder Symbole) enthalten.

- Komplex Numerisch
  Erfordert ein numerisches Passwort mit erhöhten Anforderungen, zum Beispiel ohne einfache oder leicht zu erratende Zahlenfolgen.

- Numerisch
  Das Passwort muss mindestens Ziffern enthalten (z. B. eine PIN).

- Muster
  Trotz der Bezeichnung wird kein Entsperrmuster erzwungen. Es muss lediglich eine beliebige Sperre eingerichtet sein (z. B. Muster, PIN oder Passwort), Vorgaben zum Inhalt gibt es nicht.

- Biometrisch (schwach)
  Es kann eine schwächere biometrische Entsperrmethode verwendet werden, sofern vom Gerät unterstützt. Bei dieser Auswahl werden die Felder Minimale Länge, Maximales Alter (in Tagen), Passworthistorie und Anzahl fehlgeschlagener Passwortversuche bevor alle Daten gelöscht werden ausgeblendet und können nicht konfiguriert werden.

Für Version 26.4.0

Welche Optionen tatsächlich verfügbar und durchsetzbar sind, hängt vom Gerät, der Android-Version und den Herstelleranpassungen ab.

Minimale Länge

Legt die minimale Anzahl an Zeichen für das Passwort fest. Das Feld ist ein Pflichtfeld. Standardwert und kleinster zulässiger Wert ist `4`.

Beispiel:

- `4` → Das Passwort muss mindestens 4 Zeichen lang sein.

Maximales Alter (in Tagen)

Bestimmt, nach wie vielen Tagen das Passwort geändert werden muss.

Anzahl an Tagen bis ein neues Passwort gesetzt werden muss. Bei Angabe des Werts 0 läuft das Passwort nie ab.

Beispiel:

- `0` → Kein Ablauf des Passworts.

Passworthistorie

Legt fest, wie viele vorherige Passwörter nicht erneut verwendet werden dürfen.

Anzahl gespeicherter und bereits verwendeter Passwörter, die nicht mehr verwendet werden dürfen.

Beispiel:

- `0` → Es gibt keine Einschränkung für die Wiederverwendung.

Anzahl fehlgeschlagener Passwortversuche bevor alle Daten gelöscht werden

Für Version 26.4.0

Definiert, nach wie vielen falschen Eingaben ein Zurücksetzen oder Löschen ausgelöst wird.

Wenn kein Wert gesetzt ist, erfolgt in der Regel keine automatische Löschung.

Apps im Arbeitsprofil deaktivieren, bis Anwender die Kennwortanforderungen erfüllen

Wenn diese Option aktiviert ist, bleiben Apps im Arbeitsprofil deaktiviert, bis das konfigurierte Passwort den Anforderungen entspricht. Die Option ist standardmäßig aktiviert.

Nach welcher Frist bei nicht erfüllten Kennwortanforderungen gesperrt und gelöscht wird, legt die Konfiguration Durchsetzung der Konformität → fest. Standardmäßig werden nur die Apps im Arbeitsprofil gesperrt. Beim Löschen wird auf Geräten mit Arbeitsprofil (BYOD) nur das Arbeitsprofil entfernt; Geräte mit persönlichem Profil (COPE) werden auf Werkseinstellungen zurückgesetzt.

Separater Passcode für das Arbeitsprofil erforderlich

Wenn aktiviert, muss für das Arbeitsprofil ein eigener, separater Passcode gesetzt werden.

Ist die Option deaktiviert, kann unter Umständen der gleiche Gerätesperrcode verwendet werden.

Sofern diese Option nicht aktiviert ist, wird automatisch ein systemweiter Timeout von 60 Sekunden eingestellt.

Hinweise

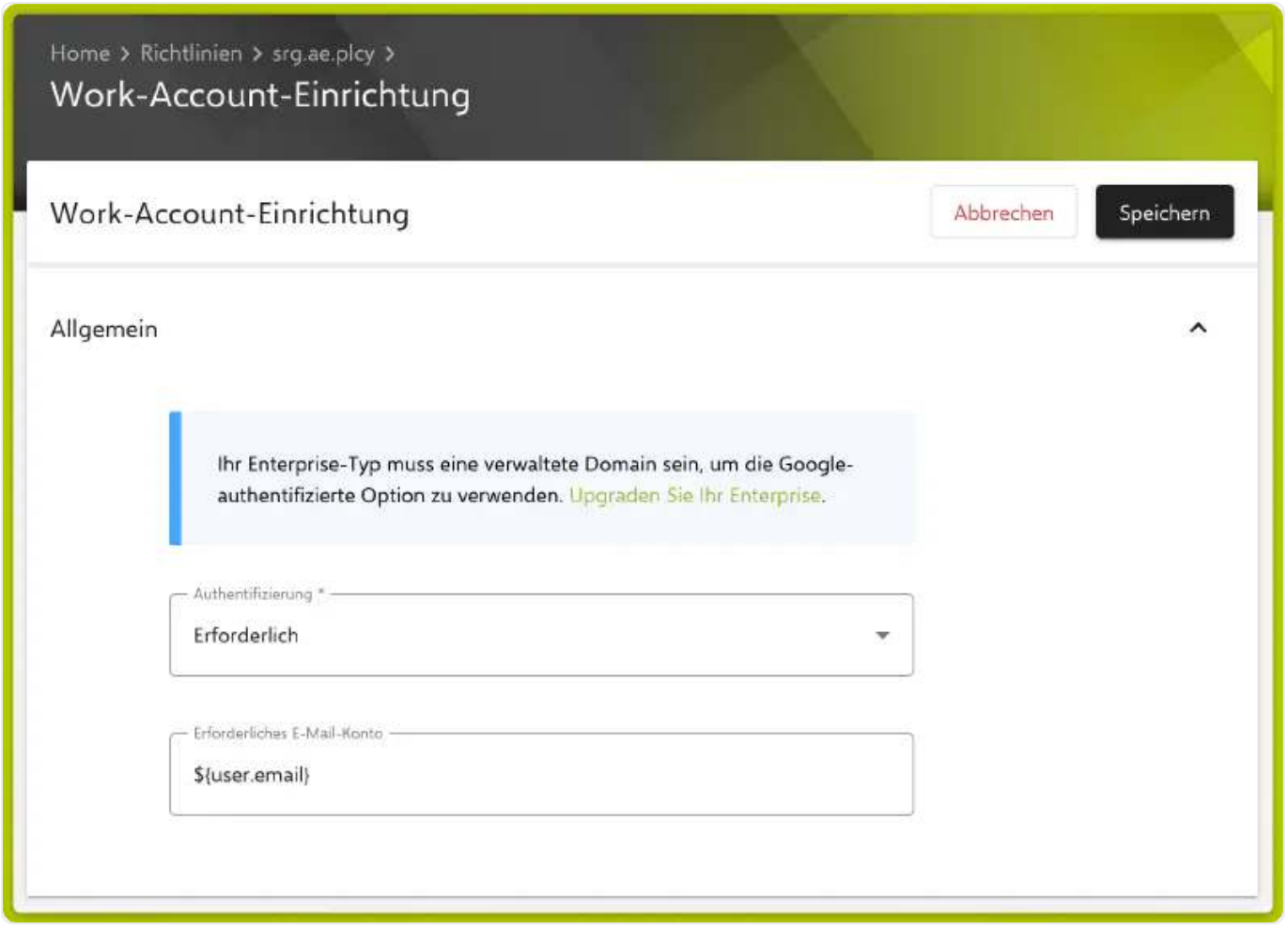
- Diese Einstellungen gelten ausschließlich für das Arbeitsprofil, auch auf verwalteten Geräten mit persönlichem Profil (COPE).
- Nicht alle Optionen sind auf jedem Gerät oder jeder Android-Version im gleichen Umfang verfügbar.
- Die tatsächliche Durchsetzung hängt von Hersteller, Android-Version und Gerätemodus ab.

Für Version 26.4.0

Work-Account-Einrichtung

Über die Richtlinienkonfiguration Work-Account-Einrichtung können Einstellungen für das Google Work Account auf vollständig verwalteten Geräten (Fully Managed Device) zentral konfiguriert werden.

Die Option Erforderlich setzt voraus, dass die Relution-Organisation mit einem Enterprise vom Typ verwaltete Google-Domain verknüpft ist. Zusätzlich muss in der Google Admin-Konsole (`admin.google.com`) die Nutzerauthentifizierung für die verwaltete Google-Domain aktiviert sein, sonst wird die Konfiguration nicht wirksam. Ist die Organisation noch mit einem GooglePlay Enterprise-Konto verknüpft, zeigt das Formular einen Hinweis zum Upgrade (siehe Upgrade von GooglePlay Enterprise-Konto auf verwaltete Google-Domain →). Weitere Informationen zur Einrichtung enthält der Artikel Verwaltetes Gerät →.



Authentifizierung

Legt fest, ob Benutzer sich bei der Geräteeinrichtung mit einem Google Work Account authentifizieren müssen.

Option	Beschreibung
Nicht spezifiziert (Standard)	Es wird keine Vorgabe gemacht. Das Verhalten entspricht Nicht erforderlich.
Nicht erforderlich	Es wird keine Google Work Account-Authentifizierung verlangt.
Erforderlich	Benutzer müssen sich mit einem Google Work Account authentifizieren.

Erforderliches E-Mail-Konto

Wird Erforderlich ausgewählt, erscheint das Feld Erforderliches E-Mail-Konto. Hier kann die verwaltete Domänen-E-Mail-Adresse hinterlegt werden, mit der sich Benutzer anmelden müssen. Platzhalter ermöglichen eine dynamische Zuweisung.

Für Version 26.4.0

Sicherheitsüberschreibungen

Für Geräte, die in Android Enterprise eingeschrieben sind, bietet die Konfiguration Erweiterte Sicherheitsüberschreibungen tiefgreifende Kontrollmöglichkeiten. Administratoren können hier festlegen, ob die Installation von APK-Dateien aus Drittquellen zulässig ist, ob die Google Play Protect-Überprüfung erzwungen wird und ob der Entwicklermodus für Testzwecke zur Verfügung steht. Darüber hinaus stehen Einstellungen zur Memory Tagging Extension, zum Inhaltsschutz und zu Benachrichtigungen aus dem Arbeitsprofil zur Verfügung.

Aus unbekannten Quellen zulassen

Diese Einstellung steuert, ob Apps außerhalb des Google Play Stores (Side-loading) installiert werden dürfen. Es stehen folgende Optionen zur Verfügung:

- Nicht spezifiziert (Standard bei neuen Konfigurationen): Relution gibt keinen Wert vor, es gilt das Standardverhalten von Android Enterprise.
- Installation nicht vertrauenswürdiger Apps auf dem gesamten Gerät verbieten: Side-loading ist auf dem gesamten Gerät untersagt.
- Installation nicht vertrauenswürdiger Apps nur im persönlichen Profil zulassen: Side-loading ist ausschließlich im privaten Bereich des Nutzers erlaubt.
- Installation nicht vertrauenswürdiger Apps auf dem gesamten Gerät erlauben: Side-loading ist auf dem gesamten Gerät gestattet.

Für Version 26.4.0

Google Play-Überprüfung erzwingen

Legt fest, ob die Sicherheitsüberprüfung durch Google Play Protect obligatorisch ist, um schädliche Software zu identifizieren.

- Nicht spezifiziert (Standard bei neuen Konfigurationen): Relution gibt keinen Wert vor, es gilt das Standardverhalten von Android Enterprise.
- Ja: Die Überprüfung wird systemweit erzwungen und kann vom Nutzer nicht deaktiviert werden.
- Wahl durch Benutzer: Der Endanwender entscheidet selbst, ob die Überprüfung aktiv sein soll.

Richtlinie zur Geräteverschlüsselung

Bestimmt das Sicherheitsniveau der Datenverschlüsselung auf dem physischen Speicher.

Option	Beschreibung
Keine Verschlüsselung erforderlich (Standard)	Es wird keine Verschlüsselung der Nutzerdaten erzwungen.
Verschlüsselung erforderlich, zum Booten ist kein Passwort erforderlich	Daten sind verschlüsselt; beim Booten ist jedoch keine Passworteingabe nötig.
Verschlüsselung erforderlich, zum Booten ist ein Passwort erforderlich	Verschlüsselung ist aktiv und erfordert ein Passwort bereits beim Startvorgang.

Wie mit Geräten verfahren wird, die die geforderte Verschlüsselung nicht erfüllen, legt die Konfiguration Durchsetzung der Konformität → in der Zeile Erweiterte Sicherheitsüberschreibungen fest.

Entwicklereinstellungen

Hier kann definiert werden, ob der Entwicklermodus auf dem Gerät freigeschaltet werden darf. Dies ist primär für Debugging-Zwecke oder App-Tests relevant. Im produktiven Standardbetrieb sollte diese Option aus Sicherheitsgründen deaktiviert bleiben.

Für Version 26.4.0

Common Criteria-Modus

Der Common Criteria-Modus dient der Einhaltung internationaler Sicherheitsstandards für Informationstechnik.

Die Einstellung wird nur auf vollständig verwalteten Geräten und auf verwalteten Geräten mit persönlichem Profil (COPE) angewendet. Auf Geräten mit Arbeitsprofil (BYOD) überträgt Relution sie nicht.

Funktionsweise: Durch die Aktivierung werden spezifische Sicherheitskomponenten verstärkt. Dies betrifft insbesondere die AES-GCM-Verschlüsselung von Bluetooth Long Term Keys sowie eine gehärtete Speicherung der WLAN-Konfigurationen.

Der Common Criteria-Modus erzwingt ein extrem strenges Sicherheitsmodell. Dieses ist typischerweise nur für IT-Infrastrukturen in nationalen Sicherheitssystemen oder hochsensiblen Organisationen erforderlich. Die Nutzung von Standard-Apps oder alltäglichen Gerätefunktionen kann dadurch eingeschränkt werden. Nur bei expliziter Anforderung aktivieren.

Memory Tagging Extension

Legt die Richtlinie für die Memory Tagging Extension (MTE) fest. Die Einstellung ist mit den Badges Android 14+, COPE Arbeitsprofil und Verwaltetes Gerät gekennzeichnet.

Es stehen die Optionen Nicht spezifiziert (Standard bei neuen Konfigurationen), Wahl durch Benutzer, Aktiviert und Deaktiviert zur Verfügung.

Inhaltsschutz

Der Inhaltsschutz scannt nach betrügerischen Apps. Die Einstellung ist mit dem Badge Android 15+ gekennzeichnet.

Es stehen die Optionen Nicht spezifiziert (Standard bei neuen Konfigurationen), Wahl durch Benutzer, Aktiviert und Deaktiviert zur Verfügung.

Persönliche Apps, die Benachrichtigungen aus dem Arbeitsprofil lesen können

Legt fest, welche Apps im persönlichen Profil Benachrichtigungen aus dem Arbeitsprofil lesen dürfen. Die Einstellung ist mit dem Badge COPE Arbeitsprofil gekennzeichnet.

Über Hinzufügen öffnet sich eine App-Auswahl, in der eine oder mehrere Apps gewählt werden. Übernommen werden deren Paketnamen, einzelne Einträge lassen sich wieder entfernen. Bleibt die Liste leer, überträgt Relution keine Einstellung an Google.

Für Version 26.4.0

Relution Files Android

Relution bietet für Android die Möglichkeit, lokale Dateifreigaben, auch Netzwerklaufwerke genannt, über SMB und WebDAV zu integrieren. Über die Anbindung von beispielsweise Schul- oder Unternehmens-Serverlösungen kann so auf relevante Dokumente und Inhalte zugegriffen sowie Daten und Arbeitsergebnisse sicher auf einem zentralen Server abgespeichert werden.

Vorteile von Relution Files

Daten sollten nicht in einer ungesicherten Cloud mit Servern außerhalb der EU gespeichert werden, wenn DSGVO-konform gearbeitet werden muss. Ebenso ist es ratsam, die Daten nicht direkt auf Geräten zu speichern, wenn Geräte von mehreren Benutzer genutzt werden. Durch das Speichern und Ablegen von Dokumenten auf eigenen lokalen Servern über `Relution Files` wird die Datensicherheit und Datenhoheit für alle Benutzer gewährleistet.

Lokale Netzlaufwerke für Relution Files konfigurieren

Lokale Dateifreigaben können auf zwei Arten in Relution eingerichtet werden:

Für die manuelle Einrichtung ist die Dokumentation der App selbst zu beachten -> Relution Files →

Für Version 26.4.0

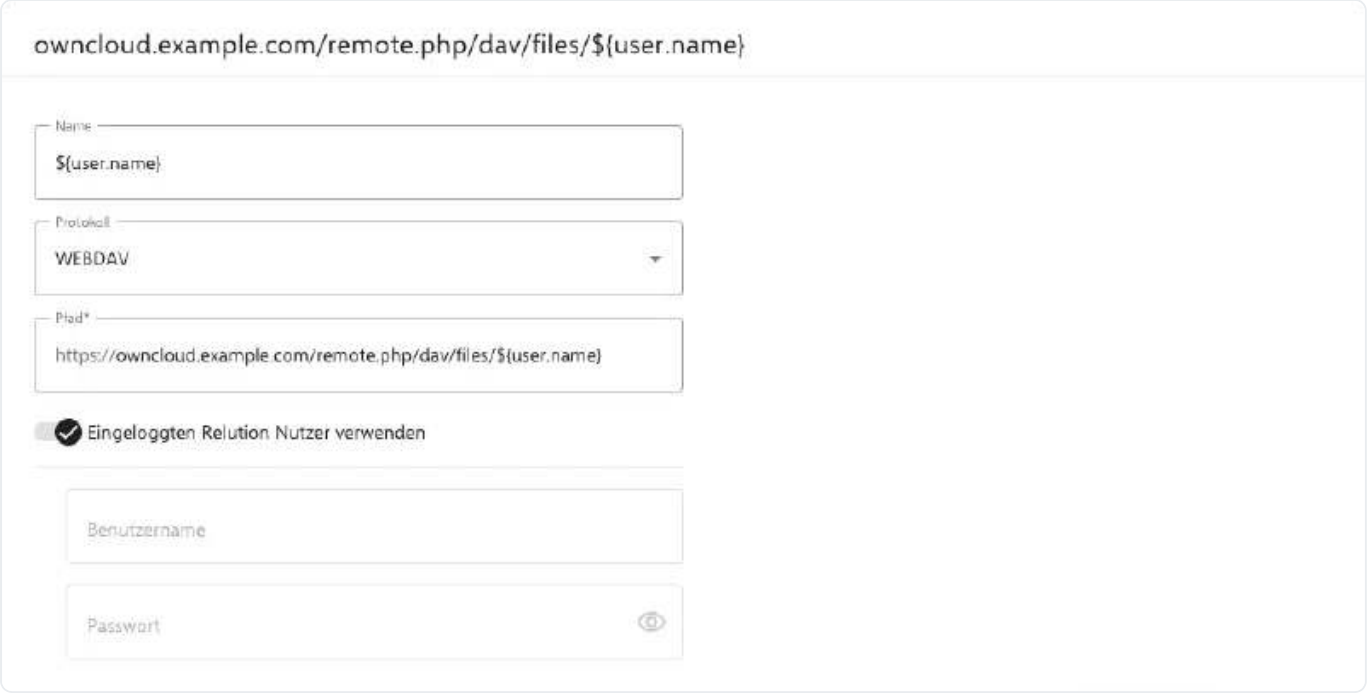
Automatische Konfiguration von Relution Files über Richtlinien

Durch eine verwaltete Konfiguration, die der Administrator über das Relution Portal vornimmt, entfällt für den Endanwender nahezu jede Hürde bei der Einrichtung des Gerätes. Auf diese Weise lässt sich die Dateifreigabe nahtlos nutzen.

Mit der Konfiguration von `Relution Dateifreigaben` in einer Richtlinie kann eine WebDAV- oder SMB-Verbindung für die Nutzung vorbereitet werden. Unter Android steht die Konfiguration nur in Android-Enterprise-Richtlinien zur Verfügung und kann einmal pro Richtlinie hinzugefügt werden. Enthält eine Richtlinie die Konfiguration, installiert Relution die App Relution Files automatisch als Pflicht-App und überträgt ihr die nötige verwaltete Konfiguration. Eine separate Verteilung der App ist nicht erforderlich. Ist Relution Files zusätzlich in Apps verwalten → eingetragen, gelten die dortigen Einstellungen (z. B. Installationstyp).

Über Hinzufügen öffnet sich der Dialog Neue Dateifreigabe. Eine Konfiguration kann mehrere Freigaben enthalten, mindestens eine ist zum Speichern erforderlich. Pro Freigabe werden ein optionaler Name, das Protokoll (SMB oder WEBDAV) und der Pfad (Pflichtfeld) angegeben. Ohne Namen wird das letzte Pfadsegment verwendet. Bei SMB muss der Pfad den eigentlichen Share enthalten (z. B. `server/share`, das Präfix `smb://` ist vorgegeben). WebDAV-Verbindungen erfolgen immer über HTTPS (das Präfix `https://` ist vorgegeben). Platzhalter wie `${user.name}` sind in Name, Pfad, Benutzername und Passwort möglich und vereinfachen den Anmeldeprozess.

Zudem lässt sich in der Freigabe die Option Eingeloggten Relution Nutzer verwenden aktivieren. Dann werden die Zugangsdaten des am Gerät angemeldeten Relution-Benutzers verwendet. Ist die Option deaktiviert, können Benutzername und Passwort fest hinterlegt werden.



Hintergrundbild

Für Version 26.4.0

Ab Relution 5.33 steht die Konfiguration Hintergrundbild für Android Enterprise sowie Android Classic/Legacy zur Verfügung. Unter Android Enterprise ist sie mit dem Badge Verwaltetes Gerät gekennzeichnet und wirkt auf vollständig verwalteten Geräten sowie auf verwalteten Geräten mit persönlichem Profil (COPE), nicht auf Geräten mit Arbeitsprofil (BYOD). Mit dieser lässt sich ein Bild für den Homescreen hinterlegen, das nach Anwendung der Richtlinie auf den Geräten erscheint. Die Richtlinie ermöglicht auch das Hinzufügen von Text (inklusive Platzhaltern) um dynamische Texte auf dem Hintergrundbild anzuzeigen.

Android Enterprise benötigt Relution Companion Version 1.18.

Android Classic benötigt Relution Companion Version 5.37.

Die Konfiguration Hintergrundbild legt das Bild fest, verhindert aber nicht, dass Benutzer es auf dem Gerät ändern.

Relution Decon (Inhaltsfilter)

Ab Version 26.3 ermöglicht Relution die Einrichtung eines DNS-basierten Inhaltsfilters für Android-Enterprise-Geräte. Diese Funktion sorgt für einen sicheren und fokussierten Internetzugang, indem der Zugriff auf ausgewählte Webseiten eingeschränkt wird. Dank der KI-gestützten Kategorisierung von Inhalten bietet Relution Decon einen umfassenden Jugendschutzfilter mit erweiterten Einstellungsmöglichkeiten.

Was ist Relution Decon?

Relution Decon ist ein KI-gestütztes Add-on für Android Enterprise, das Inhalte in Echtzeit filtert und ein sicheres digitales Umfeld schafft. Mithilfe der DNS-basierten Inhaltskontrolle blockiert Decon unerwünschte Webseiten, sodass Benutzer in einem geschützten, ablenkungsfreien Raum arbeiten und lernen können.

Relution Decon nutzt einen DNS-Proxy, um alle Anfragen an den Decon-Server weiterzuleiten. Dort werden Webseiten klassifiziert und gemäß den Richtlinien entweder erlaubt oder blockiert. Dank SSL-Verschlüsselung bleiben alle Datenübertragungen sicher, und die Nutzeraktivitäten geschützt.

Decon App

Für Version 26.4.0

Die Decon-App (`io.relution.decon`) wird von Relution automatisch auf den Geräten installiert, sobald eine Richtlinie mit einer Decon-Konfiguration veröffentlicht ist. Eine vorherige Verteilung über Apps verwalten → ist nicht erforderlich. Ein Eintrag dort übernimmt nur Zusatzoptionen wie Update-Verhalten, Mindestversion oder Berechtigungen, nicht den Installationstyp. Nach der Installation fungiert sie als Always-On-VPN des Geräts und überwacht die DNS-Anfragen, um sicherzustellen, dass nur zugelassene Inhalte aufgerufen werden können.

Funktionen der App:

- Aktiviert einen systemweiten DNS-Proxy, der vom Benutzer nicht deaktiviert werden kann
- Zeigt den aktuellen Status von Relution Decon an
- Gibt Einsicht in blockierte Webseiten und die angewendeten Filterkategorien

Manuelle VPN-Änderungen verhindern

Da Relution Decon als Always-On-VPN arbeitet, könnten Benutzer es sonst über die VPN-Einstellungen des Geräts deaktivieren oder ersetzen. Um dies zu verhindern, müssen folgende zwei Konfigurationen kombiniert werden:

- Restriktionen →: Option Verbieten, VPN zu konfigurieren aktivieren
- Always-On VPN →: `io.relution.decon` als Always-On-VPN-App auswählen

Decon Richtlinie

In der Geräte-Richtlinie auf `Hinzufügen` → `Relution Decon` klicken. Mit dieser Richtlinie wird die Decon-App auf den zugeordneten und unterstützten Geräten automatisch konfiguriert und fungiert als Proxy für alle DNS-Anfragen.

Die Konfiguration wird mit der Veröffentlichung der Richtlinie abgeschlossen.

Hierarchie der Richtlinienkonfiguration (höchste zu niedrigste Priorität)

1. Erlaubte Domains
2. Gesperrte Domains
3. Blockierte Kategorien

Decon in Relution Teacher

Auf Android-Enterprise-Geräten kann Decon ab Relution Server 26.3 in Unterrichtsprofilen ausgewählt und gesteuert werden. Voraussetzung: Auf den Schülergeräten ist die Decon-App installiert, und sie sind mit einer Decon-Richtlinie versehen. Einen Hinweis auf eine fehlende Decon-Konfiguration zeigt Relution Teacher nur für iOS-Geräte an.

Mehr zu Relution Teacher →

Für Version 26.4.0

Filtern

Im Abschnitt Filtern der Decon-Richtlinie wird über Filter-Typ festgelegt, wonach Webseiten gefiltert werden:

- Aus: Es wird weder nach Kategorien noch nach Altersstufe gefiltert.
- Kategorien (Standard): Die zu blockierenden Kategorien werden einzeln per Schalter gewählt. Die Schalter erscheinen nur bei diesem Filter-Typ. Standardmäßig blockiert sind Erwachseneninhalte, Werbung und Phishing.
- Altersstufe: Gefiltert wird nach einer Altersstufe (0+, 6+, 12+ oder 16+, Standard 12+).

Unabhängig vom Filter-Typ stehen zwei weitere Schalter zur Verfügung:

- BPJM-Liste: Filtert zusätzlich Inhalte, die von der BPjM als unzulässig eingestuft wurden. Einträge unter Erlaubte Domains können den Zugriff auf solche Inhalte dennoch ermöglichen.
- Sichere Suche: Wird unabhängig von den blockierten Kategorien und der Altersstufe geschaltet. Das Blockieren der Kategorie Erwachseneninhalte aktiviert die sichere Suche nicht.

Werden auf einem Gerät mehrere Decon-Konfigurationen verwendet, kommt automatisch die stärkste Filterung zum Tragen: Filter nach Altersstufe gehen Filtern nach Kategorien vor. Konfigurationen ohne Filterung werden ignoriert.

Klassifizierung nach Kategorien

Relution Decon ordnet Webseiten automatisch einer Kategorie zu. Beim Filter-Typ Kategorien legen Administratoren fest, welche Kategorien blockiert werden:

Kategorie	Beschreibung	Beispiele
Erwachseneninhalte	Nicht für Jugendliche geeignete Seiten	Pornografie, Gewalt, Waffen, Drogen, Gambling, Adult Entertainment, Adult Shopping, Dating
Werbung	Werbeseiten	Ad Providers
Soziale Medien	Social-Media-Inhalte	Facebook, Instagram, TikTok, etc.
Unterhaltung	Unterhaltung, z. B. Streaming oder Spiele	Movies, Games, Videos
Musik	Musik-Streaming-Anbieter	Spotify, Tidal, etc.
Nachrichten	Nachrichten und Magazine	News, Wetter
Einkaufen	Online-Shops (außer adult content)	Amazon, eBay, etc.
Bildung	Lerninhalte	Wikipedia, Google Scholar
Generative KI	KI-spezifische Webseiten	ChatGPT, Perplexity.ai, etc.
Phishing	Potenzielle Phishing-Webseiten	Potential scams, Data theft
Sonstiges	Alles Andere	Rest

Für ve

Erlaubte und gesperrte Domains

- Erlaubte Domains / Gesperrte Domains (Abschnitt Domains): Spezifische Domains gezielt freigeben oder sperren (keine Pfadunterscheidung). Erlaubte Domains sind auch dann erreichbar, wenn der Filter sie als unpassend einstuft. Die Anzahl gesperrter Domains sollte auf etwa 500 begrenzt werden.

Datenschutz

Im Abschnitt Datenschutz steht für Android Enterprise die Option Datenweitergabe automatisch akzeptieren zur Verfügung (standardmäßig deaktiviert). Ist sie aktiviert, wird die Datenweitergabe im Namen des Benutzers automatisch akzeptiert.

Apps verwalten

Mit Relution lassen sich Android Enterprise Geräte mit konfigurierten Apps ausstatten. Hierzu kann eine Apps verwalten-Konfiguration mit den gewünschten Apps an die Endgeräte verteilt werden.
Für die App-Auswahl stehen mehrere Quellen zur Verfügung:

- Apps aus dem Relution App Store
- Apps aus dem Managed Google Play Store
- Apps manuell hinzufügen.

Apps aus dem Relution App Store

Im Relution App Store stehen alle Apps zur Verfügung, die aus dem Managed Google Play Store hinzugefügt wurden.
Der Vorteil ist die übersichtliche Anzahl der Apps, da nicht der komplette Managed Google Play Store dargestellt wird.

> Zudem können ab Relution Server 26.2 mit den Relution Client Apps ab Version 26.x APKs aus dem Relution App Store verteilt werden. Hierbei kann entweder die Apps verwalten-Liste verwendet werden (Installationstyp Benutzerdefiniert) oder die Benutzer laden sich die APKs direkt über den Relution Agent herunter. Alternativ steht die Aktion App aus dem Relution Store installieren zur Verfügung. Das funktioniert nur auf vollständig verwalteten Geräten, auch mit persönlichem Profil. Auf Geräten, die als Arbeitsprofil eingeschrieben sind, werden APK-Apps nicht installiert.

Weitere Details: APK-Apps verwalten →

Für Version 26.4.0

Apps aus dem Managed Google Play Store

Es stehen alle Apps aus dem Managed Google Play Store zur Verfügung. Dieser ist wie ein gewöhnlicher Play Store aus dem privaten Umfeld anzusehen.

Private Apps aus dem Managed Google Play Store

Zusätzlich bietet der Managed Google Play Store die Möglichkeit, private Apps hochzuladen. Private Apps sind auch als Bezahl-Apps zu verstehen, da Google im Enterprise-Umfeld keine Option zum Bezahlen anbietet.
Für diesen Anwendungsfall gibt es drei Optionen:

Installation via Private Play Store

Entwickler erstellen Apps mit einem Unique Package Name.
Diese Apps werden mit einem firmeneigenen Google-Konto in den privaten Store bei Google geladen und können anschließend über Relution im Bereich Managed Google Play Store ausgewählt werden.

Installation via Public Play Store

Entwickler stellen Apps im öffentlichen Bereich des Managed Google Play Store für jedermann zur Verfügung.
Diese können, wie oben beschrieben, zum Relution App Store hinzugefügt oder direkt aus dem Managed Google Play Store ausgewählt werden.

Manuelle Installation via Entwicklermodus mit manueller Verteilung (nicht signierte App)

Hierzu müssen für alle Geräte, die diese Apps erhalten sollen, die Entwickleroptionen aktiviert und die Installation aus unbekannten Quellen erlaubt werden.
Anschließend werden die `.apk`-Dateien manuell auf den Geräten installiert. In diesem Fall sind die Apps nicht verwaltet (managed), können nicht über Relution verwaltet werden und erhalten keine App-Updates.

Apps manuell hinzufügen

Apps, die bereits auf einem Gerät vorinstalliert sind, können über diesen Weg verwaltet werden.
Hierzu wird zwingend der Package Name der App benötigt, anhand dessen Apps auf den Geräten eindeutig identifiziert werden.

App-Paket Namen bei Samsung Geräten

Version 26.4.0

- `com.samsung.android.dialer` | Telefon App
- `com.samsung.android.messaging` | Message App
- `com.sec.android.widgetapp.samsungapps` | Homescreen Widget
- `com.sec.android.app.sbrowser` | Samsung Internet
- `com.sec.android.easyMover.Agent` | Samsung Smart Switch
- `com.sec.android.daemonapp` | Samsung Weather
- `com.samsung.ecomm.global` | Samsung Shop
- `com.sec.android.app.voicenote` | Voice Recorder
- `com.samsung.android.oneconnect` | Smart Things
- `com.samsung.android.voc` | Samsung Members
- `com.sec.android.app.popupcalculator` | Samsung Calculator
- `com.mobeam.barcodeService` | Barcode Scanner
- `com.samsung.android.app.dressroom` | Samsung Wallpapers
- `com.samsung.android.scloud` | Samsung Cloud
- `com.samsung.android.widgetapp.yahooedge.finance` | Finance Widget
- `com.samsung.android.widgetapp.yahooedge.sport` | Sports Widget
- `com.samsung.app.highlightplayer` | Samsung Story Video Editor
- `com.samsung.android.app.aodservice` | Always on Display
- `com.sec.android.app.dexonpc` | Samsung Dex
- `com.samsung.android.email.provider` | Samsung Email
- `com.samsung.android.calendar` | Samsung Calendar
- `com.sec.android.gallery3d` | Samsung Gallery
- `com.sec.android.app.camera` | Samsung Kamera

Installationstyp

- Verfügbar – Apps stehen Benutzer über den Play Store zum Download und Installation zur Verfügung.
- Vorinstalliert – Apps werden auf den Geräten vorinstalliert. Benutzer können die Apps jedoch löschen.
- Installation erzwungen – Apps werden immer automatisch heruntergeladen und auf den Geräten installiert.
- Blockiert – Installationen der Apps werden gezielt blockiert.
- Benutzerdefiniert – wird automatisch für APK-Apps aus dem Relution App Store gesetzt und ist nicht auswählbar oder änderbar.

Konfiguration

Manche App-Hersteller bieten zusätzlich eine Managed-Konfiguration an. Relution stellt diese, sofern verfügbar, dar.
Bei APK-Apps aus dem Relution Store können Konfigurationen im JSON-Format mitgegeben werden.

Berechtigung

Hier können App-Berechtigungen für Apps aus dem Google Play Store gesetzt werden, z. B.:

- Standard-Antwort auf Berechtigungsanforderungen
- Zugriff auf ungefähre Position
- Zugriff auf genaue Position
- Bluetooth verbinden

Für Version 26.4.0

Erweitert

Erweiterte Konfigurationen für Play Store Apps, z. B.:

- Informationen profilübergreifend teilen
- Automatischer Aktualisierungsmodus
- Zertifikate installieren
- Konfigurationen verwalten
- Deinstallation verhindern
- Always-On VPN Lockdown-Ausnahme – legt fest, ob die App bei aktivem Lockdown-Modus auch ohne VPN-Verbindung kommunizieren darf (siehe Always-On VPN →)

Diese Optionen stehen auch für manuell hinzugefügte Apps zur Verfügung. Bei APK-Apps aus dem Relution App Store enthält Erweitert nur die Option App-Deinstallationsmodus für Benutzer mit den Werten Nicht spezifiziert, Zulassen und Nicht zulassen. Bei Zulassen darf die App vom Benutzer deinstalliert werden; eine so entfernte App wird von Relution nicht erneut installiert. Nicht spezifiziert wirkt wie Nicht zulassen.

Restriktionen

Für Android-Geräte mit Android Enterprise-Einschreibung stehen in Relution eine Vielzahl an Restriktionen zur Verfügung. Grundsätzlich ist es ratsam, sich genau darüber im Klaren zu sein, welche Einschränkungen miteinander kombiniert werden. So lässt sich ausschließen, dass Geräte so konfiguriert werden, dass sie nicht mehr nutzbar sind.

Die Konfiguration ist im Portal in mehrere Bereiche gegliedert. Die folgende Übersicht folgt dieser Gliederung. Gilt eine Option nur für bestimmte Einschreibungsarten oder Android-Versionen, ist das bei der Option vermerkt.

Benutzerkontorestriktionen

- Verbieten, neue Benutzer und Profile anzulegen
- Verbieten, andere Benutzer zu entfernen
- Verbieten, Konten hinzuzufügen und zu entfernen
- Verbieten, Anmeldeinformationen des Benutzers zu konfigurieren
- Erlauben, einen privaten Schlüssel zu wählen, wenn keine Regel definiert wurde: Der Benutzer kann einen privaten Schlüssel auswählen, wenn keine Regeln definiert sind, um automatisch einen privaten Schlüssel und ein Zertifikat zur Authentifizierung des Geräts gegenüber einem Server auszuwählen. Bei Geräten unter Android 9 kann diese Einstellung zu einer Gefährdung der Unternehmensschlüssel führen.

Für Version 26.4.0

Vorgegebene Restriktionen

Dieser Bereich wird nur angezeigt, wenn die veraltete Einstellung Apps aus unbekannten Quellen in einer bestehenden Konfiguration auf einen anderen Wert als Installation nicht vertrauenswürdiger Apps auf dem gesamten Gerät verbieten gesetzt ist.

> Die Einstellung Apps aus unbekannten Quellen ist veraltet. Stattdessen wird die Konfiguration Erweiterte Sicherheitsüberschreibungen verwendet. Ist diese konfiguriert, wird die veraltete Einstellung ignoriert.

Weitere Informationen: Sicherheitsüberschreibungen →

App-Restriktionen

- Verbieten, Apps zu installieren
- Verbieten, Apps zu deinstallieren
- Verbieten, das Easter-Egg in den Einstellungen zu verwenden

Restriktionen für Anpassungen

- Verbieten, das Benutzer-Icon anzupassen
- Verbieten, das Hintergrundbild anzupassen
- Automatische Datums- und Zeitzoneneinstellung aktivieren (nur Verwaltetes Gerät): Legt fest, ob die automatische Datums-, Zeit- und Zeitzoneneinstellung auf einem firmeneigenen Gerät aktiviert ist. Zur Auswahl stehen Default, Wahl durch Benutzer und Erzwungen.

Geräterestriktionen

Der Bereich enthält allgemeine Einschränkungen des Geräts sowie profilübergreifende Einstellungen für Geräte mit Arbeitsprofil.

Allgemein

- Verbieten, die Tastensperre zu verwenden (nur Verwaltetes Gerät): Betrifft die Tastensperre als Ganzes. Einzelne Funktionen des Sperrbildschirms werden über Erweiterte Keyguard-Verwaltung → deaktiviert.
- Aktivieren Sie den Factory Reset-Schutz (FRP) (nur Verwaltetes Gerät und Persönliches Profil) und Google account email für FRP: siehe Factory Reset-Schutz →.
- Kontotypen, für die die Verwaltung deaktiviert ist: Kontotypen, die der Benutzer nicht verwalten kann.
- Zulässige Eingabemethoden und Zulässige Barrierefreiheitsdienste: Zur Auswahl stehen Alle erlaubt, Nur System-Apps sowie System und weitere spezifizierte Apps. Bei der letzten Option werden die zusätzlich erlaubten Apps in einer Liste hinterlegt.
- Sichtbarkeit des Anzeigenamens des Unternehmens: Legt fest, ob der Anzeigename des Unternehmens auf dem Gerät angezeigt wird (Nicht spezifiziert, Auf dem Gerät angezeigt, Auf dem Gerät ausgeblendet). Der Anzeigename selbst wird im Feld Anzeigename des Unternehmens unter `Einstellungen` → `Geräteplattformspezifisch` → `Android Enterprise` gepflegt.
- Assistenzinhalt-Richtlinie (ab Android 15): Steuert, ob Assistenzinhalte wie Screenshots und App-Informationen an eine privilegierte App wie eine Assistenz-App gesendet werden dürfen (Nicht spezifiziert, Erlaubt, Nicht Erlaubt).
- Autofill-Richtlinie: Steuert den Autofill-Dienst des Systems (ab Android 8) mit den Optionen Nicht spezifiziert, Wahl durch Benutzer und Deaktiviert. Um die Verwaltung von Anmeldeinformationen umfassend einzuschränken, wird zusätzlich die Standard-Anmeldeinformationsanbieter-Richtlinie konfiguriert.
- Standard-Anmeldeinformationsanbieter-Richtlinie (ab Android 14): Nicht spezifiziert, Nicht zugelassen oder Nicht zugelassen außer System.
- Drucken: Nicht spezifiziert, Erlaubt oder Nicht Erlaubt.

Profilübergreifende Einstellungen

Diese Einstellungen gelten nur für die Einschreibungsarten Arbeitsprofil und Persönliches Profil. Auf verwalteten Geräten ohne Arbeitsprofil werden sie nicht angewendet.

Für Version 26.4.0

- Standardwert für Widgets für Arbeitsprofile: Legt fest, ob Apps des Arbeitsprofils standardmäßig Widgets zum Startbildschirm hinzufügen dürfen, wenn für die App nichts anderes festgelegt ist (Nicht spezifiziert, Erlaubt, Nicht Erlaubt). Nicht spezifiziert entspricht Nicht Erlaubt.
- Kopieren und Einfügen: Nicht spezifiziert, Erlaubt oder Vom Arbeitsprofil zum persönlichen Profil nicht zulassen.
- Teilen von Daten: Nicht spezifiziert, Erlaubt, Vom Arbeitsprofil zum persönlichen Profil nicht zulassen oder Unzulässig.
- Arbeitsprofil Kontakte im persönlichen Profil anzeigen (Abschnitt Kontakte): Nicht spezifiziert, Unzulässig, Erlaubt oder Erlauben Sie nur System-Apps den Zugriff auf geschäftliche Kontakte im persönlichen Profil. Zusätzlich lässt sich eine App-Liste pflegen: Bei Nicht spezifiziert und Erlaubt enthält sie die Apps, die nicht zugreifen dürfen, bei den übrigen Optionen die Apps, die zugreifen dürfen.

Multimediarestriktionen

- Verbieten, Bildschirmfotos zu machen
- Verbieten, die globale Lautstärke zu modifizieren
- Verbieten, den Standort zu teilen
- Verbieten, Kontakte über Bluetooth zu teilen
- Zugriff auf die Kamera: Default, Wahl durch Benutzer, Kamera deaktiviert oder Kamerazugriff erzwingen. Steuert die Verwendung der Kamera und ob der Benutzer den Schalter für den Kamerazugriff (ab Android 12) nutzen kann. Das Deaktivieren der Kamera gilt auf vollständig verwalteten Geräten für das gesamte Gerät, auf Geräten mit Arbeitsprofil nur innerhalb des Arbeitsprofils.
- Zugriff auf das Mikrofon: Default, Wahl durch Benutzer, Mikrofon deaktiviert oder Mikrofonzugriff erzwingen. Steuert die Verwendung des Mikrofons und ob der Benutzer den Schalter für den Mikrofonzugriff (ab Android 12) nutzen kann. Die Einstellung wirkt nur auf vollständig verwalteten Geräten.

Für Version 26.4.0

Netzwerkrestriktionen

- Verbieten, Bluetooth zu konfigurieren
- Verbieten, das mobile Netzwerk zu konfigurieren
- Verbieten, die Netzwerkeinstellungen zurückzusetzen
- Verbieten, VPN zu konfigurieren
- Verbieten, WLAN Netzwerke zu konfigurieren (veraltet, siehe Hinweis unten): siehe WLAN-Konfiguration verbieten →.
- Verbieten, Android Beam (NFC) zum Teilen von App-Daten zu verwenden
- Verbieten, Bluetooth zu verwenden
- Erlauben, den Netzwerk-Notausgang zu verwenden: Kann beim Booten keine Netzwerkverbindung hergestellt werden, fordert der Notausgang den Benutzer auf, sich vorübergehend mit einem Netzwerk zu verbinden, um die Geräterichtlinie zu aktualisieren. Nach dem Anwenden der Richtlinie wird das temporäre Netzwerk wieder entfernt.
- Bevorzugter Netzwerkdienst (nur Arbeitsprofil): Steuert, ob der bevorzugte Netzwerkdienst im Arbeitsprofil aktiviert ist (Unspezifiziert, Deaktiviert, Aktiviert). Auf vollständig verwalteten Geräten hat die Einstellung keine Auswirkung.

Restriktionen für Speicher

- Verbieten, externe physikalische Medien einzubinden
- Verbieten, Dateien über USB zu übertragen (veraltet, siehe Hinweis unten)

Restriktionen für Telefonie

- Verbieten, SMS zu senden und zu empfangen
- Verbieten, ausgehende Anrufe zu tätigen
- Verbieten, Roaming für Datendienste zu verwenden
- Verbieten, Tethering und tragbare Hotspots zu konfigurieren (veraltet, siehe Hinweis unten)
- Verbieten, Cell Broadcasts zu konfigurieren

Die Optionen Verbieten, WLAN Netzwerke zu konfigurieren, Verbieten, Dateien über USB zu übertragen und Verbieten, Tethering und tragbare Hotspots zu konfigurieren sind veraltet. Stattdessen wird die Konfiguration Gerätekonnektivität → verwendet. Sind beide Konfigurationen vorhanden, werden diese drei Optionen ignoriert.

Mögliche Fallstricke

Die folgenden Optionen können dazu führen, dass Geräte nicht mehr wie gewünscht nutzbar oder erreichbar sind.

Factory Reset-Schutz

Mit der Option Aktivieren Sie den Factory Reset-Schutz (FRP) lässt sich auf verwalteten Geräten das Zurücksetzen auf die Werkseinstellungen über die Android-Geräteeinstellungen blockieren. Das Zurücksetzen über das Wiederherstellungsmenü ist davon nicht betroffen.

Im Feld Google account email für FRP werden die E-Mail-Adressen von Geräte-Admins hinterlegt. Diese Adressen müssen Google-Konten sein. Wurde das Gerät auf Werkseinstellungen zurückgesetzt, muss sich einer dieser Geräte-Admins mit seinem Google-Konto (E-Mail und Passwort) anmelden, um das Gerät zu entsperren. Sind keine Adressen angegeben, bietet das Gerät keinen Schutz beim Zurücksetzen auf die Werkseinstellungen. Diese Einstellung sollte daher mit erhöhter Vorsicht genutzt werden.

Für Version 26.4.0

WLAN-Konfiguration verbieten

Ist Verbieten, WLAN Netzwerke zu konfigurieren aktiv und werden keine WLAN-Netzwerke vorgegeben, wird WLAN auf dem Gerät deaktiviert. Können Geräte keine WLAN-Verbindung herstellen, weil die konfigurierten Netzwerke nicht erreichbar oder fehlerhaft sind, besteht keine Möglichkeit, manuell einzugreifen. Die Einstellung lässt sich dann auch nicht mehr zurücknehmen, da die Geräte offline sind.

Diese Option sollte nur in Verbindung mit Erlauben, den Netzwerk-Notausgang zu verwenden genutzt werden. Kann beim Booten keine Netzwerkverbindung hergestellt werden, lässt sich damit vorübergehend ein WLAN-Netzwerk konfigurieren, um die Geräterichtlinie zu aktualisieren.

System-Updates

System-Updates sind ein zentraler Bestandteil der Geräteverwaltung in Android Enterprise. Sie ermöglichen die Steuerung von Aktualisierungsrichtlinien für verwaltete Geräte, um Sicherheit und Stabilität zu gewährleisten.

System-Update-Typ

Im Bereich System-Updates verwalten kann der System-Update-Typ für verwaltete Geräte festgelegt werden. Die verfügbaren Optionen sind:

- Unspezifiziert (Unspecified): Folgt dem Standard-System-Update-Verhalten des Geräts. Dies erfordert in der Regel, dass System-Updates manuell akzeptiert werden.
- Automatisch (Automatic): Automatische Installation von System-Updates, sobald ein Update verfügbar ist.
- Wartungsfenster (Maintenance Window): Automatische Installation von System-Updates innerhalb eines täglichen Wartungsfensters. Dadurch werden auch Play-Apps so konfiguriert, dass sie innerhalb des Fensters aktualisiert werden. Diese Option wird für Kioskgeräte empfohlen, um sicherzustellen, dass dauerhaft in den Vordergrund gepinnte Apps von Play aktualisiert werden können.
- Aufschieben (Postpone): Verschieben der automatischen Installation von System-Updates um bis zu maximal 30 Tage.

Bei Auswahl von Wartungsfenster erscheinen die Pflichtfelder Startzeit und Endzeit (voreingestellt 00:00 und 00:30). Die Zeiten beziehen sich auf die Ortszeit des Geräts. Liegt die Endzeit vor der Startzeit, reicht das Wartungsfenster über Mitternacht. Start- und Endzeit müssen mindestens 30 Minuten auseinanderliegen, andernfalls lässt sich die Konfiguration nicht speichern.

Für Version 26.4.0

Jährlicher System-Update-Einfrierzeitraum

Der Jährliche System-Update-Einfrierzeitraum legt Zeiträume fest, in denen keine System-Updates installiert werden. Start- und Enddatum bestehen nur aus Monat und Tag, der Zeitraum wiederholt sich jedes Jahr.

Eigenschaften des Einfrierzeitraums

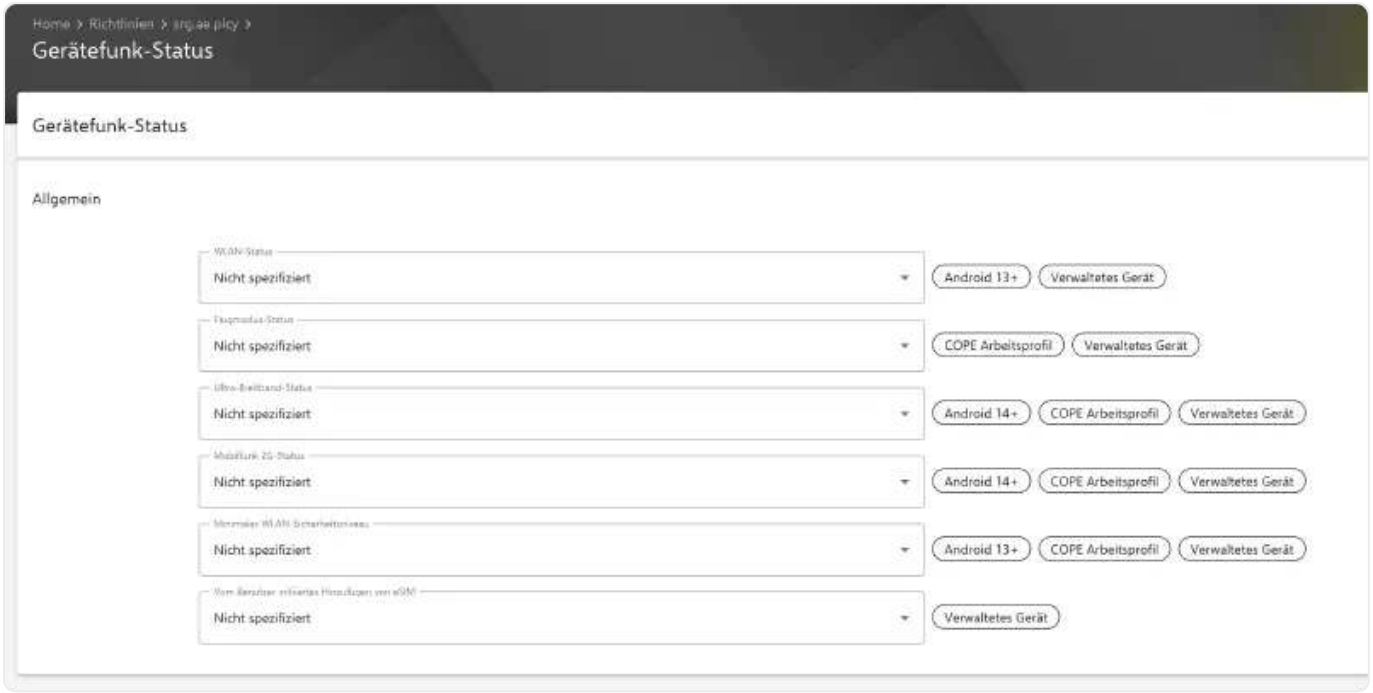
- Während des Einfrierzeitraums werden alle eingehenden System-Updates (einschließlich Sicherheitspatches) blockiert.
- Außerhalb des Einfrierzeitraums gilt das normale Aktualisierungsverhalten.
- Einfrierzeiträume werden über Hinzufügen angelegt. Es lassen sich mehrere Zeiträume festlegen und einzeln wieder entfernen.
- Ein Zeitraum darf höchstens 90 Tage umfassen. Zwischen zwei Zeiträumen müssen mindestens 60 Tage liegen.
- Liegt das Enddatum vor dem Startdatum, umfasst der Zeitraum den Jahreswechsel.

Gerätefunk-Status

Diese Richtlinie steuert zentral den Status und die Nutzung von Funktechnologien auf verwalteten Android-Geräten.

Die Richtlinie Gerätefunk-Status ermöglicht die zentrale Verwaltung verschiedener Funktechnologien auf Android Enterprise Geräten. Administratoren können festlegen, ob Benutzer bestimmte Funktionen selbst steuern dürfen oder ob diese erzwungen aktiviert bzw. deaktiviert werden.

Jede Einstellung bietet zusätzlich die Option Nicht spezifiziert, die bei einer neuen Konfiguration vorausgewählt ist. In diesem Fall gilt das von Google festgelegte Standardverhalten von Android Enterprise: Wahl durch Benutzer für WLAN, Flugmodus, Ultra-Breitband und Mobilfunk 2G, Offene Netzwerksicherheit für das minimale WLAN-Sicherheitsniveau und Erlaubt für das Hinzufügen von eSIM.



WLAN-Status

Definiert den Zustand der WLAN-Funktion.

Optionen:

- Wahl durch Benutzer – Benutzer können WLAN selbst ein- oder ausschalten.
- Aktiviert – WLAN ist dauerhaft aktiviert.
- Deaktiviert – WLAN ist dauerhaft deaktiviert.

Unterstützung:

- Android 13+
- Verwaltete Geräte

Flugmodus-Status

Steuert, ob der Flugmodus aktiviert werden darf.

Optionen:

- Wahl durch Benutzer – Benutzer können den Flugmodus selbst aktivieren oder deaktivieren.
- Deaktiviert – Der Flugmodus ist dauerhaft deaktiviert.

Unterstützung:

- COPE Arbeitsprofil
- Verwaltete Geräte

Ultra-Breitband-Status (UWB)

Regelt die Nutzung von Ultra-Breitband (z. B. für präzise Ortung).

Optionen:

- Wahl durch Benutzer – Benutzer können UWB selbst aktivieren oder deaktivieren.
- Deaktiviert – UWB ist dauerhaft deaktiviert.

Unterstützung:

- Android 14+
- COPE Arbeitsprofil
- Verwaltete Geräte

Für Version 26.4.0

Mobilfunk 2G-Status

Ermöglicht die Einschränkung der Nutzung von 2G-Netzen (relevant aus Sicherheitsgründen).

Optionen:

- Wahl durch Benutzer – Benutzer können die Nutzung von 2G-Netzen selbst steuern.
- Deaktiviert – 2G-Netze sind dauerhaft deaktiviert.

Unterstützung:

- Android 14+
- COPE Arbeitsprofil
- Verwaltete Geräte

Minimales WLAN-Sicherheitsniveau

Legt fest, welche Sicherheitsstandards für WLAN-Verbindungen mindestens erfüllt sein müssen.

Optionen:

- Offene Netzwerksicherheit – Keine Einschränkung.
- Persönliche Netzwerksicherheit – Mindestanforderung an WPA/WPA2.
- Enterprise-Netzwerksicherheit – Erfordert WPA2-Enterprise.
- Enterprise 192-Bit-Netzwerksicherheit – Höchste Sicherheitsanforderung.

Hinweis: Unsichere Netzwerke können blockiert werden, wenn strengere Richtlinien definiert sind.

Unterstützung:

- Android 13+
- COPE Arbeitsprofil
- Verwaltete Geräte

Vom Benutzer initiiertes Hinzufügen von eSIM

Bestimmt, ob Benutzer eigenständig eSIM-Profile hinzufügen dürfen.

Für Version 26.4.0

Optionen:

- Erlaubt – Benutzer dürfen eSIM-Profile hinzufügen.
- Unzulässig – Benutzer dürfen keine eSIM-Profile hinzufügen.

Unterstützung:

- Verwaltete Geräte

Kiosk-Modus

Mit der Richtlinienkonfiguration Kiosk-Modus bietet Relution die Möglichkeit, die Bedienung von Android-Geräten mit Android Enterprise-Einschreibung stark zu beschränken und die Geräte vor Fehlbedienungen zu schützen.

Relution Homescreen Layout

Auf vollständig verwalteten Geräten (Device Owner) aktiviert die Konfiguration Relution Homescreen Layout im Hintergrund automatisch den Kiosk-Modus und setzt die Relution Homescreen Layout App als Launcher ein. Bei den übrigen Android-Enterprise-Einschreibungen (verwaltetes Gerät mit persönlichem Profil und Arbeitsprofil) erhält die App zwar das konfigurierte Layout, wird aber nicht als Kiosk-Launcher gesetzt. Die Relution Homescreen Layout-Konfiguration bietet die Möglichkeit, über das Relution Portal bequem per Drag & Drop das App-Layout auf den Geräten anzupassen. Zusätzlich besteht die Möglichkeit, ein Hintergrundbild zu definieren und eigene, statische oder dynamische Texte auf dem Hintergrund zu platzieren.

Der Relution Homescreen unterdrückt in dieser Konfiguration Benachrichtigungen auf dem Lockscreen.

> Die Konfigurationen Relution Homescreen Layout und Kiosk-Modus schließen sich gegenseitig aus. Enthält die Richtlinie bereits eine der beiden (auch eine deaktivierte), kann die andere nicht hinzugefügt werden.

Für Version 26.4.0

Standard-Launcher verwenden

Die Konfiguration Kiosk-Modus ersetzt den Startbildschirm des Geräts durch den Standard-Launcher von Android Enterprise. Dieser zeigt ausschließlich verwaltete Apps, die über die Konfiguration Apps verwalten installiert wurden (z. B. mit dem Installationstyp Installation erzwungen oder Vorinstalliert), auf einer einzigen Seite in alphabetischer Reihenfolge an. Alle anderen Apps auf den Geräten sind für Benutzer ausgeblendet und können nicht genutzt werden.

> Die Nutzung des Kiosk-Modus setzt ein vollständig verwaltetes Gerät oder ein verwaltetes Gerät mit persönlichem Profil (COPE) voraus; auf Geräten mit Arbeitsprofil (BYOD) steht er nicht zur Verfügung. Durch die Aktivierung des Kiosk-Modus wird im Standard die Nutzung der Telefonfunktion verhindert, was auch das Absetzen von Notrufen unterdrückt.

Einstellungen

Neben dem Abschnitt Benutzerdefinierte Launcher-App (siehe unten) enthält die Konfiguration Kiosk-Modus die Abschnitte Allgemein und Kiosk-Anpassung.

Allgemein

- Bleibt eingeschaltet, solange die Batterie geladen wird – Mehrfachauswahl der Lademodi `AC`, `USB` und `WIRELESS`, in denen das Gerät eingeschaltet bleibt.
- Maximale Zeit bis zum Sperren des Gerätes – Auswahl zwischen 15 Sekunden und 20 Minuten. Ohne Auswahl gilt die Standardeinstellung des Geräts. Ein fester Bildschirm-Timeout aus der Konfiguration Bildschirm → wird nur übertragen, wenn er kürzer ist als dieser Wert.
- Toasts und Overlays deaktivieren – unterbindet die Anzeige von Toasts und Overlays auf dem Gerät.

Kiosk-Anpassung

Bei einer neuen Konfiguration sind folgende Werte vorausgewählt:

Feld	Vorauswahl	Weitere Optionen
Power-Button Aktionen	Verfügbar	Nicht verfügbar, Verfügbar - (Standard)
Systemfehler Warnungen	Unterdrückt	Aktiviert, Unterdrückt - (Standard)
Systemnavigation	Deaktiviert	Aktiviert, Nur Home-Button, Deaktiviert - (Standard)
Statusleiste	Deaktiviert	Aktiviert, Nur Systeminfo, Deaktiviert - (Standard)
Geräteinstellungen	Erlaubt	Blockiert, Erlaubt - (Standard)

Die Optionen mit dem Zusatz - (Standard) übernehmen das Standardverhalten von Android Enterprise. Der Abschnitt Kiosk-Anpassung ist nur in der Konfiguration Kiosk-Modus verfügbar, nicht in Relution Homescreen Layout.

Alternativen Launcher verwenden

Sollen außer den in der Richtlinienkonfiguration Apps verwalten hinzugefügten Apps weitere Funktionen und Apps auf den Android-Geräten verfügbar sein, beispielsweise System-Apps, ist es notwendig, einen alternativen Launcher zu verwenden. Dazu wird im Abschnitt Benutzerdefinierte Launcher-App der Schalter Statt dem Standard-Launcher eine benutzerdefinierte Kiosk-App verwenden aktiviert. Anschließend öffnet die Schaltfläche Auswählen im Feld Benutzerdefinierte Launcher-App wählen den Dialog App auswählen. Dort wird als Quelle Managed Google Play Store App (Android Enterprise) gewählt und die Launcher-App hinzugefügt. Alternativ stehen die Quellen Relution App Store App und App manuell hinzufügen zur Verfügung.

Im Anschluss besteht die Möglichkeit, den Launcher zu konfigurieren. Die Funktion Benutzerdefinierte Launcher-App konfigurieren nutzen, um die Konfiguration manuell vorzunehmen.

Play Store Verwaltung

Mit der Richtlinienkonfiguration Play Store Verwaltung bietet Relution die Möglichkeit, die Bedienung von Android-Geräten mit Android Enterprise-Einschreibung zu steuern indem die verfügbaren Inhalte im Google Play Store auf den Inhalt der Apps-Verwalten konfiguration reduziert werden. Zudem ist es möglich, App Updates zu konfigurieren.

Eingeschränkter Google Play Store

Eingeschränkter Google Play Store - Deaktiviert

- Öffnet der Benutzer den Google Play Store auf dem Gerät kann er alle öffentlichen Apps sehen und installieren.

Eingeschränkter Google Play Store - Aktiviert

- Öffnet der Benutzer den Google Play Store auf dem Gerät so sind keine oder die Apps aus der Apps-Verwalten Konfiguration sichtbar. Je nach vorgegebenem Installations Typ aus der Apps-verwalten Liste kann der Benutzer freigegebene Apps nachinstallieren.

Ist der eingeschränkte Google Play Store aktiviert, werden Apps, die nicht in der Konfiguration Apps verwalten enthalten sind, automatisch vom Gerät deinstalliert. Ausgenommen sind Systemapps sowie Apps, die Relution selbst in die Richtlinie aufnimmt (z. B. Relution Agent und Companion). Das gilt auch, wenn der eingeschränkte Google Play Store über einen Unterricht aktiviert wird.

Für Version 26.4.0

App-Updates

Über das Feld Automatisches App-Update in der Konfiguration Play Store Verwaltung stehen 4 Optionen zur Wahl:

- Wahl durch Benutzer
- Nie
- Nur über WLAN
- Immer

Der Kiosk-Modus kann automatische Updates unterbinden.

Die Optionen Verbieten, Apps zu installieren und Verbieten, Apps zu deinstallieren (Konfiguration Restriktionen, Bereich App-Restriktionen) verhindern jegliche Installation bzw. Deinstallation, auch die per MDM ausgelöste.

Benutzer-Meldungen

Bei verwalteten Android-Enterprise-Geräten ist es möglich, eine Nachricht auf dem Sperrbildschirm anzuzeigen. Dies erleichtert die Identifizierung des Geräts oder kann bei Verlust für eine Kontaktmöglichkeit genutzt werden. Zusätzlich lassen sich eine kurze und eine lange Supportmeldung einrichten, die als Pop-up in den Systemeinstellungen angezeigt werden, z. B. wenn eine gesperrte Einstellung aufgerufen wird.

Meldung	Anzeigeort	Auslöser
Nachricht auf dem Sperrbildschirm	Sperrbildschirm des Geräts	dauerhaft sichtbar
Kurze Supportmeldung	Pop-up in den Systemeinstellungen	Zugriff auf eine gesperrte Einstellung
Lange Supportmeldung	Pop-up in den Systemeinstellungen	Zugriff auf die Geräteadministrator-Einstellung

Alle Meldungen können zusätzlich landesspezifisch angepasst werden: Ist ein Gerät z. B. auf Englisch eingestellt, wird die zur Systemsprache passende Meldung angezeigt. Jede Meldung besteht aus einer Standard-Benachrichtigung und optional aus landesspezifischen Benachrichtigungen, die in der Tabelle darunter mit der jeweiligen Sprache angelegt werden. Passt die Systemsprache des Geräts zu keiner landesspezifischen Meldung, erscheint die Standard-Benachrichtigung. Sobald eine landesspezifische Meldung angelegt ist, ist die Standard-Benachrichtigung ein Pflichtfeld.

Für Version 26.4.0

In allen drei Meldungen können Platzhalter verwendet werden, die Relution für jedes Gerät einzeln ersetzt, z. B. `${device.name}`, `${device.serialnumber}`, `${device.uuid}` oder Benutzer-Platzhalter. Die verfügbaren Platzhalter werden im Bereich Verfügbare Platzhalter unterhalb des Formulars angezeigt.

Nachricht auf dem Sperrbildschirm

Diese Meldung wird auf dem Sperrbildschirm des Geräts angezeigt. Sinnvolle Inhalte sind:

- Name der Firma / Organisation
- Gerätename, Seriennummer oder Geräte-ID (per Platzhalter)
- Kontakt-E-Mail oder Telefonnummer

Kurze Supportmeldung

Diese Meldung wird innerhalb der Einstellungen am Gerät als Pop-up angezeigt, sobald der Zugriff auf eine gesperrte Einstellung versucht wird.

Lange Supportmeldung

Diese Meldung wird innerhalb der Einstellungen am Gerät als Pop-up angezeigt, sobald der Zugriff auf die Geräteadministrator-Einstellung versucht wird.

Laufzeitberechtigungen

Über die Richtlinienkonfiguration Laufzeitberechtigungen verwalten können Standard-Antworten auf Berechtigungsanforderungen von verwalteten Apps pauschal festgelegt werden.

Im Abschnitt Standard-Antwort auf Berechtigungsanforderungen steht im Feld Wenn eine App eine Berechtigung anfordert: eine der Optionen Den Anwender fragen (Standard), Berechtigung geben oder Berechtigung verweigern zur Auswahl. Voreingestellt ist Den Anwender fragen (Standard).

> Vorsicht bei pauschalen Verboten: Wird zu restriktiv vorgegangen, funktionieren einige Apps gegebenenfalls nicht mehr so wie gewünscht.

Des Weiteren gibt es neben dem definierten Standardverhalten Ausnahmen für spezifische Berechtigungen.

Für Version 26.4.0

Standard Android-Berechtigungen

Es lassen sich die im Android-Betriebssystem vorhandenen Berechtigungsanfragen in der Konfiguration Laufzeitberechtigungen verwalten und das dazu gewünschte Verhalten konfigurieren. Beim Hinzufügen einer Berechtigung wird im Feld Verhalten eine der drei Optionen gewählt (Vorgabe: Den Anwender fragen (Standard)).

> Berechtigungen, die hier definiert werden, überschreiben die oben im Abschnitt Standard-Antwort auf Berechtigungsanforderungen festgelegte Einstellung. Das gilt ebenso für benutzerdefinierte Berechtigungen.

Benutzerdefinierte Berechtigungen

Es können App-spezifische Berechtigungsanfragen konfiguriert werden, falls dies von einer App erfordert wird. Die Namen dieser Berechtigungen lassen sich in der Regel den Dokumentationen des jeweiligen App-Herstellers entnehmen. Auch hier wird beim Hinzufügen im Feld Verhalten eine der drei Optionen gewählt (Vorgabe: Den Anwender fragen (Standard)).

WLAN

Diese Richtlinie verteilt WLAN-Netzwerkdefinitionen zentral auf Android-Enterprise-Geräte.

Die Richtlinie WLAN ermöglicht es, WLAN-Netzwerke zentral auf Android Enterprise Geräten einzurichten, ohne dass Benutzer die Zugangsdaten selbst eingeben müssen. Es können mehrere WLAN-Konfigurationen gleichzeitig einer Richtlinie hinzugefügt werden.

Tethering wird nicht über diese Richtlinie gesteuert, sondern über die Option Tethering-Einstellungen der Konfiguration Gerätekonnektivität →.

Netzwerkdefinition

- Name der WLAN-Konfiguration – interner Name zur Wiedererkennung in Relution.
- Netzwerk SSID – Netzwerkname im Klartext. Alternativ Hex-Darstellung der Netzwerk-SSID, erforderlich für SSIDs, die sich nicht mit UTF-8 kodieren lassen. Mindestens eines der beiden Felder ist Pflicht. Sind beide ausgefüllt, müssen sie übereinstimmen.
- Verstecktes Netzwerk – aktivieren, wenn das Netzwerk seine SSID nicht sendet.
- Netzwerk automatisch beitreten – verbindet das Gerät ohne weiteres Zutun, sobald das Netzwerk in Reichweite ist.

Für Version 26.4.0

Sicherheitstyp

- Sicherheitstyp: Keiner / Offen für alle, WEP PSK, WPA/WPA2/WPA3 PSK, WEP 802.1x, WPA/WPA2/WPA3 EAP.
- Passphrase: bei PSK-basierten Sicherheitstypen erforderlich.

EAP-Authentifizierung (WEP 802.1x, WPA/WPA2/WPA3 EAP)

- Akzeptierte EAP-Typen: PEAP, TLS, TTLS, SIM, AKA oder PWD, dazu Identität (Pflichtfeld). Bei PWD zusätzlich Passwort.
- Bei PEAP und TTLS zusätzlich Anonyme Identität, Passwort und Interne Authentifizierung (Phase 2): PAP oder MSCHAPv2.
- Bei TLS, PEAP und TTLS: Client-Zertifikat-Typ bzw. Zertifikatsvorlage (siehe Zertifikatsverwaltung →) und maximale TLS-Version.
- Prüfung des Serverzertifikats: Vertrauenswürdige CA Zertifikate, Domain-Suffix-Übereinstimmung (Pflichtfeld, eine leere Liste lehnt Android als unsicher ab), Subject Alternative Name (SAN) Übereinstimmung sowie optional Teilzeichenfolge des Zertifikatssubject-Namens vertrauenswürdiger RADIUS-Dienste.
- Opportunistisches Schlüssel-Caching für schnelles Roaming aktivieren

MAC-Adressen-Randomisierung

Randomisierungsmodus für MAC-Adressen (Hardware/Automatisch, Standard: Automatisch) – wird nur an Geräte ab Android 13 übertragen.

Proxy

Im Abschnitt Proxy Einstellungen legt Proxy Typ die Art des Proxys fest: Keine, Manuell oder Automatisch konfigurieren (PAC).

- Bei Manuell: Host und Portnummer für HTTP-Proxy, HTTPS-Proxy, FTP-Proxy und/oder SOCKS-Proxy, wobei mindestens ein Proxy angegeben sein muss, sowie Proxy umgehen für (Liste von Adressen, die nicht über den Proxy geleitet werden).
- Bei Automatisch konfigurieren: PAC URL.

Ein Proxy, der unabhängig vom verbundenen Netzwerk gilt, wird über die Konfiguration Globaler Proxy → festgelegt.

Unterstützung

- Verwaltete Geräte (Device Owner)
- COPE Arbeitsprofil (Personal Profile Enabled)
- Nicht verfügbar für reines Arbeitsprofil (BYOD/Profile Owner)

Für Version 26.4.0

Always-On VPN

Diese Richtlinie bestimmt, welche VPN-App auf dem Gerät dauerhaft aktiv gehalten wird.

Die Richtlinie Always-On VPN legt fest, welche bereits installierte VPN-App auf einem Android Enterprise Gerät dauerhaft aktiv sein soll. Anders als die StrongSwan-Konfigurationen →, die eine konkrete VPN-App mit eigenem Profil ausstatten, wählt diese Richtlinie lediglich aus, welche App als Always-On-VPN fungiert – die App selbst muss über Apps verwalten → separat installiert werden, da sie durch diese Richtlinie nicht automatisch bereitgestellt wird.

Einstellungen

Die Always-On-VPN-Einstellungen können vom Benutzer am Gerät geändert werden, sofern in den Restriktionen → nicht die Option Verbieten, VPN zu konfigurieren aktiviert ist.

- Wählen Sie die Always-On VPN-App (Pflichtfeld, Schaltfläche Auswählen) – die App, die dauerhaft als VPN-Verbindung aktiv bleiben soll.
- Netzwerkverbindung ablehnen, wenn VPN nicht verbunden ist (Lockdown-Modus) – erlaubt Netzwerkverkehr ausschließlich über die VPN-Verbindung. Solange das VPN nicht verbunden ist, besteht kein Netzwerkzugriff. Auch bei bestehender VPN-Verbindung bleibt jeglicher Datenverkehr außerhalb des Tunnels gesperrt, sofern die jeweilige App nicht als Lockdown-Ausnahme → freigestellt ist.

Bei aktivem Lockdown-Modus muss das Gerät eine Verbindung zum VPN herstellen können. Andernfalls ist auch keine WLAN-Verbindung möglich und das Gerät kann nicht mit Relution kommunizieren.

Für Version 26.4.0

Split Tunneling

Die Richtlinie Always-On VPN legt ausschließlich fest, welche VPN-App dauerhaft aktiv ist. Welcher Datenverkehr durch den Tunnel geleitet wird, bestimmt die Konfiguration der VPN-App bzw. des VPN-Gateways. Enthält diese keine Einschränkung auf bestimmte Apps oder Zielnetze, leitet Android den gesamten Datenverkehr durch das VPN.

Split Tunneling ist daher auch in Kombination mit Always-On VPN möglich, sofern die VPN-App dies unterstützt:

- App-Konfiguration der VPN-App – Bietet der Hersteller eine Managed-Konfiguration an, steht sie in Apps verwalten → über die Aktion Konfiguration zur Verfügung. Ob und in welcher Form dort Apps oder Netze für den Tunnel festgelegt werden können, hängt vom jeweiligen VPN-Client ab.
- StrongSwan – Im StrongSwan VPN Profil → wird im Bereich Apps zwischen Nur diese Apps können das VPN nutzen und Diese Apps werden das VPN nicht verwenden (Standard) gewählt. Bleibt die Liste bei Diese Apps werden das VPN nicht verwenden leer, nutzen alle Apps das VPN. Im Bereich Split tunneling lässt sich der Datenverkehr zusätzlich nach Zielnetzen aufteilen: Nur Datenverkehr zu definierten Subnetzen über VPN routen, alles andere wird so geroutet, als gäbe es kein VPN oder Der Datenverkehr zu diesen Subnetzen wird nicht über VPN geroutet. Optional wird über IPv4-Verkehr blockieren, der nicht für das VPN bestimmt ist bzw. IPv6-Verkehr blockieren, der nicht für das VPN bestimmt ist der übrige Datenverkehr der jeweiligen Protokollversion gesperrt.
- VPN-Gateway – Alternativ werden am Gateway nur die internen Netze als Routen an das Gerät übergeben, statt den gesamten Datenverkehr zu tunneln.

Lockdown-Modus und Ausnahmen

Bei aktivem Lockdown-Modus sperrt Android jeglichen Datenverkehr, der nicht über das VPN läuft. Apps, die per Split Tunneling vom Tunnel ausgenommen sind, haben in diesem Fall keine Netzwerkverbindung. Dasselbe gilt für Datenverkehr zu Zielnetzen, für die das VPN keine Route bereitstellt. Ein Split Tunneling, das nur nach Zielnetzen unterscheidet, ist mit aktivem Lockdown-Modus daher nicht nutzbar. Das gilt auch für die Aufteilung nach Subnetzen im Bereich Split tunneling des StrongSwan VPN Profils.

Einzelne Apps lassen sich vom Lockdown ausnehmen. Dazu wird in Apps verwalten → über die Aktion Erweitert die Option Always-On VPN Lockdown-Ausnahme gesetzt:

- Nicht spezifiziert / Erzwingen – die App unterliegt dem Lockdown-Modus.
- Freistellung – die App darf auch ohne aktive VPN-Verbindung kommunizieren. Die Einstellung wird ab Android 10 unterstützt.

Die Option steht nicht für APK-Apps aus dem Relution App Store zur Verfügung. Bei diesen enthält Erweitert nur die Option App-Deinstallationsmodus für Benutzer.

Eine freigestellte App nutzt das VPN weiterhin, sofern die VPN-App sie in den Tunnel einbezieht. Damit eine App bei aktivem Lockdown-Modus am Tunnel vorbei kommuniziert, muss sie daher sowohl als Freistellung markiert als auch in der VPN-App vom Tunnel ausgenommen sein.

Unterstützung

- Verwaltete Geräte (Device Owner)
- COPE Arbeitsprofil (Personal Profile Enabled)
- Arbeitsprofil (Profile Owner/BYOD)

Für Version 26.4.0

StrongSwan

Diese Richtlinien konfigurieren die App StrongSwan sowie deren VPN-Profile auf Android-Enterprise-Geräten.

Relution bietet zwei zusammengehörige Richtlinien für die App StrongSwan → (`org.strongswan.android`): StrongSwan Restriktionen steuert das Verhalten der App und referenziert ein Standardprofil, StrongSwan VPN Profil definiert die eigentliche IKEv2-VPN-Verbindung. Über Always-On VPN → kann die App StrongSwan zusätzlich als dauerhaft aktive VPN-App festgelegt werden. Welches Profil dabei verbunden wird, bestimmt die Einstellung Wählen Sie ein Standard-VPN-Profil in den StrongSwan Restriktionen.

Sobald eine Richtlinie eine der beiden Konfigurationen enthält, installiert Relution die App StrongSwan automatisch als Pflicht-App, gewährt ihr die angeforderten Berechtigungen und erlaubt ihr, Zertifikate zu installieren. Eine separate Zuweisung über Apps verwalten → ist nicht erforderlich. Eine dort für StrongSwan hinterlegte Einstellung, z. B. ein abweichender Installationstyp, wird überschrieben.

StrongSwan Restriktionen

- Benutzern erlauben, Profile zu erstellen
- Benutzern erlauben, Profile zu importieren
- Benutzern erlauben, vorhandene Profile zu verwenden
- Benutzern erlauben, Zertifikate zu importieren
- Benutzern den Zugriff auf Einstellungen erlauben
- Keine Warnung anzeigen, wenn die App nicht auf der Power-Whitelist des Geräts steht
- Wählen Sie ein Standard-VPN-Profil (Schaltfläche Auswählen) – Referenz auf eine StrongSwan-VPN-Profil-Konfiguration derselben Richtlinienversion

Für Version 26.4.0

StrongSwan VPN Profil

Es können mehrere VPN-Profile angelegt und im Portal verwaltet werden. Das Formular besteht aus dem Bereich StrongSwan VPN Profil mit den Abschnitten Allgemein, Benutzerzertifikat und CA Zertifikat sowie dem Bereich Erweiterte Einstellungen.

Allgemein

- Name des Profils
- Server – Adresse des VPN-Servers. Der Port wird unter Erweiterte Einstellungen festgelegt.
- VPN-Typ:
  - IKEv2 EAP (Benutzername/Passwort)
  - IKEv2-Zertifikat
  - IKEv2-Zertifikat + EAP (Benutzername/Passwort)
  - IKEv2 EAP-TLS (Zertifikat)
  - IKEv2 EAP-TNC (Benutzername/Passwort)
- Benutzername – nur bei VPN-Typen mit Benutzername/Passwort

Benutzerzertifikat

Der Abschnitt erscheint nur bei VPN-Typen mit Zertifikat. Hier wird das Benutzerzertifikat festgelegt (siehe Zertifikatsverwaltung →).

CA Zertifikat

CA- bzw. Server-Zertifikat, mit dem der VPN-Server geprüft wird.

Erweiterte Einstellungen

Der Bereich Erweiterte Einstellungen ist in die folgenden Abschnitte gegliedert.

Allgemein

- Serveridentität und Identität des Clients
- DNS-Server, MTU des VPN-Tunnelgeräts, Port und NAT-T Keepalive-Intervall
- Zertifikatsanfragen senden
- Zertifikatsprüfung per OCSP bzw. CRL sowie Strenge Widerrufsprüfung verwenden
- RSA/PSS-Signaturen verwenden und IPv6-Transportadressen verwenden

Split tunneling

- Ein-/auszuschließende Subnetze
- IPv4-/IPv6-Datenverkehr blockieren, der nicht für das VPN bestimmt ist

Für Version 26.4.0

Proxy

Host, Port und Hosts vom Proxy ausschließen.

Apps

- Nur diese Apps können das VPN nutzen – ausschließlich die gelisteten Apps verwenden das VPN, alle übrigen Apps kommunizieren am Tunnel vorbei
- Diese Apps werden das VPN nicht verwenden – die gelisteten Apps kommunizieren am Tunnel vorbei, alle übrigen Apps verwenden das VPN. Bleibt die Liste leer, wird der gesamte Datenverkehr über das VPN geleitet.

Bei aktivem Lockdown-Modus in Always-On VPN → haben Apps außerhalb des Tunnels nur dann eine Netzwerkverbindung, wenn sie als Lockdown-Ausnahme freigestellt sind.

> Ein automatischer Verbindungsaufbau bei Bedarf (On Demand) ist unter Android Enterprise nicht möglich. Das VPN wird einmal manuell in der App StrongSwan verbunden; danach wird der Datenverkehr der festgelegten Apps durch den Tunnel geleitet. Das gilt auch mit Always-On VPN →: Die erste Verbindung baut der Benutzer selbst auf.

Algorithmen

IKEv2-Algorithmen und IPsec/ESP-Algorithmen.

Unterstützung

- Verwaltete Geräte (Device Owner)
- COPE Arbeitsprofil (Personal Profile Enabled)
- Arbeitsprofil (Profile Owner/BYOD)

Persönliche Nutzung

Diese Richtlinie konfiguriert die persönliche Nutzung für ein vollständig verwaltetes Gerät mit Arbeitsprofil.

Die Richtlinie Persönliche Nutzung schränkt den privaten Bereich eines vollständig verwalteten Geräts mit Arbeitsprofil (COPE) ein.

Einstellungen

- Deaktiviere Kamera – deaktiviert die Kamera im privaten Profil.
- Verbieten, Bildschirmfotos zu machen – unterbindet Screenshots im privaten Profil.
- Kontotypen, für die die Verwaltung deaktiviert ist – verhindert das Hinzufügen bestimmter Kontotypen im privaten Profil.
- Maximale Anzahl von Tagen, für die der Arbeitsmodus deaktiviert werden kann – begrenzt, wie lange Benutzer den Arbeitsmodus pausieren dürfen (mindestens 3 Tage, Standard 90).
- Teilen über Bluetooth zulassen – steuert, ob Inhalte aus dem privaten Profil per Bluetooth geteilt werden dürfen. Werte: Nicht spezifiziert (Standard, verhält sich wie Erlaubt), Erlaubt, Unzulässig. Unzulässig setzt Android 8 voraus; auf älteren Geräten wird eine Compliance-Verletzung gemeldet.
- Benutzer können ein privates Bereichsprofil erstellen – erlaubt oder verbietet das Anlegen eines zusätzlichen Private Space-Profils. Werte: Nicht spezifiziert (Standard, verhält sich wie Erlaubt), Erlaubt, Unzulässig. Bei Unzulässig werden bereits vorhandene private Bereiche entfernt.

Für Version 26.4.0

Privater Play Store

- Listenart: Sperrliste oder Positivliste
- Apps auf der Sperrliste bzw. Apps auf der Positivliste – steuert, welche Apps im privaten Profil über den Play Store installiert werden dürfen.

Unterstützung

- COPE Arbeitsprofil (vollständig verwaltetes Gerät mit Arbeitsprofil)

Gerätekennwort

Diese Konfiguration legt die Kennwortanforderungen für die Sperre des gesamten Geräts fest.

Über die Konfiguration Gerätekennwort werden die Anforderungen an die Gerätesperre von Android Enterprise Geräten festgelegt. Die Vorgaben gelten für das gesamte Gerät. Anforderungen an ein eigenes Passwort für das Arbeitsprofil werden dagegen über die Konfiguration Arbeitsprofil-Passwort → definiert.

Abgrenzung zum Arbeitsprofil-Passwort

Beide Konfigurationen verwenden dasselbe Formular für die Kennwortanforderungen, unterscheiden sich aber im Geltungsbereich:

	Gerätekennwort	Arbeitsprofil-Passwort
Geltungsbereich	Gerätesperre (gesamtes Gerät)	Nur das Arbeitsprofil
Badges im Formular	keine	Arbeitsprofil, Persönliches Profil
Vollständig verwaltete Geräte	wird angewendet	wird serverseitig ignoriert
Zusätzliche Optionen	keine	Apps im Arbeitsprofil deaktivieren, bis Anwender die Kennwortanforderungen erfüllen, Separater Passcode für das Arbeitsprofil erforderlich

Beide Konfigurationen können in derselben Richtlinie enthalten sein. Relution überträgt dann beide Anforderungen an das Gerät: eine für das Gerät und eine für das Arbeitsprofil.

Auf vollständig verwalteten Geräten → gibt es kein Arbeitsprofil. Dort wird eine Konfiguration Arbeitsprofil-Passwort nicht übertragen, die Gerätesperre wird ausschließlich über Gerätekennwort gesteuert.

Unterstützte Einschreibungsarten

Das Formular zeigt keine Badges, die Konfiguration ist also für keine Einschreibungsart eingeschränkt. Sie steht für alle Android Enterprise Einschreibungsarten zur Verfügung:

- Verwaltetes Gerät →
- Verwaltetes Gerät mit persönlichem Profil →
- Gerät mit Arbeitsprofil →

Mindestqualität

Mindestgrad an Komplexität, der beim Setzen des Kennworts erfüllt sein muss. Bei einer neuen Konfiguration ist Numerisch vorausgewählt.

Folgende Optionen stehen zur Verfügung:

- Komplex (stark)
  Das Kennwort muss mindestens einen Buchstaben, eine Ziffer und ein Sonderzeichen enthalten. Bei dieser Auswahl erscheinen zusätzlich folgende Pflichtfelder (kleinster zulässiger Wert in Klammern):
  - Minimale Anzahl von Buchstaben (1)
  - Minimale Anzahl von Kleinbuchstaben (0)
  - Minimale Anzahl von Großbuchstaben (0)
  - Minimale Anzahl von Nicht-Buchstaben (0)
  - Minimale Anzahl numerischer Zahlen (1)
  - Minimale Anzahl von Symbolen (1)

  Die Felder sind bei einer neuen Konfiguration nicht vorbelegt. Gespeichert werden kann die Konfiguration erst, wenn alle Felder ausgefüllt sind.

- Alphanumerisch
  Das Kennwort muss Ziffern und Buchstaben (oder Symbole) enthalten.

- Alphabetisch
  Das Kennwort muss Buchstaben (oder Symbole) enthalten.

- Komplex Numerisch
  Das Kennwort besteht aus Ziffern ohne Wiederholungen oder Zahlenfolgen. Das Portal zeigt dazu den Hinweis: „Der Nutzer darf keine Zahlenfolgen verwenden, die sich wiederholen (4444) oder sortiert sind (1234, 4321, 2468).“

- Numerisch
  Das Kennwort muss Ziffern enthalten.

- Muster
  Trotz der Bezeichnung wird kein Entsperrmuster erzwungen. Es muss lediglich eine beliebige Sperre eingerichtet sein (z. B. Muster, PIN oder Kennwort), Vorgaben zum Inhalt gibt es nicht.

- Biometrisch (schwach)
  Das Gerät muss mindestens mit einer biometrischen Entsperrmethode niedriger Sicherheitsstufe geschützt sein. Bei dieser Auswahl werden alle weiteren Felder ausgeblendet.

> Welche Optionen tatsächlich verfügbar und durchsetzbar sind, hängt vom Gerät, der Android-Version und den Herstelleranpassungen ab.

Für Version 26.4.0

Minimale Länge

Legt die minimale Anzahl an Zeichen für das Kennwort fest. Das Feld ist ein Pflichtfeld, vorbelegt mit `4`. Der kleinste zulässige Wert ist ebenfalls `4`.

Maximales Alter (in Tagen)

Anzahl an Tagen, bis ein neues Kennwort gesetzt werden muss. Bei Angabe des Werts `0` läuft das Kennwort nie ab. Das Feld ist ein Pflichtfeld und mit `0` vorbelegt.

Passworthistorie

Anzahl gespeicherter und bereits verwendeter Kennwörter, die nicht erneut verwendet werden dürfen. Das Feld ist ein Pflichtfeld und mit `0` vorbelegt, damit gibt es keine Einschränkung bei der Wiederverwendung.

Anzahl fehlgeschlagener Passwortversuche bevor alle Daten gelöscht werden

Legt fest, nach wie vielen falschen Eingaben die Daten gelöscht werden. Der kleinste zulässige Wert ist `1`. Das Feld ist optional: Kein Wert bedeutet, dass es nie zum Löschen der Daten kommt.

Verhalten bei Nichterfüllung

Für Version 26.4.0

Erfüllt das Gerätekennwort die Anforderungen nicht, meldet das Gerät eine Compliance-Verletzung. Nach welcher Frist das Gerät deswegen gesperrt und zurückgesetzt wird, legt die Konfiguration Durchsetzung der Konformität → in der Zeile Gerätekennwort fest. Diese Zeile gilt für vollständig verwaltete Geräte und verwaltete Geräte mit persönlichem Profil. Auf Geräten mit Arbeitsprofil greift stattdessen die Zeile Arbeitsprofil-Passwort. Ohne eigene Regel gelten die Standardfristen.

Eine Option, Apps bis zur Erfüllung der Anforderungen zu deaktivieren, bietet nur die Konfiguration Arbeitsprofil-Passwort.

Hinweise

- Pro Richtlinie kann die Konfiguration Gerätekennwort nur einmal hinzugefügt werden.
- Nicht alle Optionen sind auf jedem Gerät oder jeder Android-Version im gleichen Umfang verfügbar.
- Die tatsächliche Durchsetzung hängt von Hersteller, Android-Version und Einschreibungsart ab.

Erweiterte Keyguard-Verwaltung

Diese Konfiguration deaktiviert ausgewählte Funktionen des Sperrbildschirms auf verwalteten Geräten.

Über die Konfiguration Erweiterte Keyguard-Verwaltung werden einzelne Funktionen des Sperrbildschirms (Keyguard) von Android Enterprise Geräten deaktiviert, etwa die Kamera, Benachrichtigungen oder biometrische Entsperrmethoden. Die Sperre selbst bleibt dabei bestehen. Anforderungen an das Kennwort der Gerätesperre werden über die Konfiguration Gerätekennwort → festgelegt.

Unterstützte Einschreibungsarten

Das Badge Verwaltetes Gerät im Formular zeigt, dass die Konfiguration für Firmengeräte vorgesehen ist:

- Verwaltetes Gerät →
- Verwaltetes Gerät mit persönlichem Profil →

Für Geräte mit Arbeitsprofil → (BYOD) ist die Konfiguration nicht vorgesehen. Pro Richtlinie kann sie nur einmal hinzugefügt werden.

Deaktiviere Keyguard-Einstellungen

Der Bereich Allgemein enthält je Funktion ein Kontrollkästchen. Bei einer neuen Konfiguration ist keines davon aktiviert. Jedes aktivierte Kontrollkästchen deaktiviert die jeweilige Funktion auf gesicherten Sperrbildschirmen.

Für Version 26.4.0

Option	Wirkung (Hinweistext im Portal)
Deaktiviere alle	Deaktiviert alle jetzigen und zukünftigen Keyguard-Einstellungen
Deaktiviere Biometrie	Deaktiviert alle biometrischen Authentifizierungen auf Keyguard-Bildschirmen
Deaktiviere Kamera	Deaktiviert die Kamera auf Keyguard-Bildschirmen (z. B. PIN-Eingabe)
Fingerabdrucksensor deaktivieren	Deaktiviert den Fingerabdrucksensor auf Keyguard-Bildschirmen
Deaktiviere Benachrichtigungs-Texteingabe	Deaktiviert die Texteingabe in Benachrichtigungen auf Keyguard-Bildschirmen
Gesichtserkennung deaktivieren	Deaktiviert die Gesichtserkennung für die Authentifizierung auf sicheren Keyguard-Bildschirmen
Irisscanner deaktivieren	Deaktiviert den Iris-Scanner für die Authentifizierung auf sicheren Keyguard-Bildschirmen
Deaktiviere Benachrichtigungen	Deaktiviert Benachrichtigungen auf Keyguard-Bildschirmen
Ignoriere Trust Agent-Status	Ignoriert den Trust Agent-Status auf Keyguard-Bildschirmen
Sensible Inhalte bei Benachrichtigungen verbergen	Blendet sensible Inhalte von Benachrichtigungen auf dem Sperrbildschirm aus

Für Version

Wird Deaktiviere alle aktiviert, werden alle übrigen Kontrollkästchen deaktiviert und abgewählt, da sie in dieser Auswahl bereits enthalten sind. Erst nach dem Abwählen von Deaktiviere alle lassen sich die einzelnen Funktionen wieder wählen.

> Ob eine Funktion auf dem Sperrbildschirm tatsächlich vorhanden ist (z. B. Iris-Scanner oder Gesichtserkennung), hängt vom Gerät ab.

Abgrenzung zu Restriktionen

Die Konfiguration Restriktionen → enthält die Option Verbieten, die Tastensperre zu verwenden. Diese Option betrifft die Tastensperre als Ganzes, während Erweiterte Keyguard-Verwaltung nur einzelne Funktionen auf dem Sperrbildschirm abschaltet.

Durchsetzung der Konformität

Diese Konfiguration legt fest, wann nicht konforme Geräte gesperrt und zurückgesetzt werden.

Über die Konfiguration Durchsetzung der Konformität werden Sperr- und Löschaktionen für Android Enterprise Geräte definiert, die bestimmte Vorgaben einer Richtlinie nicht erfüllen. Für jede unterstützte Konfiguration lässt sich festlegen, nach wie vielen Tagen der Nichtkonformität das Gerät gesperrt und anschließend zurückgesetzt wird.

Die Konfiguration steht für alle Android Enterprise Einschreibungsarten zur Verfügung und kann pro Richtlinie nur einmal hinzugefügt werden. Für welche Einschreibungsart eine einzelne Regel greift, hängt von der Zeile ab (siehe unten).

Standardverhalten

Ohne eigene Regel setzt Relution für die überwachten Einstellungen Standardregeln: Nicht konforme Geräte werden nach 20 Tagen gesperrt und nach 30 Tagen gelöscht.

Eigene Regeln können die Fristen nur verkürzen: Für die Sperrung sind höchstens 10 Tage, für das Zurücksetzen höchstens 30 Tage zulässig.

Konfigurationsübersicht

Für Version 26.4.0

Die Tabelle des Formulars enthält immer dieselben vier Zeilen, eine je Konfiguration, deren Nichteinhaltung durchgesetzt werden kann. Die Spalten zeigen die Werte der jeweiligen Regel: Block nach Tagen, Block-Umfang, Werkseinstellungsreset nach Tagen und Schutz von Werkseinstellungsreset beibehalten.

Zeile	Überwachte Einstellungen	Gilt für
Erweiterte Sicherheitsüberschreibungen	Richtlinie zur Geräteverschlüsselung aus Erweiterte Sicherheitsüberschreibungen →	alle Einschreibungsarten
Gerätekennwort	Kennwortanforderungen aus Gerätekennwort → und Arbeitsprofil-Passwort →	vollständig verwaltete Geräte, verwaltete Geräte mit persönlichem Profil
Arbeitsprofil-Passwort	Kennwortanforderungen aus Gerätekennwort → und Arbeitsprofil-Passwort →	Geräte mit Arbeitsprofil
Restriktion	Zulässige Eingabemethoden, Zulässige Barrierefreiheitsdienste und Verbieten, die Tastensperre zu verwenden aus Restriktionen →	alle Einschreibungsarten; Verbieten, die Tastensperre zu verwenden nur auf vollständig verwalteten Geräten

Die Zeilen Gerätekennwort und Arbeitsprofil-Passwort beziehen sich beide auf sämtliche Kennwortanforderungen des Geräts. Welche der beiden Zeilen greift, entscheidet allein die Einschreibungsart.

Über das Kontextmenü einer Zeile stehen zwei Aktionen zur Verfügung:

- Konfigurieren öffnet den Dialog Regel konfigurieren.
- Zurücksetzen entfernt die eigene Regel der Zeile. Danach gilt wieder die Standardregel.

Regel konfigurieren

Jede Regel besteht immer aus einer Sperraktion und einer Löschaktion. Eine Sperrung ohne anschließendes Zurücksetzen lässt sich nicht konfigurieren.

Block-Action

- Block nach Tagen
  Anzahl der Tage, die das Gerät nicht konform sein muss, bevor das Gerät beziehungsweise das Arbeitsprofil gesperrt wird. Vorbelegt ist `10`, zulässig sind Werte von `0` (sofortige Sperrung) bis `10`. Der Wert muss kleiner sein als Werkseinstellungsreset nach Tagen. Mit der Sperrung wird auf dem Gerät eine Benachrichtigung angezeigt, die nach Möglichkeit beschreibt, wie sich die Nichtkonformität beheben lässt.

- Block-Umfang
  Legt fest, worauf sich die Sperrung bezieht. Die Einstellung wirkt nur auf Firmengeräten. Vorausgewählt ist Nicht spezifiziert.

  - Nicht spezifiziert – entspricht Arbeitsprofil.
  - Arbeitsprofil – gesperrt werden nur die Apps im Arbeitsprofil, Apps im persönlichen Profil bleiben nutzbar.
  - Gerät – gesperrt wird das gesamte Gerät einschließlich der Apps im persönlichen Profil.

Für Version 26.4.0

Wipe-Aktion

- Werkseinstellungsreset nach Tagen
  Anzahl der Tage, die das Gerät nicht konform sein muss, bevor es gelöscht wird. Vorbelegt ist `30`, zulässig sind Werte von `0` bis `30`. Firmengeräte werden auf Werkseinstellungen zurückgesetzt, auf Geräten mit Arbeitsprofil (BYOD) wird das Arbeitsprofil entfernt.

- Schutz von Werkseinstellungsreset beibehalten
  Legt fest, ob die Daten des Schutzes vor dem Zurücksetzen auf Werkseinstellungen (Factory Reset Protection, FRP) beim Zurücksetzen erhalten bleiben. Standardmäßig ausgeschaltet. Die Einstellung gilt nicht für Arbeitsprofile.

Durch Klick auf Bestätigen wird die Regel in die Tabelle übernommen. Gespeichert wird sie erst mit der Konfiguration.

Mehrere Richtlinien

Enthalten mehrere Richtlinien eines Geräts die Konfiguration Durchsetzung der Konformität, gilt für jede überwachte Einstellung die Regel der Richtlinie mit der höheren Priorität. Einstellungen ohne eigene Regel behalten die Standardregel.

Globaler Proxy

Diese Konfiguration legt einen netzwerkunabhängigen globalen HTTP-Proxy für verwaltete Geräte fest.

Die Konfiguration Globaler Proxy legt einen HTTP-Proxy fest, der unabhängig vom verbundenen Netzwerk gilt. Sie ist für die Einschreibungsarten Verwaltetes Gerät → und Verwaltetes Gerät mit persönlichem Profil → (COPE) vorgesehen, nicht für Geräte mit Arbeitsprofil → (BYOD).

Das Portal zeigt im Formular folgenden Hinweis an:

> Normalerweise sollten Proxys pro Netzwerk konfiguriert werden. Für ungewöhnliche Konfigurationen wie allgemeine interne Filterung kann jedoch ein globaler HTTP-Proxy sinnvoll sein. Wenn der Proxy nicht erreichbar ist, kann der Netzwerkzugriff ausfallen. Der globale Proxy ist nur eine Empfehlung und wird von einigen Apps möglicherweise ignoriert.

Ein Proxy pro Netzwerk wird in der Konfiguration WLAN → im Abschnitt Proxy Einstellungen hinterlegt.

Proxy-Typ

Das Feld Proxy-Typ bestimmt, wie der Proxy festgelegt wird. Je nach Auswahl werden unterschiedliche Felder angezeigt.

- Direkt – Host, Port und Ausnahmen werden manuell angegeben. Diese Option ist bei einer neuen Konfiguration vorausgewählt.
- PAC-Skript – Der Proxy wird automatisch über ein PAC-Skript konfiguriert.

Für Version 26.4.0

Direkt

- Proxy-Host (Pflichtfeld) – IPv4-Adresse (z. B. `10.0.0.1`) oder URL mit `http://` bzw. `https://` und einem Domainnamen mit Endung in Kleinbuchstaben (z. B. `http://proxy.example.com`), jeweils ohne Port und Pfad. Ein Hostname ohne Protokoll (`proxy.example.com`) oder ohne Domain-Endung (`http://proxy`) wird nicht akzeptiert. Bei ungültiger Eingabe wird das Feld als fehlerhaft markiert und die Konfiguration lässt sich nicht speichern.
- Proxy-Port (Pflichtfeld) – Port des Proxys, zulässig sind Werte von `0` bis `65535`.
- Hosts, für die der Proxy umgangen wird – Liste von Hosts, deren Verbindungen nicht über den Proxy laufen. Hostnamen dürfen Platzhalter wie `*.example.com` enthalten.

> Bei Proxy-Port `0` überträgt Relution keinen globalen Proxy an das Gerät, die Konfiguration bleibt dann wirkungslos.

PAC-Skript

- PAC-Skript URI (Pflichtfeld) – URI des PAC-Skripts, mit dem der Proxy konfiguriert wird. Das Portal erwartet eine gültige URL.

Validierung

Beim Speichern prüft Relution, dass beim Proxy-Typ Direkt ein Proxy-Host und beim Proxy-Typ PAC-Skript eine PAC-Skript URI angegeben ist. Felder des jeweils anderen Proxy-Typs werden nicht an das Gerät übertragen.

Für Version 26.4.0

Gerätekonnektivität

Diese Konfiguration verwaltet die Konnektivitätseinstellungen von Android Enterprise Geräten.

Die Konfiguration Gerätekonnektivität fasst die Einstellungen zu USB-Datenzugriff, WLAN, Tethering, Bluetooth-Freigabe, privatem DNS, WLAN-Roaming, Zugangspunkten (APN) und bevorzugten Netzwerkdiensten zusammen. Für welche Einschreibungsarten und Android-Versionen eine Einstellung gilt, zeigt das Portal als Badge am jeweiligen Feld an; die Angaben sind unten unter Unterstützung aufgeführt.

Bei den Auswahlfeldern ist in einer neuen Konfiguration Nicht spezifiziert vorausgewählt. Ausnahme ist die WLAN-SSID-Beschränkung, bei der die Sperrliste vorausgewählt ist.

Die Konfiguration ersetzt die veralteten Optionen zu WLAN-Konfiguration, USB-Dateiübertragung und Tethering in der Konfiguration Restriktionen. Enthält eine Richtlinie beide Konfigurationen, gelten die Einstellungen der Gerätekonnektivität (siehe Restriktionen →).

USB-Datenzugriff

Steuert, welche Dateien und/oder Daten über USB übertragen werden können. Die Ladefunktion ist davon nicht betroffen.

Optionen:

- Nicht spezifiziert
- USB-Datenübertragung zulassen
- USB-Datenübertragung verbieten
- USB-Dateiübertragung verbieten

Welche Auswirkung Nicht spezifiziert auf die Dateiübertragung per USB hat, beschreibt Dateiübertragung via USB →.

Unterstützung:

- COPE Arbeitsprofil
- Verwaltetes Gerät
- Bei USB-Datenübertragung verbieten zusätzlich Android 12+ und USB HAL 1.3+

WLAN konfigurieren

Steuert, in welchem Umfang Benutzer WLAN-Netzwerke selbst konfigurieren dürfen.

Optionen:

- Nicht spezifiziert
- Konfiguration von WLAN zulassen
- Hinzufügen von WLAN nicht erlauben – unterstützt ab Android 13 auf COPE Arbeitsprofil und Verwaltetem Gerät.
- WLAN Konfiguration nicht erlauben – unterstützt auf COPE Arbeitsprofil und Verwaltetem Gerät.

Für Version 26.4.0

Bei WLAN Konfiguration nicht erlauben zeigt das Portal die Warnung „Das Gerät kann kein WLAN verwenden, sofern keine WLAN-Konfiguration hinzugefügt wird!“ an. Die benötigten Netzwerke werden in diesem Fall über die Konfiguration WLAN → verteilt.

Wi-Fi Direct-Einstellungen

Steuert die Nutzung von Wi-Fi Direct.

Optionen:

- Nicht spezifiziert
- Wi-Fi Direct zulassen
- Wi-Fi Direct nicht zulassen

Unterstützung:

- COPE Arbeitsprofil
- Verwaltetes Gerät
- Android 13+

Tethering-Einstellungen

Für Version 26.4.0

Steuert, in welchem Umfang Benutzer Tethering wie WLAN- oder Bluetooth-Tethering verwenden dürfen.

Optionen:

- Nicht spezifiziert
- Tethering erlauben
- WLAN-Tethering verbieten – unterstützt ab Android 13 auf COPE Arbeitsprofil und Verwaltetem Gerät.
- Jegliches Tethering verbieten – unterstützt auf COPE Arbeitsprofil und Verwaltetem Gerät.

Teilen über Bluetooth

Steuert, ob Inhalte über Bluetooth geteilt werden dürfen.

Optionen:

- Nicht spezifiziert
- Erlaubt
- Unzulässig

WLAN-SSID-Beschränkung

Legt fest, mit welchen WLAN-SSIDs sich das Gerät verbinden darf. Welche Netzwerke auf dem Gerät konfiguriert werden können, wird dadurch nicht beeinflusst.

Optionen:

- Verbindung nur zu folgenden WiFi SSIDs verbieten (vorausgewählt) – Sperrliste. Die SSIDs werden im Feld WiFi SSIDs, mit denen keine Verbindung hergestellt werden kann eingetragen.
- Verbindung nur zu folgenden WiFi SSIDs zulassen – Positivliste. Die SSIDs werden im Feld WiFi SSIDs, mit denen eine Verbindung hergestellt werden kann eingetragen; mindestens ein Eintrag ist Pflicht.

> Bei der Positivliste weist das Portal darauf hin, dass mindestens eine WLAN-SSID verfügbar sein muss, da das Gerät sonst keine Verbindung zu Google oder Relution herstellen kann.

Unterstützung:

- COPE Arbeitsprofil
- Verwaltetes Gerät
- Android 13+

Privates DNS

- Privater DNS-Modus – Konfigurationsmodus für die globalen privaten DNS-Einstellungen des Geräts.
  - Nicht spezifiziert – Standard ist Wahl durch Benutzer.
  - Wahl durch Benutzer – Benutzer dürfen das private DNS selbst konfigurieren.
  - Automatisch – Das Gerät versucht, den vom Netzwerk bereitgestellten DNS-Server über eine verschlüsselte Verbindung zu verwenden, bevor es auf Klartext zurückgreift. Benutzer können die Einstellung nicht ändern.
  - Angegebener Host – Das Gerät verwendet ausschließlich den im Feld Privater DNS-Host angegebenen DNS-Server. Benutzer können die Einstellung nicht ändern.
- Privater DNS-Host – Hostname des DNS-Servers. Das Feld ist nur beim Modus Angegebener Host bearbeitbar und dann erforderlich; ohne Hostname lehnt Relution das Speichern ab.

Für Version 26.4.0

Unterstützung:

- Privater DNS-Modus: Arbeitsprofil, Verwaltetes Gerät
- Privater DNS-Host: Verwaltetes Gerät

WLAN-Roaming

Im Bereich WLAN-Roaming wird über Hinzufügen je SSID eine WLAN-Roaming-Einstellung angelegt:

- SSID (Pflichtfeld) – Netzwerkname, für den die Einstellung gilt. Pro SSID ist nur eine Einstellung möglich.
- WLAN-Roaming-Modus – Standard (vorausgewählt), Deaktiviert oder Aggressiv.

Unterstützung:

- Verwaltetes Gerät
- COPE Arbeitsprofil
- Android 15+

APN

Der Bereich Zugangspunktname - Access Point Name (APN) verwaltet Mobilfunk-Zugangspunkte.

Override-APNs aktivieren

Optionen: Nicht spezifiziert, Deaktiviert, Aktiviert. Unterstützt auf Verwaltetem Gerät ab Android 10.

APN-Einstellungen

Über Hinzufügen wird eine APN-Einstellung angelegt. Das Portal weist im Dialog darauf hin, dass für die Verwendung in einem Arbeitsprofil nur der APN-Typ Enterprise ausgewählt werden sollte. Eine APN-Einstellung mit gleichem Namen oder gleichem APN wie eine vorhandene wird nicht übernommen.

Für Version 26.4.0

Feld	Beschreibung
APN-Typen	Pflichtfeld, Mehrfachauswahl: Enterprise (Android 13+), Bearer Independent Protocol (BIP) (Android 12+), Carrier Branded Services (CBS), Standard, Dial-up Networking (DUN), Notfall, Firmware Over-the-Air (FOTA), Hohe Priorität (HiPri), Initial Attach (IA), IP Multimedia Subsystem (IMS), Einsatzkritischer Dienst - Mission Critical Service (MCX), Multimedia-Mitteilungsdienst (MMS), Rich Communication Services (RCS) (Android 15+), Sicherer Standort der Benutzerebene (SUPL), Virtuelle SIM (VSIM) (Android 12+), XML-Konfigurationszugriffsprotokoll (XCAP) (Android 11+)
Name	Pflichtfeld, Anzeigename der APN-Einstellung
APN	Pflichtfeld, Name des Zugangspunkts
Numerische Operator-ID	Optional
Carrier ID	Optional, Wert ab `0`
Authentifizierungstyp	Nicht spezifiziert, Keine, PAP, CHAP, PAP oder CHAP
Benutzername, Passwort	Optional
Proxy-Adresse, Proxy-Port	Optional, Port ab `0`
Server-Adresse (MMSC)	Optional
MMS Proxy-Adresse, MMS Proxy Port	Optional, Port ab `0`
Protokoll, Roaming-Protokoll	Nicht spezifiziert, IP, IPv4/IPv6, IPv6, Nicht-IP, Point to point (PPP), Unstrukturiert
Netzwerktypen	Mehrfachauswahl: EDGE, GPRS, GSM, HSDPA, HSPA, HSPAP, HSUPA, IWLAN, LTE, NR (New Radio) 5G, TD_SCDMA, UMTS
Aktivieren der Always-on-PDU-Sitzung	Nicht spezifiziert, Nicht immer an, Immer an (Android 15+)
MVNO Typ	Nicht spezifiziert, Gruppenidentifikator Stufe 1 (GID), Integrated Circuit Card Identifier (ICCID), Internationale Mobilfunk-Teilnehmerkennung (IMSI), Dienstleistername (SPN)
MTU v4, MTU v6	Optional, Wert ab `0` (Android 13+)

Bevorzugte Netzwerkdienste

Der Bereich Einstellungen für bevorzugte Netzwerkdienste ordnet Apps dedizierten Unternehmens-Netzwerk-Slices zu, etwa 5G-Enterprise-Slices.

- Standard-Netzwerk-ID für bevorzugten Netzwerkdienst – gilt für Apps ohne eigene Konfiguration. Optionen: Nicht spezifiziert (vorausgewählt), Kein bevorzugtes Netzwerk, Bevorzugtes Netzwerk 1 bis Bevorzugtes Netzwerk 5. Ein hier gewähltes bevorzugtes Netzwerk muss auch in der Liste der Konfigurationen enthalten sein.

Unter Konfigurationen für bevorzugte Netzwerkdienste wird über Hinzufügen je Netzwerk-ID eine Konfiguration angelegt:

- Bevorzugte Netzwerk-ID (Pflichtfeld) – Bevorzugtes Netzwerk 1 bis Bevorzugtes Netzwerk 5. Jede ID kann nur einmal verwendet werden.
- Fallback auf Standardverbindung – ob die App auf die Standardverbindung zurückfallen darf, wenn das bevorzugte Netzwerk nicht verfügbar ist. Optionen: Nicht spezifiziert, Erlaubt, Unzulässig.
- Nutzung anderer Netzwerke – ob die App Netzwerke verwenden darf, die nicht den Kriterien des bevorzugten Netzwerkdiensts entsprechen. Optionen: Nicht spezifiziert, Erlaubt, Unzulässig (Android 14+).

Ist Nutzung anderer Netzwerke auf Unzulässig gesetzt, muss auch Fallback auf Standardverbindung auf Unzulässig stehen. Enthält die Liste keine Konfiguration, überträgt Relution für diesen Bereich nichts an das Gerät, auch keine Standard-Netzwerk-ID.

Unterstützung:

- Android 13+
- Verwaltetes Gerät
- Arbeitsprofil

Für Version 26.4.0

Zertifikat

Diese Konfiguration installiert ein CA-Zertifikat oder ein Zertifikat mit privatem Schlüssel auf dem Gerät.

Die Konfiguration Zertifikat verteilt ein Zertifikat aus der Relution-Zertifikatsverwaltung, ein über eine Zertifikatsvorlage ausgestelltes Zertifikat oder das Benutzerzertifikat des zugewiesenen Benutzers auf Android Enterprise Geräte. Eine Richtlinie kann mehrere Zertifikat-Konfigurationen enthalten.

Die Installation übernimmt die Relution Companion-App, der Relution dafür die Berechtigung zum Installieren von Zertifikaten erteilt (siehe Companion & Daemon →).

Allgemein

Im Bereich Allgemein wird festgelegt, welches Zertifikat installiert wird.

- Ausgewähltes Zertifikat oder Vorlage (vorausgewählt) – Über das Feld Zertifikat oder Zertifikatsvorlage öffnet Auswählen den Dialog Zertifikat oder Zertifikatsvorlage auswählen. Dort steht auf dem Reiter Zertifikate ein hochgeladenes Zertifikat und auf dem Reiter Zertifikatsvorlagen eine Zertifikatsvorlage zur Wahl. Zur Auswahl stehen Zertifikate in den Formaten PKCS#1 und PKCS#12. Ohne Auswahl kann die Konfiguration nicht gespeichert werden.
- Benutzerzertifikat für VPN und Apps – Statt eines festen Zertifikats wird das Zertifikat installiert, das im Profil des dem Gerät zugewiesenen Benutzers unter VPN und Apps hinterlegt ist.
    - Zertifikatsname – Wählt ein bestimmtes Zertifikat anhand des Namens aus, wenn der Benutzer mehrere Zertifikate dieses Typs besitzt. Das Feld kann Platzhalter enthalten, die pro Gerät aufgelöst werden (siehe Erweiterte Platzhalter →). Bleibt es leer, wird das Zertifikat mit der längsten Gültigkeit verwendet.

Für Version 26.4.0

Zertifikate im Format PKCS#1 werden als CA-Zertifikat installiert, PKCS#12-Container als Zertifikat mit privatem Schlüssel.

Hintergrund zu den Zertifikatsquellen:

- Zertifikatsverwaltung →
- Built-In CA →
- Zertifikatspool →

Alias des Zertifikats

Der Alias wird automatisch erzeugt, sobald ein Zertifikat, eine Vorlage oder die Option Benutzerzertifikat für VPN und Apps gewählt ist, und kann nicht bearbeitet werden. Über das Kopiersymbol wird er in die Zwischenablage übernommen.

Das Portal beschreibt den Zweck so: Wenn für eine verwaltete Konfiguration ein Zertifikatalias erforderlich ist, wird dieser Wert verwendet, um auf diese Konfiguration zu verweisen.

Damit der Alias auf dem Gerät eindeutig bleibt, übergibt Relution ihn an die Companion-App um die hexadezimale Seriennummer des Zertifikats in Klammern ergänzt.

Verhalten bei fehlendem Benutzerzertifikat

Besitzt der dem Gerät zugewiesene Benutzer kein passendes Benutzerzertifikat, überträgt Relution die übrigen Konfigurationen der Richtlinie trotzdem. Das Zertifikat wird dann nicht installiert und der Vorgang im Serverlog als Warnung protokolliert.

Für Version 26.4.0

Bildschirm

Diese Konfiguration verwaltet die Anzeigeeinstellungen eines verwalteten Android Enterprise Geräts.

Die Konfiguration Bildschirm legt fest, ob Helligkeit und Bildschirm-Timeout auf dem Gerät vom Benutzer gewählt werden oder fest vorgegeben sind. Im Portal ist die Konfiguration mit dem Einschreibungsmodus Verwaltetes Gerät gekennzeichnet; sie wirkt auf vollständig verwalteten Geräten und auf verwalteten Geräten mit persönlichem Profil (COPE), nicht auf Geräten mit Arbeitsprofil (BYOD). Pro Richtlinie kann sie nur einmal hinzugefügt werden.

Beide Einstellungen stehen im Abschnitt Allgemein und sind jeweils zweistufig aufgebaut: Ein Auswahlfeld bestimmt den Modus, ein eingerücktes Feld darunter den Wert. Das Wertfeld ist nur bearbeitbar, wenn der gewählte Modus einen Wert benötigt.

Helligkeit

Die Helligkeit wird über zwei Felder gesteuert: den Modus und den Helligkeitswert.

Helligkeit konfigurieren

Bestimmt, wie die Bildschirmhelligkeit gesteuert wird.

Optionen:

- Vom Benutzer konfiguriert – Die Helligkeit wird auf dem Gerät eingestellt. Diese Option ist bei einer neuen Konfiguration vorausgewählt.
- Adaptive Helligkeit – Die Helligkeit wird adaptiv geregelt; zusätzlich wird ein Wert im Feld Bildschirmhelligkeit übermittelt.
- Feste Helligkeit – Die Helligkeit wird auf den Wert im Feld Bildschirmhelligkeit festgelegt.

Für Version 26.4.0

Bildschirmhelligkeit

Pflichtfeld, sobald unter Helligkeit konfigurieren die Option Adaptive Helligkeit oder Feste Helligkeit gewählt ist. Bei Vom Benutzer konfiguriert ist das Feld gesperrt und es wird kein Helligkeitswert an das Gerät übertragen.

Der Hinweistext im Portal lautet: „Die Bildschirmhelligkeit kann auf einer Skala von 1 bis 255 konfiguriert werden, wobei 255 die maximale Helligkeit ist“. Werte außerhalb dieses Bereichs werden nicht angenommen; ein Standardwert ist nicht vorbelegt.

Bildschirm-Timeout

Der Bildschirm-Timeout wird ebenfalls über zwei Felder gesteuert: den Modus und die Zeitspanne.

Bildschirm-Timeout konfigurieren

Bestimmt, ob die Zeit bis zum Abschalten des Bildschirms vorgegeben wird.

Optionen:

- Vom Benutzer konfiguriert – Der Timeout wird auf dem Gerät eingestellt. Diese Option ist bei einer neuen Konfiguration vorausgewählt.
- Feste Zeitüberschreitung – Der Timeout wird auf den Wert im Feld Bildschirm-Timeout festgelegt.

Dauer des Bildschirm-Timeouts

Das Feld Bildschirm-Timeout ist nur bei Feste Zeitüberschreitung bearbeitbar. Zur Auswahl stehen 15 Sekunden, 30 Sekunden, 1 Minute, 2 Minuten, 5 Minuten und 10 Minuten; vorausgewählt sind 30 Sekunden.

> Enthält die Richtlinie zusätzlich eine Kiosk-Modus →-Konfiguration mit einem Wert für Maximale Zeit bis zum Sperren des Gerätes, übermittelt Relution den festen Bildschirm-Timeout nur, wenn dieser kürzer ist als die maximale Zeit bis zum Sperren. Andernfalls wird nur der Modus ohne Timeout-Wert übertragen.

Unterstützung

- Verwaltetes Gerät →
- Verwaltetes Gerät mit persönlichem Profil → (COPE)
- Nicht verfügbar für Geräte mit Arbeitsprofil → (BYOD)

Für Version 26.4.0

Bevorzugte Aktivitäten

Diese Konfiguration verwaltet, welche App standardmäßig für einen bestimmten Vorgang verwendet werden soll.

Die Konfiguration Bevorzugte Aktivitäten ordnet Android-Vorgängen (Intents) eine bestimmte App zu. Jeder Eintrag besteht aus einer App sowie optional einer Aktivität, Kategorien und Aktionen; Android verwendet für passende Vorgänge dann dauerhaft diese App. Im Portal ist die Konfiguration mit keinem bestimmten Einschreibungsmodus gekennzeichnet. Pro Richtlinie kann sie nur einmal hinzugefügt werden.

Die Konfiguration installiert die gewählte App nicht. Die Installation erfolgt separat, z. B. über Apps verwalten →. Ein vollständiges Anwendungsbeispiel – der Relution Homescreen als Standard-Launcher – steht im Artikel Homescreen als Standard-Launcher →. Für typische Standard-Apps wie Browser oder Telefon bietet die Konfiguration Standard-Anwendungen → eine eigene Auswahl.

Liste der Apps

Die Konfiguration zeigt eine Liste mit den Spalten Name, Bundle identifier, Aktivität, Aktionen und Kategorien. In den Spalten Aktionen und Kategorien wird jeweils nur der letzte Namensteil angezeigt (z. B. `HOME` für `android.intent.category.HOME`).

Über Hinzufügen wird ein neuer Eintrag angelegt. Über das Kontextmenü eines Eintrags lassen sich Bearbeiten und Löschen aufrufen; mehrere markierte Einträge werden über das Kontextmenü der Liste gelöscht. Jede App kann nur einmal in der Liste stehen: In der Auswahl aus dem Relution App Store sind bereits eingetragene Apps ausgeschlossen, und wird eine bereits eingetragene App auf anderem Weg erneut hinzugefügt, ersetzt der neue Eintrag den bisherigen. In einer bereits veröffentlichten Richtlinienversion ist die Liste schreibgeschützt.

Für Version 26.4.0

App auswählen

Der Dialog Aktivität führt in drei Schritten durch das Anlegen eines Eintrags. Im ersten Schritt wird die Quelle der App gewählt:

- Relution App Store App – App aus dem Relution App Store auswählen. Angeboten werden native und öffentliche Apps für Android und Android Enterprise.
- Managed Google Play Store App (Android Enterprise) – Kostenlose App im verwalteten Google Play Store über Android Enterprise suchen. Diese Quelle steht nur zur Verfügung, wenn Android Enterprise für die Organisation eingerichtet ist.
- App manuell hinzufügen – Name und Identifier manuell hinzufügen. Dabei sind die Felder Name und Interner Name Pflichtfelder; als interner Name wird der Paketname eingetragen (Beispiel im Portal: `com.mwaysolutions.relution`).

Im zweiten Schritt wird die App ausgewählt bzw. werden die Angaben für die manuelle App eingetragen.

Aktivität, Kategorien und Aktionen

Im dritten Schritt werden die Details des Eintrags festgelegt. Beim nachträglichen Bearbeiten eines Eintrags erscheinen nur diese Felder; die App selbst bleibt unverändert.

- Aktivität – optionaler Klassenname der Aktivität innerhalb der App, z. B. `io.relution.homescreen.MainActivity`. Ist das Feld gefüllt, übermittelt Relution `Paketname/Aktivität` als Ziel; bleibt es leer, wird nur der Paketname übermittelt.
- Kategorien – Liste von Intent-Kategorien, z. B. `android.intent.category.HOME`. Die Eingabe schlägt die Standardkategorien von Android zur Auswahl vor; eigene Werte sind möglich.
- Aktionen – Liste von Intent-Aktionen, z. B. `android.intent.action.MAIN`. Auch hier werden die Standardaktionen von Android vorgeschlagen.

Kategorien und Aktionen sind keine Pflichtfelder. Ein Hinweis im Dialog verweist für Details zu den Standardkategorien und Aktionen auf die Google-Dokumentation →.

Für Version 26.4.0

Standort-Modus

Diese Konfiguration legt fest, wie die Standorteinstellung auf einem verwalteten Android Enterprise Gerät gehandhabt wird.

Die Konfiguration Standort-Modus steuert die Standorteinstellung (Ortungsdienste) des Geräts. Im Portal ist sie mit dem Einschreibungsmodus Verwaltetes Gerät gekennzeichnet; sie wirkt auf vollständig verwalteten Geräten und auf verwalteten Geräten mit persönlichem Profil (COPE), nicht auf Geräten mit Arbeitsprofil (BYOD). Pro Richtlinie kann sie nur einmal hinzugefügt werden.

Wie sich die Einstellung zusammen mit App-Berechtigungen für den Standort auswirkt, beschreibt der Artikel Standort Dienste →.

Standorteinstellungen auf dem Gerät

Das Auswahlfeld Standorteinstellungen auf dem Gerät im Abschnitt Allgemein ist die einzige Einstellung der Konfiguration.

Optionen:

- Wahl durch Benutzer – Die Standorteinstellung wird nicht eingeschränkt. Diese Option ist bei einer neuen Konfiguration vorausgewählt.
- Standorteinstellung auf dem Gerät aktivieren – Die Standorteinstellung wird auf dem Gerät aktiviert.
- Deaktiviert – Die Standorteinstellung wird auf dem Gerät deaktiviert.

Der gewählte Wert wird zusätzlich an die Relution-Apps auf dem Gerät (z. B. den Relution Agent) übergeben.

Für Version 26.4.0

Hinweis zu Arbeitsprofilen

Im Formular blendet das Portal folgenden Hinweis ein:

> Ab Android 11 können Arbeitsprofile auf unternehmenseigenen Geräten Standortdienste nicht direkt erzwingen. Die Konformität kann erst wiederhergestellt werden, wenn der Benutzer die Standortdienste manuell über die Einstellungs-App des Geräts aktiviert oder deaktiviert.

Unterstützung

- Verwaltetes Gerät →
- Verwaltetes Gerät mit persönlichem Profil → (COPE), mit der Einschränkung aus dem Hinweis zu Arbeitsprofilen →
- Nicht verfügbar für Geräte mit Arbeitsprofil → (BYOD)

Samsung Classroom Management

Diese Konfiguration verteilt und konfiguriert die Samsung Classroom Management App für den Unterricht.

Die Konfiguration Samsung Classroom Management richtet die gleichnamige App für den Unterricht auf Android Enterprise Geräten ein. Im Portal ist sie mit keinem bestimmten Einschreibungsmodus gekennzeichnet. Pro Richtlinie kann sie nur einmal hinzugefügt werden. Für Samsung Classroom Management ist eine separate Lizenz erforderlich (siehe Teacher →).

Verhalten auf dem Gerät

Enthält eine Richtlinie diese Konfiguration, ergänzt Relution die Geräterichtlinie automatisch:

- Die App Samsung Classroom Management (`com.tabnova.classroomapp`) wird mit erzwungener Installation verteilt; ihre Laufzeitberechtigungen werden gewährt. Eine verwaltete Konfiguration für dieselbe App aus Apps verwalten → wird dabei durch die Werte dieser Konfiguration ersetzt.
- Die Klassen, denen der Benutzer des Geräts angehört, werden samt Lehrkräften und Schülern an die App übergeben. Klassen werden unter `Bildung` → `Klassen` gepflegt (siehe Bildungsfunktion →).
- Ist der Benutzer des Geräts in mindestens einer Klasse als Lehrkraft eingetragen, wird zusätzlich die Relution Teacher App (`io.relution.teacher`) mit erzwungener Installation verteilt.
- Als Land wird das in der Adresse der Organisation hinterlegte Land übergeben, ohne Angabe `Deutschland`.

Für Version 26.4.0

Allgemein

- Abonnementcode – Pflichtfeld. Code des Samsung-Classroom-Abonnements, mit dem die App freigeschaltet wird.
- Benutzername – Name, unter dem das Gerät in der App geführt wird. Vorbelegt mit dem Platzhalter `${user.name}`. Die App zeigt nur die Klassen an, in denen ein Mitglied mit genau diesem Namen eingetragen ist; der Wert sollte daher dem Relution-Benutzernamen entsprechen. Unterhalb des Formulars blendet das Portal die verfügbaren Benutzer- und Geräte-Platzhalter ein (siehe Erweiterte Platzhalter →).
- Name der Schule – optional. Bleibt das Feld leer, wird der Name der Organisation übergeben.
- Standard-Webfilterliste anwenden (`https://school.tabnova.com/block.list`) – aktiviert die Standard-Sperrliste von Samsung Classroom. Standardmäßig ausgeschaltet.
- URL der benutzerdefinierten Web-Filterliste – optional. Adresse einer eigenen Sperrliste.

Aufräumen nach dem Unterricht

Dieser Abschnitt legt fest, was nach dem Unterricht auf dem Gerät zurückgesetzt wird.

- Auslöser – Kontrollkästchen Neustart und Abmeldung; beide können gleichzeitig gewählt werden. Bei einer neuen Konfiguration ist keines ausgewählt.
- Cookies löschen – löscht die Browser-Cookies. Bei einer neuen Konfiguration eingeschaltet.
- Zu löschende Dateien und Ordner – Liste von Datei- und Ordnernamen, z. B. `Downloads` oder `DCIM`.

Zu löschende Apps

Die Liste enthält Apps, deren Daten nach dem Unterricht gelöscht oder die deinstalliert werden. Über Hinzufügen werden kostenlose öffentliche Apps aus dem Relution App Store oder aus Managed Google Play ausgewählt; eine bereits enthaltene App wird nicht doppelt aufgenommen.

Je App stehen zwei Kontrollkästchen zur Verfügung:

- Daten löschen – die App-Daten werden gelöscht.
- Deinstallieren – die App wird deinstalliert.

Beim Hinzufügen einer App sind beide Kontrollkästchen aktiviert. Über Löschen werden markierte Apps wieder aus der Liste entfernt.

Für Version 26.4.0

Standard-Anwendungen

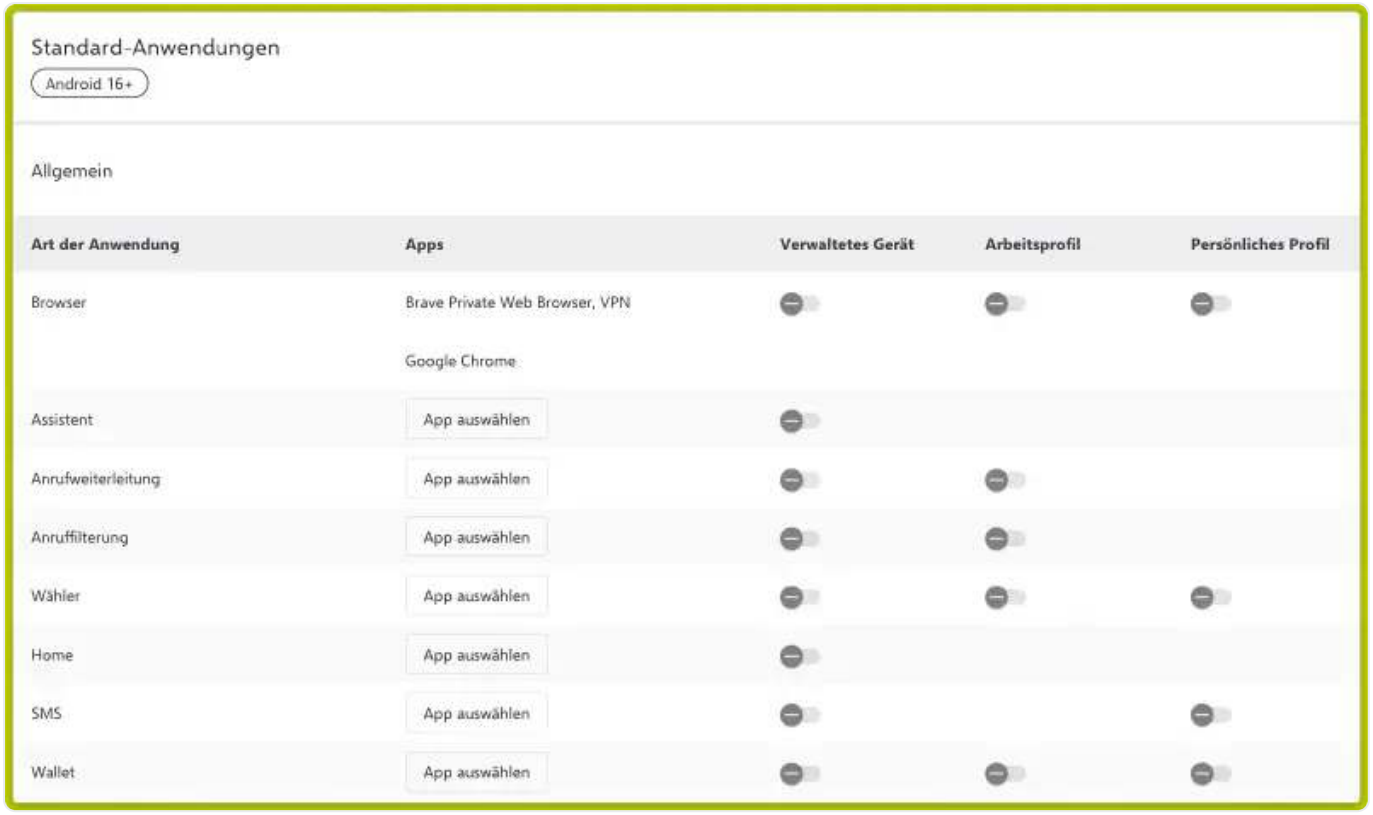
Mit dieser Richtlinie können Administratoren Standard-Apps für spezifische Funktionen auf verwalteten Android-Geräten festlegen.

Die Richtlinie Standard-Anwendungen ermöglicht es Administratoren, Standard-Apps für verschiedene Funktionen auf Android-Geräten festzulegen. Diese Einstellungen sind besonders nützlich, um die Benutzererfahrung zu standardisieren und sicherzustellen, dass nur genehmigte Anwendungen verwendet werden.

Diese Funktion ist für Geräte mit Android 16+ verfügbar.

Konfigurierbare Funktionen

In der Tabelle können Administratoren Standard-Apps für die folgenden Funktionen konfigurieren:



Art der Anwendung	Apps	Verwaltetes Gerät	Arbeitsprofil	Persönliches Profil
Browser	Brave, Google Chrome	✅		
Assistent	App auswählen			
Anrufweiterleitung	App auswählen			
Anruffilterung	App auswählen			
Wähler	App auswählen			
Home	App auswählen			
SMS	App auswählen			
Wallet	App auswählen			✅

Für Version 26.4.0

Konfigurationsoptionen

- Apps auswählen: Administratoren können die gewünschte Standard-App für jede Funktion auswählen.
- Verwaltetes Gerät: Die Konfiguration für vollständig verwaltete Geräte aktivieren oder deaktivieren.
- Arbeitsprofil: Die Konfiguration für das Arbeitsprofil aktivieren oder deaktivieren.
- Persönliches Profil: Die Konfiguration für das persönliche Profil aktivieren oder deaktivieren.

> Standard-Apps, die für Verwaltetes Gerät oder Arbeitsprofil festgelegt sind und in keiner App-Konfiguration der Richtlinie enthalten sind, stellt Relution automatisch mit dem Installationstyp Verfügbar bereit. Sie werden dadurch nicht automatisch installiert. Damit eine Standard-App sicher installiert ist, wird sie zusätzlich über die Konfiguration Apps verwalten hinzugefügt, z. B. mit Installation erzwungen. Ist eine der Standard-Apps dort auf Blockiert gesetzt, schlägt die Konfiguration fehl.

Hinweis zu mehreren Standard Apps

Für dieselbe Funktion lassen sich mehrere Apps auswählen, z. B. wie oben gezeigt Brave und Google Chrome als Browser. Sind mehrere dieser Apps auf dem Gerät installiert, verwendet Android die erste App der Liste. Maßgeblich ist die Reihenfolge, die nach dem Speichern und erneuten Öffnen der Konfiguration angezeigt wird. Sie entspricht nicht unbedingt der Reihenfolge der Auswahl und lässt sich derzeit nicht manuell ändern.

Samsung Knox

Relution unterstützt Samsung Knox, um erweiterte Sicherheits- und Verwaltungsfunktionen für Samsung-Geräte bereitzustellen. Knox-Richtlinien können geräteweit oder im Arbeitsprofil angewendet werden und sind je nach Gerätemodus (Device Owner oder Work Profile) verfügbar.

Das Samsung Knox Service Plugin wird automatisch auf Geräten bereitgestellt, auf denen die Knox Richtlinie über Relution verteilt wurde.
Folgende Funktionen sind über dieses Plugin möglich:

Funktionsübersicht

Über das Plugin stehen folgende Funktionsbereiche zur Verfügung:

Profileinstellungen

- Profilname und Version
- Knox Lizenzschlüssel (z. B. Knox Suite, DualDAR)
- Debug Mode aktivieren/deaktivieren

App- und Richtlinienverwaltung

- Getrennte App-Richtlinien (Work Profile vs. Device Owner)
- Geräteeinstellungen (z. B. Kamera, Quick Panel, Firmware-Update)
- Arbeitsprofilrichtlinien (Profile Owner)
- App-Zuweisungen für den Zugriff auf das Knox SDK

Netzwerk & Sicherheit

- Erweiterte Wi-Fi Konfigurationen *(Premium)*
- APN-Profile
- VPN-Profile *(Premium)*
- Firewall-Profile
- Proxy-Profile (manuell oder PAC)

Zertifikate & Schlüssel

- Zertifikatsverwaltung *(Premium)*
- Bereitstellung von Zertifikaten
- Erlaubte Apps zum Zugriff auf private Schlüssel *(Premium)*
- UCM-Plugin Konfigurationen *(Premium)*

Für Version 26.4.0

Gerätekonfiguration & Anpassung

- Gerätekonten und Richtlinien
- Geräte- und Einstellungsanpassungen *(Premium)*
- Key Mapping für App-Starts
- DeX-Anpassungen *(Premium)*
- Peripherie-Konfigurationen
- USB-Geräte-Whitelist

Erweiterte Profile

- NPA Data Points *(Premium)*
- RCP Data Sync *(Premium)*
- Berechtigungssteuerungen für Apps

Verhalten in Relution

- Die Konfiguration erfolgt im Editor für verwaltete App-Konfigurationen des Knox Service Plugin.
- Eine Knox-Konfiguration hat Vorrang vor einer Konfiguration des Knox Service Plugin in der Konfiguration Apps verwalten und überschreibt diese.
- Enthält die Konfiguration Apps verwalten derselben Richtlinienversion bereits eine Konfiguration des Knox Service Plugin, wird sie beim Anlegen der Knox-Konfiguration übernommen. Das Formular zeigt dazu einen Hinweis an.
- Platzhalter für Benutzer, Gerät und Zertifikate werden unterstützt.
- Meldet das Plugin Fehler, wird die Knox-Konfiguration in den Gerätedetails mit dem gelben Status Benachrichtigung statt als Verstoß (Verletzt) angezeigt. Ohne Fehler lautet der Status Behoben. Die Rückmeldungen des Plugins sind dort einsehbar.
- Wird die Knox-Konfiguration aus der Richtlinie entfernt, bleibt das Knox Service Plugin auf Geräten, auf denen es bereits installiert ist, erzwungen installiert und erhält eine leere Konfiguration. Das gilt auch dann, wenn das Plugin in Apps verwalten blockiert ist.

Für Version 26.4.0

Hinweise

- Viele Funktionen sind nur auf Knox-fähigen Samsung-Geräten verfügbar. Eine Übersicht unterstützter Geräte bietet die Samsung Knox Support-Seite →.
- Einige erweiterte Optionen erfordern eine gültige Knox Premium Lizenz.
- Vor Rollout empfiehlt sich ein Test mit Pilotgeräten, da sich Knox- und Android-Enterprise-Richtlinien überschneiden können.

App Verteilung

Unternehmen entscheiden sich immer öfter, bestimmte Arbeitsprozesse mit einer mobilen App zu unterstützen. Schnell stellt sich die Frage, wie diese App an die Nutzer verteilt werden soll. Oftmals sieht der Anwendungsfall so aus, dass nicht nur Mitarbeiter, sondern auch externe Personen die App bekommen sollen – dazu können zum Beispiel Dienstleister, Partner oder Kunden gehören. Diese App ist in den meisten Fällen auch explizit nicht für einen breiten Kundenkreis gedacht, sondern richtet sich an ausgewählte professionelle Benutzer.

Methode	Zielgruppe	Account-Voraussetzung
Apple App Store	breite Öffentlichkeit	Apple-ID
Google Play Store	breite Öffentlichkeit	Google-Konto
Apple TestFlight	ausgewählte Benutzer (Beta)	Apple-ID
Google Alpha-/Beta-Testing	ausgewählte Benutzer (Beta)	Google-ID
Interner Enterprise App Store	bekannter, definierter Nutzerkreis (z. B. Mitarbeiter, Partner)	keine, sofern über MDM verteilt

Für Version 2

Verteilung über öffentliche App Stores

Apple und Google stellen zur Verteilung von Apps jeweils eine Infrastruktur zur Verfügung. Bei Apple werden Apps für Endanwender über den Apple App Store bereitgestellt. Die Verwaltung und die Veröffentlichung von Apps erfolgen hierfür über das Developer-Portal und App Store Connect.

Bei Google werden Apps für Endanwender über den Play Store bereitgestellt. Auf jedem Android Gerät ist die App Play Store vorinstalliert. Die Verwaltung und die Veröffentlichung von Apps erfolgt hierfür über das Developer-Portal. Apple und Google definieren die Rahmenbedingungen für die Veröffentlichung von Apps über ihre Systeme.

Sofern ein Gerät über ein MDM System verwaltet wird, kann die Store App für Benutzer auch gesperrt werden und steht somit unter Umständen für Endanwender nicht zur Verfügung.

Verteilung über Apple App Store

Vorteile

- Apps stehen für Endanwender über den Standard-Mechanismus von Apple zur Verfügung.
- Apps müssen nicht nach einem Jahr mit einem aktualisierten Provisioning Profile neu signiert und bereitgestellt werden.
- Apps können – sofern notwendig – selektiv für einzelne Länder freigeschaltet bzw. gesperrt werden.
- Apps können – sofern gewünscht – in definierten Strukturen kostenpflichtig angeboten werden (Apple verlangt hierfür eine prozentuale Provisionsgebühr von 15%).
- Apple stellt die Infrastruktur für die Verteilung und Abrechnung bereit.

Nachteile

- Benutzer benötigen eine Apple-ID auf den Endgeräten, um Apps aus dem Apple App Store zu installieren.
- Bei Unternehmenskunden mit verwalteten Geräten ist der Apple App Store unter Umständen per MDM gesperrt.
- Es müssen sämtliche Apple Vorgaben eingehalten werden, wie beispielsweise Unterstützung neuer Geräteklassen wie iPhone X.
- Apple behält sich in einem Review vor, die App nicht zu veröffentlichen bzw. nachträglich zu entfernen.
- Durch den Review kann es zu Verzögerungen von bis zu 10 Tagen kommen (derzeit liegt die durchschnittliche Review Dauer bei etwa 3 Arbeitstagen).
- Apps können nur stark eingeschränkt ausgewählten Benutzergruppen bereitgestellt werden.

Verteilung über Google Play Store

Vorteile

- Apps stehen für Endanwender über den Standard-Mechanismus von Google zur Verfügung
- Apps können – sofern notwendig – selektiv für einzelne Länder freigeschaltet bzw. gesperrt werden.
- Apps können – sofern gewünscht – in definierten Strukturen kostenpflichtig angeboten werden (Google verlangt hierfür eine prozentuale Provisionsgebühr von 15%).
- Google stellt die Infrastruktur für die Verteilung und Abrechnung bereit.

Für Version 26.4.0

Nachteile

- Benutzer benötigen einen Google Account, um Apps aus dem Play Store zu installieren
- Bei Unternehmenskunden mit verwalteten Geräten ist der Play Store unter Umständen per MDM gesperrt.
- Es müssen sämtliche Google Vorgaben eingehalten werden.
- Google behält sich nach automatisierten App-Scans vor, die App auch nachträglich aus dem Store zu entfernen.
- Durch technische Scans kann sich die Veröffentlichung von Apps um wenige Stunden verzögern.
- Apps können nur stark eingeschränkt ausgewählten Benutzergruppen bereitgestellt werden.

Verteilung über Beta-Programme der öffentlichen App Stores

Apple und Google bieten zusätzlich zur Verteilung von öffentlichen Apps jeweils auch ein Beta-Testprogramm an. Bei Apple werden Apps für einen Beta-Test für Endanwender über die TestFlight App bereitgestellt. Auf iOS-Geräten kann diese App aus dem Apple Store App nachinstalliert werden.

Die Verwaltung und die Veröffentlichung von Apps erfolgen hierfür über das Developer-Portal und App Store Connect im Bereich TestFlight. Bei Google werden Apps für einen Alpha- oder Beta-Test über den Play Store bereitgestellt. Auf jedem Android Gerät ist der Play Store vorinstalliert.

Die Verwaltung und die Veröffentlichung von Apps erfolgen hierfür über das Developer-Portal im Bereich Alpha- und Beta-Testing. Apple und Google definieren die Rahmenbedingungen für die Veröffentlichung von Apps über ihre Systeme.

Verteilung über Apple Testflight

Vorteile

- Apps stehen für Benutzer über einen von Apple bereitgestellten Mechanismus zur Verfügung.
- Apps können selektiv für einzelne Benutzer freigeschaltet werden.
- Apple stellt die Infrastruktur für die Verteilung und Abrechnung bereit.

Nachteile

- Benutzer benötigen eine Apple-ID, um Apps aus dem Apple App Store zu installieren.
- Für die Installation der App ist die einmalige Installation der TestFlight App notwendig.
- Apple behält sich in einem „reduzierten“ Review vor, die App nicht zu veröffentlichen.
- Durch den Review kann es zu Verzögerungen von bis zu 10 Tagen kommen (derzeit liegt die durchschnittliche Review Dauer bei etwa zwei Arbeitstagen).
- Die Signatur von Apps läuft nach 90 Tagen ab.

Der TestFlight-Dienst ist primär für eine kurze Testphase vor der Veröffentlichung einer iOS App gedacht. Für einen dauerhaften Betrieb ist die Lösung wegen der kurzen Gültigkeit der Signatur nicht geeignet.

Verteilung über Google Alpha- und Beta-Testing

Vorteile

- Apps stehen für Benutzer über einen von Google bereitgestellten Mechanismus zur Verfügung.
- Apps können selektiv für einzelne Benutzer freigeschaltet werden.
- Google stellt die Infrastruktur für die Verteilung und Abrechnung bereit.

Nachteile

- Benutzer benötigen eine Google-ID, um Apps aus dem Play Store zu installieren.
- Bei Unternehmenskunden mit verwalteten Geräten ist der Play Store unter Umständen per MDM gesperrt.

Für Version 26.4.0

Verteilung über internen Enterprise App Store

Apple und Google bieten neben der Verteilung von Apps über die jeweiligen öffentlichen Stores auch Mechanismen zur internen Verteilung von Apps, primär für Unternehmen, an. Bei Apple wird als Voraussetzung das Apple Enterprise Programm und ein Enterprise App Store wie bspw. Relution benötigt.

Die Apps werden für Endanwender über eine separate App Store App oder eine mobile Webseite bereitgestellt. Die Verwaltung von Apps erfolgt über das Developer-Portal.

Die Verteilung der Apps erfolgt über den jeweiligen Anbieter des Enterprise App Store. Bei Google können Apps über einen Webservice zum Download und zur Installation bereitgestellt werden.

Für spezielle Geräte wie beispielsweise Samsung können optimierte Installations- und Verteilungsmechanismen genutzt werden. Apple und Google definieren die Möglichkeiten für die Verteilung von Apps parallel zu ihren Systemen.

Verteilung von iOS Apps über Enterprise App Store

Vorteile

- Apps können an ausgewählte Benutzergruppen beispielsweise als Deeplink oder nach Anmeldung mit zuvor konfigurierten Benutzernamen und Passwort verteilt werden.
- Benutzer benötigen keine Apple-ID, um Apps aus einem internen Enterprise App Store zu installieren.
- Es müssen nicht sämtliche Apple Vorgaben eingehalten werden.
- Die Veröffentlichung von App Updates wird nicht durch ein Review von Apple verzögert.
- Einige Enterprise App Stores (wie beispielsweise Relution) sind auch ohne Geräteverwaltung (MDM) nutzbar.
- Ein existierendes Benutzerverwaltungssystem (ActiveDirectory/LDAP) kann angeschlossen werden, so dass die Nutzer keine neuen Zugangsdaten benötigen.

Nachteile

- Apps stehen für Endanwender über einen speziellen Mechanismus zur Verfügung, der von Apple genehmigt ist, jedoch eine initiale Konfiguration durch den Benutzer benötigt (siehe hier →)
- *Apps müssen nach einem Jahr mit einem aktualisierten Provisioning Profile neu signiert und bereitgestellt werden. Dies kann jedoch mit Relution automatisiert werden, so dass hier eigentlich kein Nachteil entsteht.*
- Die Infrastruktur für die Verteilung kann beispielsweise als Cloud-Dienst oder On-Premise bereitgestellt werden.
- Die Verteilung von Apps darf gemäß Apple Richtlinien nur an Mitarbeiter, Interessenten und Partner, aber vor allem an einen bekannten Nutzerkreis, erfolgen.

Verteilung von Android Apps über Enterprise App Store

Vorteile

- Apps können an ausgewählte Benutzergruppen bspw. als Deeplink oder nach Anmeldung mit zuvor konfigurierten Benutzernamen und Passwort verteilt werden.
- Benutzer benötigen keine GoogleID, um Apps aus einem internen Enterprise App Store zu installieren.
- Es müssen nicht sämtliche Google Vorgaben eingehalten werden.
- Die Veröffentlichung von App Updates wird nicht durch technische Scans von Google verzögert.
- Einige Enterprise App Stores (wie beispielsweise Relution) sind auch ohne Geräteverwaltung (MDM) nutzbar.
- Ein existierendes Benutzerverwaltungssystem (ActiveDirectory/LDAP) kann angeschlossen werden, so dass die Nutzer keine neuen Zugangsdaten benötigen.

Für Version 26.4.0

Nachteile

- Apps stehen für Endanwender über einen speziellen Mechanismus zur Verfügung, der von Google genehmigt ist, jedoch eine initiale Konfiguration durch den Benutzer benötigt.
- Die Infrastruktur für die Verteilung muss beispielsweise als Cloud-Dienst bereitgestellt werden.

APK-Apps verwalten

Zum Bereitstellen von selbst entwickelten Unternehmensapps auf Android-Geräten, die über Android Enterprise eingeschrieben wurden, stehen drei Möglichkeiten zur Verfügung. Der offiziell von Google vorgesehene und von Relution vorgeschlagene Weg ist die Verteilung über den verwalteten Play Store.

Seit Relution 26.2 lassen sich im Relution App Store hochgeladene APK-Apps außerdem auf vollständig verwalteten Geräten, auch mit persönlichem Profil, als benutzerdefinierte Apps verteilen. Sicherheitsmechanismen von Android Enterprise müssen dafür nicht deaktiviert werden. Auf Geräten, die als Arbeitsprofil eingeschrieben sind, steht dieser Weg nicht zur Verfügung.

Die dritte Möglichkeit ist die direkte Verteilung einer APK-Datei, beispielsweise über die Relution Legacy App, Web oder E-Mail. Da diverse Sicherheitsmechanismen von Android Enterprise deaktiviert werden müssen, ist diese Variante nicht empfohlen und nur in Ausnahmefällen sinnvoll.

Verteilung über den Play Store

Es gibt zwei Optionen, um Apps in den Play Store hochzuladen. In beiden Fällen ist ein Entwicklerkonto notwendig. Die Kosten eines Google-Entwicklerkontos liegen bei einmalig 25$.

App über die Play Store Konsole bereitstellen (empfohlen)

Für Version 26.4.0

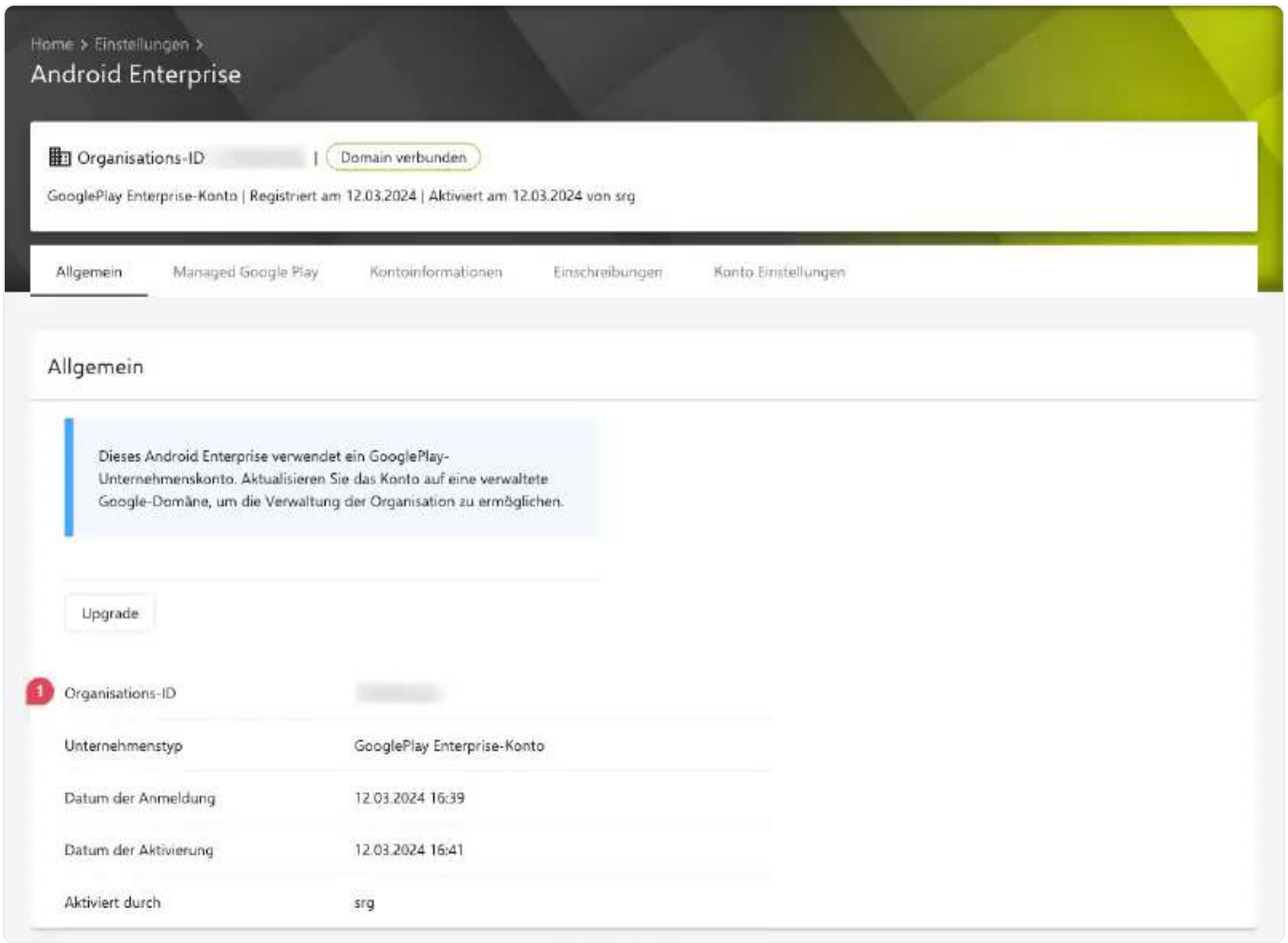
Die App wird regulär über ein beliebiges Entwicklerkonto in den Play Store hochgeladen (Google Play Console →). Empfohlen wird, dazu ein offizielles Unternehmenskonto zu verwenden.

Hierbei stehen alle Einstellungsmöglichkeiten des Play Stores zur Verfügung, wie beispielsweise die Möglichkeit, Entwicklungsversionen der App nur für bestimmte Personengruppen vorab zu veröffentlichen.

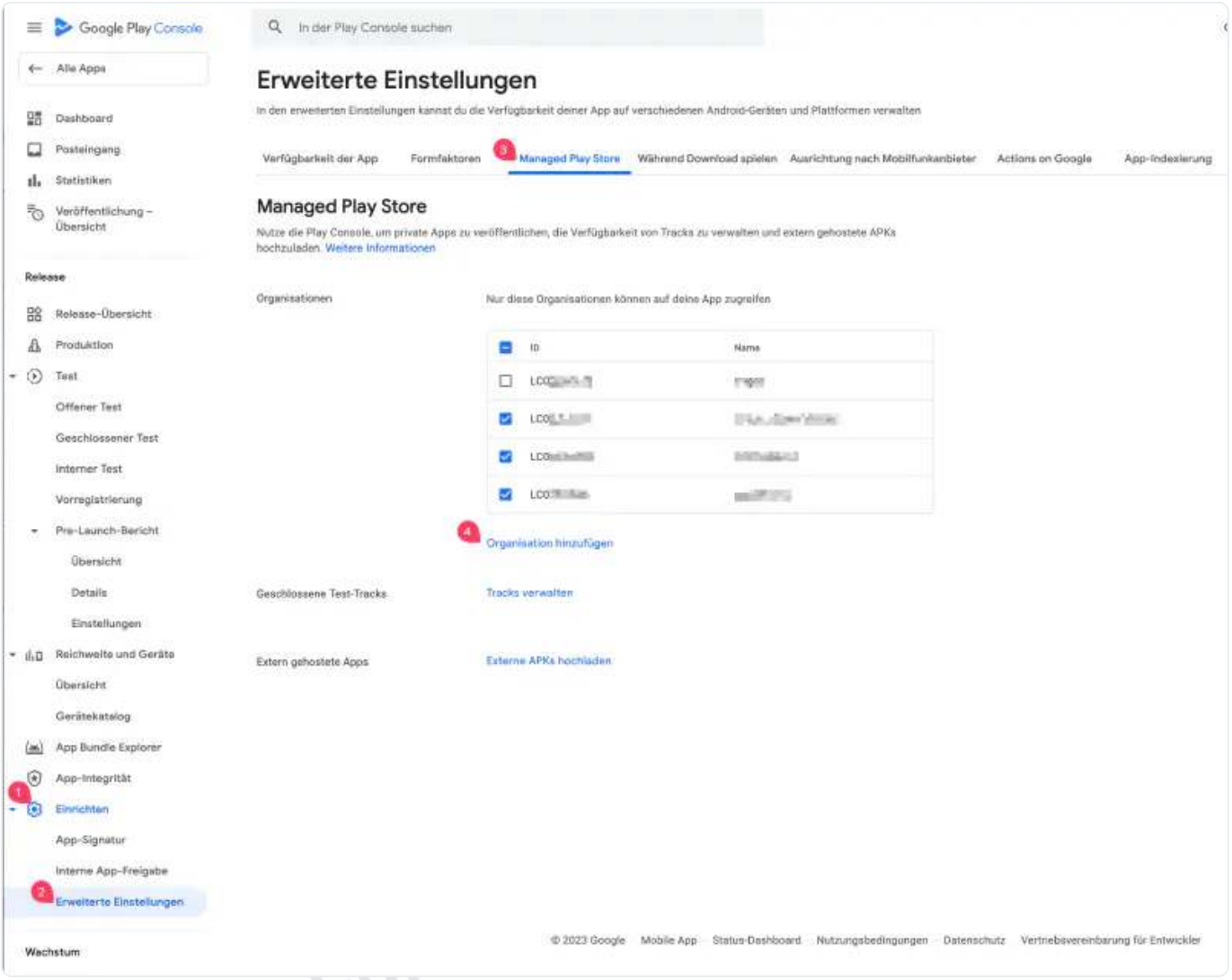
Wenn die App nicht öffentlich zur Verfügung stehen soll, kann deren Verfügbarkeit zusätzlich auf das eigene Unternehmen eingeschränkt werden. Achtung: Diese Einstellung kann im Anschluss nicht rückgängig gemacht werden. Wenn die App zukünftig auch öffentlich angeboten werden soll, muss diese unter einem anderen Package-Name erneut veröffentlicht werden.

Der große Vorteil besteht darin, dass die App im Anschluss auch für weitere Unternehmen bzw. Unternehmenskontos freigegeben werden kann. Das kann beispielsweise im Fall eines Serverumzugs, aber auch bei Verlust der Zugangsdaten zum Google-Konto, das für Android Enterprise verwendet wird, hilfreich sein.

Um die App auf das eigene Unternehmen einzuschränken, kann dessen Organisations-ID unter `Einrichten` → `Erweiterte Einstellungen` → `Managed Play Store` hinterlegt werden. Die ID beginnt dabei mit `LC0…`. Diese ID ist beispielsweise in Relution unter `Einstellungen` → `Geräteplattformspezifisch` → `Android Enterprise` sichtbar.


Home > Einstellungen >
Android Enterprise
Organisations-ID
Domain verbunden
GooglePlay Enterprise-Konto | Registriert am 12.03.2024 | Aktiviert am 12.03.2024 von srg
Allgemein
Managed Google Play
Kontoinformationen
Einschreibungen
Konto Einstellungen
Allgemein
Dieses Android Enterprise verwendet ein GooglePlay-Unternehmenskonto. Aktualisieren Sie das Konto auf eine verwaltete Google-Domäne, um die Verwaltung der Organisation zu ermöglichen.
Upgrade
1
Organisations-ID
Unternehmenstyp
GooglePlay Enterprise-Konto
Datum der Anmeldung
12.03.2024 16:39
Datum der Aktivierung
12.03.2024 16:41
Aktiviert durch
srg

Für Versi



Upload über den Play Store Dialog in Relution

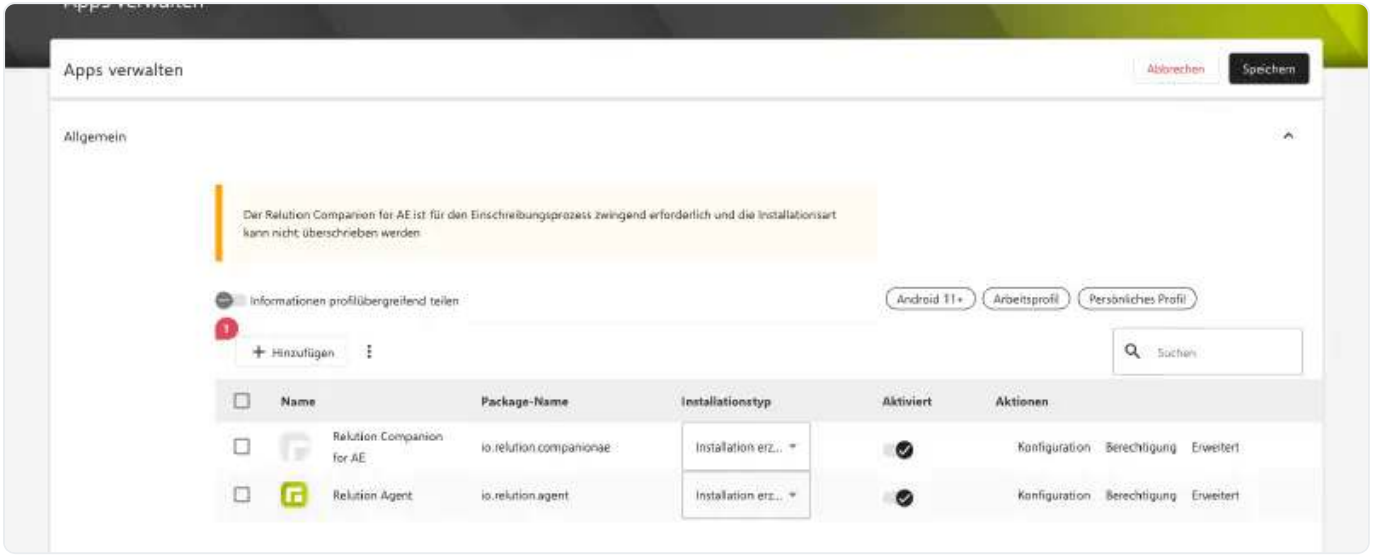
Anstatt die App über die Google Play Console hochzuladen, kann diese auch direkt von Relution heraus bereitgestellt werden. Dabei muss jedoch das Google-Konto, welches zum Einrichten von Android Enterprise verwendet wurde, ein entsprechendes Entwicklerkonto sein.

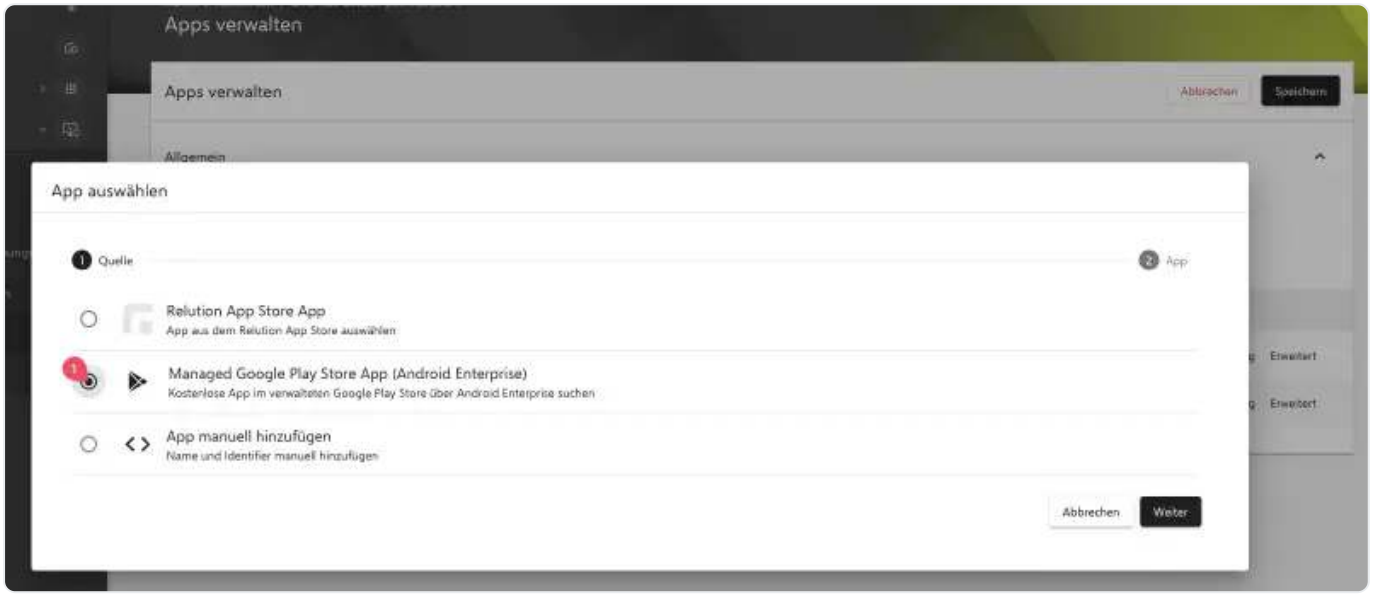
Hier können neben dem Namen der App weder weitere Einstellungen vorgenommen werden, noch besteht die Möglichkeit, die App im Anschluss für weitere Unternehmen oder Unternehmenskontos freizuschalten. Aufgrund dieser Einschränkungen wird von dieser Möglichkeit abgeraten.

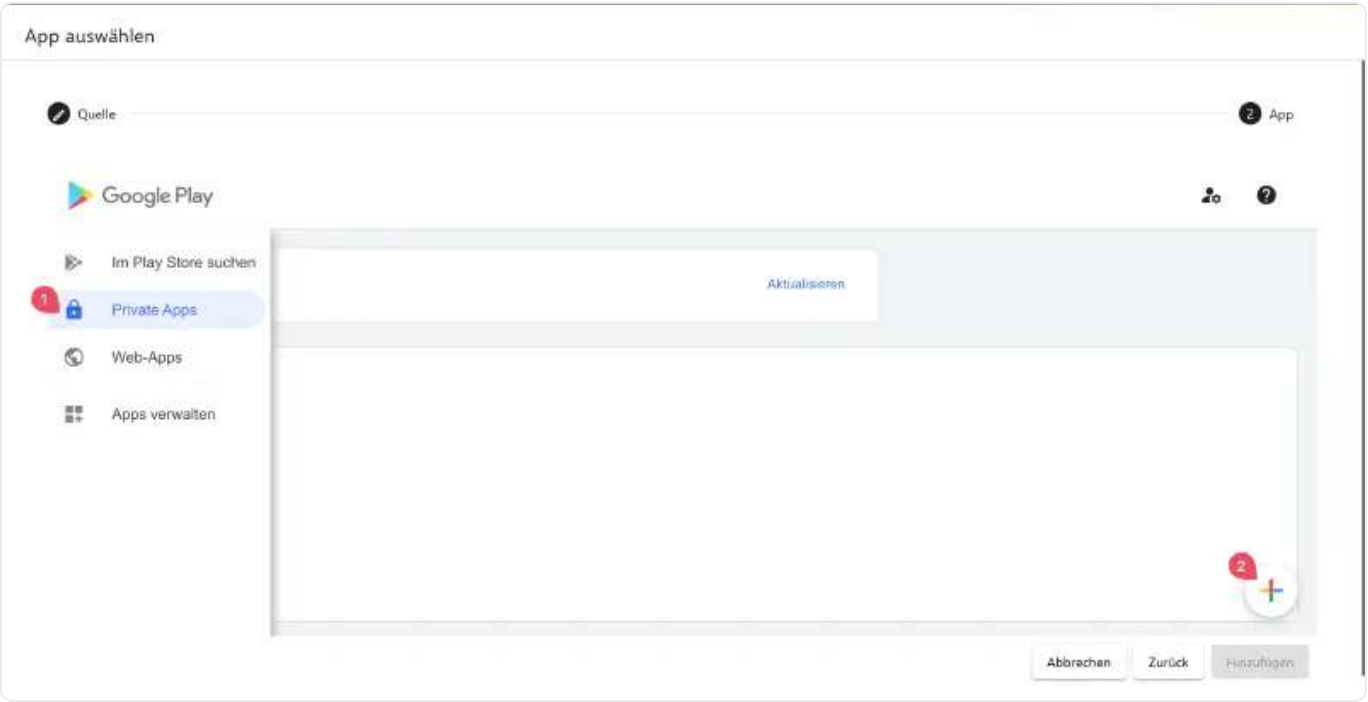
Um eine App als private App hochzuladen, wie folgt vorgehen:

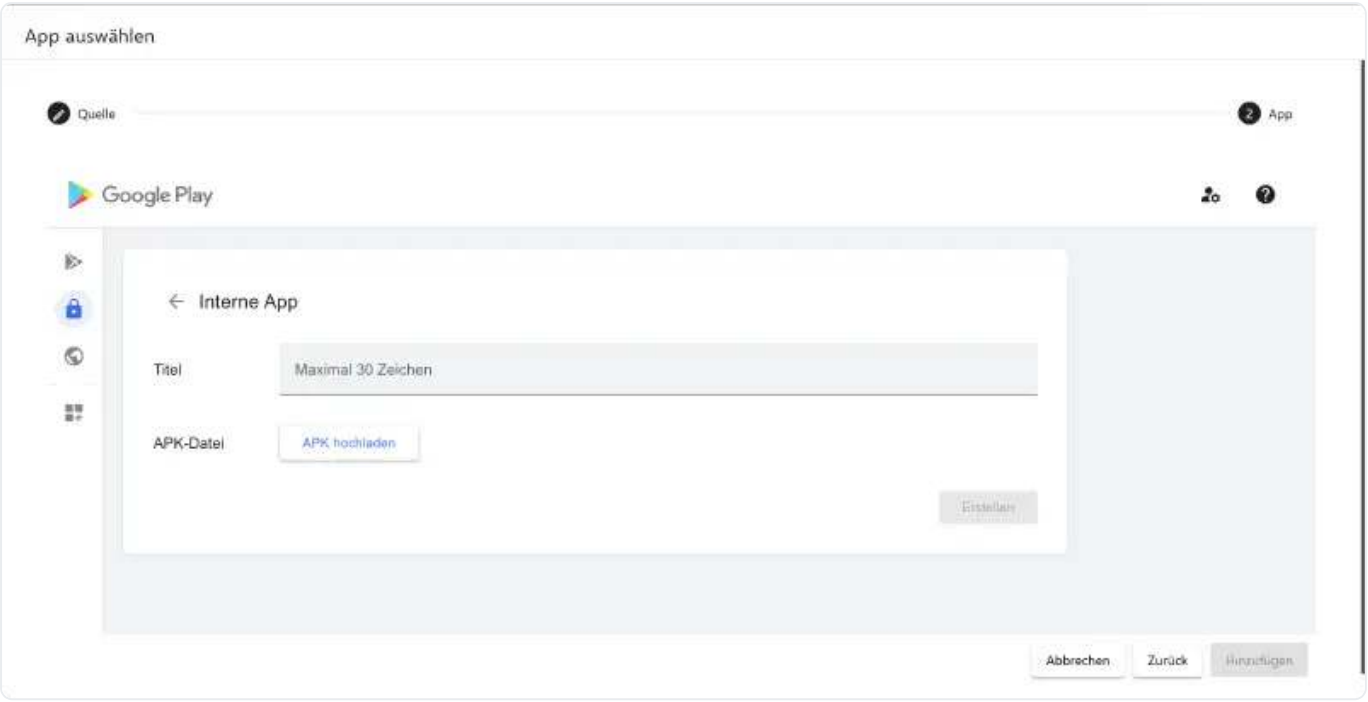
1. In Relution zu `Geräte` → `Richtlinien` gehen.
2. Eine beliebige Android Enterprise Richtlinie öffnen und eine Apps verwalten Konfiguration hinzufügen.
3. In der Konfiguration auf Hinzufügen klicken.
4. Managed Google Play Store App (Android Enterprise) wählen.
5. Im linken Menü zu Private Apps wechseln.
6. Auf + klicken, um eine neue App hinzuzufügen.

Achtung: Der Package-Name der App muss eineindeutig sein. Sollte die App bereits im Play Store verfügbar sein, auch als private App eines anderen Unternehmens, so kann diese nicht erneut hochgeladen werden. Empfohlen wird daher generell der Upload über den Play Store, über welchen die App im Anschluss auch für weitere Organisations-IDs freigeschaltet werden kann.









Verteilung einer APK-Datei

Seit Relution 26.2 lassen sich im Relution App Store hochgeladene native Apps im Format `.apk` auf vollständig verwalteten Geräten, auch mit persönlichem Profil, direkt verteilen:

- In der Richtlinienkonfiguration Apps verwalten über `Hinzufügen` → `Relution App Store App`. Die App wird mit dem Installationstyp Benutzerdefiniert übernommen.
- Über die Aktion App aus dem Relution Store installieren. Native Apps stehen dort nur zur Auswahl, wenn ausschließlich vollständig verwaltete Geräte ausgewählt sind.

Voraussetzung ist in beiden Fällen, dass Relution die Signaturzertifikate der APK ermittelt hat. Die im Folgenden beschriebenen Lockerungen der Sicherheitseinstellungen sind für diesen Weg nicht erforderlich.

Auf Geräten, die als Arbeitsprofil eingeschrieben sind, werden benutzerdefinierte Apps nicht installiert. Die dort verfügbare Aktion Play Store App aus dem Relution Store auswählen bietet nur Play Store Apps an.

Für diese Geräte sowie für die Installation heruntergeladener APK-Dateien (z. B. aus E-Mail oder Web) sind folgende Einstellungen per Richtlinie notwendig:

1. Konfiguration Erweiterte Sicherheitsüberschreibungen.
    - Die Option Aus unbekannten Quellen zulassen muss auf Installation nicht vertrauenswürdiger Apps auf dem gesamten Gerät erlauben gestellt werden.

      Damit wird Benutzer grundsätzlich erlaubt, APK-Dateien aus jeder beliebigen Quelle auf dem Gerät zu installieren!
2. Konfiguration Play Store Verwaltung
    - Die Option Eingeschränkter Google Play Store muss deaktiviert werden

      Ist der eingeschränkte Play Store aktiv, entfernt das Gerät Apps, die nicht mittels Apps verwalten Konfiguration auf dem Gerät installiert wurden oder Teil des Systems sind, nach ungefähr 10 Minuten.

      Damit wird Benutzer erlaubt, beliebige Apps aus dem Play Store im verwalteten Profil zu installieren.

Für Version 26.4.0

Wenn diese Einstellungen vorgenommen wurden, ist es wieder möglich, beliebige APK-Dateien auf dem Gerät zu installieren. Da Benutzer in diesem Modus APK-Dateien aus jeglicher Quelle installieren können, wird grundsätzlich davon abgeraten, diese Einstellungen zu aktivieren. Darüber hinaus besteht keine einfache Möglichkeit, die Aktualität von Apps zu gewährleisten.

Alternativ kann in einer Apps Verwalten Konfiguration der Package-Name der entsprechenden App manuell hinzugefügt werden, um diese zuzulassen. Damit sollte die App ebenfalls nicht mehr automatisch durch das Gerät entfernt werden.

Für die Verteilung von APK-Dateien gibt es verschiedene Möglichkeiten, zum Beispiel:

Installation über die Relution Legacy App

Dazu wird die klassische Relution Legacy App über eine Apps verwalten Konfiguration auf dem Gerät installiert. Im Anschluss können Benutzer sich in der App anmelden und bekommen dadurch Zugriff auf alle nativen Android Apps, die im Relution Store hinterlegt sind. Benutzer können diese Apps über die Legacy Apps herunterladen und installieren. Benutzer müssen je nach Android-Version der Relution App noch zusätzlich das Recht einräumen, App-Installationen anzufordern.

Wenn der klassische Companion zusätzlich eingeschrieben wird (erfordert eine weitere Gerätelizenz!), können Administratoren auf als Arbeitsprofil eingeschriebenen Geräten alternativ Apps auch per Aktion installieren. Je nach Gerätetyp müssen Benutzer der Installation dennoch manuell zustimmen. Auf vollständig verwalteten Geräten, auch mit persönlichem Profil, ist das nicht nötig: Dort steht ohne zusätzliche Einschreibung oder Gerätelizenz die Aktion App aus dem Relution Store installieren zur Verfügung (siehe oben).

Installation per E-Mail

Benutzer erhalten die zu installierende APK-Datei vom Unternehmen per E-Mail.

Installation aus dem Web

Benutzer erhalten die zu installierende APK-Datei über einen Download-Link, der beispielsweise per E-Mail, Messenger oder SMS verteilt wird.

Weiterführende Links

Android Enterprise-Hilfe →.

Für Version 26.4.0

Selbst gehostete Apps

Selbst gehostete Android Apps bieten Unternehmen und Organisationen die Kontrolle über ihre Daten und ermöglichen es ihnen, die Privatsphäre und Sicherheit zu erhöhen. Durch die Installation und Verwaltung dieser Apps auf eigenen Servern behalten sie die volle Kontrolle über sensible Informationen und reduzieren gleichzeitig ihre Abhängigkeit von externen Dienstleistern.

Diese Funktion steht ab Relution Server 5.23 bereit.

Voraussetzungen

- Es ist erforderlich, über eine aktive Android-Entwicklerlizenz zu verfügen.
- Die automatisch generierten Google Play Managed-Konten können nicht verwendet werden, wenn Apps über den Managed Play Store hochgeladen werden, da diese Konten nicht mit einem aktiven Android-Entwicklerkonto verknüpft sind und auch nicht verknüpft werden können.
- Selbst gehostete private Apps müssen im Google Play-Konto mit einer aktiven Android-Entwicklerlizenz konfiguriert werden.
- Es muss ein Google Konto mit Relution verknüpft sein `Home` → `Einstellungen` → `Android Enterprise`.

Es besteht die Möglichkeit, auf Geräten mit Arbeitsprofilen nicht von IT-Administratoren aus der Ferne installiert werden. Nutzer mit einem Arbeitsprofil müssen diese Apps manuell über Managed Google Play installieren.

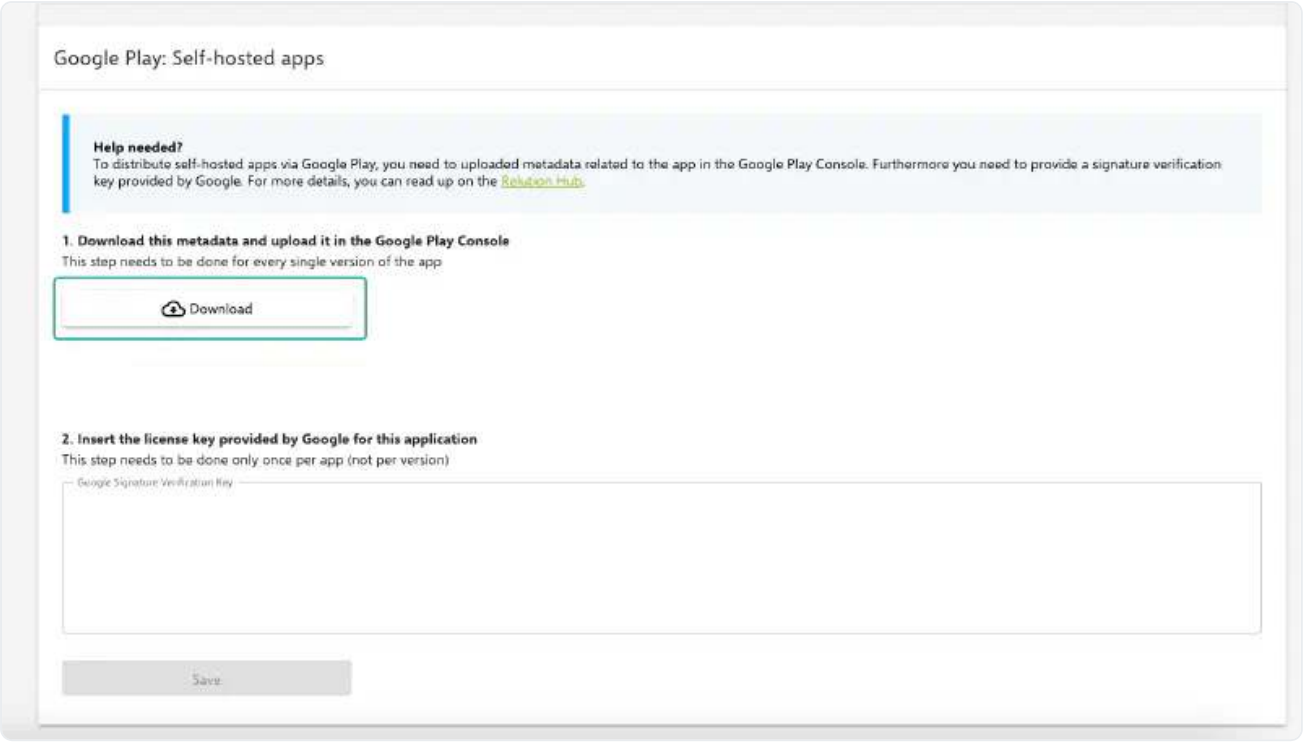
Für Version 26.4.0

App und Metadaten

1. In Relution muss die `apk` Datei unter `Home` → `Apps` → `App Store` → `Hinzufügen` (Dialog Neue Apps hinzufügen) hochgeladen werden. Es kann auch eine bestehende App verwendet werden.

   Die App-Version muss sich in Relution im Status Produktiv befinden. Der Bereich Google Play: Selbst gehostete Apps wird im Reiter Information nur angezeigt, wenn dort die Version unter Produktiv ausgewählt ist.

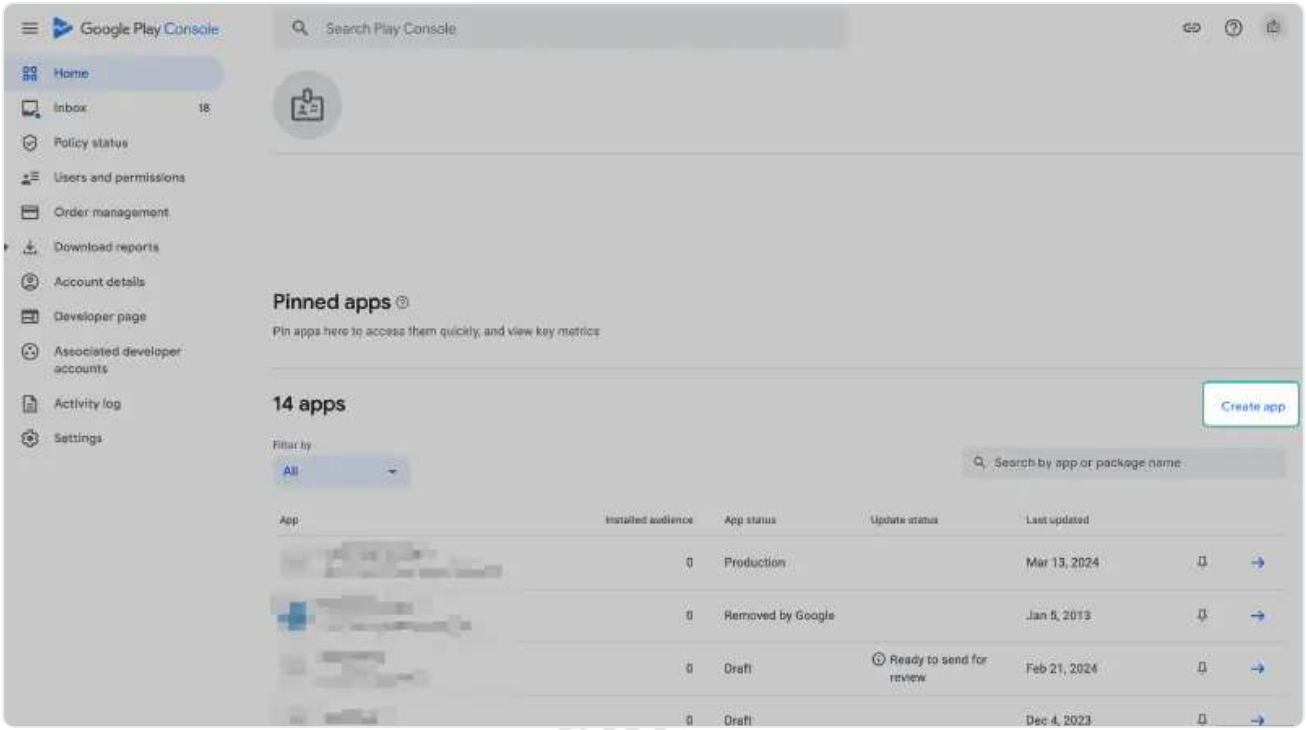
2. Im Reiter Information der App müssen im Bereich Google Play: Selbst gehostete Apps die Metadaten im `json` Format über den Download Button geladen werden.



App anlegen

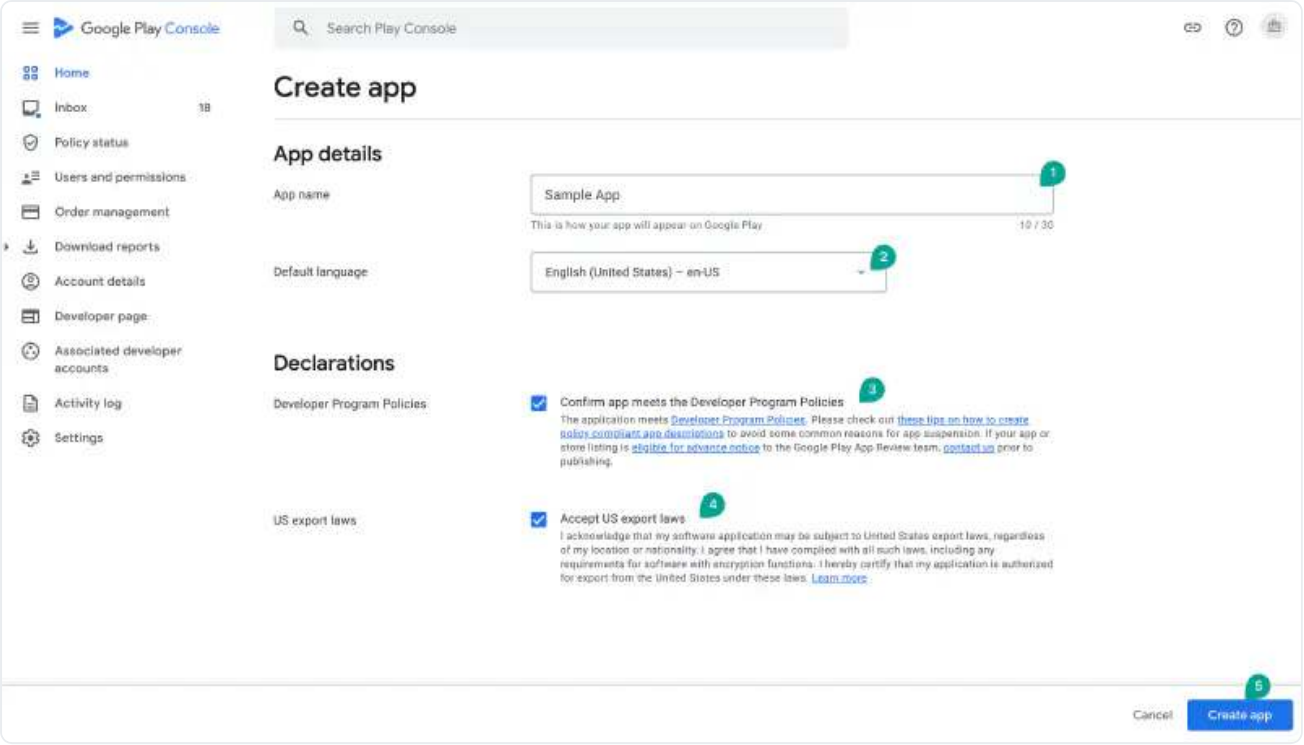
1. Wechsel zur Google Play Console →.

2. Neue App erstellen unter Create app



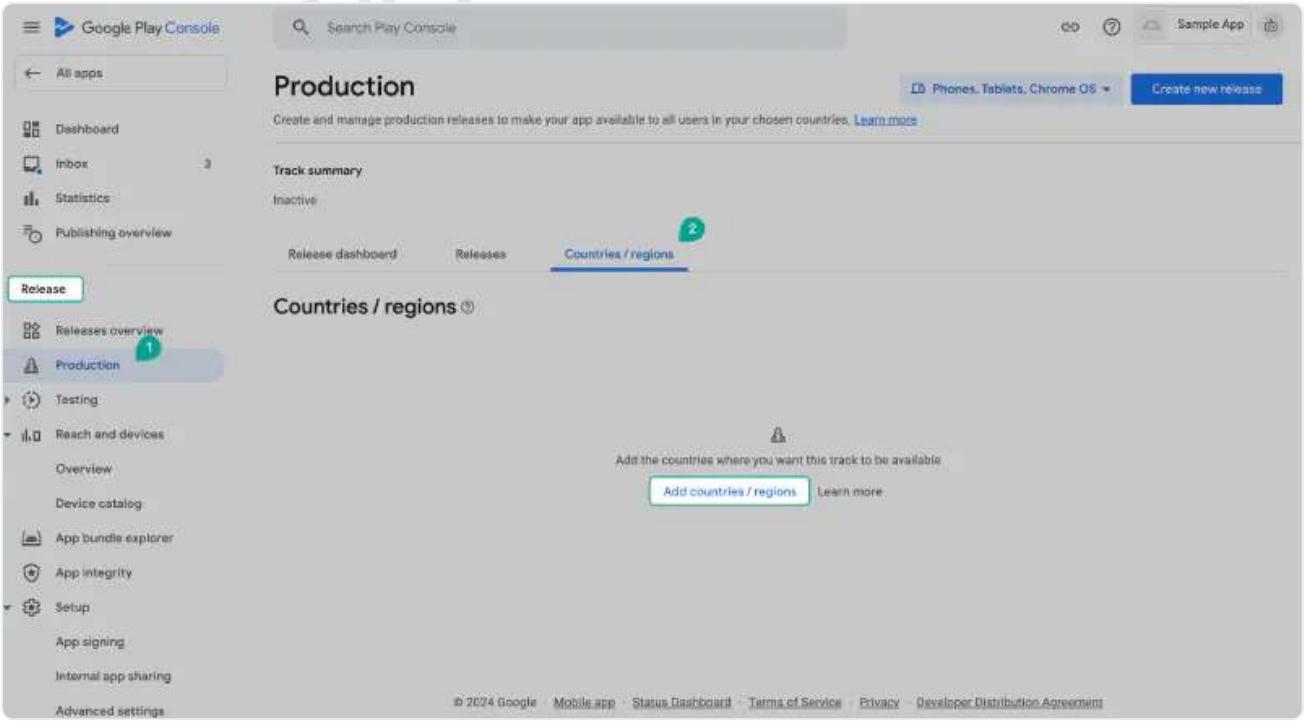
Für Versi

3. App Details hinzufügen

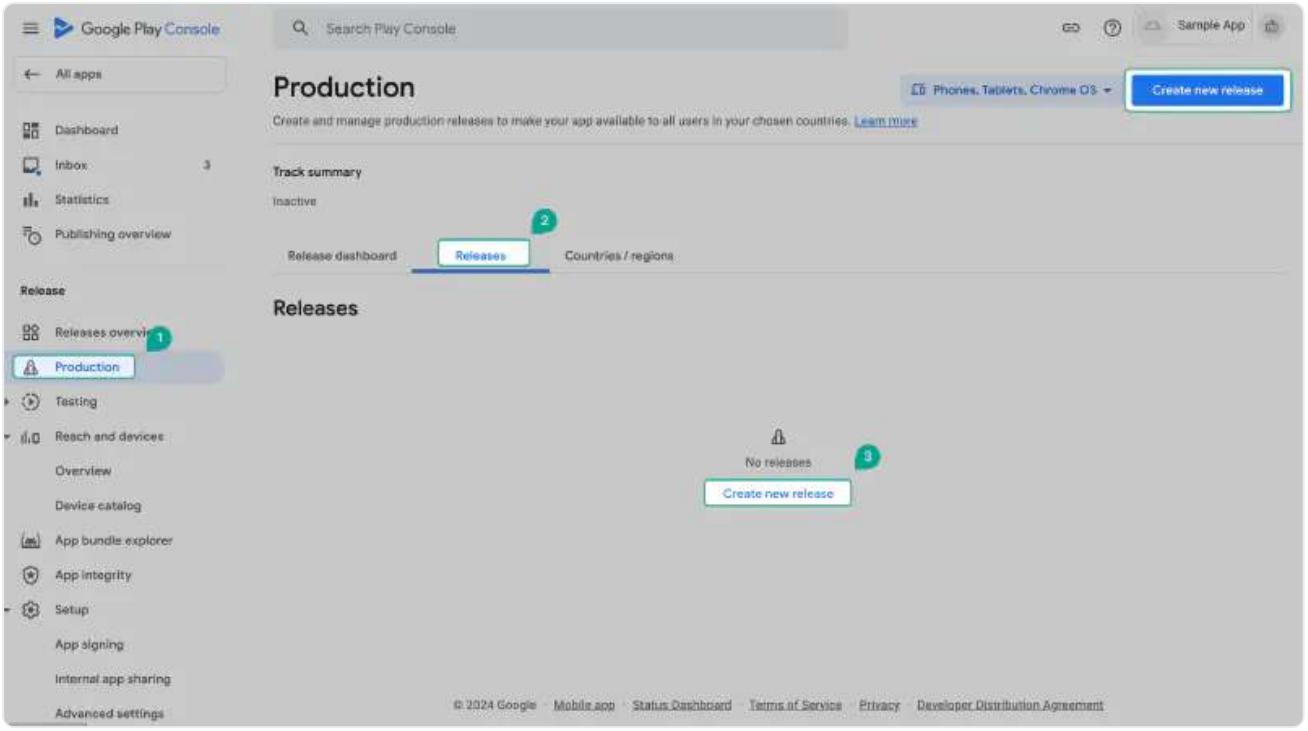


Ein App Icon kann unter Grow → Store presence → Main Store listing im Punkt Graphics hinzugefügt werden.

4. Länder hinzufügen, in denen die App verfügbar sein soll `Release` → `Production` → `Add countries / regions`



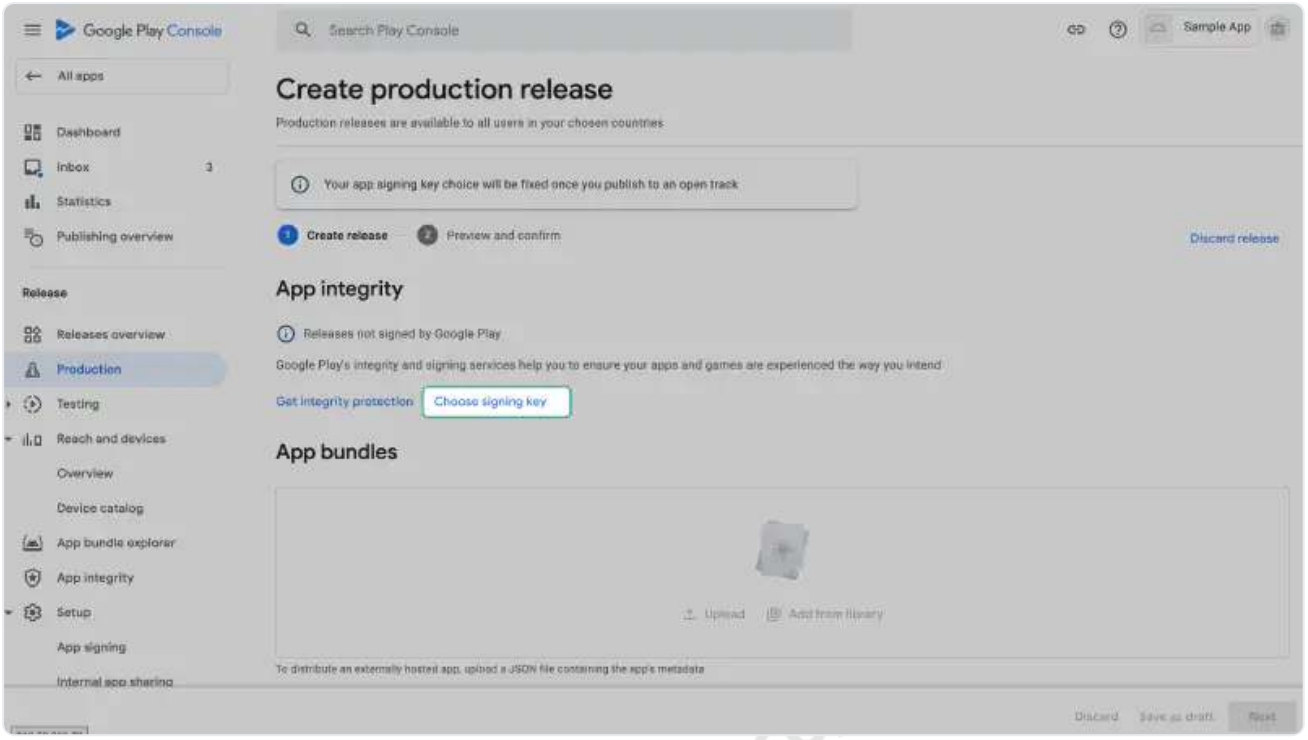
5. Neues Release anlegen `Release` → `Production` → `Releases` → `Create new release`

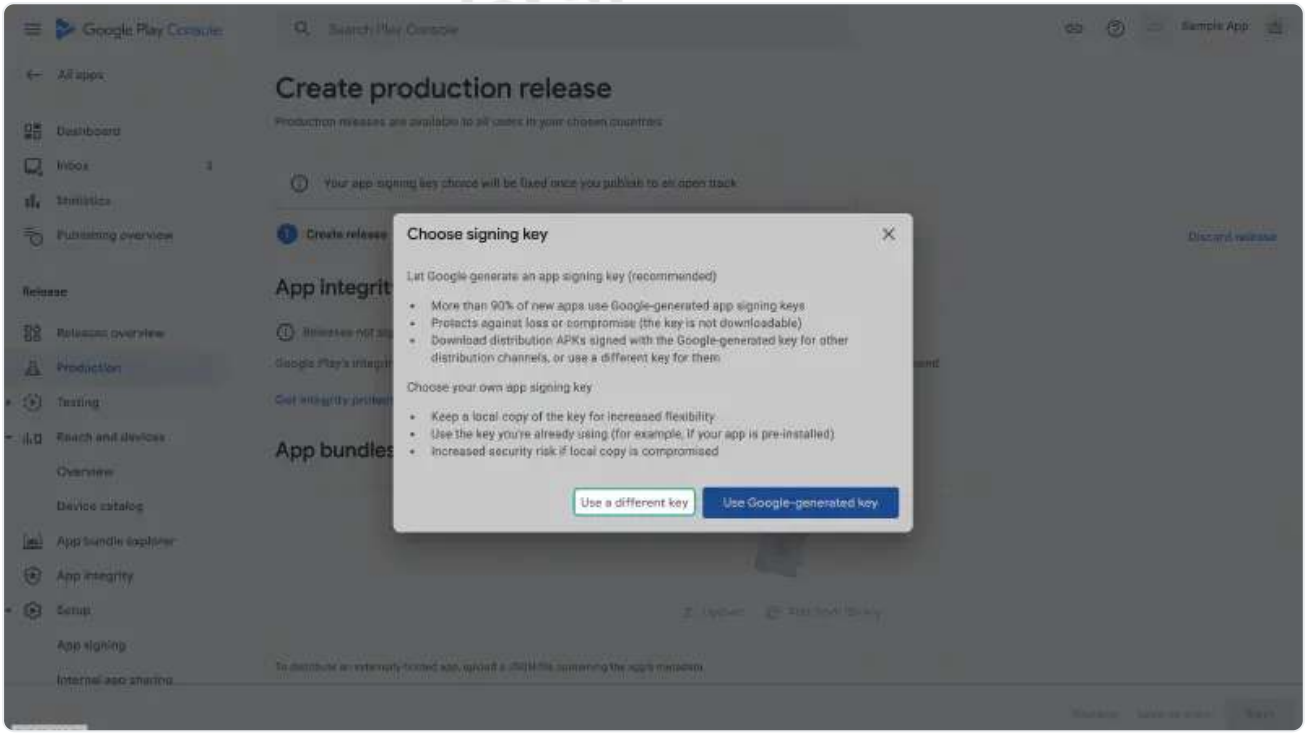


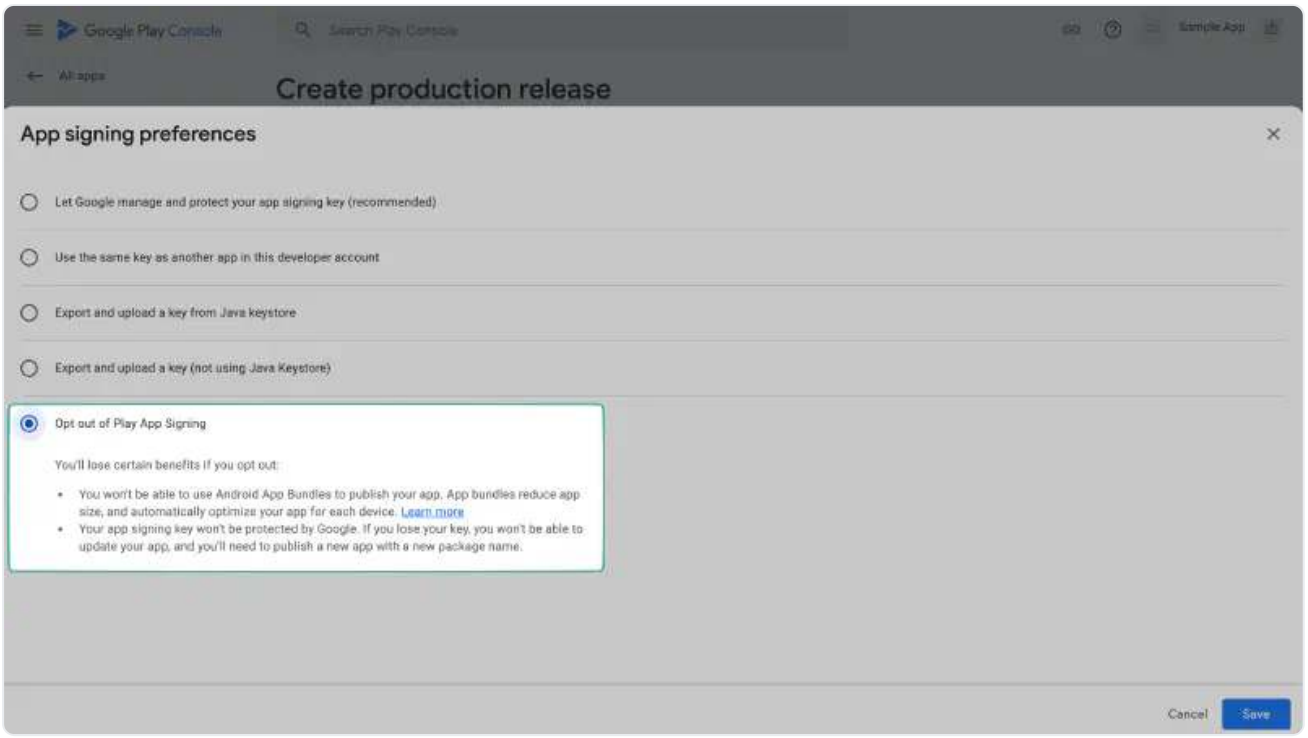
Für Version 26.4.0

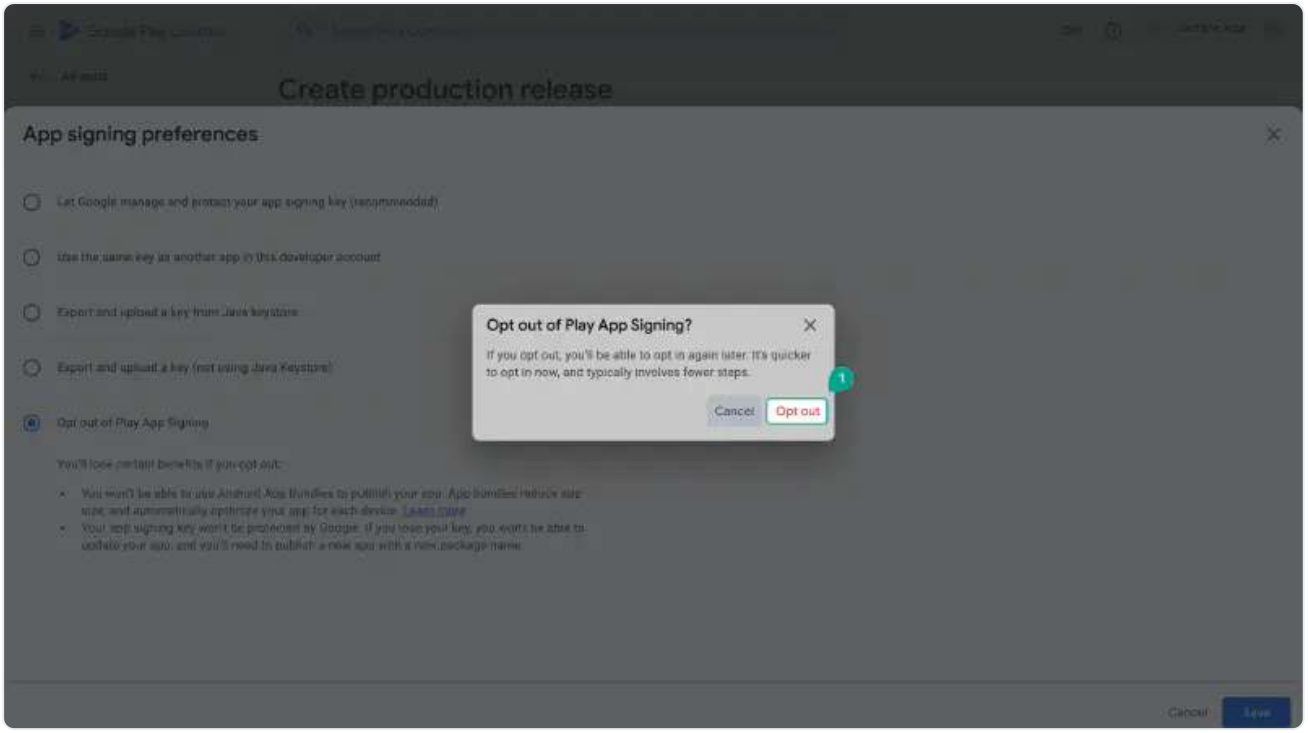
Signierung

1. Signing key auswählen `Use a different Key` → `Opt out of Play App Signing` → `Opt out`

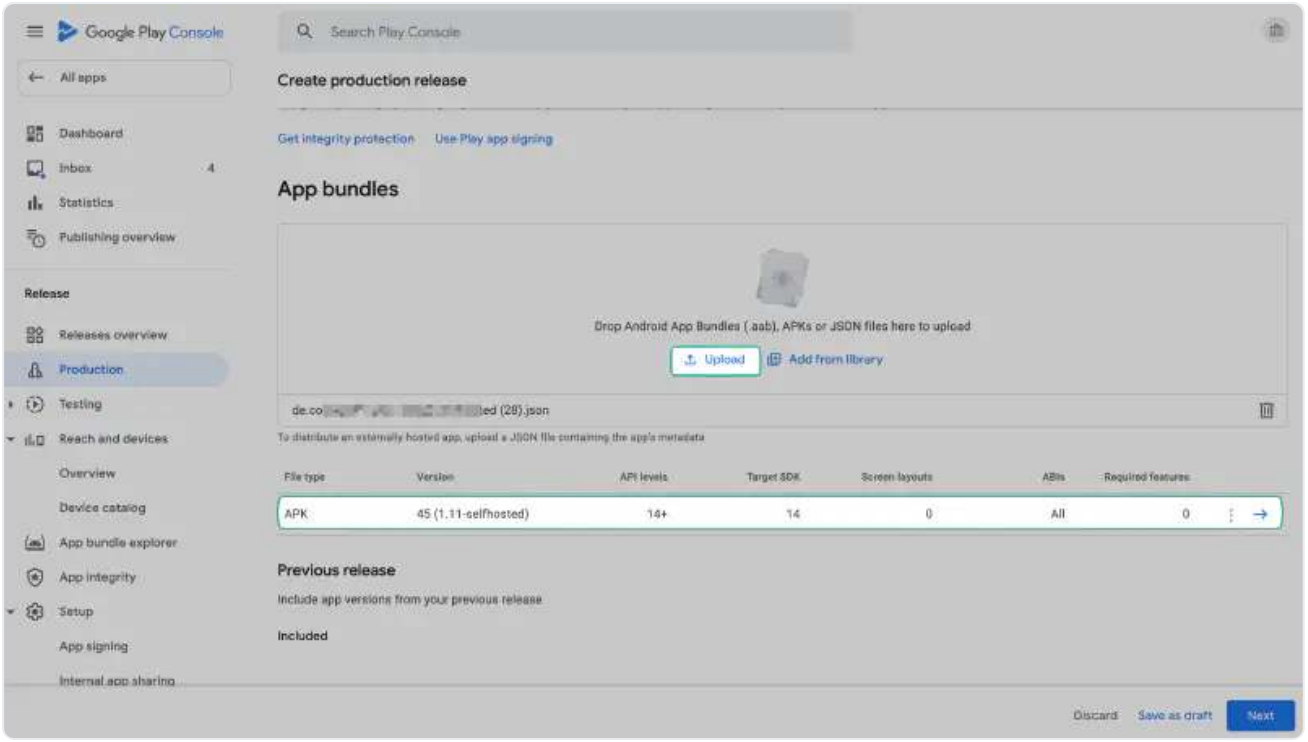




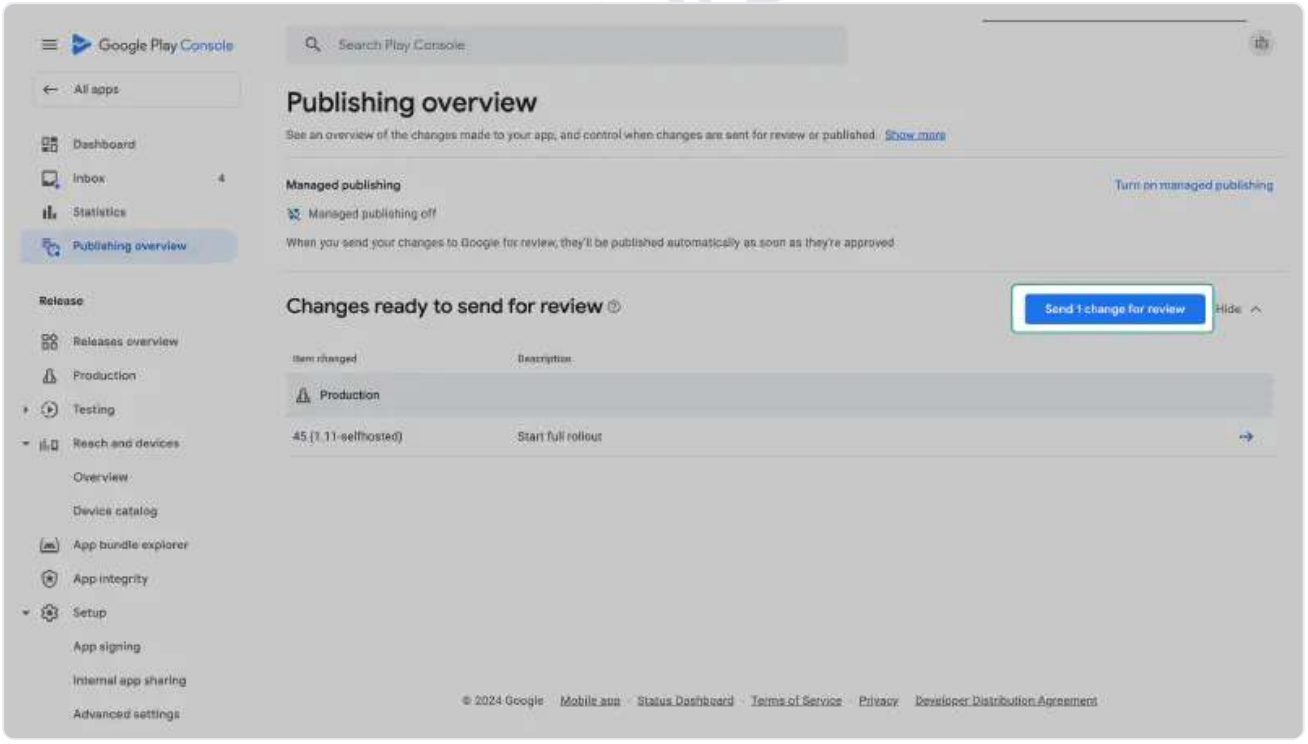

Google Play Console
Search Play Console
Sample App
All apps
Create production release
App signing preferences
Let Google manage and protect your app signing key (recommended)
Use the same key as another app in this developer account
Export and upload a key from Java keystore
Export and upload a key (not using Java Keystore)
Opt out of Play App Signing
You'll lose certain benefits if you opt out:
You won't be able to use Android App Bundles to publish your app. App bundles reduce app size, and automatically optimize your app for each device. Learn more
Your app signing key won't be protected by Google. If you lose your key, you won't be able to update your app, and you'll need to publish a new app with a new package name.
Cancel
Save


Create production release
App signing preferences
Opt out of Play App Signing?
If you opt out, you'll be able to opt in again later. It's quicker to opt in now, and typically involves fewer steps.
Cancel
Opt out

2. `json` Metadaten Datei aus Relution Portal Schritt 2 hochladen, next und save klicken

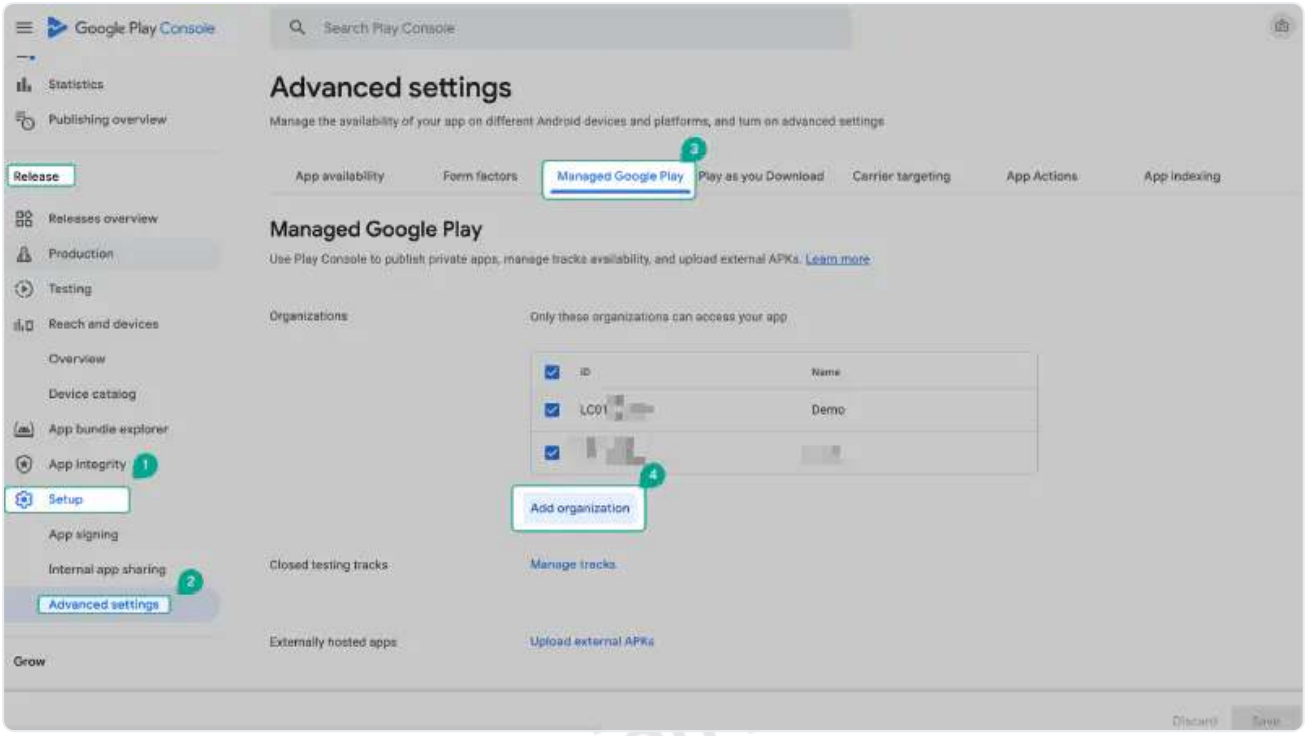


3. Änderung zum Review einreichen Send 1 change for review

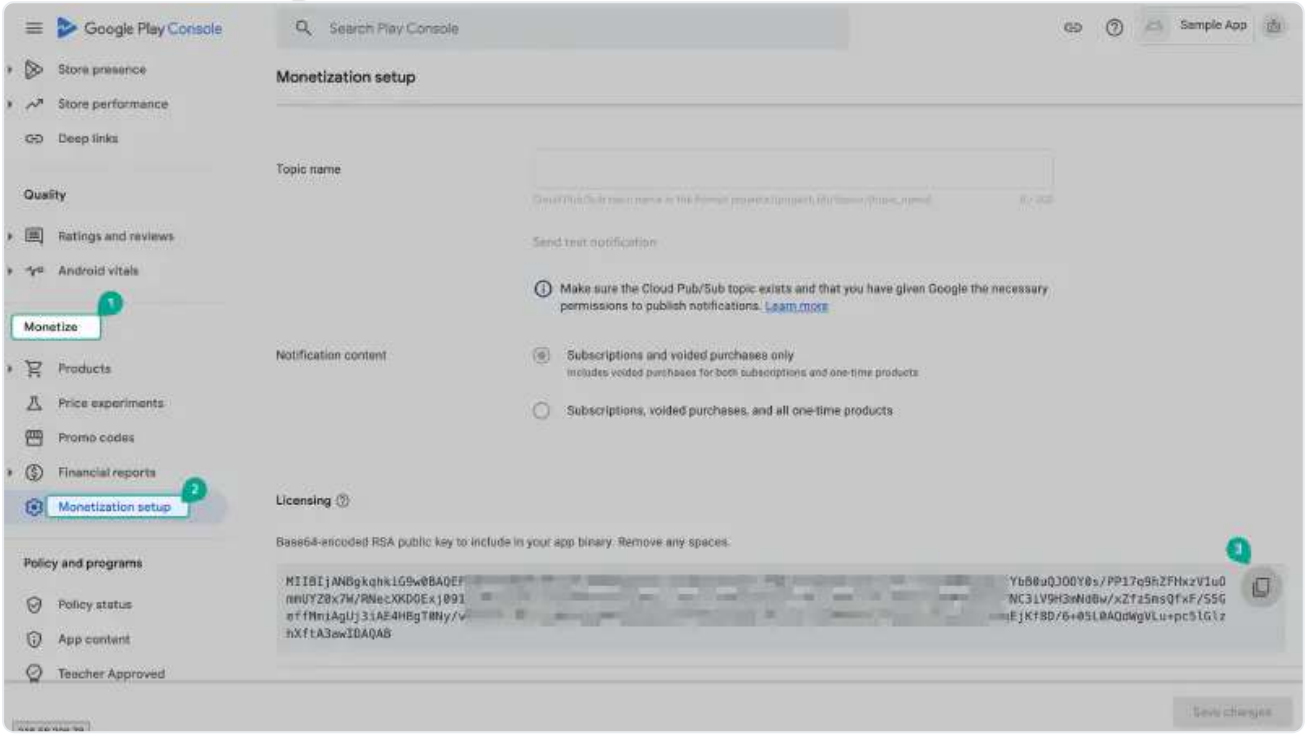


App für Organisation freigeben

1. Die Google OrganisationsID aus dem Relution Portal unter `Home` → `Einstellungen` → `Android Enterprise` kopieren und in der Google Play Console hinzufügen.

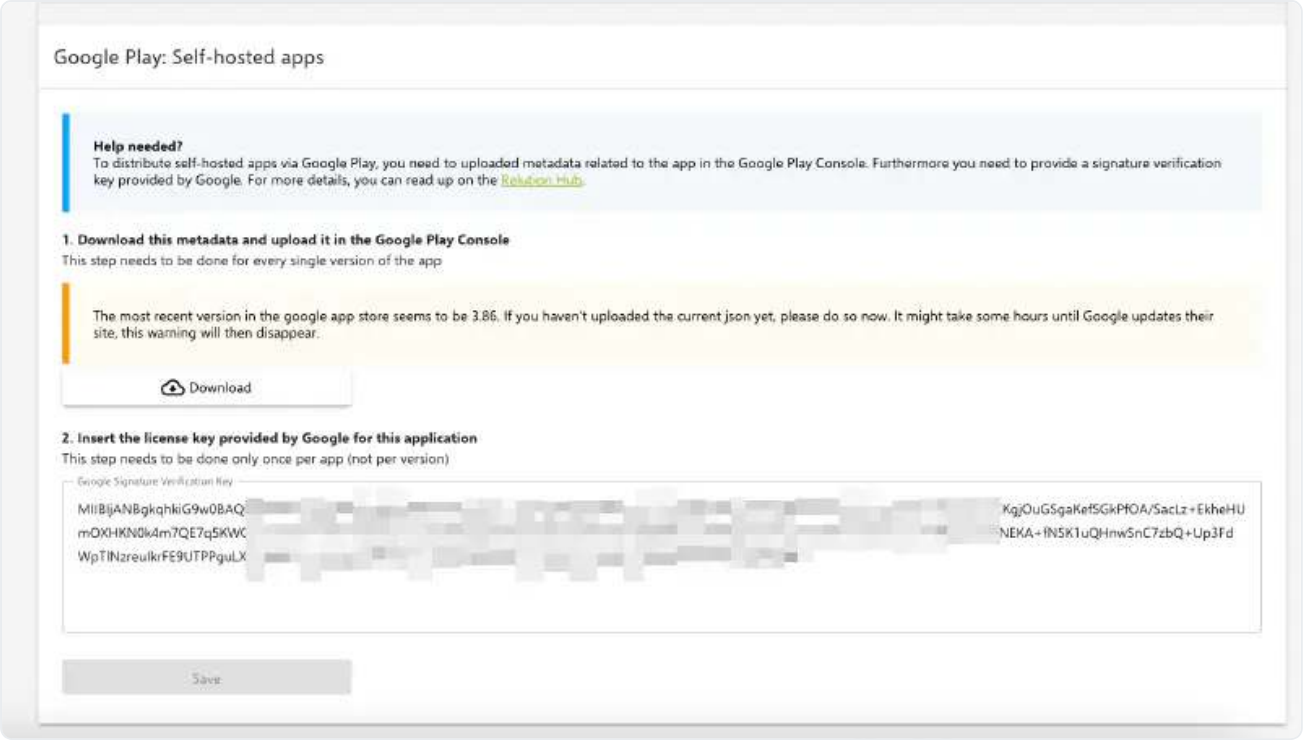


2. RSA Key der App kopieren und in Relution zur App hinzufügen. `Monetize` → `Monetization Setup`



Für Version

3. Den RSA Schlüssel in Relution im Reiter Information der produktiven App-Version im Bereich Google Play: Selbst gehostete Apps in das Feld Google Signaturprüfungsschlüssel einfügen und mit Speichern sichern. Dieser Schritt ist nur einmal pro App nötig, nicht pro Version.



Für Version 26.4.0

Bestehende App updaten

1. Neue Version der `apk` in Relution App Store hochladen `Home` → `Apps` → `App Store` → `App`.
2. Metadaten `json` herunterladen.

> Die aktuellste Version im Google App Store scheint x.xx zu sein. Sofern die aktuelle json-Datei noch nicht hochgeladen wurde, sollte dies jetzt nachgeholt werden. Es kann einige Stunden dauern, bis Google seine Seite aktualisiert, dann wird diese Warnung verschwinden.

3. Neuen App release in der Google Play Console erstellen.
4. Metadaten `json` der App aus Relution hochladen.
5. Änderung zum Review absenden.

Verwandte Themen

- Android Enterprise Einschreibung → — Einrichtung von Android Enterprise Geräten.
- MAM App-Verwaltung in Relution → — Grundlagen der App-Verwaltung.

Weblinks bereitstellen

Auf Android Enterprise-Geräten können Weblinks bereitgestellt werden. Im Gegensatz zu Apple werden Weblinks auf Geräten mit Android Enterprise-Einschreibung über den Managed Google Play Store zur Verfügung gestellt.

Konfiguration

Hierzu ist die Richtlinienkonfiguration Apps verwalten notwendig:

1. Im Relution-Portal zum Menüpunkt `Geräte` → `Richtlinien` navigieren und auf Hinzufügen klicken.
2. Eine Android Enterprise-Richtlinie erstellen und einen Namen vergeben. Auf Speichern klicken.
3. Nach Hinzufügen die Option Apps verwalten wählen und mit Details hinzufügen fortfahren.
4. Im nächsten Schritt erneut auf Hinzufügen klicken. Im Dialog App auswählen unter Quelle die Option Managed Google Play Store App (Android Enterprise) auswählen und auf Weiter klicken.
5. Im Schritt App wird der Managed Google Play Store angezeigt. Dort im linken Menü auf Web-Apps klicken.
6. Anschließend zum Erstellen einer neuen Web-App das +-Icon rechts unten anklicken.
7. Im nächsten Dialog lassen sich Weblinks erzeugen und deren Grundkonfiguration vornehmen.
8. Die neu erstellte Web-App anklicken und mit Auswählen bestätigen. Der Dialog schließt sich, und die Web-App erscheint in der Liste der Konfiguration Apps verwalten.
9. Bei Bedarf den Installationstyp anpassen und die Konfiguration mit Speichern übernehmen.
10. Die Richtlinie veröffentlichen und den gewünschten Geräten zuweisen.

Mit dem voreingestellten Installationstyp Installation erzwungen wird die Web-App automatisch auf den Geräten installiert. Mit Verfügbar steht sie im Managed Google Play Store auf dem Gerät zur Installation bereit.

Für Version 26.4.0

Play Store zeigt keine Apps

Auf Android Enterprise-Geräten kann es in manchen Fällen vorkommen, dass im Google Play Store auf dem Gerät keine Apps angezeigt werden. Dieses Verhalten tritt häufig dann auf, wenn bestimmte Einstellungen oder Zuweisungen im Managed Google Playstore oder in Relution fehlen. Hier ist eine Schritt-für-Schritt-Anleitung, um dieses Problem zu beheben:

App im Managed Google Play Store finden und genehmigen

Damit eine App auf Geräten im Play Store angezeigt werden kann, muss sie zunächst über den Managed Google Play Store gesucht und genehmigt werden. So wird vorgegangen:

1. Webbrowser öffnen und https://play.google.com/work → aufrufen.
2. Die gewünschte App suchen, die auf dem Gerät nicht angezeigt wird.
3. App genehmigen, damit diese für die Organisation verfügbar ist.

Genehmigte App zu einer Sammlung in Relution hinzufügen

Nachdem die App genehmigt wurde, muss sie in Relution einer App-Sammlung hinzugefügt werden. Vorgehen im Relution Portal:

1. Im Relution Portal anmelden.
2. In der App Verwalten Konfiguration hinzufügen.
3. Managed Google Play Store App (android Enterprise) auswählen.
4. Apps verwalten im Seitenmenü auswählen
5. Sammlung erstellen oder eine bestehende Sammlung auswählen.
6. Die App auswählen, die im Managed Google Play Store genehmigt wurde, und der Sammlung hinzufügen.

Für Version 26.4.0

App in einer Richtlinie auf verfügbar setzen

Abschließend muss sichergestellt werden, dass die App in der entsprechenden Richtlinie auf verfügbar gesetzt ist. Dies stellt sicher, dass die App auf den zugewiesenen Geräten erscheint.

1. Im Relution Portal zur AE Richtlinie navigieren.
2. Apps verwalten auswählen.
3. Die App in der Liste suchen und in der Spalte Installationstyp den Wert Verfügbar auswählen. Neu aus Managed Google Play hinzugefügte Apps stehen standardmäßig auf Installation erzwungen. Zudem muss der Schalter Aktiviert eingeschaltet sein.

Sobald alle oben genannten Schritte abgeschlossen sind, sollte die App im Google Play Store auf dem Android-Enterprise-Gerät korrekt angezeigt werden und zur Installation bereitstehen.

Managed Config Chrome

Für Google Chrome können in Relution managed App Konfigurationen erstellt und angewendet werden.

Blockliste

`Portal` → `die AE Richtlinie` → `Apps verwalten` → `Google Chrome (hinzufügen falls nicht vorhanden)` → `Konfiguration`

Hier öffnet sich ein Pop-up. Im Feld Block access to a list of URLs muss die nachfolgende Liste übergeben werden. Mehrere Webseiten werden durch Kommas getrennt.

Blockliste →

```
[
  "example.com",
  "https://ssl.server.com",
  "hosting.com/bad_path",
  "https://server:8080/path",
  ".exact.hostname.com",
  "file://*",
  "custom_scheme:*",
  "*"
]
```

Lesezeichen

`Portal` → `die AE Richtlinie` → `Apps verwalten` → `Google Chrome (hinzufügen falls nicht vorhanden)` → `Konfiguration`

Lesezeichen →

Hier öffnet sich ein Pop-up. Im Feld Bookmarks muss die nachfolgende Liste übergeben werden. Mehrere Webseiten werden durch Kommas getrennt.

```
[
  {
    "toplevel_name": "Company bookmarks"
  },
  {
    "name": "Relution",
    "url": "relution.io"
  },
  {
    "children": [
      {
        "name": "Schulungen",
        "url": "relution.io/schulungen/"
      },
      {
        "name": "Helpdesk",
        "url": "helpdesk.relution.io"
      }
    ],
    "name": "Internal URLs"
  },
  {
    "name": "Android resources",
    "url": "google.com"
  }
]
```

Für Ve

Managed Mail Client

Mit Relution Mobile Device Management (MDM) ist es möglich, gängige E-Mail-Clients wie Google Mail oder Samsung Mail zentral zu konfigurieren und diese Einstellungen anschließend mittels einer Richtlinie an alle zugewiesenen Geräte zu verteilen.

Diese Anleitung beschreibt, wie die jeweilige E-Mail-Anwendung zur Richtlinie hinzugefügt und anschließend mit dynamischen Platzhaltern für eine automatische, benutzerspezifische Konfiguration eingerichtet werden kann.

E-Mail Client App zur Richtlinie hinzufügen

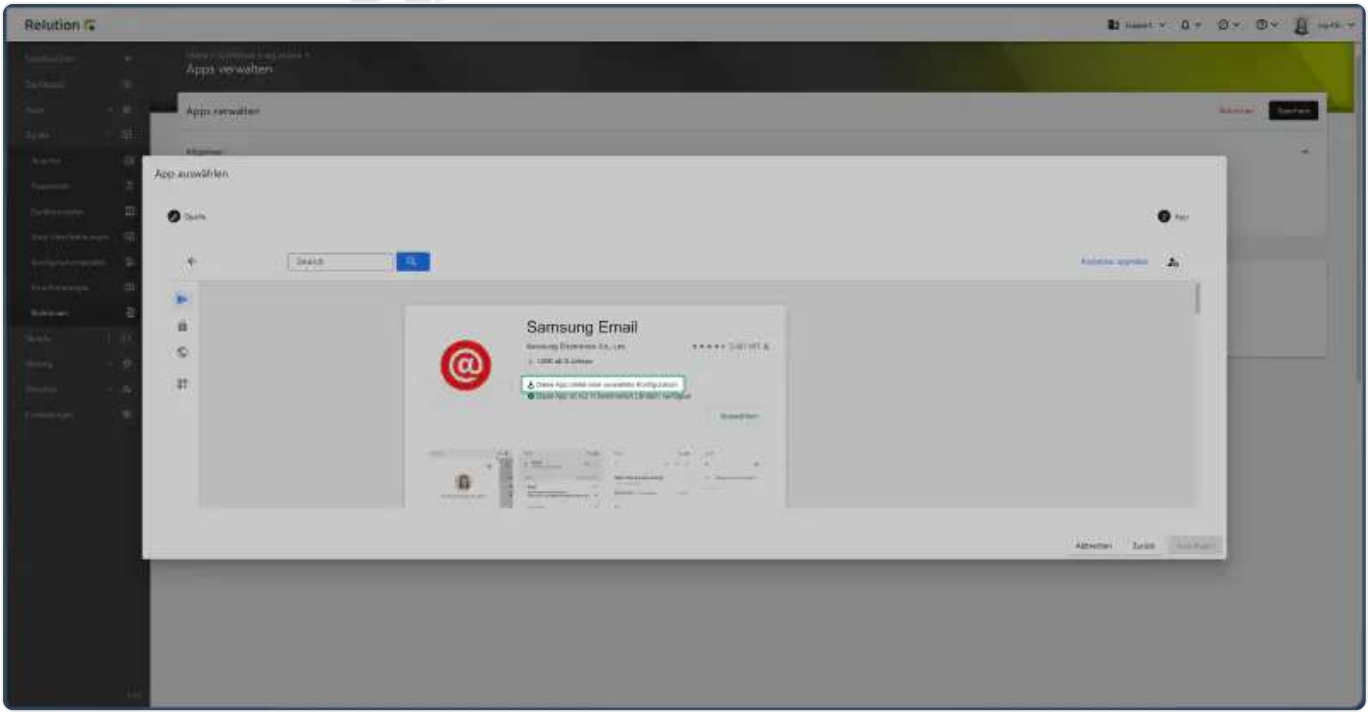
Bevor die Konfiguration vorgenommen werden kann, muss die gewünschte E-Mail-App (Google Mail oder Samsung Mail) zur Android Enterprise (AE) Richtlinie hinzugefügt werden.

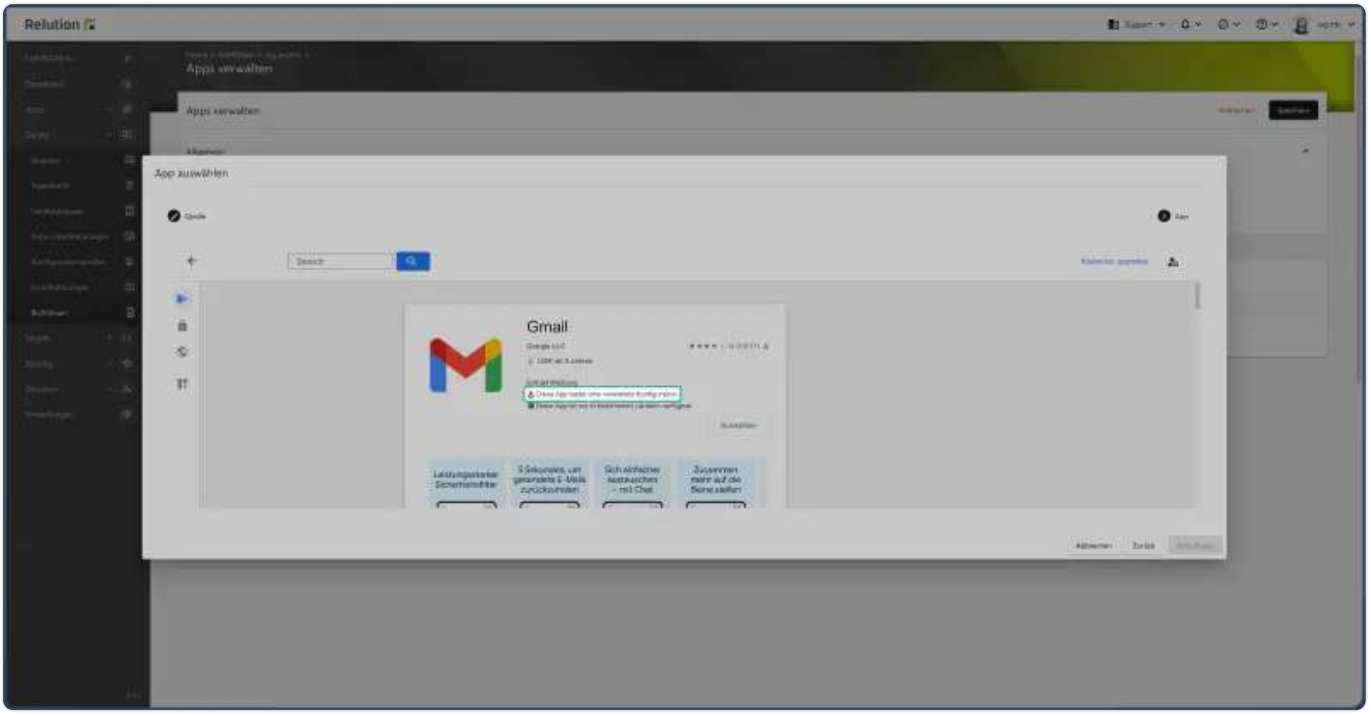
App hinzufügen

1. Im Relution Portal zur bestehenden oder neuen Android Enterprise Richtlinie navigieren.
2. Die Konfiguration Apps verwalten wählen.
3. Die gewünschte E-Mail-App (z. B. Google Mail oder Samsung Mail) aus dem Google Play Store hinzufügen, falls diese noch nicht in der Liste enthalten ist.

- Pfad `Portal` → `die AE Richtlinie` → `Apps verwalten` → `Hinzufügen` → `Managed Google Play Store App (Android Enterprise)` → `Google Mail/Samsung Mail (hinzufügen, falls nicht vorhanden)`

Für Version 26.4.0





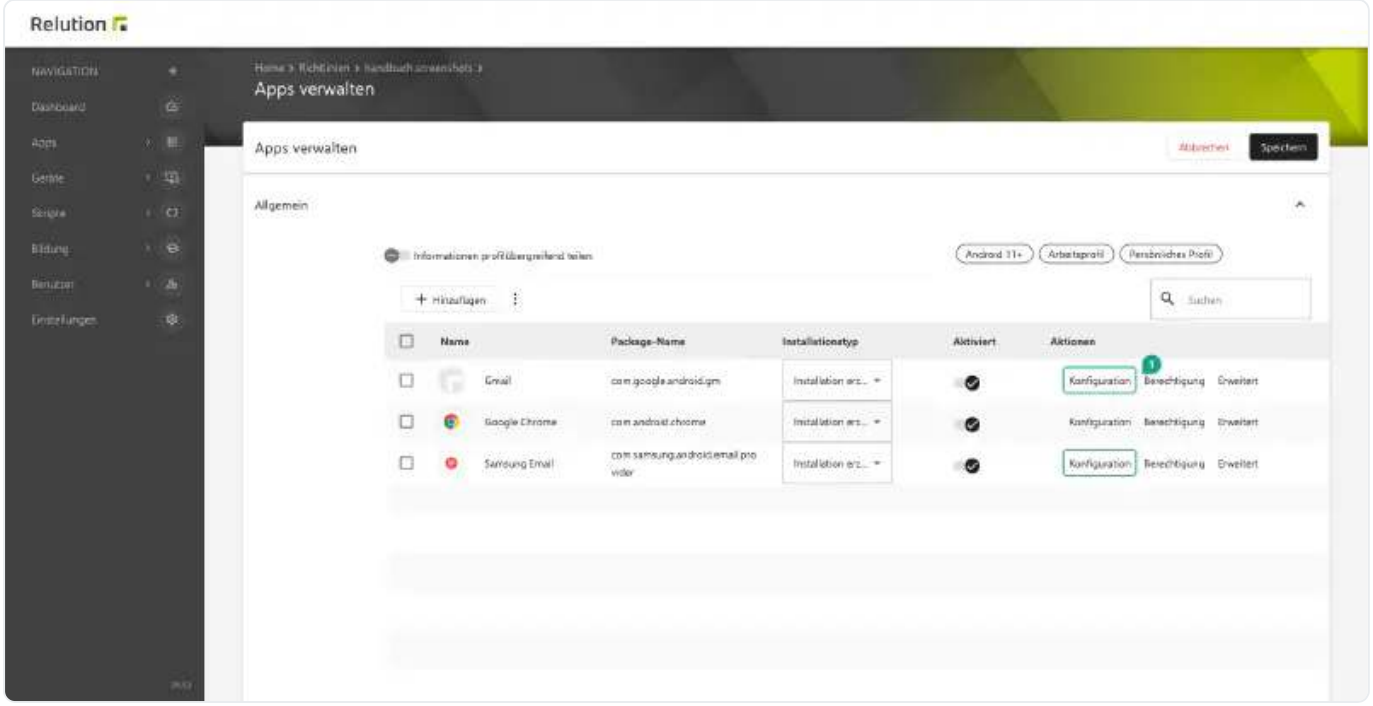
Hinweis zur App-Konfiguration: Apps, für die verwaltete Konfigurationsoptionen verfügbar sind (Managed Configs), sind direkt in der Auswahl kenntlich gemacht (wie in den Screenshots dargestellt). Zu beachten: Der Umfang dieser Konfigurationen wird ausschließlich vom jeweiligen App-Hersteller festgelegt. Relution hat keinerlei Einfluss auf die bereitgestellten Optionen.

Für Version 26.4.0

Konfiguration starten

1. Bei der hinzugefügten E-Mail-App auf Konfiguration klicken.
2. Im Dialog die gewünschten Werte eintragen (siehe unten) und mit Bestätigen übernehmen.
3. Die Konfiguration Apps verwalten anschließend mit Speichern sichern. Bestätigen übernimmt die Werte nur in die geöffnete Konfiguration, ohne Speichern gehen sie beim Verlassen der Seite verloren.

Änderungen sind nur in der neuesten, noch nicht veröffentlichten Richtlinienversion möglich. Ist diese bereits veröffentlicht, wird zuerst eine neue Version erstellt.



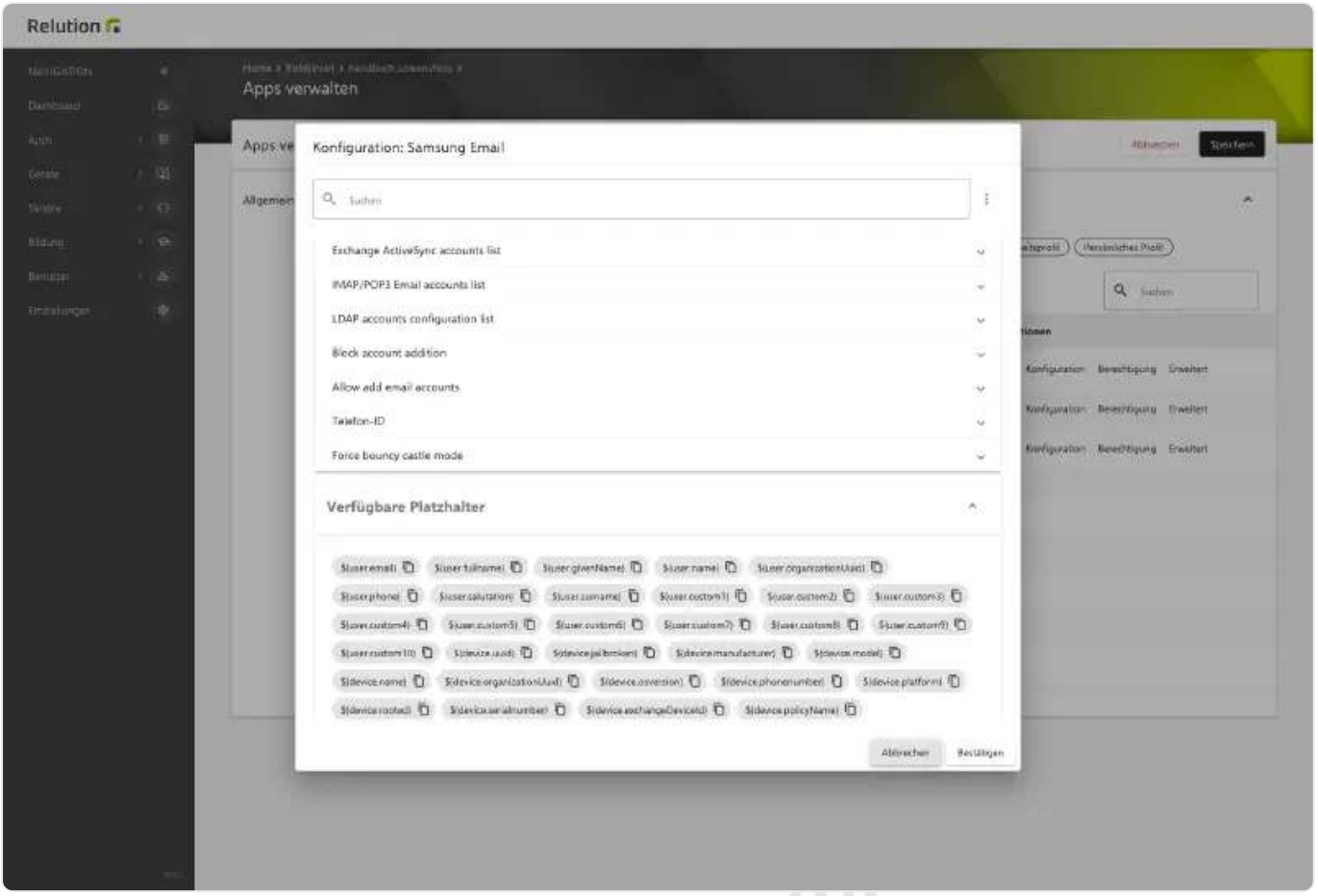
App-Konfiguration mit Platzhaltern (Managed Configuration)

Die Konfiguration des E-Mail-Clients erfolgt über die sogenannten Managed Configuration (Verwaltete Konfigurationen). Hier werden die Benutzerdaten und Serverinformationen hinterlegt, wobei Platzhalter (Variables) verwendet werden können, um die Einstellungen automatisch an den jeweiligen Benutzer anzupassen.

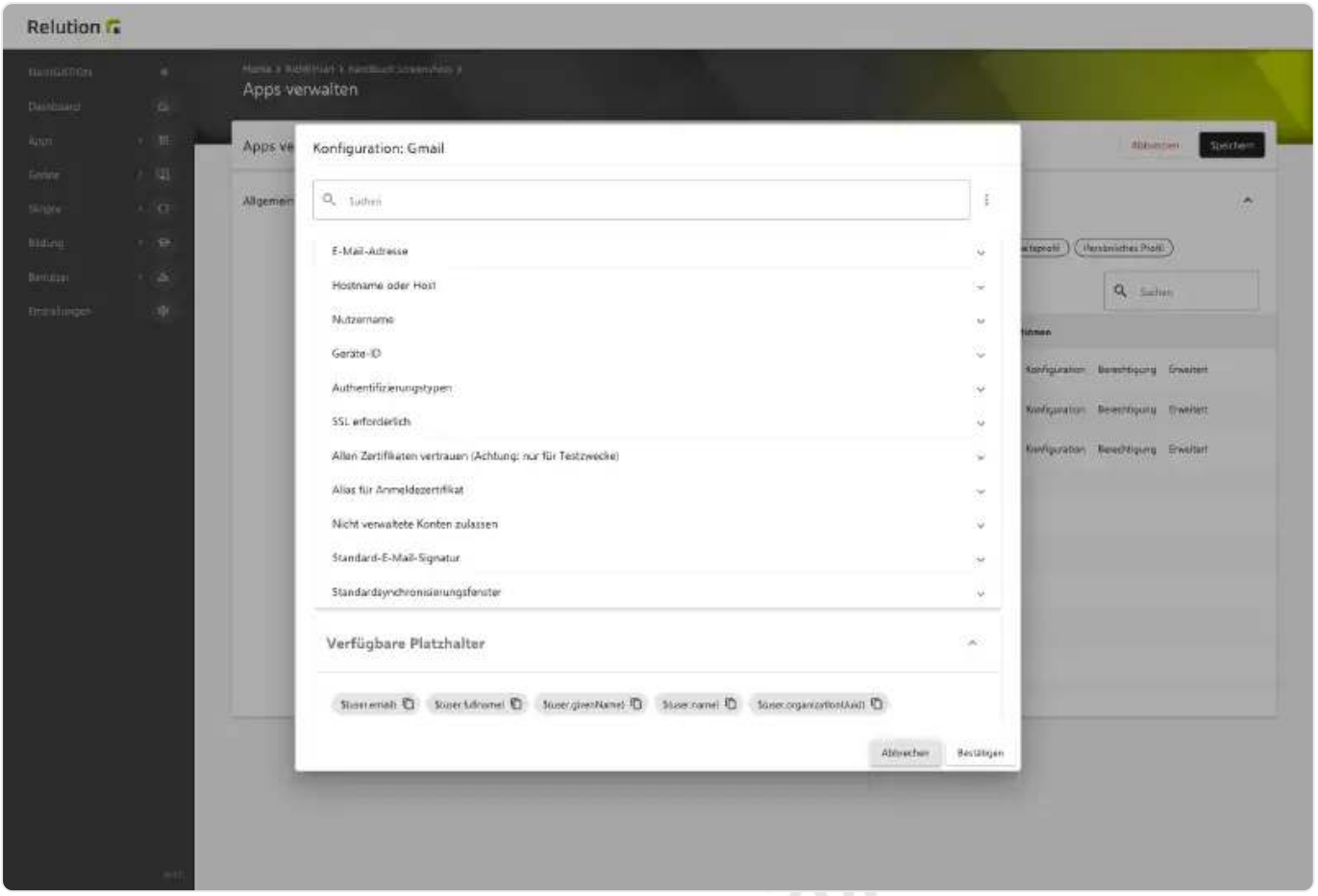
Für eine flexible und allgemeingültige Konfiguration lassen sich die Relution-Platzhalter (z.B. `${user.email}`) verwenden.

- Anzeige: Die verfügbaren Platzhalter werden in der jeweiligen Konfigurationsansicht angezeigt.
- Voraussetzungen für die Funktion: Damit diese Platzhalter korrekt aufgelöst werden, müssen folgende Bedingungen im Relution-System erfüllt sein:
  1. Gültige Daten: Die benötigten Informationen (z.B. eine E-Mail-Adresse für `${user.email}`) müssen gültig beim Benutzer hinterlegt sein.
  2. Gerätezuteilung: Der Benutzer muss dem betreffenden Gerät zugewiesen sein.

Für Version 26.4.0



Für Version 26.4.0



Für Version 26.4.0

Zusammenfassung und Verteilung

Nachdem die Managed Configuration gespeichert wurde, wird die E-Mail-App beim Veröffentlichen automatisch konfiguriert auf alle Geräte verteilt, denen die Richtlinie zugewiesen ist (z. B. über Gerätegruppen). Die Platzhalter werden dabei mit den Daten des Benutzers gefüllt, der dem jeweiligen Gerät zugewiesen ist. Die Benutzer müssen lediglich die App öffnen, ihr Passwort eingeben und können sofort ihre E-Mails abrufen, ohne manuelle Servereinstellungen vornehmen zu müssen.

Sollten die Daten in der Konfiguration in Relution angepasst aber auf dem Endgerät nicht angewendet werden, muss die entsprechende App gelöscht werden und die neue Konfiguration erneut angewendet werden.

Die Konfiguration zunächst mit einer kleinen Gruppe von Geräten testen, um sicherzustellen, dass alle Platzhalter und Servereinstellungen korrekt übernommen werden.

Konfiguration von Google Mail und Samsung Mail mit Secure Mail Gateway (SMG)

Beim Einsatz eines Secure Mail Gateway (SMG) sind spezifische Konfigurationsanpassungen der Mail-Apps erforderlich. Eine detaillierte Anleitung zur Durchführung dieser Integration und Anpassungen ist in der Knowledge Base zu finden: SMG-Integration für Gmail →

Für Version 26.4.0

GMail für SMG konfigurieren

Um das Secure Mail Gateway mit GMail zu nutzen, sind unter Android Enterprise einige Konfigurationen notwendig. Im Folgenden gibt es eine Übersicht der nötigen Parameter, welche konfiguriert werden müssen. Wichtig ist, dass es auf dem Gerät zuvor noch keine Konfigurationsversuche hinsichtlich GMail gab, da sonst Fragmente dieser Konfigurationen zu Fehlern führen können.

GMail von Google eignet sich als Mail Client und als Beispiel für diesen Artikel besonders gut, da die App in der Regel für alle Android Versionen und Gerätemodelle verfügbar ist.

Die App kann nicht von Hand auf dem Gerät konfiguriert werden, wenn das Secure Mail Gateway genutzt werden soll.

Diese Anleitung setzt ein funktionierendes und konfiguriertes Secure Mail Gateway voraus.

Konfiguration

Es werden folgende Konfigurationsparameter benötigt.

E-Mail-Adresse

Die wichtigste Frage, die sich stellt, ist, welche E-Mailadresse konfiguriert werden soll. Hier kann wahlweise eine feste Adresse oder die Variable `${user.email}` verwendet werden.

Für Version 26.4.0

Hostname

Als Hostname muss der Hostname der SMG Service-URL eingetragen werden, die in den Einstellungen des Secure Mail Gateway → hinterlegt ist. Je nach Einrichtung ist das der Hostname des Relution Servers oder eine eigene Subdomain des SMG-Dienstes.

> Wichtig: https:// darf nicht mit angegeben werden.

Nutzername

Der Nutzername muss in der Schreibweise `eindeutiger-Name-der-Relution-Organisation\Benutzername` angegeben werden. Der eindeutige Name der Organisation kann unter `Einstellungen` → `Allgemeine Organisations-Einstellungen` eingesehen werden.

Geräte ID

Hier muss zwingend die Variable `${device.exchangeDeviceId}` verwendet werden.

Authentifizierungstypen

Basisauthentifizierung zulassen muss aktiviert und Moderne Authentifizierung zulassen deaktiviert sein.

Outlook konfigurieren

In Relution kann Microsoft Outlook für Android Enterprise über eine Managed App Konfiguration vorkonfiguriert werden. Das E-Mail-Konto wird dabei über Platzhalter (z. B. `${user.email}`) automatisch befüllt, sodass beim ersten Start der App lediglich das Passwort eingegeben werden muss.

Nachfolgend wird eine minimale Konfiguration für ein Microsoft-365-Konto beschrieben.

Konfiguration

`Portal` → `die AE Richtlinie` → `Apps verwalten` → `Microsoft Outlook (hinzufügen falls nicht vorhanden)` → `Konfiguration`

Im Konfigurations-Pop-up werden die folgenden Felder befüllt. Alle Schlüssel besitzen das gemeinsame Präfix `com.microsoft.outlook.EmailProfile.`.

Für Version 26.4.0

Schlüssel	Wert	Beschreibung
`ServerHostName`	`outlook.office365.com`	Adresse des Microsoft-365-/Exchange-Servers
`EmailUPN`	`${user.email}`	User Principal Name (Anmeldename des Kontos)
`EmailAddress`	`${user.email}`	E-Mail-Adresse des Kontos
`EmailAccountName`	`${user.fullname}`	Anzeigename des Kontos
`AccountType`	`ModernAuth`	Authentifizierungsverfahren (moderne Authentifizierung)

Die Platzhalter `${user.email}` und `${user.fullname}` werden je Benutzer automatisch aufgelöst. Weitere Platzhalter und Funktionen sind unter Erweiterte Platzhalter → beschrieben.

Datentrennung

Für die Trennung von geschäftlichen und privaten Daten auf Android-Geräten stehen drei grundlegende Ansätze zur Verfügung: die vollständige Geräteverwaltung eines organisationseigenen Geräts, das verwaltete Gerät mit persönlichem Profil (COPE) als organisationseigenes Gerät mit getrenntem privatem Bereich oder das Arbeitsprofil als abgegrenzter Container auf einem privaten Gerät.

Vollständige Geräteverwaltung (Device Owner, ab Android 9)

Spätestens seit Relution 5 ist bei der Verwaltung von Android-Geräten in Relution verstärkt die Android Enterprise Einschreibung als vollständig verwaltetes Gerät (Device Owner) gebräuchlich. Die MDM-Funktionen sind dabei im Betriebssystem integriert und standardisiert. Dies ermöglicht eine weitgehend herstellerunabhängige, einheitliche MDM-Funktionalität auf der Android-Plattform. Die Android Enterprise Funktionen stehen ausschließlich für zertifizierte Geräte zur Verfügung. Samsung-Geräte können mittels der KNOX-Funktionen noch umfangreicher administriert und abgesichert werden. Die Relution Client App wird bei der Android Enterprise Einschreibung nicht mehr zwingend benötigt.

Zusätzlich steht weiterhin die klassische Einschreibung als Device Administrator zur Verfügung. Dabei erhält die Relution Client App besondere Rechte auf dem Gerät, damit sie die MDM-Funktionen ausführen darf. Bei dieser Art der Einschreibung sind die Möglichkeiten des MDM-Eingriffs jedoch stark vom verwendeten Android-Gerät abhängig.

Bei der Verwaltung von Android-Geräten stehen vielfältige Konfigurationen und Funktionen zur Verfügung:

- Installation und Konfiguration von Apps (bspw. Exchange-Client)
- Managed Google Play Store
- WLAN- und VPN-Konfiguration
- Vollautomatische Einschreibung der Geräte (KNOX Mobile Enrollment).

Für Version 26.4.0

Verwaltetes Gerät mit persönlichem Profil (COPE)

Mit der Einschreibungsart Verwaltetes Gerät mit persönlichem Profil einrichten (Company Owned, Personally Enabled – COPE) wird ein organisationseigenes Gerät an Benutzer ausgegeben, die es auch privat nutzen dürfen. Neben dem verwalteten Bereich steht ein persönliches Profil zur Verfügung, auf das Administratoren weder Einblick noch Zugriff haben. Relution verwaltet dabei das gesamte Gerät und kann es beispielsweise auf Werkseinstellungen zurücksetzen, wodurch auch alle privaten Daten gelöscht werden.

Persönliches Profil →

Arbeitsprofil Einschreibung

Android Enterprise bietet zusätzlich das sogenannte Arbeitsprofil an, das für private Geräte gedacht ist und einen Container (Arbeit) auf dem Gerät einrichtet, der von Relution verwaltet werden kann. In diesem Container findet sich ein Managed Play Store, der lediglich freigegebene Apps zur Installation bereitstellt. Die Installation der Apps aus dem Managed Google Play Store ist ohne einen lokalen Google-Account möglich. Zusätzlich können die Apps über Relution konfiguriert werden, sofern eine Managed App Configuration von der jeweiligen App unterstützt wird (z. B. eine E-Mail-App mit vorgegebener Server-Adresse und Benutzerkennung). Der Container kann auch ein eigenes Adressbuch zur Trennung von geschäftlichen und privaten Kontakten enthalten.

Alles außerhalb des Containers (Persönlich) kann Relution nicht beeinflussen, das Gerät kann also beispielsweise nicht auf Werkseinstellungen zurückgesetzt werden. Der Container lässt sich aber über Relution entfernen, womit dann alle darin vorhandenen Daten gelöscht werden. Die Aktion Gerät vollständig sperren steht auch für Geräte mit Arbeitsprofil zur Verfügung. Ob dabei nur das Arbeitsprofil oder das gesamte Gerät gesperrt wird, hängt von Android und den Sperreinstellungen auf dem Gerät ab.

Relution unterstützt das Arbeitsprofil in einer Organisation parallel zur vollständigen Geräteverwaltung von Android Enterprise und der klassischen Einschreibung als Device Administrator. In Relution ist somit ein Mischbetrieb mit unterschiedlichen Geräten möglich.

Funktions-Einschränkungen

Ferner können im Container Arbeit folgende Funktionen per Restriktion ebenfalls abgeschaltet werden:

- App Block-/Allow-Listing
- Neue Benutzer und Profile anlegen
- Konten hinzuzufügen und entfernen
- Apps installieren
- Apps deinstallieren
- Kamera verwenden
- Bildschirmfotos machen
- Bluetooth konfigurieren und verwenden
- Kontakte über Bluetooth teilen
- Mobiles Netzwerk konfigurieren
- VPN konfigurieren
- Android Beam (NFC) zum Teilen von App-Daten verwenden
- Externe physikalische Medien einbinden

Die Konfiguration von WLAN-Netzwerken und die Dateiübertragung per USB lassen sich nur auf verwalteten Geräten und Geräten mit persönlichem Profil (COPE) einschränken, nicht im Arbeitsprofil privater Geräte.

Für Version 26.4.0

Homescreen als Standard-Launcher

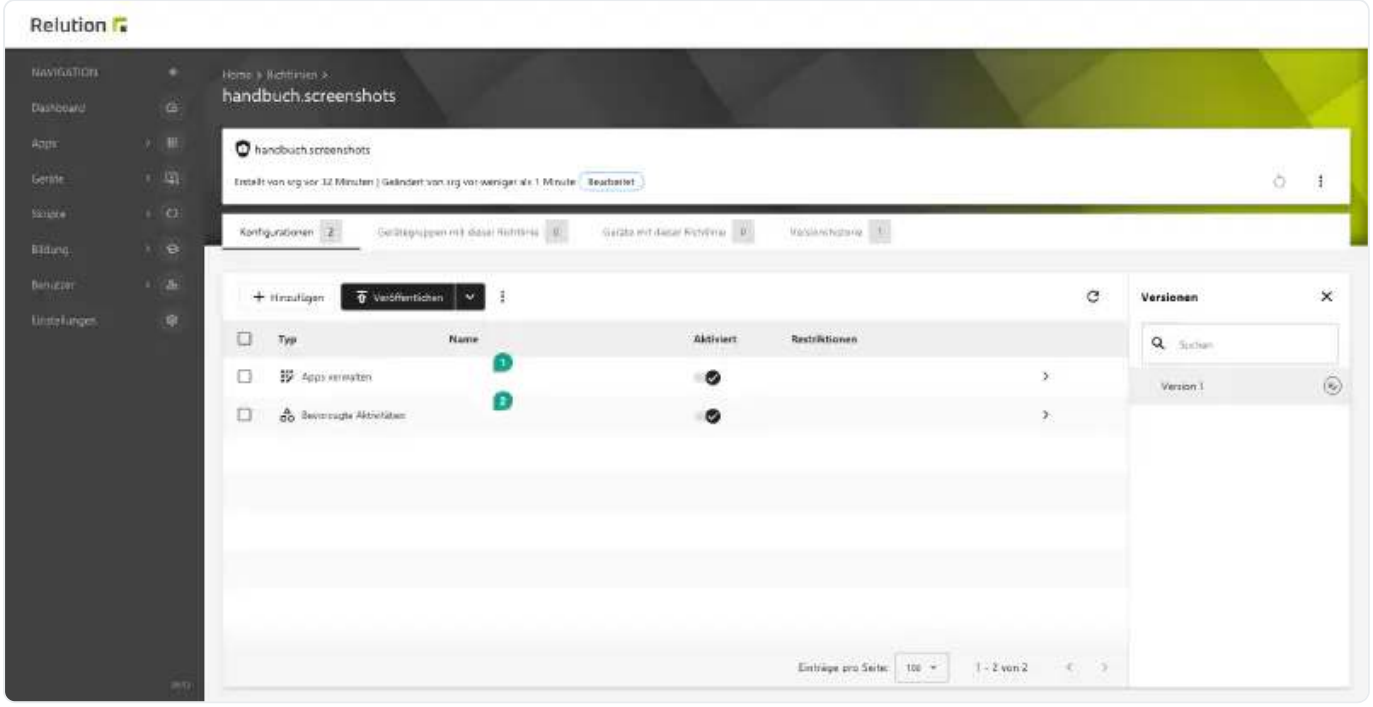
Der Relution Homescreen kann auf zwei Arten genutzt werden:

1. Kiosk-Modus →: Über die dedizierte Relution Homescreen-Konfiguration (strikt abgeriegelt).
2. Separater Launcher: Durch das Setzen als Standard-App.

Die Nutzung als Standard-Launcher bietet den Vorteil, dass Benachrichtigungen auf dem Sperrbildschirm sichtbar bleiben, das System-Menü vom oberen Bildschirmrand erreichbar ist und System-Apps bei Bedarf eingeblendet werden können.

Richtlinie mit den Konfigurationen

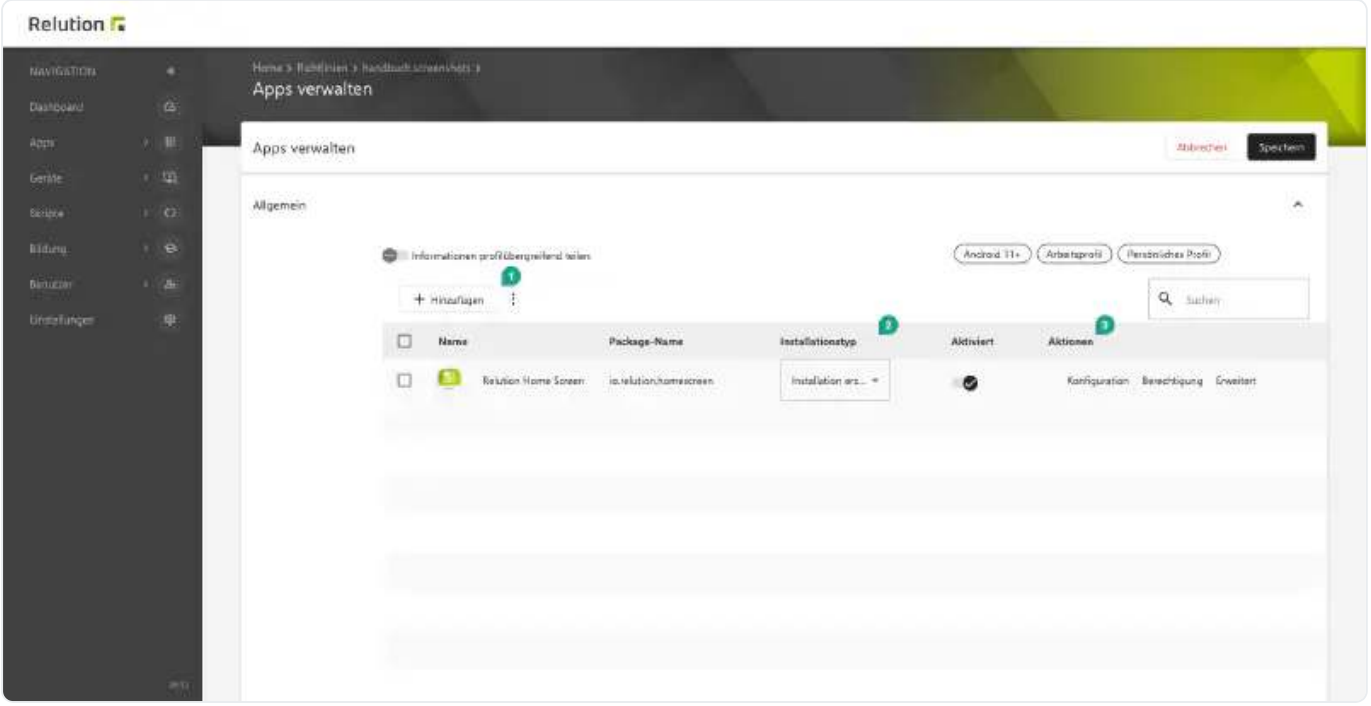
Damit der Relution Homescreen als Standard-Launcher fungiert, ohne den restriktiven Kiosk-Modus zu erzwingen, müssen zwei spezifische Konfigurationen innerhalb einer Richtlinie kombiniert werden: Apps verwalten und Bevorzugte Aktivitäten.

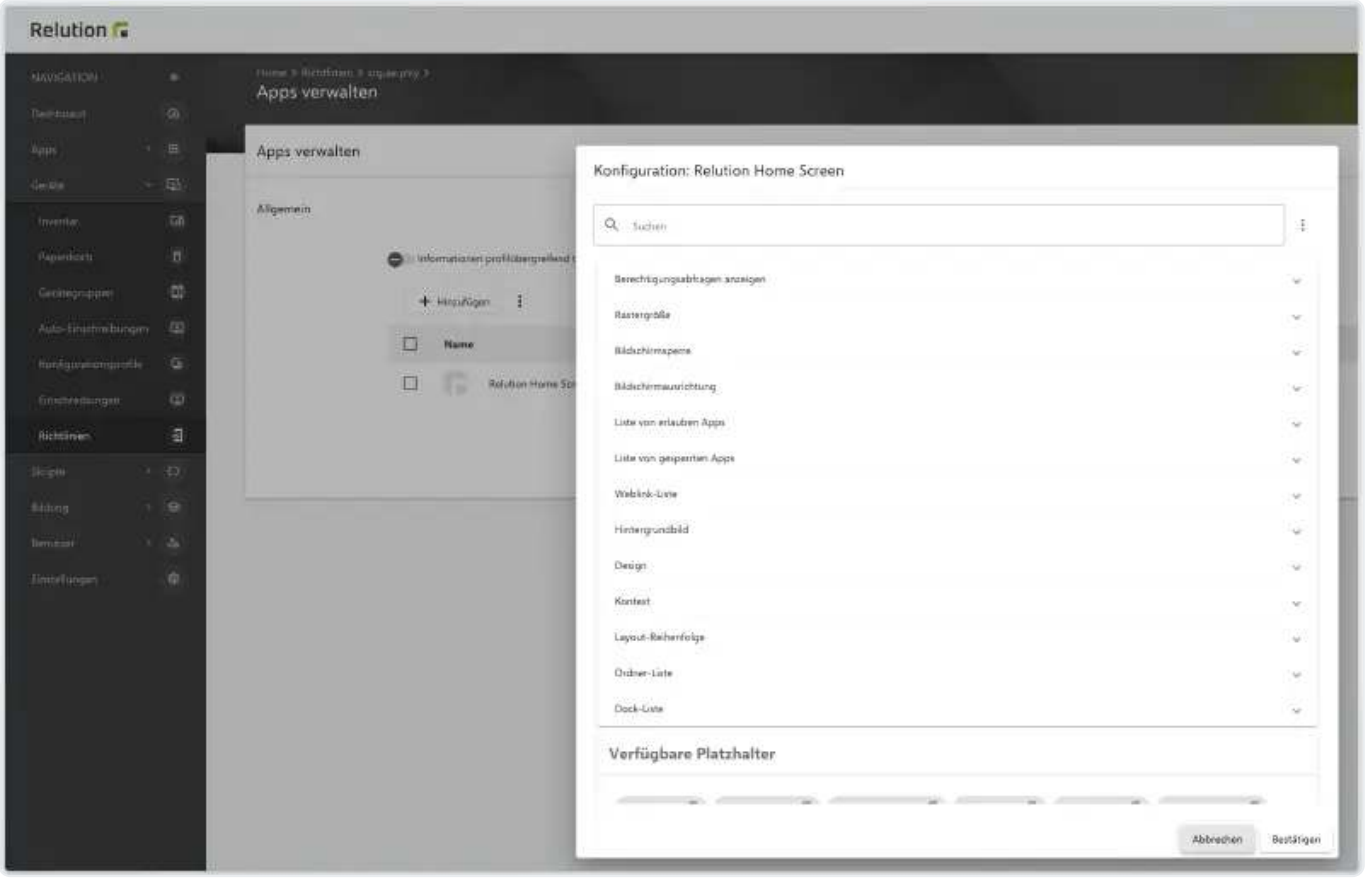


Apps verwalten

Diese Konfiguration stellt sicher, dass die App auf dem Gerät vorhanden und korrekt eingestellt ist.

- Die App Relution Homescreen (`io.relution.homescreen`) über den Hinzufügen-Button aus dem Google Play Store zur Apps-verwalten-Liste hinzufügen (1).
- Den Installationstyp auf Installation erzwungen setzen (2).
- Über den Link Konfiguration in der Spalte Aktionen lassen sich die gewünschten Einstellungen für das Layout und die Funktionen des Homescreens manuell hinterlegen (3).

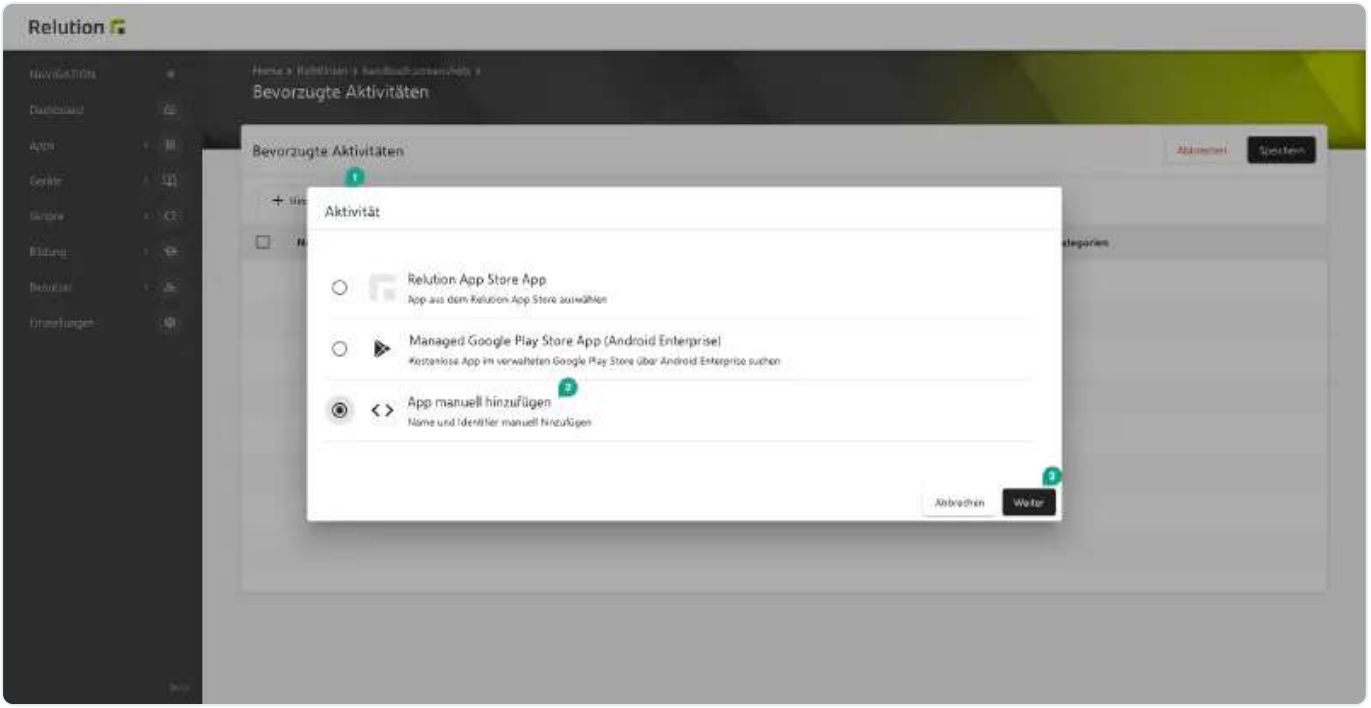




Bevorzugte Aktivitäten

Diese Konfiguration ändert das Standardverhalten von Android und legt fest, dass der Relution Homescreen die primäre Benutzeroberfläche (Home) ist. Alle Felder beschreibt der Artikel Bevorzugte Aktivitäten →.

In der Konfiguration auf Hinzufügen klicken und App manuell hinzufügen wählen.



Folgende Identifikatoren angeben:

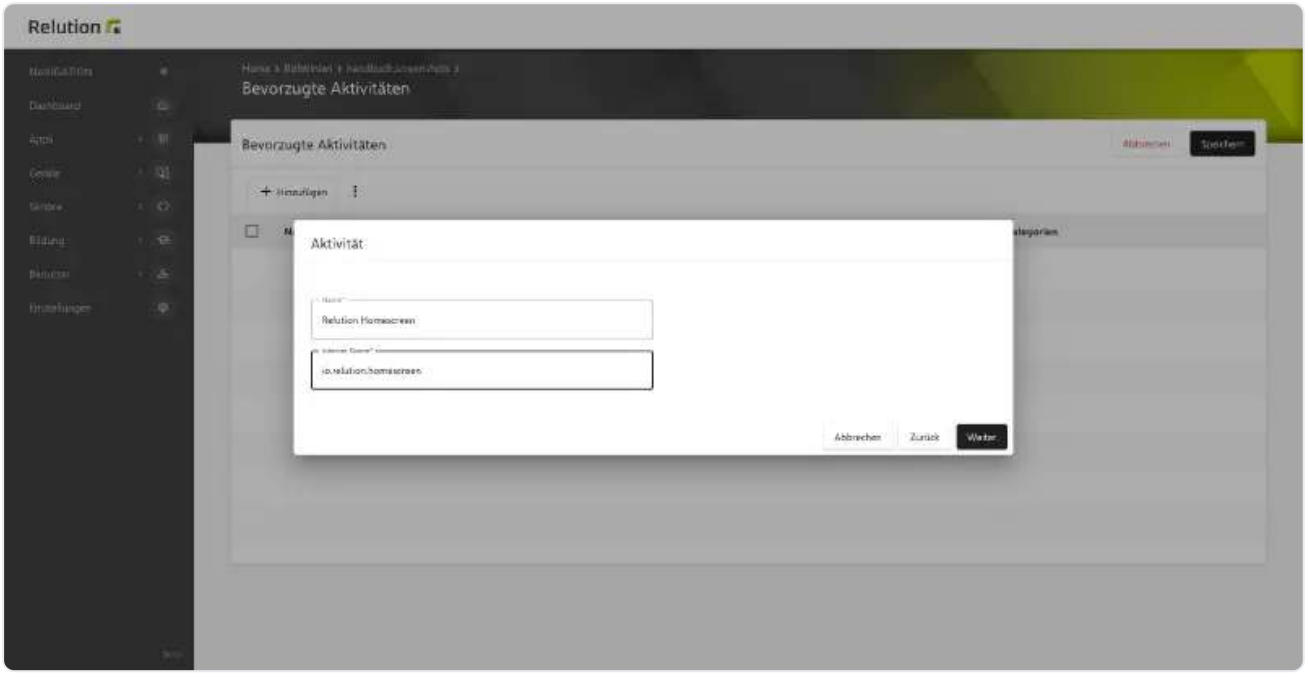
Für Version 26.4.0

- Name:

```
Relution Homescreen
```

- Interner Name (Package Name):

```
io.relution.homescreen
```



Die Parameter exakt wie folgt befüllen:

- Aktivität:

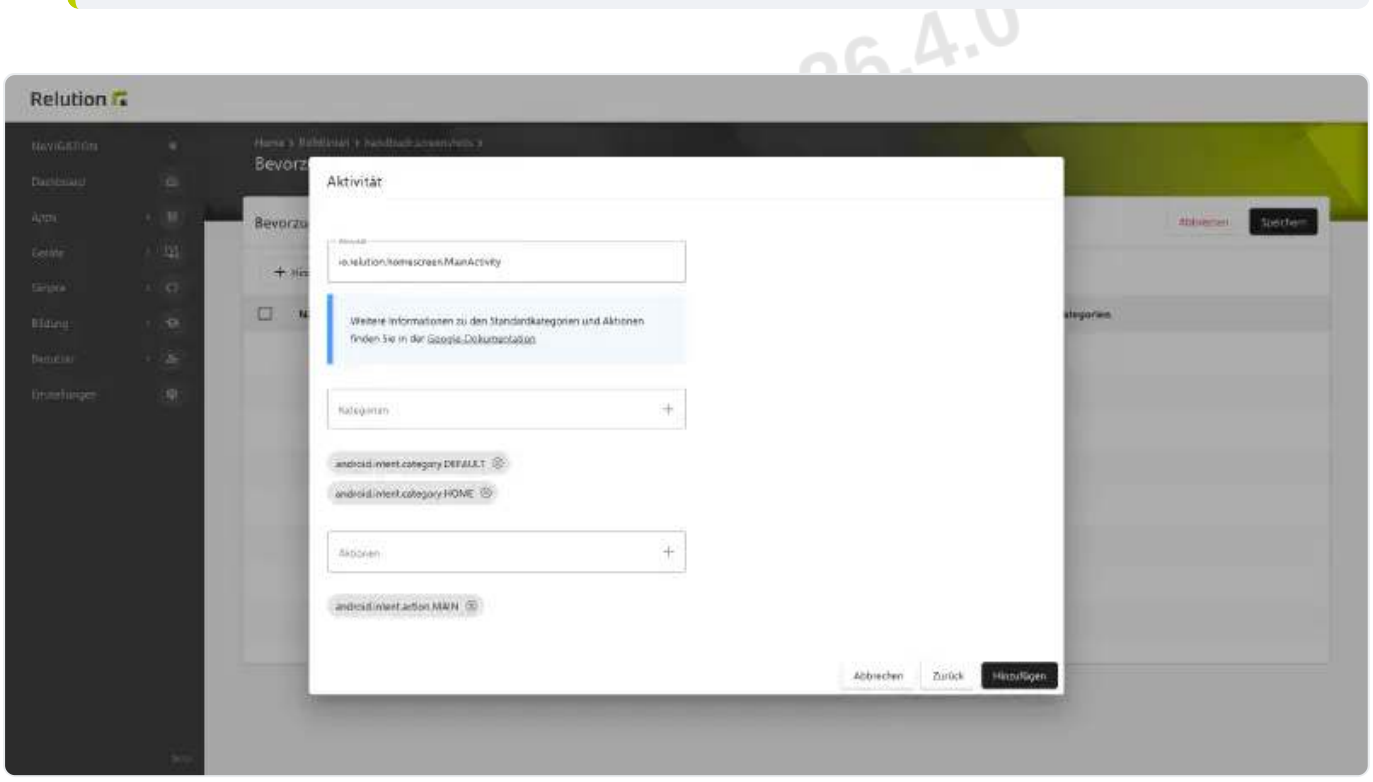
```
io.relution.homescreen.MainActivity
```

- Kategorien:

```
android.intent.category.DEFAULT
android.intent.category.HOME
```

- Aktionen:

```
android.intent.action.MAIN
```



Zuweisung

Nachdem beide Konfigurationen in der Richtlinie gespeichert wurden, muss diese einer entsprechenden Gerätegruppe zugewiesen werden. Nach dem Push der Richtlinie wird der Relution Homescreen automatisch als Standard-Launcher aktiviert.

Standort Dienste

Mit Relution ist es möglich, Standortdienste für Android Enterprise-Geräte zu konfigurieren. Der Administrator kann dabei die Ortungsdienste des Geräts und Standortberechtigungen für einzelne Apps fest vorgeben oder dem Benutzer überlassen.

Ortungsdienste

Über die Konfiguration Standort-Modus → legen Administratoren im Feld Standorteinstellungen auf dem Gerät fest, ob Benutzer die Ortungsdienste an- oder ausschalten können. Dazu muss das Feld auf Wahl durch Benutzer gestellt werden. Wird keine Konfiguration vorgegeben, so ist Wahl durch Benutzer die Voreinstellung.

Werden die Ortungsdienste nachträglich oder während der Einrichtung des Gerätes deaktiviert, können Apps das Gerät nicht orten, unabhängig davon, welche Berechtigungen vergeben wurden. Das betrifft alle Apps, z.B. auch Google Maps oder Waze.

- Die Option Standorteinstellung auf dem Gerät aktivieren aktiviert die Standorteinstellung auf dem Gerät. Ab Android 11 können Arbeitsprofile auf unternehmenseigenen Geräten die Standortdienste nicht direkt erzwingen; in diesem Fall muss der Benutzer die Standortdienste manuell in den Geräteeinstellungen aktivieren.
- Die Option Deaktiviert deaktiviert und verbietet die Änderung der Standorteinstellung

Standard App-Berechtigungen

Für Version 26.4.0

Ob die Relution Agent und Companion Apps die Berechtigung zur Ortung bekommen, hängt davon ab, was unter `Portal` → `Einstellungen` → `Geräteverwaltung` → `Einschreibungen` in der Zeile Gerät orten eingestellt ist. Wenn hier die Ortung für COD abgeschaltet ist, erhalten beide Apps keine Berechtigung zur Ortung.

> Companion: seit Server-Version 5.18.0, Agent: seit Server-Version 5.19.3.

Individuelle App-Berechtigungen

Diese Voreinstellung lässt sich zusätzlich noch individuell überschreiben, indem eine App der Konfiguration Apps verwalten hinzugefügt wird. Wenn hier der Relution Agent und/oder der Companion hinzugefügt wird, können die Berechtigungen der App einzeln eingestellt werden. So lässt sich dem Benutzer zum Beispiel das Recht geben, alle Berechtigungen der App selbst einzustellen.

> Companion: seit Server-Version 5.18.0, Agent: seit Server-Version 5.19.3.

Ohne Berechtigung für den Agent kann beispielsweise die Vergabe von Richtlinien, abhängig von Geofences und iBeacons, nicht verwendet werden. Ohne Berechtigung für den Companion kann die Aktion `Gerät orten` nicht verwendet werden.

Die Standard-Antwort auf Berechtigungsanforderungen wird wie folgt gesetzt: `Portal` → `die AE Richtlinie` → `Apps verwalten` → `Relution Companion for AE` (hinzufügen, falls nicht vorhanden) → `Berechtigung` Hier öffnet sich ein PopUp mit dem Punkt Standard-Antwort auf Berechtigungsanforderungen

Wenn die Google Location Services bei der Geräteeinrichtung deaktiviert wurden, müssen sie im Relution Companion nachträglich für die Ortung aktiviert werden.

Factory Reset Protection

Für Android Enterprise Geräte bietet Relution in den Restriktionen einer Richtlinie zwei Einstellungen rund um das Zurücksetzen auf Werkseinstellungen. Beide wirken unabhängig voneinander und lassen sich kombinieren:

- Der Schalter Aktivieren Sie den Factory Reset-Schutz (FRP) sperrt auf verwalteten Geräten das Zurücksetzen über die Android-Einstellungen. Ein Zurücksetzen über das Wiederherstellungsmenü bleibt möglich.
- Im Feld Google account email für FRP werden Google-Konten hinterlegt. Nach einem Zurücksetzen wird im Einrichtungsprozess des Geräts eine Aufforderung angezeigt, sich mit einem dieser Konten anzumelden, um das Gerät wieder betriebsbereit zu machen. Ist kein Konto eingetragen, ist FRP nicht aktiv.

FRP konfigurieren

1. Im Relution-Portal zum Menüpunkt `Geräte` → `Richtlinien` navigieren und auf Hinzufügen klicken.
2. Eine Android-Enterprise-Richtlinie erstellen und einen Namen vergeben. Auf Speichern klicken.
3. Nach Klick auf Hinzufügen anschließend die Option Restriktionen wählen und mit Details hinzufügen fortfahren.
4. Optional den Schalter Aktivieren Sie den Factory Reset-Schutz (FRP) aktivieren, um das Zurücksetzen über die Android-Einstellungen zu sperren. Über das Wiederherstellungsmenü bleibt das Zurücksetzen möglich.
5. Optional im Feld Google account email für FRP ein oder mehrere Google-Konten eintragen. Nach einem Zurücksetzen muss sich eines dieser Konten anmelden, um das Gerät zu entsperren. Bleibt das Feld leer, ist FRP nicht aktiv.
6. Die Konfiguration speichern und die aktuelle Version der Richtlinie veröffentlichen.
7. Um die Richtlinie auf Android-Enterprise-Geräten anzuwenden, die gewünschten Geräte über das Tab Geräte mit dieser Richtlinie hinzufügen. Die gewählten Einstellungen werden anschließend automatisch auf den Geräten ausgeführt.

Für Version 26.4.0

Captive Portal anzeigen

Um eine Verbindung mit einem WLAN herzustellen, muss bei Android Enterprise ein Packagename freigegeben werden. Dieser lautet `com.android.captiveportallogin` und muss in der Apps verwalten Konfiguration manuell als Verfügbar hinzugefügt werden. Das Hinzufügen erfolgt über Hinzufügen mit der Quelle App manuell hinzufügen, der Paketname wird dabei im Feld Interner Name eingetragen. Manuell hinzugefügte Apps erhalten zunächst den Installationstyp Installation erzwungen, daher wird der Wert in der Spalte Installationstyp anschließend auf Verfügbar umgestellt.

Anschließend ist es möglich, eine Verbindung mit einem WLAN herzustellen, das ein Captive Portal einblendet.

Anrufe werden nicht angezeigt

Im Kiosk-/Homescreen Layout Modus zeigt Android Enterprise eingehende und ausgehende Anrufe nicht an: Das Gerät klingelt oder vibriert zwar, es erscheint jedoch kein Anruf-Overlay auf dem Bildschirm. Grund dafür ist, dass Android in diesem Modus alle Apps und Overlays blockiert, die nicht explizit per Richtlinie freigegeben sind – die Anruf-UI wird über herstellerspezifische System-Pakete gesteuert, die dafür in der Whitelist stehen müssen. Folgende Anpassungen an der Richtlinie beheben das Problem:

Richtlinien-Einstellungen anpassen

Damit das Anruf-Fenster technisch als System-Overlay agieren und einfliegen kann, muss der Kiosk-Modus anstelle des Homescreen Layout verwendet werden.

Zudem müssen in der Konfiguration Kiosk-Modus folgende Parameter zwingend gesetzt werden:

- Toasts und Overlays deaktivieren (Abschnitt Allgemein): Muss deaktiviert sein (damit Overlays zugelassen sind).
- Statusleiste (Abschnitt Kiosk-Anpassung): Muss auf Aktiviert stehen (da das Anruf-Banner technisch als System-Benachrichtigung einfliegt).

Falls der native Kiosk-Modus für den Anwendungsfall nicht flexibel genug ist, kann über die Option Statt dem Standard-Launcher eine benutzerdefinierte Kiosk-App verwenden ein alternativer Launcher wie der Microsoft Managed Homescreen eingebunden werden. Dieser bietet für komplexe Szenarien weitreichendere Konfigurationsmöglichkeiten.

Für Version 26.4.0

> Bei Verwendung des Relution Homescreens – sowohl in der Kiosk- als auch in der Layout-Konfiguration – können diese System-Overlays aus technischen Gründen nicht erzwungen und auch keine Benachrichtigungstöne abgespielt werden.

Soll der Relution Homescreen verwendet werden, muss dieser über bevorzugte Aktivitäten → konfiguriert werden.

Erforderliche Paketnamen nach Hersteller freigeben

Die benötigten System-Apps für die Telefoniefunktion müssen über ihren exakten Paketnamen in der Konfiguration Apps verwalten eingetragen und in der Spalte Installationstyp auf Verfügbar gesetzt werden.

Samsung Geräte

- `com.samsung.android.incallui` — Zuständig für das visuelle Anruffenster und die Steuerung während des Telefonats.
- `com.android.systemui` — Erlaubt Head-up-Benachrichtigungen (Anruf-Banner) bei aktivem Bildschirm.
- `com.samsung.android.dialer` — Die eigentliche Samsung Telefon-App (Wähltastatur).
- `com.samsung.android.smartcall` — Samsung Anruferkennung und systemseitiger Spam-Schutz.

Google Pixel Geräte

- `com.google.android.dialer` — Die Google Telefon-App inklusive der nativen, integrierten InCall-UI.
- `com.android.systemui` — Steuert die Benachrichtigungszeile und das Einblenden des oberen Anrufbanners.
- `com.google.android.as` — Android System Intelligence (notwendig für die KI-gestützte Anrufverarbeitung auf Pixel-Geräten).

Benachrichtigungstöne

Neben der Anruf-UI ist auch die Wiedergabe von Benachrichtigungstönen vom eingesetzten Launcher abhängig.

In den übrigen Launchern werden Benachrichtigungstöne abgespielt, sofern das Paket `com.android.systemui` in der Konfiguration Apps verwalten in der Spalte Installationstyp auf Verfügbar gesetzt ist:

- Nativer Kiosk-Modus (Standard-Launcher der Android Enterprise Konfiguration)
- Microsoft Managed Homescreen (über die Option Statt dem Standard-Launcher eine benutzerdefinierte Kiosk-App verwenden)

Dateiübertragung via USB

Für Version 26.4.0

Die USB-Datenübertragung (Dateien/Bilder) ist auf Android-Geräten nicht mehr auswählbar, der entsprechende Menüpunkt fehlt am Gerät. Grund dafür ist, dass Google ein Feld in der API nicht mehr berücksichtigt, das den USB-Zugriff regelt – als neuer Standardwert wird die Funktion seitdem deaktiviert.

Funktion wiederherstellen

Ab Relution 5.22.4 ist serverseitig für vollständig verwaltete Geräte und verwaltete Geräte mit persönlichem Profil (COPE) ein neuer Standardwert hinterlegt, der die Funktion wieder aktiviert:

1. Relution auf mindestens Version 5.22.4 aktualisieren (siehe Changelog →).
2. Richtlinie prüfen, da der Standardwert nur greift, wenn die Richtlinie die USB-Dateiübertragung nicht selbst regelt:
   - In der Konfiguration Restriktionen darf die Option Verbieten, Dateien über USB zu übertragen nicht aktiviert sein (siehe Restriktionen →).
   - Enthält die Richtlinie eine Konfiguration Gerätekonnektivität → (ab Relution 5.24.0), gilt anstelle des Standardwerts deren Einstellung USB-Datenzugriff. Dort muss USB-Datenübertragung zulassen gewählt sein. Bei der Vorauswahl Nicht spezifiziert bleibt die Dateiübertragung per USB gesperrt.
3. Richtlinien auf den betroffenen Geräten erneut anwenden: Unter `Geräte` → `Inventar` einen Filter auf alle Android-Geräte setzen, alle markieren und über das Drei-Punkte-Menü die Richtlinien neu anwenden.

Manuelle Einschreibung

Um Geräte in Relution verwalten zu können, müssen diese eingeschrieben werden. Dazu wird in Relution eine Einschreibung (Registrierung) erstellt, die anschließend auf dem Gerät durchgeführt werden muss.

Die Erstellung einer Einschreibung in Relution ist für alle Plattformen gleich. Der anschließende Einschreibeprozess auf den Geräten ist plattformspezifisch `Android Classic/Legacy`.

Seit dem 1. Januar 2025 unterstützt Relution nur noch Android 10 und neuer. Dies gilt sowohl für Android Enterprise als auch für Android Classic/Legacy. Der Support für frühere Android-Versionen wurde eingestellt.

Relution stellt den Support für Samsung-Geräte mit Android 15+ ein, wenn diese über Android Classic verwaltet werden. Wir empfehlen den Wechsel auf Android Enterprise.

Samsung-Geräte mit Android 15 können zwar noch über Android Classic verwaltet werden. Grundfunktionen wie das Installieren oder Aktualisieren von nativen Apps stehen dann jedoch nicht mehr zur Verfügung. Mit Android 16 wird der KIOSK Modus ebenfalls seitens Samsung entfernt.

Für Version 26.4.0

Vorbedingungen für Einschreibungen

- Für die Erstellung von Einschreibungen müssen Benutzer der Benutzergruppe `Administrator` oder `Device Manager` der Organisation zugeordnet sein.
- Zur Durchführung der Registrierung auf den Geräten müssen Endanwender mindestens der Benutzergruppe `User` der Organisation zugeordnet sein.
- Einschreibungen werden in der Organisation erstellt, in der das Gerät verwaltet werden soll. In der globalen Organisation können keine Geräte eingeschrieben werden.
- Hintergrundwissen, welche Einschreibung für welche Android-Plattform genutzt wird - `Android Classic/Legacy` im Gegensatz zu `Android Enterprise`.

Manuelle Einschreibungen anlegen

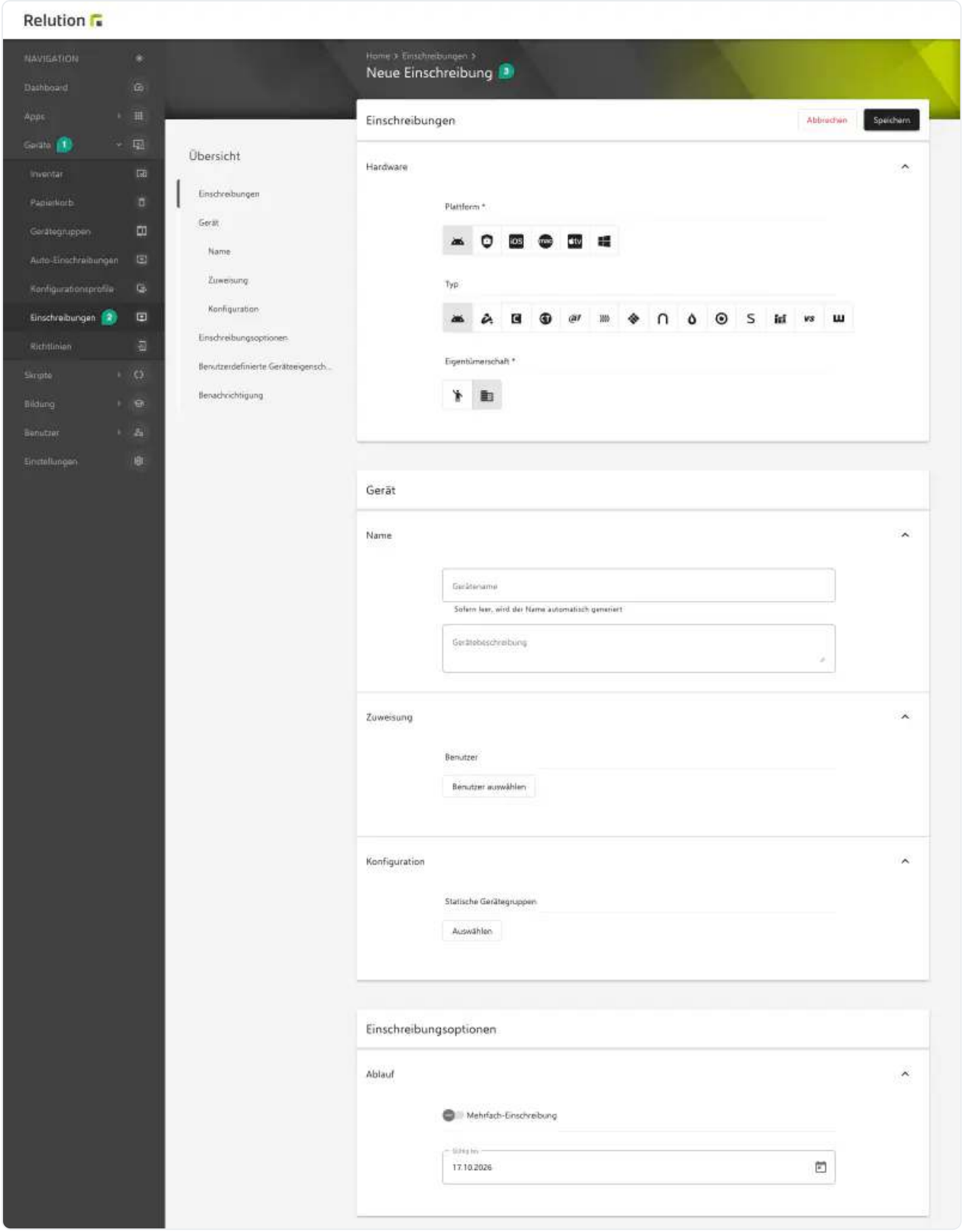
1. Zu `Geräte` → `Inventar` navigieren und auf Einschreiben klicken (alternativ unter `Geräte` → `Einschreibungen` auf Hinzufügen).
2. Als Plattform Android sowie die Eigentümerschaft, z. B. COD - Company Owned Device, wählen. Unter Typ bleibt Android ausgewählt. Die übrigen Typen sind für die Einschreibung von interaktiven Displays vorgesehen, siehe Whiteboards →.
3. Auf Speichern klicken, um die Einschreibung zu erstellen.

Optional

- Gerätename und Gerätebeschreibung: Das Gerät und die Einschreibung werden benannt. Die Beschreibung wird beim Gerät im Inventar angezeigt. Beide Felder können Benutzer-Platzhalter wie `${user.givenName}` enthalten, die bei der Einschreibung anhand des zugewiesenen Benutzers ersetzt werden, siehe Erweiterte Platzhalter →.
- Benutzer: Relution Benutzer können z. B. für eine 1:1-Ausstattung Geräten zugewiesen werden. Es kann immer nur ein Benutzer einem Gerät zugewiesen werden.
- Statische Gerätegruppen: Das Gerät wird nach erfolgreicher Einschreibung den ausgewählten Gerätegruppen → hinzugefügt. Die diesen Gruppen zugewiesenen Richtlinien werden anschließend auf dem Gerät angewendet. Das Feld ist nur mit der Berechtigung zum Bearbeiten von Gerätegruppen sichtbar.
- Mehrfach-Einschreibung: Wenn aktiviert, können mit einer Einschreibung mehrere Geräte eingeschrieben werden.
- Gültig bis: Datum, nach dem die Einschreibung nicht mehr verwendet werden kann. Vorbelegt ist das Ende des siebten Tages nach der Erstellung, das Datum kann beliebig geändert werden. Bleibt das Feld leer, ist die Einschreibung unbefristet gültig.
- Benutzerdefinierte Geräteeigenschaften: Anpassbare Felder für weitere Informationen.

Für Version 26.4.0

- Benachrichtigung: Auswahl, ob der Benutzer per E-Mail oder SMS über die Registrierung benachrichtigt werden soll. Der Abschnitt wird nur angezeigt, wenn die Benachrichtigung per E-Mail bzw. SMS unter `Einstellungen` → `Benachrichtigungen` aktiviert ist. Für die E-Mail muss ein Benutzer mit hinterlegter E-Mail-Adresse zugewiesen sein. Für die SMS muss eine Telefonnummer eingetragen sein; ist beim zugewiesenen Benutzer eine Telefonnummer hinterlegt, wird sie automatisch übernommen.



Zusätzliche Hinweise

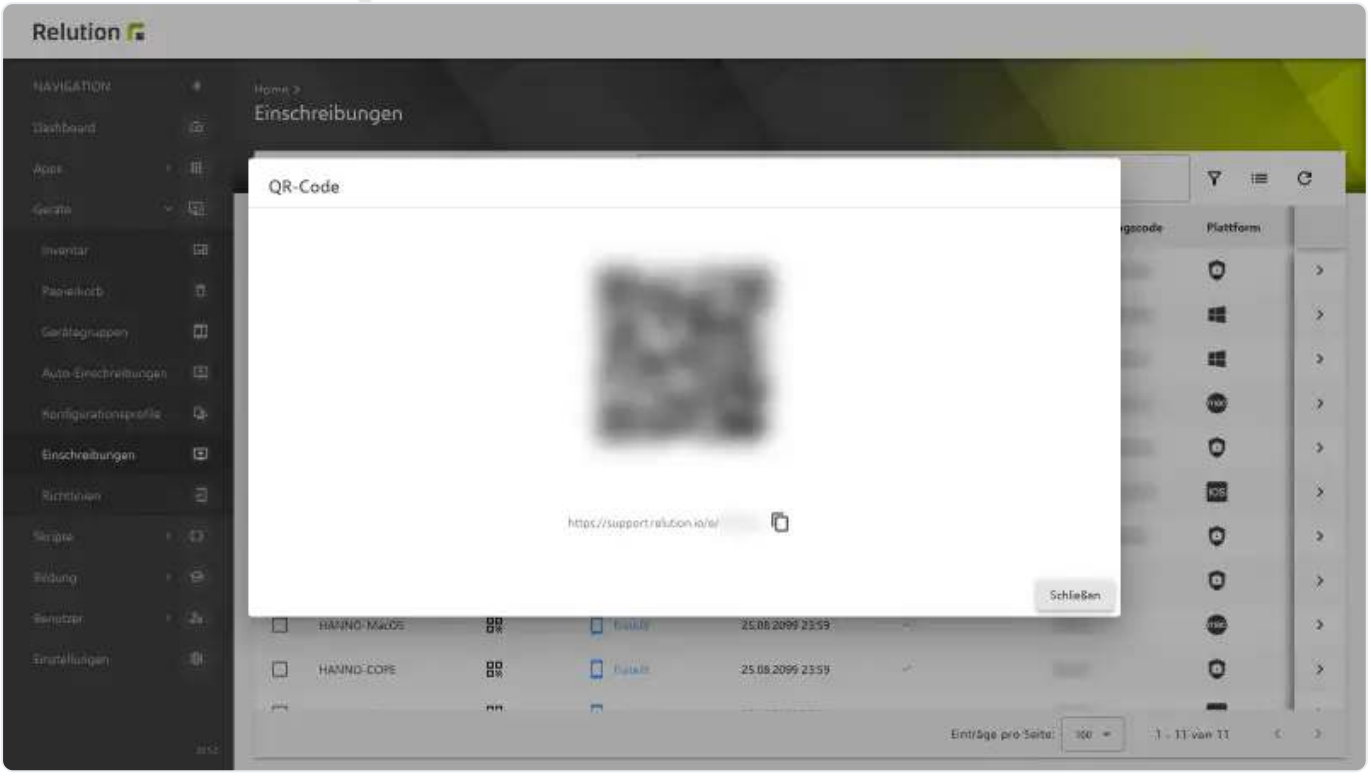
- Wurde kein Gerätename festgelegt, wird der Gerätename nach der erfolgreichen Registrierung des Gerätes aus Hersteller und Modell gebildet.
- Nach dem Speichern zeigt die Detailansicht der Einschreibung den Einschreibungscode und den Link zur Einschreibung an. Beide lassen sich in die Zwischenablage kopieren, etwa um die Einschreibung ohne Benachrichtigung weiterzugeben.
- Standardmäßig ist der Einschreibungscode 16 Zeichen lang (seit Relution 26.5.2, vorher 6). Die Länge kann über folgende globale Konfigurationseigenschaft zwischen 12 und 32 Zeichen festgelegt werden (erfordert einen Neustart der Instanz); Werte außerhalb dieses Bereichs werden auf die jeweilige Grenze gesetzt:

```
relution:
  enrollment:
    passcodeLength: 24
```

Manuelle Einschreibungen durchführen

Die folgenden Schritte müssen von den Benutzern der Android-Geräte durchgeführt werden. Basierend auf der gewählten Benachrichtigungsoption wird der Gerätebenutzer per E-Mail oder SMS benachrichtigt. Ist der Gerätebenutzer gleichzeitig Mitglied der Benutzergruppe `Device Manager`, kann der QR-Code für die Einschreibung auch direkt in der Organisation gescannt werden. Dieser wird per Klick auf das Symbol in der Spalte QR-Code unter `Geräte` → `Einschreibungen` aufgerufen (der QR-Code steht außerdem in der Detailansicht der Einschreibung). Dies ist in der Regel die bevorzugte Methode zur Einschreibung eines Android-Geräts.

Für Version 26.4.0



Folgende Schritte sind anschließend durchzuführen:

Für Version 26.4.0

1. Sicherstellen, dass das Android-Gerät mit dem Internet verbunden ist (WLAN oder Mobilfunknetz).

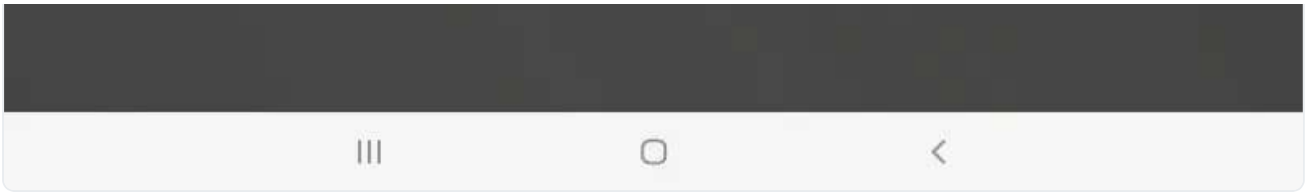
Für Version 26.4.0

2. Registrierungslink öffnen:

    - Bei E-Mail: die E-Mail auf dem Android-Gerät öffnen und auf den Link klicken, oder die E-Mail auf einem anderen Gerät öffnen und den QR-Code mit dem Android-Gerät scannen.
    - Bei SMS: auf den Link in der SMS klicken.
    - Wurde keines der beiden empfangen: die URL aus der Einschreibung manuell im Browser eingeben oder sich an den entsprechenden Administrator wenden.

Für Version 26.4.0

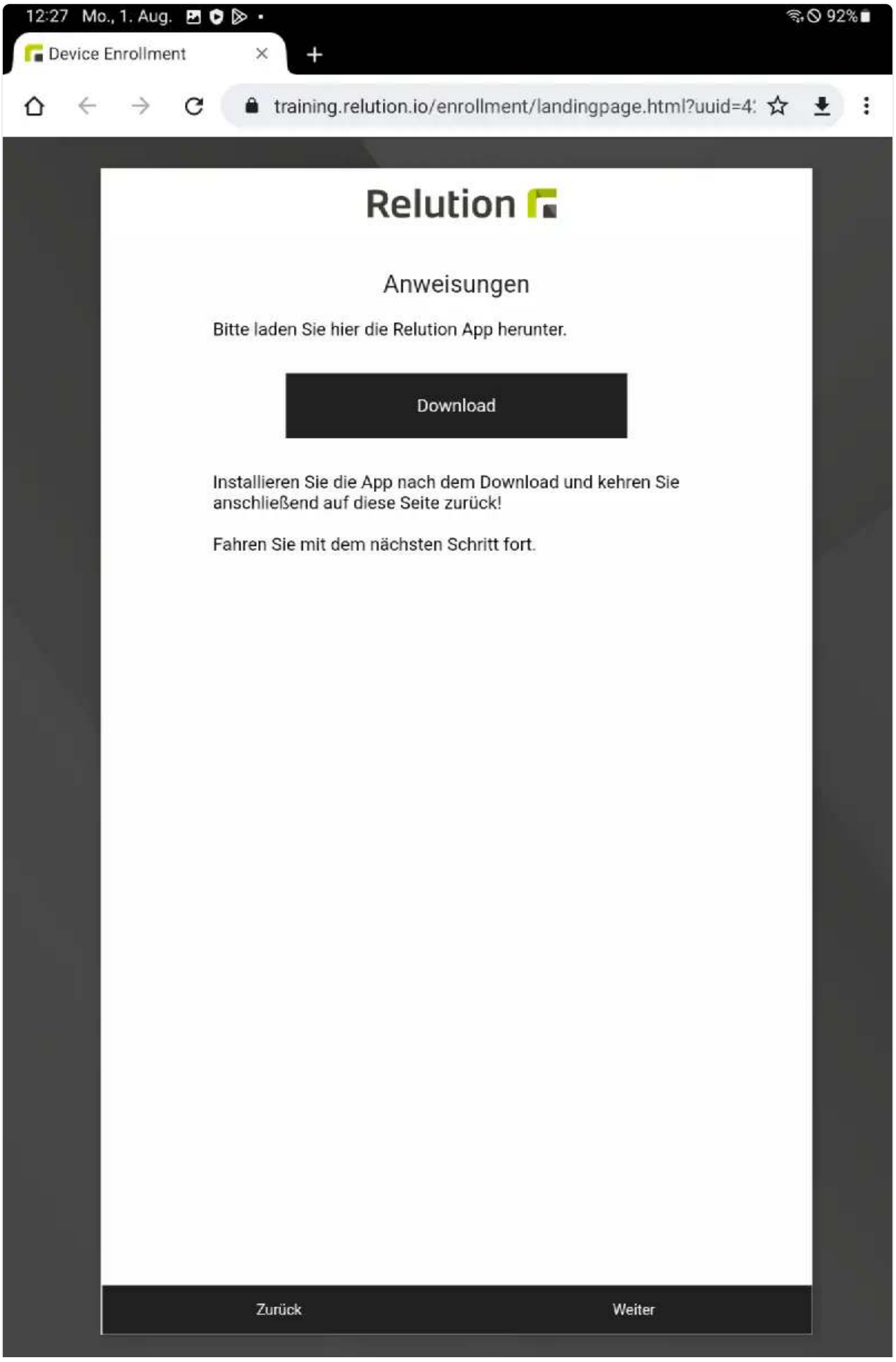
12:27 Mo., 1. Aug.
92%
Device Enrollment
training.relution.io/enrollment/landingpage.html?uuid=4:
Relution
Anweisungen
Willkommen zur Geräteeinschreibung für die Organisation _Support. Bitte führen Sie die folgenden Schritte aus, um Ihr Gerät anzumelden..
Zurück
Weiter

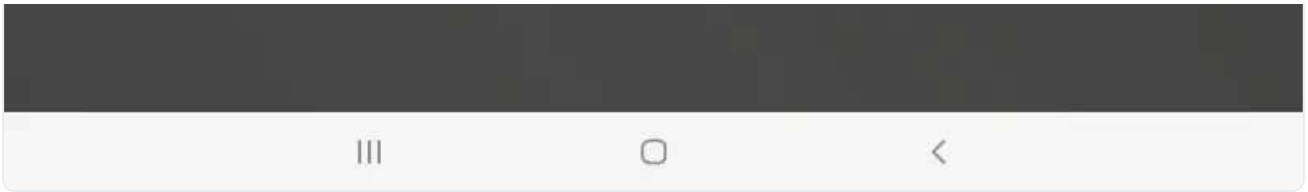


Für Version 26.4.0

3. Auf dem Browser des Android-Gerätes sollte dieser Willkommens-Bildschirm angezeigt werden. Zum Fortfahren auf Weiter tippen.

Für Version 26.4.0


12:27 Mo., 1. Aug.
92%
Device Enrollment
training.relution.io/enrollment/landingpage.html?uuid=4:
Relution
Anweisungen
Bitte laden Sie hier die Relution App herunter.
Download
Installieren Sie die App nach dem Download und kehren Sie anschließend auf diese Seite zurück!
Fahren Sie mit dem nächsten Schritt fort.
Zurück
Weiter



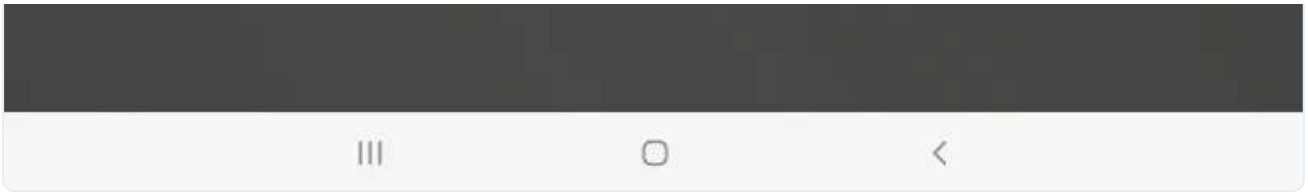
Für Version 26.4.0

4. Es erfolgt die Aufforderung, den `Relution Companion` für Android herunterzuladen und zu installieren, alternativ als `.apk` von unserem Server erhältlich: Relution Companion APK →.

   Nach Abschluss der Installation zum Browser zurückkehren, um mit der Anmeldung fortzufahren. Schlägt die Installation fehl, ist die Installation von Apps aus unbekannten Quellen auf dem Android-Gerät nicht erlaubt. Ab Android 8 wird diese Erlaubnis je App erteilt, und zwar für die App, mit der die Relution-App heruntergeladen wurde, z. B. den Browser (Unbekannte Apps installieren, je nach Hersteller unter `Einstellungen` → `Apps` → `Spezieller App-Zugriff`). Bis Android 7 befindet sich die Einstellung unter `Einstellungen` → `Sicherheit` → `Unbekannte Quellen`.

Für Version 26.4.0

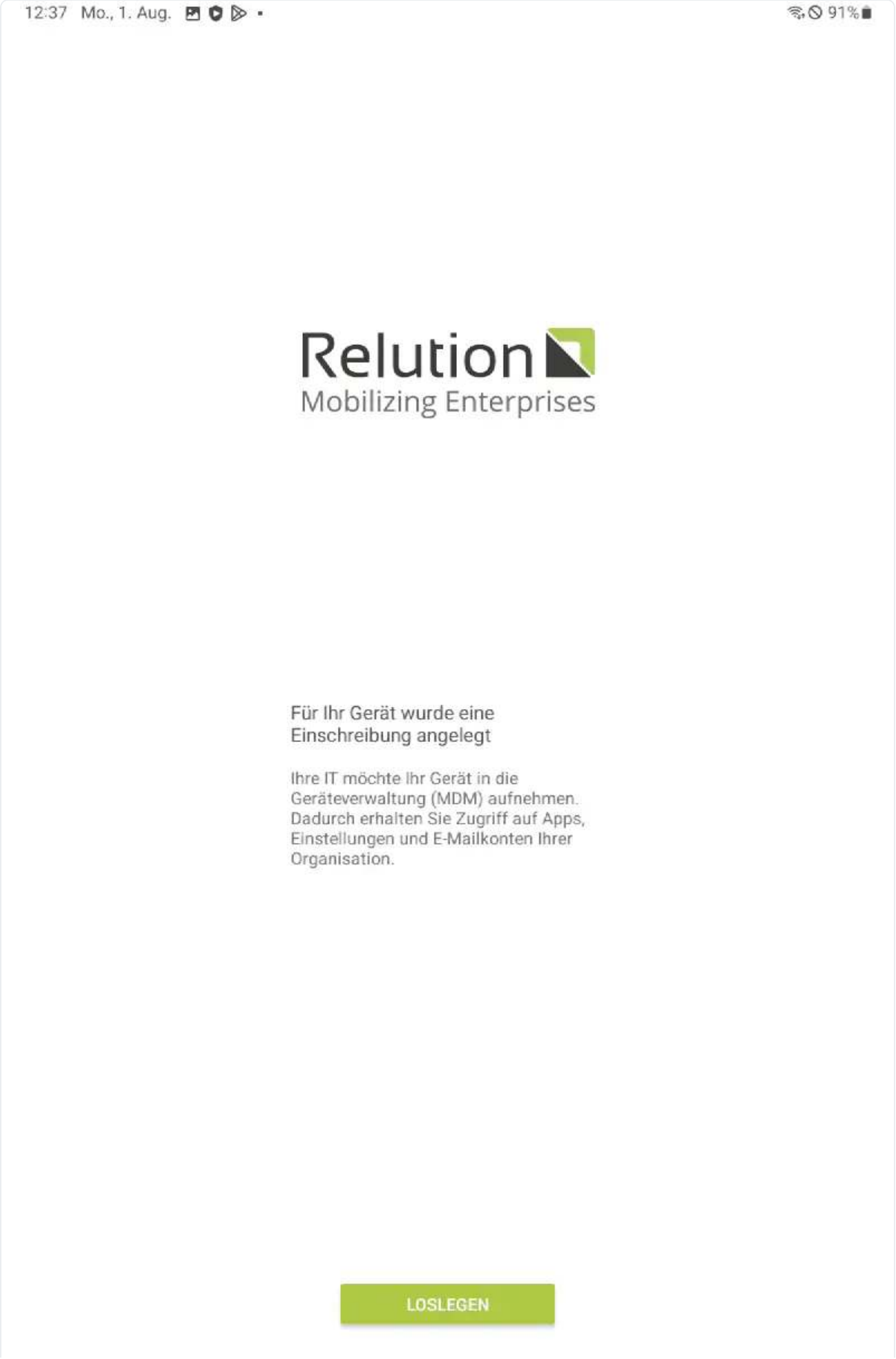
12:37 Mo., 1. Aug.
91%
Device Enrollment
training.relution.io/enrollment/landingpage.html?uuid=4:
Relution
Anweisungen
Starten Sie hier die automatische Einschreibung. Bestätigen Sie dabei die Geräteadministration.
Einschreibung starten
Falls die automatische Einschreibung nicht durchgeführt wird, melden Sie sich bitte manuell mit folgenden Daten in der installierten Relution App an:
SERVER URL:
https://training.relution.io
BENUTZERNAME:
SUPPORT Device User
ORGANISATION:
_Support
EINSCHREIBUNGSCODE:
5ac638
Zurück
Weiter



Für Version 26.4.0

5. Auf die Schaltfläche Einschreibung starten tippen, um den `Relution Companion` für Android zu öffnen.

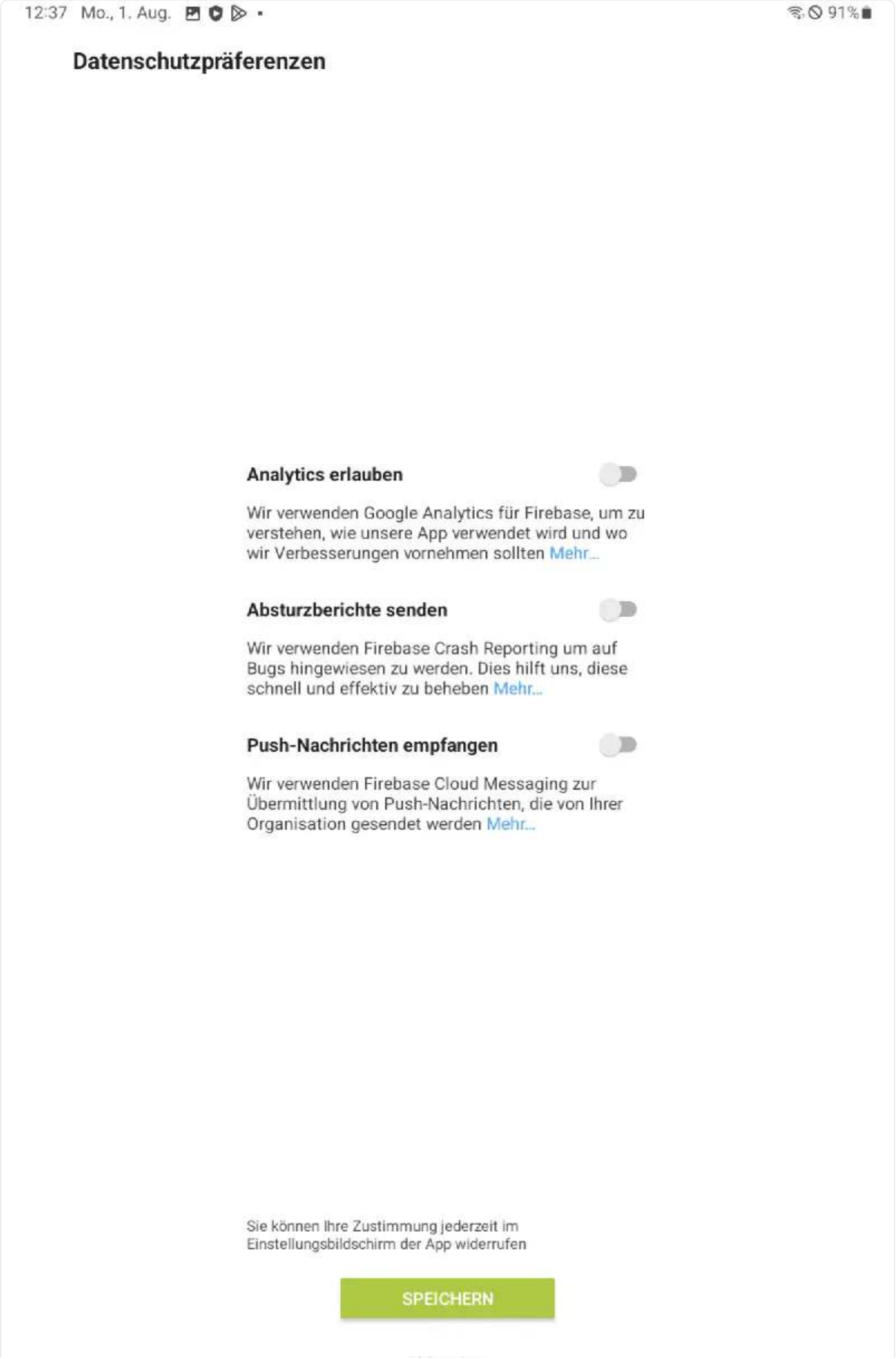
Für Version 26.4.0


12:37 Mo., 1. Aug.
91%
Relution
Mobilizing Enterprises
Für Ihr Gerät wurde eine Einschreibung angelegt
Ihre IT möchte Ihr Gerät in die Geräteverwaltung (MDM) aufnehmen. Dadurch erhalten Sie Zugriff auf Apps, Einstellungen und E-Mailkonten Ihrer Organisation.
LOSLEGEN

Für Version 26.4.0

6. Den Lizenzvereinbarungen zustimmen und auf Loslegen tippen.

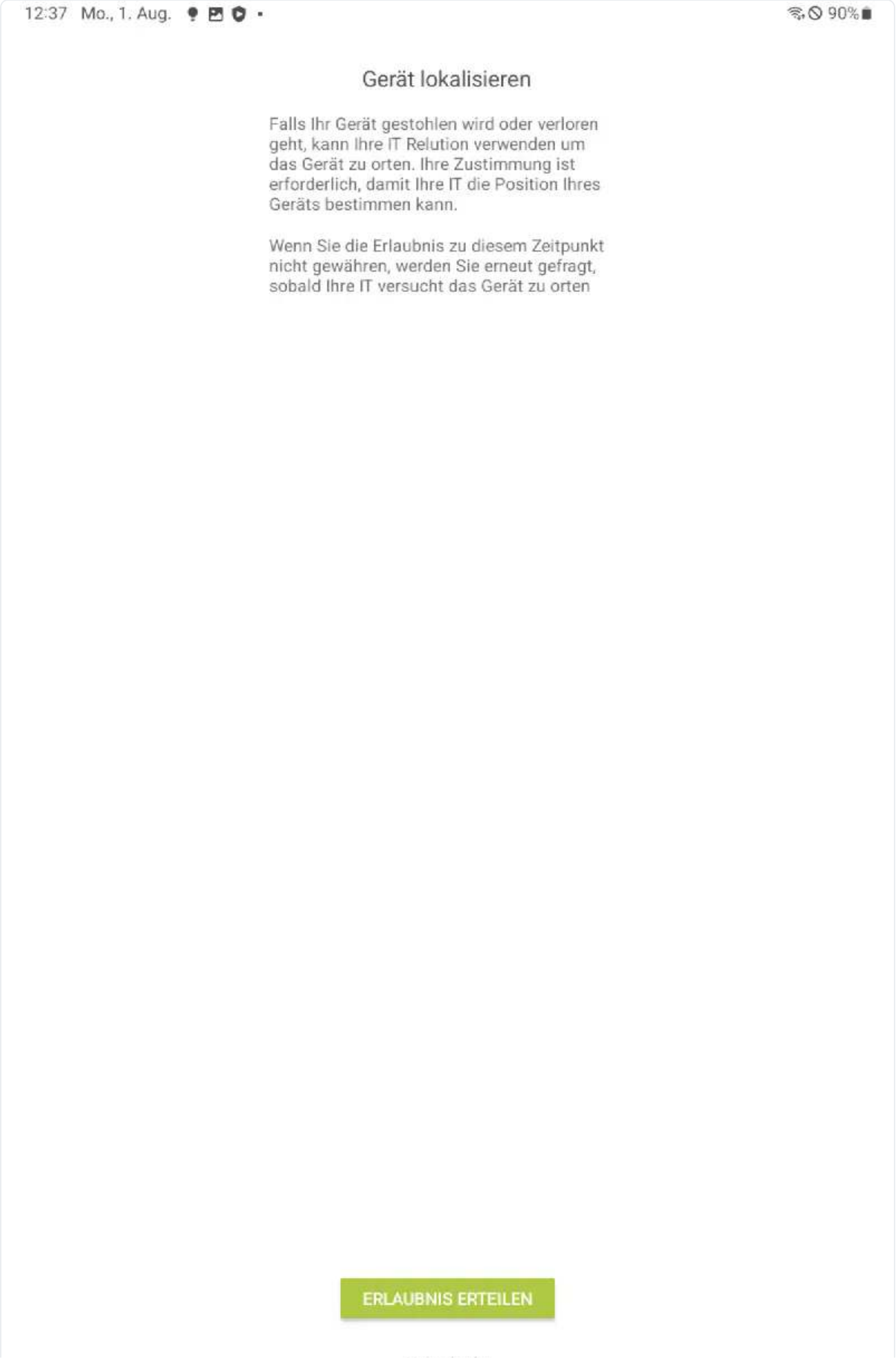
Für Version 26.4.0

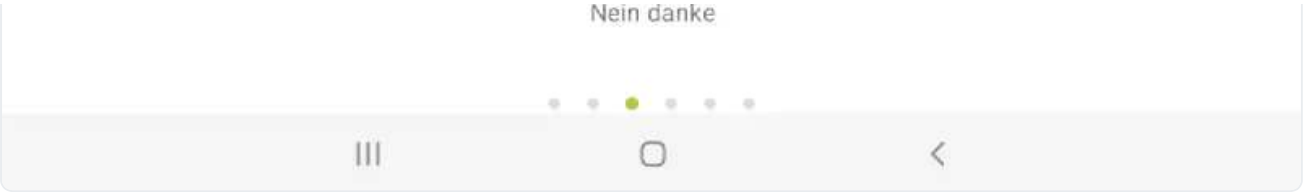

12:37 Mo., 1. Aug.
91%
Datenschutzpräferenzen
Analytics erlauben
Wir verwenden Google Analytics für Firebase, um zu verstehen, wie unsere App verwendet wird und wo wir Verbesserungen vornehmen sollten Mehr...
Absturzberichte senden
Wir verwenden Firebase Crash Reporting um auf Bugs hingewiesen zu werden. Dies hilft uns, diese schnell und effektiv zu beheben Mehr...
Push-Nachrichten empfangen
Wir verwenden Firebase Cloud Messaging zur Übermittlung von Push-Nachrichten, die von Ihrer Organisation gesendet werden Mehr...
Sie können Ihre Zustimmung jederzeit im Einstellungsbildschirm der App widerrufen
SPEICHERN

Für Version 26.4.0

7. Im Bildschirm Datenschutzpräferenzen wird festgelegt, welche optionalen Daten der `Relution Companion` übermitteln darf, z. B. automatische Absturzberichte. Die Auswahl wird mit Speichern übernommen und kann später in den Einstellungen der App widerrufen werden.

Für Version 26.4.0


12:37 Mo., 1. Aug.
90%
Gerät lokalisieren
Falls Ihr Gerät gestohlen wird oder verloren geht, kann Ihre IT Relution verwenden um das Gerät zu orten. Ihre Zustimmung ist erforderlich, damit Ihre IT die Position Ihres Geräts bestimmen kann.
Wenn Sie die Erlaubnis zu diesem Zeitpunkt nicht gewähren, werden Sie erneut gefragt, sobald Ihre IT versucht das Gerät zu orten
ERLAUBNIS ERTEILEN

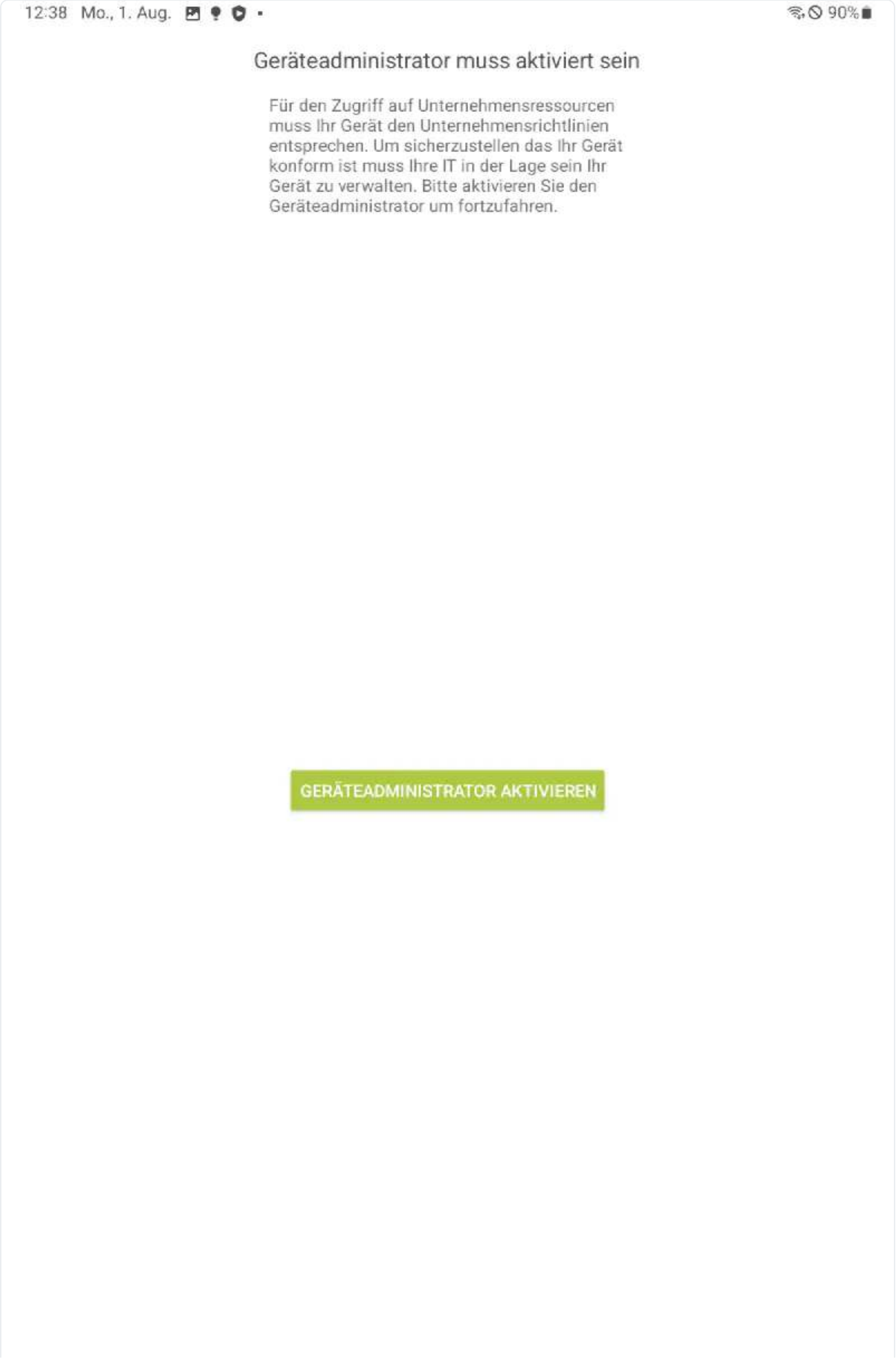


8. Anschließend kann die Erlaubnis erteilt werden, das Gerät zu orten. Wird die Erlaubnis nicht erteilt, kann der Administrator das Android-Gerät nicht orten, falls es gestohlen wird oder verloren geht.

Für Version 26.4.0

9. Zudem kann Relution erlaubt werden, den Status des Gerätes auszulesen, um die Telefonnummer und IMEI mit dem Administrator zu teilen. Diese Informationen werden verschlüsselt übertragen und niemals an Dritte weitergegeben.

Für Version 26.4.0


12:38 Mo., 1. Aug.
90%
Geräteadministrator muss aktiviert sein
Für den Zugriff auf Unternehmensressourcen muss Ihr Gerät den Unternehmensrichtlinien entsprechen. Um sicherzustellen das Ihr Gerät konform ist muss Ihre IT in der Lage sein Ihr Gerät zu verwalten. Bitte aktivieren Sie den Geräteadministrator um fortzufahren.
GERÄTEADMINISTRATOR AKTIVIEREN

Für Version 26.4.0

10. Anschließend erfolgt die Aufforderung, Relution administrative Rechte zu gewähren. Dies ist erforderlich, um sicherzustellen, dass das Android-Gerät den Anforderungen der Organisation entspricht, wie z. B. Passwortrichtlinien. Ist unter `Einstellungen` → `Geräteverwaltung` die Option Verwaltung auf älteren Android-Geräte entfernen, falls dem Geräteadministrator die Berechtigung nicht erteilt wird aktiviert, wird die Verwaltung des Gerätes entfernt, wenn die Berechtigung nicht erteilt oder später widerrufen wird.

Für Version 26.4.0

12:38 Mo., 1. Aug. 90%

Aktivieren der Geräteadministrator-App

Relution MDM

Relution wird von Ihrem Administrator verwendet um Ihr Gerät aus der Ferne zu verwalten, Unternehmensanwendungen bereitzustellen und um sicherzustellen, dass Ihr Gerät den Unternehmensrichtlinien entspricht. Wenn Sie diese Berechtigung nicht gewähren können Sie möglicherweise einige Unternehmensfunktionen nicht verwenden.

Durch die Aktivierung dieser Administrator-App kann Relution die folgenden Aktionen ausführen:

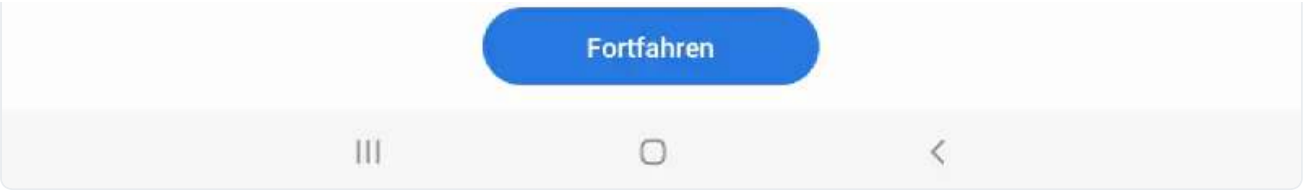
- **Alle Daten löschen**
  Auf Werkseinstellungen zurücksetzen und Daten auf dem Tablet ohne Warnung löschen
- **Displaysperre ändern**
  Ändern der Displaysperre
- **Passwortregeln festlegen**
  Zulässige Länge und Zeichen für Passwörter für die Displaysperre festlegen
- **Versuche zum Entsperren des Displays überwachen**
  Anzahl der falsch eingegebenen Passwörter beim Entsperren des Displays überwachen und Tablet sperren oder alle Daten auf dem Tablet löschen, wenn zu häufig ein falsches Passwort eingegeben wird.
- **Bildschirm sperren**
  Festlegen, wie und wann der Bildschirm gesperrt wird
- **Passwortablauf für Sperre festlegen**
  Häufigkeit ändern, mit der das Passwort, die PIN oder das Muster für die Displaysperre geändert werden muss
- **Speicherverschlüsselung**
  Anforderung, dass gespeicherte App-Daten verschlüsselt werden
- **Kameras deaktivieren**
  Nutzung sämtlicher Gerätekameras unterbinden
- **Displaysperre teilweise deaktivieren**
  Verwendung einiger Funktionen der Displaysperre verhindern
- **SD-Karten-Verschlüsselung festlegen**
  Verschlüsselung der Anwendung auf SD-Karte vorschreiben
- **Anwendungen verwalten**
  Installieren, deinstallieren, deaktivieren, aktivieren Sie den App-Status und fragen Sie diesen ab. Schränken Sie die Fähigkeit zum installieren und deinstallieren bestimmter Apps ein.
- **Geräteinventar überwachen**
  Gerätestatus und -daten überwachen und abfragen
- **Exchange-Konto konfigurieren**
  Erstellen, ändern und löschen Sie Exchange ActiveSync-Kontoeinstellungen.
- **Konfigurieren und verwalten von WLAN-Profilen**
  Erstellen, bearbeiten oder löschen Sie WLAN-Profile.
- **Einrichten der Gerätesicherheit**
  Sie können Zertifikate installieren, Gerät verschlüsseln, ausgewählte Daten vom Gerät entfernen und Gerät vollständige Löschen.
- **Festlegen von Hardwarebeschränkungen**
  Schränken Sie den Zugriff auf verschiedene Hardwarefunktionen ein.

Für Version 26.4.0

11. Auf Aktivieren tippen, um die administrativen Berechtigungen zu erteilen. Je nach Hersteller und Android-Version des Gerätes kann das Layout des Bildschirms vom obigen Screenshot abweichen.

Für Version 26.4.0

12:38 Mo., 1. Aug.
90%
Knox-Lizenzaktivierung
Aktivieren Sie Ihre Lizenz, um Knox-Berechtigungen zu erhalten, mit denen Sie mehr Funktionen für die Geräteverwaltung verwenden können.
Lesen Sie die Datenschutzrichtlinie von Samsung Knox, um zu erfahren, wie wir Ihre Daten verwalten.

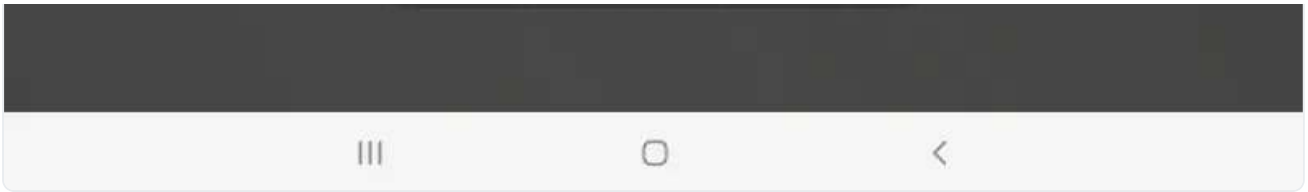


Für Version 26.4.0

12. Auf Samsung-Geräten erscheint zusätzlich der Dialog zur Knox-Lizenzaktivierung mit einem Verweis auf die Datenschutzrichtlinie von Samsung Knox. Auch dieser Dialog ist mit Fortfahren zu bestätigen.

Für Version 26.4.0

12:38 Mo., 1. Aug.
90%
Device Enrollment
training.relution.io/enrollment/landingpage.html?uuid=4:
Relution
Anweisungen
Herzlichen Glückwunsch
Ihr Gerät ist jetzt erfolgreich angemeldet. Sie können den Browser jetzt schließen.
Vielen Dank!
Zurück
Weiter
KNOX Lizenzvalidierung erfolgreich



13. Das Android-Gerät schließt nun den Anmeldevorgang ab und taucht anschließend im Geräte-Inventar der entsprechenden Relution Organisation zur Verwaltung auf.

Für Version 26.4.0

Verfügbare Aktionen

Relution stellt eine Auswahl an Aktionen bereit, um Android Legacy-/Classic-Geräte direkt zu kontrollieren und zu lenken. Ein herausragender Vorteil liegt darin, dass diese Aktionen gezielt auf einzelne Geräte angewendet werden können.

Ein Teil dieser Aktionen steht auch für Android Classic Whiteboards zur Verfügung. Welche Aktionen angeboten werden, hängt vom Hersteller ab und ist auf der jeweiligen Herstellerseite → aufgeführt. So gibt es etwa Shortcut hinzufügen, Shortcut entfernen und Gerät orten nur auf wenigen Whiteboards, Passwort zurücksetzen auf keinem. Speziell für interaktive Whiteboards entwickelte Aktionen sind unter Aktionen (Whiteboards) → zu finden.

Für Version 26.4.0

Verfügbare Aktionen

Aktion	Beschreibung
Alarm auslösen →	Löst einen Alarm auf dem Gerät aus, auch wenn das Gerät lautlos ist
App aus dem Prowise App Store installieren →	Eine App aus dem Prowise App Store zur Installation auswählen (nur Prowise-Whiteboards)
App entfernen →	Deinstalliert eine App vom Gerät
Datei an Gerät senden →	Eine Datei in ein Verzeichnis des Geräts hochladen
Gerät auf Werkszustand zurücksetzen →	Setzt das Gerät auf den Werkszustand zurück und löscht alle Daten vom Gerät
Gerät neu starten →	Das Gerät wird neu gestartet
Gerät orten	Fragt die aktuelle Position des Geräts ab. Kann fehlschlagen, wenn die Standortberechtigung auf dem Gerät nicht erteilt ist
Gerät vollständig sperren →	Das Gerät wird mit dem aktuell gesetzten Passwort gesperrt. Falls kein Passwort gesetzt ist, kann das Gerät ohne Passwort entsperrt werden
Geräteinformationen aktualisieren →	Aktualisiert alle verfügbaren Informationen zu dem Gerät, die im Reiter Informationen aufgelistet sind
Nachricht senden →	Zeigt eine Textnachricht auf dem Gerät an
Passwort zurücksetzen	Setzt ein neues Gerätepasswort. Nur bis Android 10 verfügbar; unter Android 7–10 nur, wenn auf dem Gerät noch kein Passwort gesetzt ist
Prowise-Update installieren →	Installiert das neueste Prowise-Firmware-Update (nur Prowise-Whiteboards)
Relution Store App bereitstellen →	Eine App im Relution Store suchen und auf den Geräten verteilen
Shortcut entfernen →	Entfernt einen Shortcut vom Homescreen
Shortcut hinzufügen →	Fügt einen Shortcut zu einer Webseite auf dem Homescreen hinzu
Update installieren →	Installiert ein gewünschtes Update auf dem ausgewählten Gerät

Alarm auslösen

Die Aktion Alarm auslösen löst einen Alarm auf dem ausgewählten Gerät aus, auch wenn das Gerät auf lautlos gestellt ist. So lässt sich das Gerät beispielsweise leichter im Raum lokalisieren. Über den Parameter Dauer (in Sekunden) lässt sich festlegen, wie lange der Alarm ertönt; standardmäßig sind 30 Sekunden eingestellt, höchstens sind 60 Sekunden möglich.

Die Aktion lässt sich auch über Gerätegruppen auslösen, ereignis- oder zeitgesteuert: Aktionen mit Gerätegruppen →

App entfernen

Die Aktion App entfernen deinstalliert eine ausgewählte App vom Gerät. Die App lässt sich über vier Quellen auswählen: Relution App Store App, Google Play Store App, Installierte App oder Interner Name einer App (Angabe des Paketnamens). In den Listen können mehrere Apps gleichzeitig ausgewählt werden.

Die Liste Installierte App enthält nur Apps, die das Gerät zuletzt als installiert gemeldet hat; Systemapps, die Relution-App und Apps, die gerade installiert werden, sind dort ausgeblendet. Bei mehreren ausgewählten Geräten erscheinen nur Apps, die auf allen Geräten installiert sind.

Ist eine sofortige Deinstallation nicht möglich, wird der Benutzer alle 1440 Minuten (einmal täglich) erneut zum Entfernen der App aufgefordert.

Alternativ lassen sich Apps in den Gerätedetails im Reiter Installierte Apps über Deinstallieren entfernen.

Für Version 26.4.0

Datei an Gerät senden

Die Aktion Datei an Gerät senden lädt eine ausgewählte Datei in ein Verzeichnis auf dem Gerät hoch. Das Zielverzeichnis wird im Feld Verzeichnis relativ zum externen Speicher des Geräts (`/sdcard/`) angegeben; vorbelegt ist `Download/`. ZIP-Archive werden dabei automatisch entpackt, sofern die Option ZIP-Archive nicht dekomprimieren nicht aktiviert ist – APK-, JAR- und OBB-Dateien werden hingegen nie automatisch entpackt. Seit Android 6.0 muss der Empfang der Datei zusätzlich auf dem Gerät bestätigt werden.

Die Aktion lässt sich auch über Gerätegruppen auslösen, ereignis- oder zeitgesteuert: Aktionen mit Gerätegruppen →

Gerät auf Werkszustand zurücksetzen

Die Aktion Gerät auf Werkszustand zurücksetzen setzt das Gerät auf den Werkszustand zurück und löscht dabei alle Daten vom Gerät.

Die Aktion wird in den Details eines Geräts unter `Geräte` → `Inventar` im Reiter `Aktionen` über Aktion anwenden ausgewählt. Der Dialog weist vor dem Ausführen darauf hin, dass alle gespeicherten Inhalte unwiderruflich gelöscht werden und nach dem Zurücksetzen nicht wiederhergestellt werden können. Weitere Optionen bietet der Dialog für Android-Classic-Geräte nicht.

Voraussetzung

Die Aktion muss unter `Einstellungen` → `Geräteverwaltung` → `Einschreibungen` in der Zeile Gerät auf Werkszustand zurücksetzen für die Eigentümerschaft des Geräts (COD oder BYOD) aktiviert sein. Standardmäßig ist sie für COD aktiviert, für BYOD deaktiviert. Für Geräte mit unbekannter Eigentümerschaft ist sie immer verfügbar; diese Einstellung ist im Portal nicht änderbar. Ist die Aktion für die Eigentümerschaft deaktiviert, bietet Relution sie nicht an.

Für Whiteboards von Prowise und SMART steht die Aktion nicht zur Verfügung.

Status und Abbruch

Für Version 26.4.0

Android-Classic-Geräte bestätigen nur den Empfang der Aktion. Relution setzt den Status deshalb bereits bei der Zustellung auf Ausgeführt; ob das Gerät tatsächlich zurückgesetzt wurde, lässt sich daran nicht ablesen. Eine angelegte Aktion kann nicht abgebrochen werden.

Gerät neu starten

Die Aktion Gerät neu starten startet das Gerät neu oder fährt es herunter. Im Portal ist die Aktion für Android-Classic-Geräte mit dem Badge Interactive Whiteboard gekennzeichnet.

Die Aktion wird in den Details eines Geräts unter `Geräte` → `Inventar` im Reiter `Aktionen` über Aktion anwenden ausgewählt. Im folgenden Schritt stehen diese Optionen zur Verfügung:

- Grund für den Neustart: optionale Angabe, warum das Gerät neu gestartet wird.
- Ausschalten (ebenfalls mit dem Badge Interactive Whiteboard gekennzeichnet): Das Gerät wird heruntergefahren statt neu gestartet.

Bei KION- und Newline-Geräten stehen weder der Grund noch die Option Ausschalten zur Verfügung.

Gerät vollständig sperren

Die Aktion Gerät vollständig sperren sperrt das Gerät mit dem aktuell gesetzten Passwort. Falls kein Passwort gesetzt ist, kann das Gerät ohne Passwort entsperrt werden.

Für Android Classic-Geräte ist dies die einzige Sperraktion. Beim Senden sind keine weiteren Angaben erforderlich.

Whiteboards

Auf Whiteboards von ADVANTouch, CTOUCH, i3-Technologies, Newline, Promethean, Prowise und VS muss vor dem Sperren ein Passwort oder eine PIN festgelegt sein, entweder lokal am Gerät oder, falls vorhanden, über die Konfiguration.

Auf Whiteboards von Clevertouch, heinekingmedia, SMART und ViewSonic steht die Aktion nicht zur Verfügung.

Entsperren

Eine Aktion zum Entsperren gibt es nur für Whiteboards von CTOUCH, i3-Technologies und Newline, siehe Gerät entsperren →. Alle anderen Geräte werden am Gerät selbst mit dem Passwort entsperrt.

Ab Android 7 lässt sich ein unbekanntes Gerätepasswort auch über die Aktion Passwort zurücksetzen nicht ersetzen: Unter Android 7 bis 10 setzt sie nur dann ein neues Passwort, wenn auf dem Gerät noch keines gesetzt ist, ab Android 11 steht sie nicht mehr zur Verfügung.

Für Version 26.4.0

Verfügbarkeit nach Eigentümerschaft

Die Aktion wird nur angeboten, wenn sie unter `Einstellungen` → `Geräteverwaltung` → `Einschreibungen` in der Zeile Gerät vollständig sperren für die Eigentümerschaft des Geräts (COD oder BYOD) aktiviert ist. Standardmäßig ist sie für beide aktiviert.

Geräteinformationen aktualisieren

Die Aktion Geräteinformationen aktualisieren aktualisiert alle verfügbaren Informationen zu dem Gerät, die in den Gerätedetails im Reiter Informationen angezeigt werden.

In den Details eines Geräts unter `Geräte` → `Inventar` wird die Aktion direkt über das Symbol Geräteinformation aktualisieren im Kopfbereich ausgelöst; ein Dialog öffnet sich dabei nicht. Alternativ steht sie im Reiter `Aktionen` unter Aktion anwenden zur Verfügung.

Relution sendet die Aktion per Push-Benachrichtigung an den Relution Companion auf dem Gerät. Ist keine Push-Zustellung möglich, bleibt die Aktion im Status Ausstehend, bis das Gerät sie bei der nächsten Verbindung selbst abruft. Die angezeigten Informationen werden erst aktualisiert, wenn das Gerät geantwortet hat.

Nachricht senden

Die Aktion Nachricht senden zeigt eine Textnachricht auf dem Gerät an. Dafür sind ein Titel und der Nachrichtentext (Inhalt) anzugeben; beide Angaben sind Pflichtfelder.

Für Version 26.4.0

Auf Smartphones und Tablets wird die Nachricht per Push an die Relution-App zugestellt. Ist der Versand erfolgreich, erhält die Aktion direkt den Status Ausgeführt und als Kommentar Titel und Inhalt der zugestellten Nachricht. Der Status bestätigt die Zustellung, nicht das Lesen der Nachricht auf dem Gerät. Schlägt der Push-Versand fehl, bleibt die Aktion im Status Ausstehend, bis das Gerät sie selbst abruft. Interaktive Displays (Whiteboards) erhalten die Nachricht nicht per Push an die Relution-App, sondern wie andere Aktionen über den Gerätekanal.

Abgeschlossene Nachrichten-Aktionen werden standardmäßig nach 10 Tagen automatisch aus dem Aktionsverlauf entfernt.

Relution Store App bereitstellen

Die Aktion Relution Store App bereitstellen ermöglicht es, nach einer App im Relution Store zu suchen und diese auf dem Gerät zu verteilen. Zur Auswahl stehen native Android-Apps aus dem Relution Store; je Aktion wird eine App ausgewählt und in ihrer freigegebenen Version verteilt. Die Installation aus unbekannten Quellen muss dafür auf dem Gerät aktiviert sein.

Im Dialog stehen zwei Schalter zur Verfügung, die beide standardmäßig aktiv sind:

- Wenn möglich im Hintergrund installieren: Die Installation wird im Hintergrund versucht. Gelingt dies nicht automatisch, wird der Benutzer auf dem Gerät zur Installation aufgefordert.
- App bei Enterprise Wipe entfernen: Die App wird bei einem Enterprise Wipe wieder vom Gerät entfernt.

Für Prowise-Whiteboards steht die Aktion nicht zur Verfügung; dort werden Apps über App aus dem Prowise App Store installieren → installiert.

Shortcut hinzufügen

Die Aktion Shortcut hinzufügen fügt einen Shortcut zu einer Webseite auf dem Homescreen des Geräts hinzu. Pflichtfelder sind Bezeichnung (Beschriftung des Shortcuts) und URL (gültige Ziel-URL). Optional kann über Icon ein eigenes Symbol im Format JPEG oder PNG mit höchstens 1 MB hinterlegt werden.

Bezeichnung und URL werden auch zum späteren Entfernen über die Aktion Shortcut entfernen → benötigt.

Die Aktion steht für Android Classic-Geräte zur Verfügung, von den Whiteboards nur für Promethean → sowie wende.interaktiv → (Wende 8 und Wende 9).

Shortcut entfernen

Die Aktion Shortcut entfernen entfernt einen Shortcut vom Homescreen des Geräts. Der zu entfernende Shortcut wird über die Pflichtfelder Bezeichnung und URL angegeben; eine Auswahlliste vorhandener Shortcuts gibt es nicht. Einzutragen sind die Werte, mit denen der Shortcut über die Aktion Shortcut hinzufügen → angelegt wurde.

Die Aktion steht für Android Classic-Geräte zur Verfügung, von den Whiteboards nur für Promethean →.

Für Version 26.4.0

Verfügbare Konfigurationen

Eine Richtlinie ist eine Sammlung von einer oder mehreren Konfigurationen. Jede Richtlinie kann auf einem oder auf mehreren Geräten gleichzeitig angewendet werden. Zudem können mit jedem Gerät eine oder mehrere Richtlinien verknüpft sein.

Für Version 26.4.0

Verfügbare Konfigurationen

Konfiguration	Beschreibung
ADVANTouch →	ADVANTouch Whiteboards verwalten
App Konformität →	Verwaltung appspezifischer Einschränkungen
Clevertouch →	Clevertouch Whiteboards verwalten
CTOUCH →	CTOUCH Whiteboards verwalten
Dahua →	Dahua Whiteboards verwalten
EShare →	EShare App konfigurieren
Exchange	Verwaltung von Exchange-Konten
Geplantes OTA-Update →	Firmware-Updates für Clevertouch, i3 und Newline Whiteboards zeitgesteuert installieren
Hintergrundbild →	Hintergrundbild festlegen
Hotspot →	Hotspot-Konfiguration verwalten
i3 →	i3 Whiteboards verwalten
Interaktive Whiteboard Konfiguration	Einschränkungen für interaktive Whiteboards verwalten
Kiosk-Modus →	Kiosk-Modus-Einstellungen
Konfiguration des Zugangspunktnamens	Einen Zugangspunktname verwalten
Newline	Newline Whiteboards verwalten
Passwort	Verwaltung der Passwortrichtlinien für Android Geräte
Promethean →	Verwalten der Promethean-Einstellungen
Restriktionen →	Verwaltung der Geräterestriktionen
Restriktionen für drahtlose Netzwerke	Verwaltung der WLAN Restriktionen
SMART →	SMART Whiteboards verwalten
VPN	Verwaltung von VPN Einstellungen
ViewSonic →	ViewSonic Whiteboards verwalten
VS →	VS Whiteboards verwalten

Konfiguration	Beschreibung
WLAN →	Verwaltung der WLAN Einstellungen
Zertifikat →	Auswahl eines Zertifikats, das standardmäßig auf dem Gerät installiert wird

Hintergrundbild

Ab Relution 5.33 steht die Konfiguration Hintergrundbild für Android Enterprise sowie Android Classic/Legacy zur Verfügung. Mit dieser lässt sich ein Bild für den Homescreen hinterlegen, das nach Anwendung der Richtlinie auf den Geräten erscheint. Die Richtlinie ermöglicht auch das Hinzufügen von Text (inklusive Platzhaltern), um dynamische Texte auf dem Hintergrundbild anzuzeigen.

> Android Enterprise benötigt Relution Companion Version 1.18.
>
> Android Classic benötigt Relution Companion Version 5.37.

Die Konfiguration Hintergrundbild legt das Bild fest, verhindert aber nicht, dass Benutzer es auf dem Gerät ändern.

Für Version 26.4.0

Konfiguration

Im Abschnitt Allgemein stehen folgende Felder zur Verfügung:

- Text auf dem Hintergrundbild – optionaler Text, der auf das Bild gesetzt wird. Platzhalter werden pro Gerät aufgelöst; die unterstützten Platzhalter listet das Formular unterhalb der Eingabefelder auf.
- Farbe des Textes – Hex-Farbcode, z. B. `#ffffff` (Standard), wahlweise über den Farbwähler.
- Hintergrundbild – das Bild selbst (Pflichtfeld). Die maximale Dateigröße beträgt standardmäßig 3 MB; auf eigenen Servern lässt sie sich über den Parameter `relution.wallpaper.max-file-size.android` anpassen. Ist das Bild größer, zeigt das Portal eine Fehlermeldung an und die Konfiguration lässt sich nicht speichern.

App Konformität

Android Classic/Legacy ermöglicht es, Native Apps als `.apk`-Dateien in den Relution App Store hochzuladen und per Aktion oder Richtlinie auf eingeschriebene Android-Geräte zu verteilen. Die Verteilung per Aktion ist unter Relution Store App bereitstellen → beschrieben.

> Google-Play-Apps können in Android Classic nicht automatisch installiert werden. Unter Erforderliche Apps eingetragene Apps aus dem Google Play Store muss der Benutzer selbst installieren; die Option Auto Installation steht nur für native Apps aus dem Relution App Store zur Verfügung. Für eine verwaltete Verteilung von Google-Play-Apps ist Android Enterprise (Managed Google Play) zu verwenden.

Native apk über eine Richtlinie

Diese Variante bietet keine automatische Aktualisierung bei neuen App-Versionen.

Zuerst erfolgt die Bereitstellung der App im Relution App Store, anschließend die Verteilung über eine Richtlinie mit der Konfiguration App Konformität.

> Pro Gerät kann nur eine Richtlinie mit der Konfiguration App Konformität angewendet werden. Wird einem Gerät eine weitere Konfiguration dieses Typs zugewiesen, wird diese übersprungen und nicht angewendet.

File Version 26.4.0

1. Im Relution-Portal zum Menüpunkt `Apps` → `App Store` navigieren und auf Hinzufügen klicken.
2. Anschließend die Option Native App wählen und auf Weiter klicken.
3. Unter Datei wählen auf Auswählen klicken und die gewünschte `.apk`-Datei auswählen.
4. Auf der folgenden Seite muss der Freigabestatus der App von Entwicklung (blaues Icon) auf Produktiv (grünes Icon) geändert werden. Auf Speichern klicken.
5. Anschließend zu `Geräte` → `Richtlinien` navigieren und auf Hinzufügen klicken.
6. Eine Android-Richtlinie erstellen und einen Namen vergeben. Auf Speichern klicken.
7. Nach Klick auf Hinzufügen anschließend die Option App Konformität wählen und mit Details hinzufügen fortfahren.
8. Die Listenart ist standardmäßig auf Alle Apps in der folgenden Liste sind nicht erlaubt (Sperrliste) gesetzt. Unabhängig davon unter Erforderliche Apps die gewünschten Apps aus dem Relution App Store hinzufügen.
9. Die Konfiguration speichern und die aktuelle Version der Richtlinie veröffentlichen.
10. Um die Richtlinie auf Android-Geräten anzuwenden, die gewünschten Geräte über das Tab Geräte mit dieser Richtlinie hinzufügen. Die Geräte werden dabei einer vorhandenen statischen Gerätegruppe mit dieser Richtlinie oder einer neu angelegten statischen Gerätegruppe zugeordnet. Die gewählten Einstellungen und Apps werden anschließend automatisch auf den Geräten ausgeführt bzw. installiert.

Mit aktivierter Option Auto Installation werden die entsprechenden Apps automatisch auf den Android-Geräten installiert. Für die Installation der Apps müssen den Geräten Benutzer zugewiesen sein, die Mitglieder der Benutzergruppe AppStore User sind.

Einstellungen der Konfiguration

Die Konfiguration App Konformität ist in drei Bereiche gegliedert.

Allgemein

- Sperr-/ Positivliste nur im Roaming-Modus aktivieren – die Sperr- bzw. Positivliste wird nur angewendet, solange sich das Gerät im Roaming befindet. Ist die Option deaktiviert, gilt die Liste unabhängig vom Roaming-Status.
- Sperr-/ Positivliste gilt nicht im WLAN – nur verfügbar, wenn die vorige Option aktiv ist. Ist das Gerät per WLAN verbunden, werden die Apps auch im Roaming zugelassen.
- Listenart – Alle Apps in der folgenden Liste sind nicht erlaubt (Sperrliste, Standard) oder Alle Apps in der folgenden Liste sind erlaubt (Positivliste).

Bei einer Positivliste wird unter Apps, die nicht auf der Positivliste stehen festgelegt, wie mit allen übrigen Apps verfahren wird:

- Deinstallieren – der Benutzer wird aufgefordert, die App vom Gerät zu deinstallieren. Die Option steht nicht zur Verfügung, wenn Sperr-/ Positivliste nur im Roaming-Modus aktivieren aktiv ist.
- Deaktivieren – die App bleibt installiert, kann vom Benutzer aber nicht mehr gestartet werden.
- Internet blockieren – entzieht der App den Internetzugriff. Bei vorinstallierten Apps wirkt die Option nicht, und manche Apps können dadurch abstürzen; in diesem Fall ist Deaktivieren vorzuziehen.

Apps auf der Sperrliste bzw. Positivliste

Je nach Listenart heißt der Bereich Apps auf der Sperrliste oder Apps auf der Positivliste. Apps können aus dem Relution App Store, aus dem Google Play Store oder manuell über den Paketnamen hinzugefügt werden.

Die Option Systemapps deaktivieren versucht, alle System- und vorinstallierten Apps zu blockieren. Davon ist auch die Telefon-App betroffen, sodass keine Notrufe mehr abgesetzt werden können. Wird Telefonie benötigt, ist die Telefon-App auf die Positivliste zu setzen.

Für Version 26.4.0

Erforderliche Apps

Die hier eingetragenen Apps müssen auf dem Gerät installiert sein, andernfalls gilt das Gerät als nicht konform. Apps aus dem Google Play Store muss der Benutzer selbst installieren; Auto Installation ist nur für native Apps aus dem Relution App Store möglich.

Beim Speichern wird die Konfiguration abgelehnt, wenn

- eine App gleichzeitig auf der Sperrliste und unter Erforderliche Apps steht oder
- ein Weblink als erforderliche App eingetragen ist.

Restriktionen

Gezielte Einschränkungen von Geräte- und App-Funktionen erhöhen die Sicherheit beim Einsatz von Android-Geräten und können durch mehr Fokussierung die Gerätenutzung optimieren. Durch die Kontrolle der Geräteeinstellungen und die Einschränkung des Zugriffs wird auch verhindert, dass Apps von Drittanbietern auf Unternehmensdaten und -ressourcen zugreifen können. Die Verfügbarkeit von Restriktionen kann, abhängig vom Gerätehersteller und der vorhandenen Betriebssystem-Version, variieren. Ein Teil der Restriktionen steht nur auf Samsung-Knox-Geräten zur Verfügung (Gruppe Knox spezifische Restriktionen).

Anwendung von Restriktionen auf Android-Geräte

1. Im Relution-Portal zum Menüpunkt `Geräte` → `Richtlinien` navigieren und auf Hinzufügen klicken.
2. Eine Android-Richtlinie erstellen und einen Namen vergeben. Auf Speichern klicken.
3. Nach Klick auf Hinzufügen anschließend die Option Restriktionen wählen und mit Details hinzufügen fortfahren.
4. Die Konfiguration nach Auswahl der gewünschten Optionen speichern und die aktuelle Version der Richtlinie veröffentlichen.

   Ist Geräteverschlüsselung erzwingen oder Verschlüsselung der SD-Karte erzwingen aktiviert, muss die Richtlinie zusätzlich eine aktivierte Konfiguration Passwort enthalten. Andernfalls lässt sich die Version weder veröffentlichen noch testen. Für eine wirksame Verschlüsselung sollte in der Passwort-Konfiguration außerdem eine Passwortqualität festgelegt sein.
5. Um die Richtlinie auf Android-Geräten anzuwenden, die gewünschten Geräte über das Tab Geräte mit dieser Richtlinie hinzufügen. Die Geräte werden dabei einer vorhandenen statischen Gerätegruppe mit dieser Richtlinie oder einer neu angelegten statischen Gerätegruppe zugeordnet. Die gewählten Restriktionen werden anschließend automatisch auf den Geräten ausgeführt.

Für Version 26.4.0

Viele Optionen in den Restriktionen bieten über ein Mouse-over Erläuterungen und erweiterte Informationen an. Optionen, die ein Samsung-Knox-Gerät voraussetzen, sind unter Knox spezifische Restriktionen zusammengefasst.

Verfügbare Restriktionen

Die Konfiguration Restriktionen ist in drei Gruppen gegliedert. Über das Download-Symbol (Restriktionen als CSV-Datei exportieren) oberhalb der Gruppen lassen sich alle Restriktionen mit ihren aktuellen Werten als CSV-Datei exportieren.

Generelle Restriktionen

- Geräteverschlüsselung erzwingen – verschlüsselt Konten, Einstellungen, Apps mit ihren Daten sowie Medien und andere Dateien. Danach ist bei jedem Einschalten die Eingabe einer PIN oder eines Passworts erforderlich. Die Verschlüsselung lässt sich nur durch Zurücksetzen auf die Werkseinstellungen aufheben, wobei alle Daten gelöscht werden. Der Vorgang dauert mindestens eine Stunde; das Gerät sollte dabei geladen und am Netz angeschlossen sein, da eine Unterbrechung zu Datenverlust führen kann.
- Kamera verbieten
- Kamera und Widgets auf dem Lockscreen verbieten – der Sperrbildschirm muss dafür mit PIN, Muster oder Passwort gesichert sein.
- Root-Erkennung deaktivieren – gerootete Geräte werden nicht mehr als nicht konform gemeldet. In den Gerätedetails wird das Gerät weiterhin als gerootet angezeigt.

Roaming

- Restriktionen nur im Roaming-Modus aktivieren – die Restriktionen werden nur angewendet, solange sich das Gerät im Roaming befindet.
- Im WLAN erlauben – nur verfügbar, wenn die vorige Option aktiv ist. Die Restriktionen greifen dann nur im Roaming außerhalb eines WLANs.

Knox spezifische Restriktionen

Diese Optionen stehen nur auf Samsung-Knox-Geräten zur Verfügung.

Für Version 26.4.0

Bereich	Optionen
Allgemein	Bildschirmfotos verbieten, Zwischenablage verbieten, GPS an- oder ausschalten verbieten, Datum und Uhrzeit einstellen verbieten, Widgets auf Sperrbildschirm verbieten, Shortcuts auf Sperrbildschirm verbieten
Storage	Verschlüsselung der SD-Karte erzwingen, Zugriff auf SD-Karte verbieten, Schreibrechte auf SD-Karte verbieten
Debugging	USB Debugging verbieten, Google Crash Reporting verbieten
USB Beschränkungen	Media Transfer Protokol (MTP) verbieten, USB Tethering ablehnen, USB-Host-Speicher verbieten
Backup & Zurücksetzen	Google Backup verbieten, Zurücksetzen auf Werkseinstellungen verbieten, OTA Upgrade verbieten, Safe-Boot verbieten
App-Restriktionen	Installation von Apps von anderen Quellen als Play Store verbieten, Google Play verbieten, Youtube verbieten, Browser verbieten, Einstellungen verbieten, Voice Dialer verbieten

Hinweise zu einzelnen Optionen:

- Verschlüsselung der SD-Karte erzwingen setzt ein alphanumerisches Gerätepasswort voraus. Die Passwortrichtlinie kann nur geändert werden, solange die Verschlüsselung deaktiviert ist.
- Media Transfer Protokol (MTP) verbieten unterbindet jeden Dateitransfer über USB, da Android Dateien nur über MTP überträgt. PTP (Picture Transfer Protocol) ist ebenfalls betroffen.
- USB-Host-Speicher verbieten verhindert, dass USB-Sticks, externe Festplatten oder SD-Kartenleser per USB OTG als Speicher eingebunden werden.
- Safe-Boot verbieten verhindert den Start im abgesicherten Modus, über den sich sonst der Kiosk-Modus verlassen ließe.
- Installation von Apps von anderen Quellen als Play Store verbieten sperrt die Installation von Apps außerhalb von Google Play; der Benutzer kann sie in den Android-Einstellungen nicht freigeben. Ist die Option deaktiviert, kann der Benutzer die Installation in den Android-Einstellungen selbst zulassen; aktiviert wird sie dadurch nicht.

Für Version 26.4.0

Kiosk-Modus

Durch den Kiosk-Modus werden Android-Geräte zu zweckgebundenen Geräten, welche für arbeitsbezogene Anwendungen geeignet sind. Endanwender können auf bereitgestellten Geräten mit aktiviertem Kiosk-Modus folglich nur die von der Organisation genehmigte App verwenden und freigegebene Gerätefunktionen nutzen.

Hierfür gibt es zwei Modi, die auf den Android-Geräten Anwendung finden können – zum einen den Einzel-App-Modus (Single App Mode) und den Multi-App-Modus (Multi App Mode).

Bei aktivem Kiosk-Modus erscheint auf dem Gerät der Relution Launcher, dessen Aktivierung der Benutzer bestätigen muss; auf Samsung-Geräten mit SAFE entfällt diese Bestätigung. Auf die Systemeinstellungen hat der Benutzer keinen Zugriff.

> Notrufe sind im Kiosk-Modus nur möglich, wenn die Telefon-App zu den freigegebenen Apps gehört oder unter Geräteeinstellungen eine Notfall-Telefonnummer hinterlegt ist.

Kiosk im Einzel-App-Modus

Der Einzel-App-Modus ist ein Sperrmechanismus, der den Gerätezugriff auf eine einzige Anwendung beschränkt. Geräte, die im Einzel-App-Modus ausgeführt werden, dienen nur einem Zweck: Der Ausführung einer speziellen Anwendung mit minimalen Gerätefunktionen. Die Anwendung startet sich selbst, läuft im Vordergrund und wird auch dann wieder gestartet, wenn die Geräte heruntergefahren oder neu gestartet werden. Auf diese Weise gewährleistet der Kiosk-Modus die ordnungsgemäße Nutzung der Geräte und vermeidet gleichzeitig unnötige Ablenkungen für Benutzer.

Für Version 26.4.0

1. Im Relution-Portal zum Menüpunkt `Geräte` → `Richtlinien` navigieren und auf Hinzufügen klicken.
2. Eine Android-Richtlinie erstellen und einen Namen vergeben. Auf Speichern klicken.
3. Nach Klick auf Hinzufügen anschließend die Option Kiosk-Modus wählen und mit Details hinzufügen fortfahren.
4. Der Schalter An/Aus bleibt aktiviert (Standard). Im Pflichtfeld Passwort wird das Passwort hinterlegt, mit dem sich der Kiosk-Modus am Gerät verlassen lässt (Kiosk-Modus verlassen →). Ohne Passwort lässt sich die Konfiguration nicht speichern.
5. Die Option Einzel-App-Modus aktivieren einschalten und genau eine App auswählen. Die gewählte App muss bereits auf dem Gerät installiert sein, z. B. über die Aktion Relution Store App bereitstellen →.
6. Die Konfiguration nach Auswahl weiterer Optionen und Einschränkungen (Weitere Einstellungen →) speichern und die aktuelle Version der Richtlinie veröffentlichen.
7. Um die Richtlinie auf Android-Geräten anzuwenden, die gewünschten Geräte über das Tab Geräte mit dieser Richtlinie hinzufügen. Die gewählten Einstellungen werden anschließend automatisch auf den Geräten ausgeführt.

Kiosk im Multi-App-Modus

Der Multi-App-Modus beschränkt Geräte auf eine bestimmte Auswahl von Anwendungen, die für die Arbeitsanforderungen der Organisation relevant sind. Benutzer haben die Möglichkeit, auf freigegebene Anwendungen zuzugreifen und diese zu nutzen. Mit dem Kiosk-Modus lässt sich die vollständige Kontrolle über die Gerätenutzung ausüben und es wird sichergestellt, dass Geräte nur für bestimmte Zwecke genutzt und verwendet werden.

1. Im Relution-Portal zum Menüpunkt `Geräte` → `Richtlinien` navigieren und auf Hinzufügen klicken.

2. Eine Android-Richtlinie erstellen und einen Namen vergeben. Auf Speichern klicken.

3. Nach Klick auf Hinzufügen anschließend die Option Kiosk-Modus wählen und mit Details hinzufügen fortfahren.

4. Der Schalter An/Aus bleibt aktiviert (Standard). Im Pflichtfeld Passwort wird das Passwort hinterlegt, mit dem sich der Kiosk-Modus am Gerät verlassen lässt (Kiosk-Modus verlassen →). Ohne Passwort lässt sich die Konfiguration nicht speichern.

5. Ist die Option Einzel-App-Modus aktivieren ausgeschaltet, lässt sich eine App-Auswahl hinzufügen. Die ausgewählten Apps müssen bereits auf dem Gerät installiert sein. Sobald mehr als eine App ausgewählt ist, lässt sich der Einzel-App-Modus nicht mehr einschalten.

6. Des Weiteren stehen weitere Optionen zur Verfügung, von denen folgende relevant sind:

    - Alle über den Relution App Store bereitgestellten Nativen Apps zulassen - standardmäßig aktiv. Der Kiosk zeigt dann zusätzlich zur App-Auswahl alle nativen Apps des Relution App Store an; nicht installierte Apps werden zum Download angeboten. Damit nur die ausgewählten Apps erscheinen, wird die Option deaktiviert.
    - App-Store Aktualisierungs-Interval - nur bei aktiver vorheriger Option; legt fest, wie oft das Gerät die Liste des Relution App Store aktualisiert (1, 2, 4, 6, 12 oder 24 Stunden; Standard 12 Stunden). Ein kürzeres Intervall lässt neue Apps früher erscheinen, erhöht aber Akkuverbrauch und Datenvolumen.
    - Nur installierte Apps anzeigen - wenn deaktiviert, werden alle verfügbaren Apps angezeigt und zum Download angeboten.
    - Vom Administrator installierte Apps anzeigen - Apps, die per Aktion Relution Store App bereitstellen auf den Geräten installiert wurden, erscheinen automatisch im Kiosk-Modus, auch wenn sie nicht mehr im Store verfügbar sind.
    - Apps nach Kategorie gruppieren - ordnet die Apps im Launcher in Ordnern nach ihrer Kategorie an. Eine App mit mehreren Kategorien erscheint in jedem dieser Ordner.
    - App-Anordnungstyp - bei Dynamisch (Standard) wird das Raster automatisch berechnet. Bei Fixiert und Fixiert und zentriert (Raster ab der Bildschirmmitte) werden Anzahl der App-Symbole pro Zeile und Anzahl der App-Symbole pro Spalte festgelegt (jeweils 1 bis 12).
7. Die Konfiguration nach Auswahl weiterer Optionen und Einschränkungen (Weitere Einstellungen →) speichern.

8. Bei Bedarf die Konfiguration Kiosk-Modus mit der Konfiguration App Konformität ergänzen.

9. Die aktuelle Version der Richtlinie veröffentlichen.

10. Um die Richtlinie auf Android-Geräten anzuwenden, die gewünschten Geräte über das Tab Geräte mit dieser Richtlinie hinzufügen. Die gewählten Einstellungen werden anschließend automatisch auf den Geräten ausgeführt.

Weitere Einstellungen

Unabhängig vom gewählten Modus bietet die Konfiguration folgende Einstellungen:

Für Version 26.4.0

- Gerätename anzeigen - zeigt einen Namen auf dem Launcher an. Ist das Feld Gerätename leer, erscheint der Name des Geräts. Änderungen am Gerätenamen können mehrere Stunden dauern, bis sie auf dem Gerät sichtbar sind.
- Geräteeinstellungen - Bildschirm beim Laden anlassen, Notfall-Telefonnummer sowie Homescreen Hintergrundbild und Sperrbildschirm Hintergrundbild (jeweils PNG oder JPEG). Die Notfall-Telefonnummer und das Sperrbildschirm-Hintergrundbild erscheinen auf dem Sperrbildschirm und setzen daher einen Sperrbildschirm voraus, der sich über eine Passwort-Konfiguration erzwingen lässt. Über die Notfall-Telefonnummer lässt sich auch bei gesperrtem Gerät oder aktivem Kiosk-Modus ein Notruf absetzen.
- Geräteeinschränkungen - u. a. Navigationsleiste, Statusleiste, Systemleiste, Task Manager und Home-Taste sowie Samsung-Funktionen wie Airview, S-Voice, Edge-Screen, Multi-Fenster und Smart-Clip. Navigationsleiste, Statusleiste und deren Erweiterung, Systemleiste, Task Manager, Home-Taste und Edge-Screen sind standardmäßig erlaubt. Bei deaktivierter Navigations- oder Systemleiste ist die App selbst für die Navigation zuständig. Benachrichtigungen löschen und Taskmanager leeren entfernen Benachrichtigungen bzw. die Liste der zuletzt verwendeten Apps.
- Hardware Einschränkungen - unter Deaktiviere Hardwaretasten lassen sich An-/Ausschalter, Lautstärketasten sowie Home-, Zurück- und Menü-Taste sperren.

Kiosk-Modus verlassen

Am Gerät erscheint die Passworteingabe, wenn der Bildschirm zügig 2-mal, 4-mal, 1-mal und 3-mal angetippt wird, mit einer Pause von jeweils mehr als 0,5 Sekunden zwischen den Gruppen. Nach Eingabe des in der Konfiguration hinterlegten Passworts lässt sich der Kiosk-Modus verlassen.

Für Version 26.4.0

WLAN

Die Richtlinie WLAN ermöglicht es, die WLAN-Einstellungen auf Android Classic-Geräten zu verwalten. Eine Richtlinie kann mehrere WLAN-Konfigurationen enthalten, z. B. für unterschiedliche Netzwerke. In der Konfiguration können Platzhalter verwendet werden, die beim Übertragen pro Gerät aufgelöst werden; die verfügbaren Platzhalter zeigt das Formular unterhalb der Eingabefelder an.

Einschränkungen der WLAN-Nutzung, z. B. erlaubte oder gesperrte SSIDs und eine Mindest-Sicherheitsstufe, werden nicht hier, sondern über die separate Konfiguration Restriktionen für drahtlose Netzwerke festgelegt.

Allgemein

- Netzwerk SSID – Name des Netzwerks (Pflichtfeld).
- Priorität – ganze Zahl ab 0. Sind mehrere Netzwerke verfügbar, verbindet sich das Gerät zunächst mit dem Netzwerk mit der höchsten Priorität. Standardmäßig haben alle Netzwerke die Priorität 0.
- Verstecktes Netzwerk – für Netzwerke, die ihre SSID nicht senden.
- Sicherheitstyp – Keiner / Offen für alle (Standard), WEP, WPA/WPA2 PSK oder 802.1x EAP (EAP). Bei WEP und WPA/WPA2 PSK ist das Feld Passwort Pflicht; bei WPA/WPA2 PSK muss es 8 bis 63 Zeichen lang sein.

802.1x EAP (EAP)

Für Version 26.4.0

Dieser Abschnitt erscheint nur beim Sicherheitstyp 802.1x EAP (EAP). Unter Akzeptierte EAP-Typen stehen PEAP (Standard), TLS, TTLS und PWD zur Wahl. Je nach Typ werden folgende Felder angezeigt:

- PEAP und TTLS: Interne Authentifizierung (Phase 2) (Keine, MSCHAP, MSCHAPv2, GTC oder PAP, Standard: Keine), CA Zertifikat, Identität, Anonyme Identität und Passwort. Bei PEAP werden PAP und MSCHAP beim Speichern abgelehnt.
- TLS: CA Zertifikat, Benutzer-Authentifizierungszertifikat und Identität. Für das Benutzer-Authentifizierungszertifikat gibt es zwei Optionen:
  - Zertifikat wählen – ein Zertifikat mit privatem Schlüssel (PKCS#12) aus der Zertifikatsverwaltung →.
  - Benutzerdefiniertes Zertifikat verwenden – das WLAN-Zertifikat aus dem Profil des Benutzers, der dem Gerät zugewiesen ist (siehe Benutzerzertifikate →). Das optionale Feld Zertifikatsname wählt ein bestimmtes Zertifikat anhand des Namens aus, wenn der Benutzer mehrere WLAN-Zertifikate besitzt, und kann Platzhalter enthalten. Bleibt es leer, wird das am längsten gültige Zertifikat verwendet.
- PWD: Identität und Passwort.

Als CA Zertifikat stehen Zertifikate ohne privaten Schlüssel (PKCS1) aus der Zertifikatsverwaltung zur Auswahl.

> Auf Samsung Knox-Geräten wird eine Konfiguration mit dem EAP-Typ PEAP, TLS oder TTLS nur angewendet, wenn die Richtlinie zusätzlich eine aktivierte Konfiguration Passwort enthält. Fehlt sie oder ist sie deaktiviert, zeigt das Formular einen entsprechenden Hinweis an.

Proxy Typ

- Keine (Standard) – kein Proxy.
- Manuell – Host (ohne Protokoll) und Portnummer (1 bis 65535) des Proxy-Servers sind Pflicht. Unter Proxy umgehen für wird eine Liste von Adressen eingetragen, die nicht über den Proxy geleitet werden.
- Automatisch konfigurieren – PAC URL mit der Adresse der PAC-Datei (Pflichtfeld).

Zertifikat

Die Richtlinie Zertifikat ermöglicht es, ein Zertifikat auszuwählen, das standardmäßig auf dem Gerät installiert werden soll. Eine Richtlinie kann mehrere Zertifikat-Konfigurationen enthalten, jedes Zertifikat jedoch nur einmal.

Voraussetzungen

- Das Zertifikat wurde zuvor unter `Einstellungen` → `Zertifikate` hochgeladen (siehe Zertifikatsverwaltung →).
- Auswählbar sind nur Zertifikate vom Typ PKCS1, also Zertifikate ohne privaten Schlüssel (z. B. `crt`, `cer`). PKCS#12-Dateien (`pfx` / `p12`) erscheinen nicht in der Auswahl.
- Auf Samsung Knox-Geräten wird das Zertifikat nur installiert, wenn die Richtlinie zusätzlich eine aktivierte Konfiguration Passwort enthält. Fehlt sie oder ist sie deaktiviert, zeigt das Formular einen entsprechenden Hinweis an.

Für Version 26.4.0

Konfiguration

Im Dialog Zertifikat hinzufügen wird im Abschnitt Allgemein über Auswählen am Feld Zertifikat der Dialog Wählen Sie ein Zertifikat aus geöffnet. Zertifikate, die bereits in einer anderen Zertifikat-Konfiguration derselben Richtlinie verwendet werden, sind dort ausgeblendet. Das Feld ist ein Pflichtfeld; Speichern ist erst nach der Auswahl eines Zertifikats aktiv. Der Name der Konfiguration wird automatisch aus dem Namen des Zertifikats übernommen.

Factory Reset Protection

Organisationen müssen die Sicherheit und Konformität der für die Leistungserbringung eingesetzten Android-Geräte gewährleisten. Mit Relution können dabei Aufwände minimiert und die Sicherheit erhöht werden, indem arbeitsrelevante Geräte aus der Ferne eingerichtet, verwaltet, überwacht und auftretende Fehler zeitnah behoben werden. Ein auf den Geräten installierter Relution Companion für Android ermöglicht die Android Classic / Legacy-Einschreibung der Geräte in Relution. Zusätzlich kann ein Factory Reset auf den Geräten verboten werden.

Das Verbot des Factory Resets ist eine Knox-spezifische Restriktion der Konfiguration Restriktionen und steht nur auf Samsung-Geräten mit Knox zur Verfügung. Auf Geräten anderer Hersteller hat die Option keine Wirkung.

FRP konfigurieren

1. Im Relution-Portal zum Menüpunkt `Geräte` → `Richtlinien` navigieren und auf Hinzufügen klicken.
2. Eine Android-Richtlinie erstellen und einen Namen vergeben. Auf Speichern klicken.
3. Nach Klick auf Hinzufügen anschließend die Option Restriktionen wählen und mit Details hinzufügen fortfahren.
4. Unter Knox spezifische Restriktionen im Abschnitt Backup & Zurücksetzen sicherstellen, dass die Option Zurücksetzen auf Werkseinstellungen verbieten aktiviert ist. In neuen Restriktionen-Konfigurationen ist die Option standardmäßig aktiv.
5. Die Konfiguration speichern und die aktuelle Version der Richtlinie veröffentlichen.
6. Um die Richtlinie auf Android-Geräten anzuwenden, die gewünschten Geräte über das Tab Geräte mit dieser Richtlinie hinzufügen. Alternativ wird die Richtlinie über das Tab Gerätegruppen mit dieser Richtlinie ganzen Gerätegruppen zugewiesen. Die gewählten Einstellungen werden anschließend automatisch auf den Geräten ausgeführt.

Für Version 26.4.0

> Auf Samsung-Geräten mit Knox ist anschließend die Schaltfläche Gerät auf Werkseinstellungen zurücksetzen ausgegraut. Auch ein Zurücksetzen über den Recovery Mode ist nicht mehr möglich.

Da die Option standardmäßig aktiv ist, verbietet jede Restriktionen-Konfiguration das Zurücksetzen auf Werkseinstellungen, solange die Option nicht deaktiviert wird. Soll ein Gerät gezielt zurückgesetzt werden, wird die Option Zurücksetzen auf Werkseinstellungen verbieten deaktiviert und eine neue Version der Richtlinie veröffentlicht.

Alle weiteren Optionen der Konfiguration sind unter Restriktionen → beschrieben.

ADVANTouch

Mit Relution ist es möglich, interaktive Whiteboards der Marke ADVANTouch zentral zu verwalten.

Unterstützte Produktserien und Modelle

Relution unterstützt folgende ADVANTouch-Produktserien:

- ADVANTouch PRO 1, 2.0, 2.1 und 3
- ADVANTouch vGAP 2, 3, 4 und 5

Die Unterstützung gilt grundsätzlich ab Android API 24 (entspricht Android 7.0 oder höher).

Einschreibung

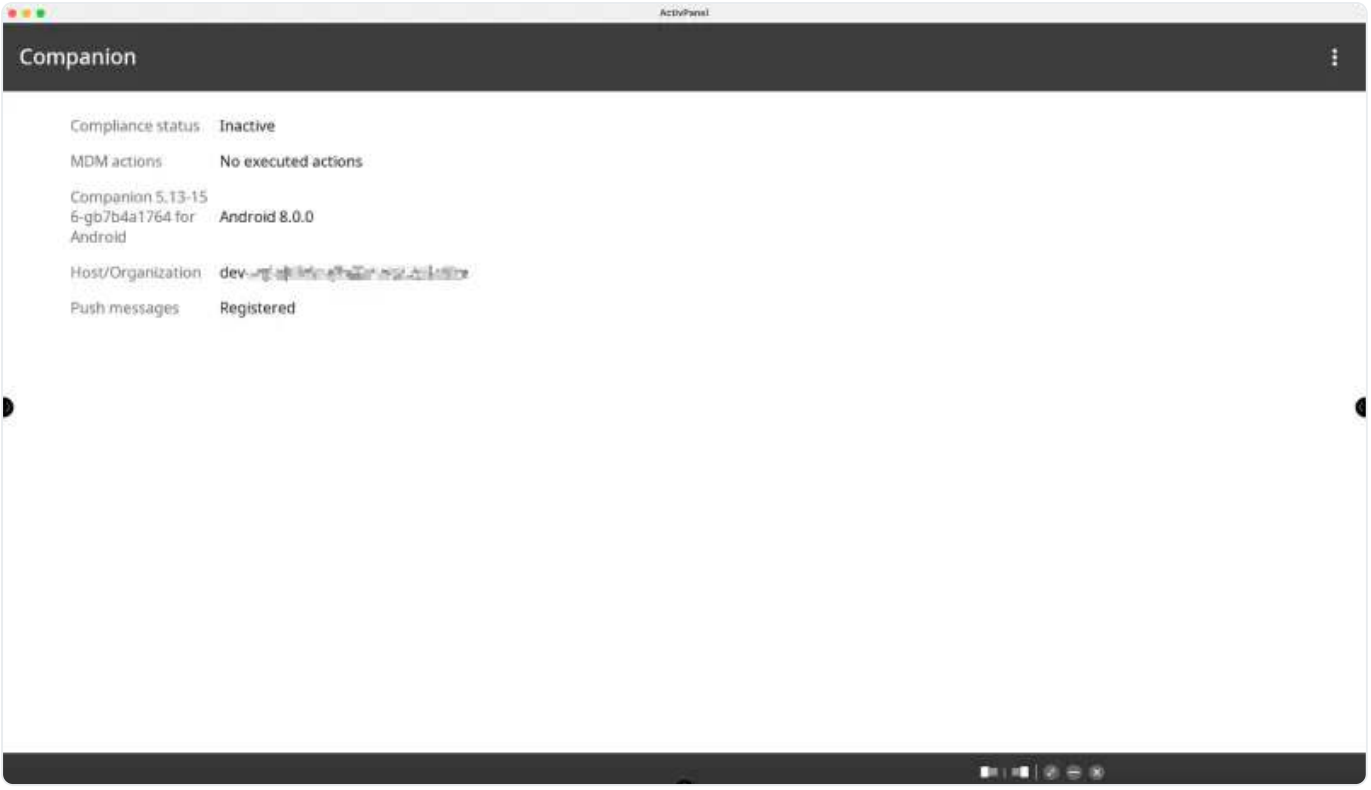
Für Version 26.4.0

Eine Einschreibung für die Plattform Android erstellen und den Typ ADVANTouch auswählen.

Sicherstellen, dass vor der Einschreibung der Relution Companion für ADVANTouch (Paketname `com.mwaysolutions.relution.advantouch`) installiert ist. Der Standard-Relution-Companion kann sich nicht mit einer Einschreibung vom Typ ADVANTouch einschreiben; der Server lehnt die Einschreibung ab.

Den Relution Companion öffnen und die Serveradresse sowie den Einschreibungscode eingeben.

Der Companion fordert mehrere Bestätigungen. Die angezeigten Hinweise und Berechtigungsabfragen bestätigen. Nach erfolgreicher Einschreibung erscheint ein entsprechender Bestätigungsbildschirm. Dieser sieht so oder so ähnlich aus.



Das Gerät sollte nun im Inventar des Relution Portals sichtbar sein.

Unterstützte Aktionen

Für Version 26.4.0

Auf ADVANTouch-Whiteboards können über Relution folgende Aktionen ausgeführt werden:

Aktion	Beschreibung
Alarm auslösen →	
App entfernen →	
Datei an Gerät senden →	
Gerät auf Werkszustand zurücksetzen →	
Gerät neu starten →	Neustart oder Herunterfahren (Option Ausschalten)
Gerät vollständig sperren →	Voraussetzung: Ein Passwort oder eine PIN ist lokal am Gerät oder über die herstellerspezifische Richtlinie (Sperrbildschirm-PIN aktivieren) gesetzt
Geräteinformationen aktualisieren →	
Nachricht senden →	
Relution Store App bereitstellen →	
Update des Betriebssystems →	

Für Vers

Unterstützte Richtlinien

Folgende Richtlinien werden auf ADVANTouch-Whiteboards unterstützt:

Richtlinie	Einschränkungen
Hotspot →	
App Konformität →	
Zertifikat →	Device Owner

Herstellerspezifische Richtlinie

Die herstellerspezifische Richtlinie ADVANTouch stellt folgende Einstellungen bereit:

Für Version 26.4.0

Einstellung	Beschreibung
Helligkeit	Helligkeit auf einen festen Wert von 0 bis 100 setzen
Eye Care an	
Touch-Eingabe sperren	
Boot-Quelle	Aktive Quelle nach dem Hochfahren des Displays setzen (Nicht ändern, Android, HDMI 1–3, USB-C 1–2 oder VGA)
Aktuelle Quelle	Aktuelle Quelle setzen (Auswahl wie bei Boot-Quelle)
Keine Signalabschaltung	Ausschalten, wenn nach der eingestellten Zeit kein Signal anliegt
Kein Signal Ausschaltzeit	Zeit von 1 Minute bis 1 Stunde bis zum Ausschalten ohne Signal; nur einstellbar, wenn Keine Signalabschaltung aktiviert ist
Anschalten, wenn die Quelle angeschlossen wird	
Quellalias zulassen	Nach dem Aktivieren Aliase für Android, HDMI1, HDMI2, HDMI3 und USB-C1 festlegen
Ethernet aktivieren	
Wake on LAN	Wake-on-LAN-Funktion aktivieren
Stummschalten	
Lautstärke	Lautstärke auf einen festen Wert von 0 bis 100 setzen
Sperrbildschirm-PIN aktivieren	PIN für den Sperrbildschirm setzen (genau 4 Stellen)
Administratorsperre aktivieren	Passwort für die Administratorsperre setzen (genau 4 Stellen)
Einstellungssperre aktivieren	Nur verfügbar, wenn die Administratorsperre aktiviert ist
Sprache	Gerätesprache setzen (Englisch, Deutsch oder Spanisch)
Automatische OTA-Updates aktivieren	
Installation aus unbekannten Quellen zulassen	Erlaubt die Installation von unbekannten Quellen, einschließlich von USB-Sticks
Einschaltzeit setzen	Wochentage und Uhrzeit für das automatische Einschalten des Displays setzen
Ausschaltzeit setzen	Wochentage und Uhrzeit für das automatische Ausschalten des Displays setzen
Zeit, bis das Display in den Standby-Modus wechselt	Nicht ändern, Nie, 15 oder 30 Minuten, 1, 1,5 oder 2 Stunden

Eine neue Konfiguration ist mit folgenden Werten vorbelegt: Helligkeit 100, Lautstärke 33, Sprache Deutsch, Standby Nie; Ethernet aktivieren, Installation aus unbekannten Quellen zulassen und Anschalten, wenn die Quelle angeschlossen wird sind aktiviert. Für Helligkeit, Lautstärke und Sprache gibt es keine Option „Nicht ändern“, diese Werte werden mit der Richtlinie immer gesetzt.

Nach dem Ändern von Sperrbildschirm-PIN oder Administratorsperre kann ein Neustart des Geräts erforderlich sein, damit die Änderungen wirksam werden.

Device Owner aktivieren

Um geräteeigentümerspezifische Funktionen zu aktivieren, den Anweisungen für Android Debug Bridge Einrichtung und Verbindung → folgen.

Nachdem das Gerät verbunden wurde, den Geräteeigentümer-Modus durch Ausführen des Befehls aktivieren:

```
adb shell dpm set-device-owner
com.mwaysolutions.relution.advantouch/com.mwaysolutions.relution.receiver.MdmDeviceAdmi
nReceiver
```

Für Version 26.4.0

Clevertouch

Mit Relution ist es möglich, interaktive Whiteboards der Marke Clevertouch zentral zu verwalten.

Unterstützte Produktserien und Modelle

Relution unterstützt folgende Clevertouch-Produktserien:

- IMPACT Lux

Einschreibung

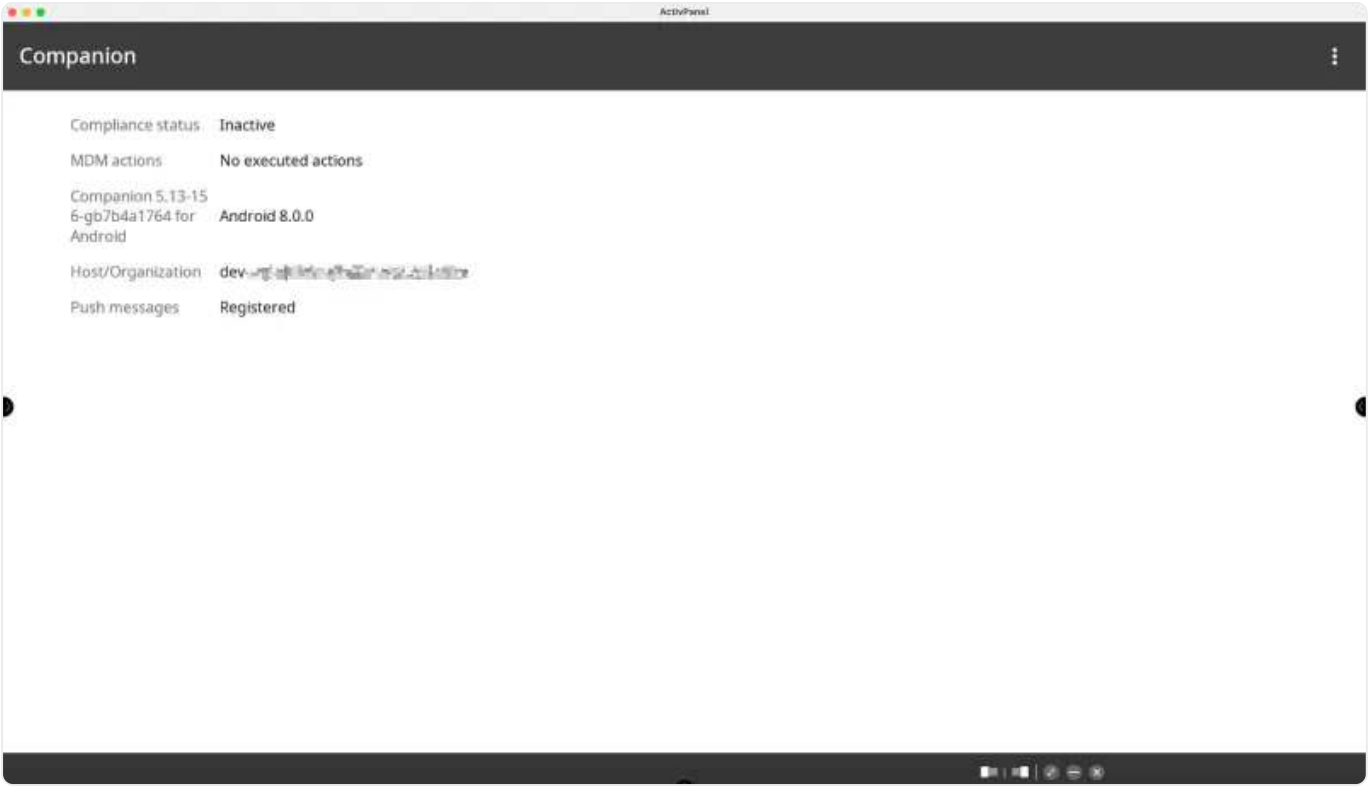
Eine Einschreibung für die Plattform Android erstellen und den Typ Clevertouch auswählen. Den Einschreibelink auf dem Gerät öffnen und den Anweisungen auf der Seite folgen.

Über den angezeigten Download-Button lässt sich der Relution Companion für Clevertouch herunterladen und installieren.

Nach erfolgreicher Installation des Companions zur Einschreibungsseite zurückkehren, um die Einschreibung zu starten.

Der Companion öffnet sich anschließend automatisch und fordert zur Bestätigung mehrerer Hinweise und Berechtigungen auf. Nach erfolgreicher Einschreibung erscheint ein entsprechender Bestätigungsbildschirm. Dieser sieht so oder so ähnlich aus.

Für Version 26.4.0



Das Gerät sollte nun im Inventar des Relution Portals sichtbar sein.

Unterstützte Aktionen

Für Version 26.4.0

Auf Clevertouch-Whiteboards können über Relution folgende Aktionen ausgeführt werden:

Aktion	Beschreibung
Alarm auslösen →	
App entfernen →	
Datei an Gerät senden →	
Gerät auf Werkszustand zurücksetzen →	
Gerät neu starten →	Neustart oder Herunterfahren (Option Ausschalten)
Geräteinformationen aktualisieren →	
Nachricht senden →	
Relution Store App bereitstellen →	
Update des Betriebssystems →	

Unterstützte Richtlinien

Folgende Richtlinien werden auf Clevertouch-Whiteboards unterstützt:

Richtlinie	Einschränkungen
Geplantes OTA-Update →	
Hotspot →	
WLAN →	
App Konformität →	

Herstellerspezifische Richtlinie

Die herstellerspezifische Richtlinie Clevertouch stellt folgende Einstellungen bereit:

Für Version 26.4.0

Einstellung	Beschreibung
Helligkeit	Helligkeit auf einen festen Wert von 0 bis 100 setzen
Eye Care an	
Touch-Eingabe sperren	
Boot-Quelle	Aktive Quelle nach dem Hochfahren des Displays setzen (Nicht ändern, Android, HDMI 1–3, USB-C 1–2 oder VGA)
Aktuelle Quelle	Aktuelle Quelle setzen (Auswahl wie bei Boot-Quelle)
Keine Signalabschaltung	Ausschalten, wenn nach der eingestellten Zeit kein Signal anliegt
Kein Signal Ausschaltzeit	Zeit von 1 Minute bis 1 Stunde bis zum Ausschalten ohne Signal; nur einstellbar, wenn Keine Signalabschaltung aktiviert ist
Quellalias zulassen	Nach dem Aktivieren Aliase für Android, HDMI1, HDMI2, HDMI3 und USB-C1 festlegen
Ethernet aktivieren	
Stummschalten	
Lautstärke	Lautstärke auf einen festen Wert von 0 bis 100 setzen
Sperrbildschirm-PIN aktivieren	PIN für den Sperrbildschirm setzen (genau 4 Stellen)
Sprache	Gerätesprache setzen (Englisch, Deutsch oder Spanisch)
Automatische OTA-Updates aktivieren	
Installation aus unbekannten Quellen zulassen	Erlaubt die Installation von unbekannten Quellen, einschließlich von USB-Sticks
Einschaltzeit setzen	Wochentage und Uhrzeit für das automatische Einschalten des Displays setzen
Ausschaltzeit setzen	Wochentage und Uhrzeit für das automatische Ausschalten des Displays setzen
Zeit, bis das Display in den Standby-Modus wechselt	Nicht ändern, Nie, 15 oder 30 Minuten, 1, 1,5 oder 2 Stunden

Eine neue Konfiguration ist mit folgenden Werten vorbelegt: Helligkeit 100, Lautstärke 33, Sprache Deutsch, Standby Nie; Ethernet aktivieren und Installation aus unbekannten Quellen zulassen sind aktiviert. Für Helligkeit, Lautstärke und Sprache gibt es keine Option „Nicht ändern“, diese Werte werden mit der Richtlinie immer gesetzt.

Nach dem Ändern der Sperrbildschirm-PIN kann ein Neustart des Geräts erforderlich sein, damit die Änderung wirksam wird.

CTOUCH

Mit Relution ist es möglich, interaktive Whiteboards der Marke CTOUCH zentral zu verwalten.

Unterstützte Produktserien und Modelle

Folgende Produktserien werden unterstützt:

- Riva D2

Einschreibung

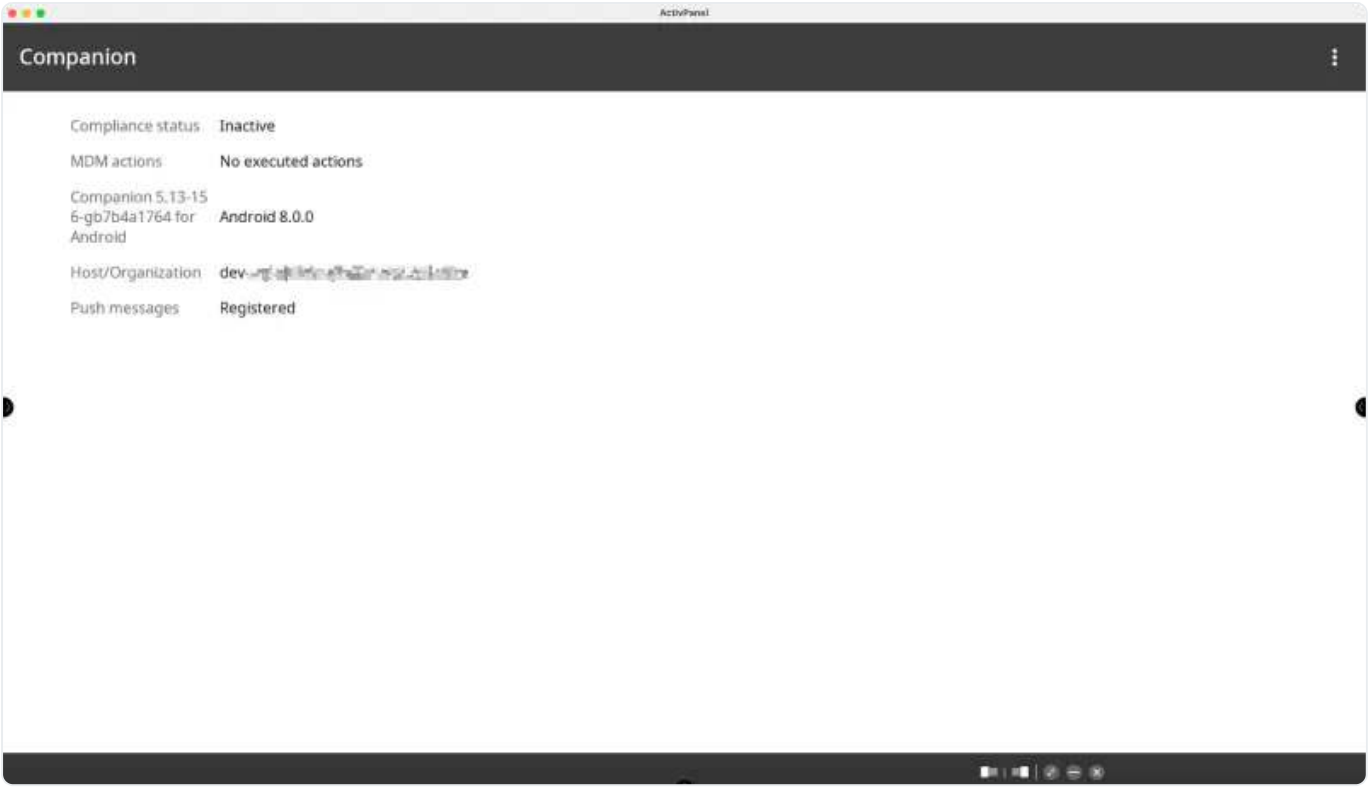
Eine Einschreibung für die Plattform Android erstellen und den Typ CTOUCH auswählen. Den Einschreibelink auf dem Gerät öffnen und den Anweisungen auf der Seite folgen.

Über den angezeigten Download-Button lässt sich der Relution Companion für CTOUCH herunterladen und installieren.

Nach erfolgreicher Installation des Companions zur Einschreibungsseite zurückkehren, um die Einschreibung zu starten.

Der Companion öffnet sich anschließend automatisch und fordert zur Bestätigung mehrerer Hinweise und Berechtigungen auf. Nach erfolgreicher Einschreibung erscheint ein entsprechender Bestätigungsbildschirm.

Für Version 26.4.0



Das Gerät sollte nun im Inventar des Relution Portals sichtbar sein.

Unterstützte Aktionen

Für Version 26.4.0

Auf CTOUCH-Whiteboards können über Relution folgende Aktionen ausgeführt werden:

Aktion	Beschreibung
Alarm auslösen →	
App entfernen →	
Datei an Gerät senden →	
Gerät auf Werkszustand zurücksetzen →	
Gerät entsperren →	
Gerät neu starten →	Neustart oder Herunterfahren (Option Ausschalten)
Gerät vollständig sperren →	Voraussetzung: Ein Passwort oder eine PIN ist lokal am Gerät oder über die herstellerspezifische Richtlinie (LockScreen Passwort aktivieren) gesetzt
Geräteinformationen aktualisieren →	
Nachricht senden →	
Relution Store App bereitstellen →	Native Apps über Relution bereitstellen. Installation aus unbekannten Quellen zulassen muss aktiviert sein

Für Vers

Unterstützte Richtlinien

Folgende Richtlinien werden auf CTOUCH-Whiteboards unterstützt:

Richtlinie	Einschränkungen
WLAN →	
App Konformität →	
Zertifikat →	Nur Installation wird unterstützt

Herstellerspezifische Richtlinie

Die herstellerspezifische Richtlinie CTOUCH stellt folgende Einstellungen bereit:

Einstellung	Beschreibung
LockScreen Passwort aktivieren	Passwort des Sperrbildschirms setzen; bei aktiviertem Schalter ist das Feld Lockscreen Passwort Pflicht (mindestens 6 Zeichen)
Wake on LAN	Wake-on-LAN-Funktion aktivieren (in neuen Konfigurationen vorbelegt)
Installation aus unbekannten Quellen zulassen	Erlaubt die Installation von Apps aus unbekannten Quellen; Voraussetzung für Relution Store App bereitstellen
Einschaltzeit setzen	Wochentage und Uhrzeit für das automatische Einschalten des Displays setzen
Ausschaltzeit setzen	Wochentage und Uhrzeit für das automatische Ausschalten des Displays setzen
OTA-Update aktivieren	Automatische Suche nach OTA-Updates aktivieren

Für Version 26.4.0

Dahua

Mit Relution ist es möglich, interaktive Whiteboards der Marke Dahua zentral zu verwalten.

Unterstützte Produktserien und Modelle

Relution unterstützt folgende Dahua-Produktserien:

- LPHXX-ST420

Einschreibung

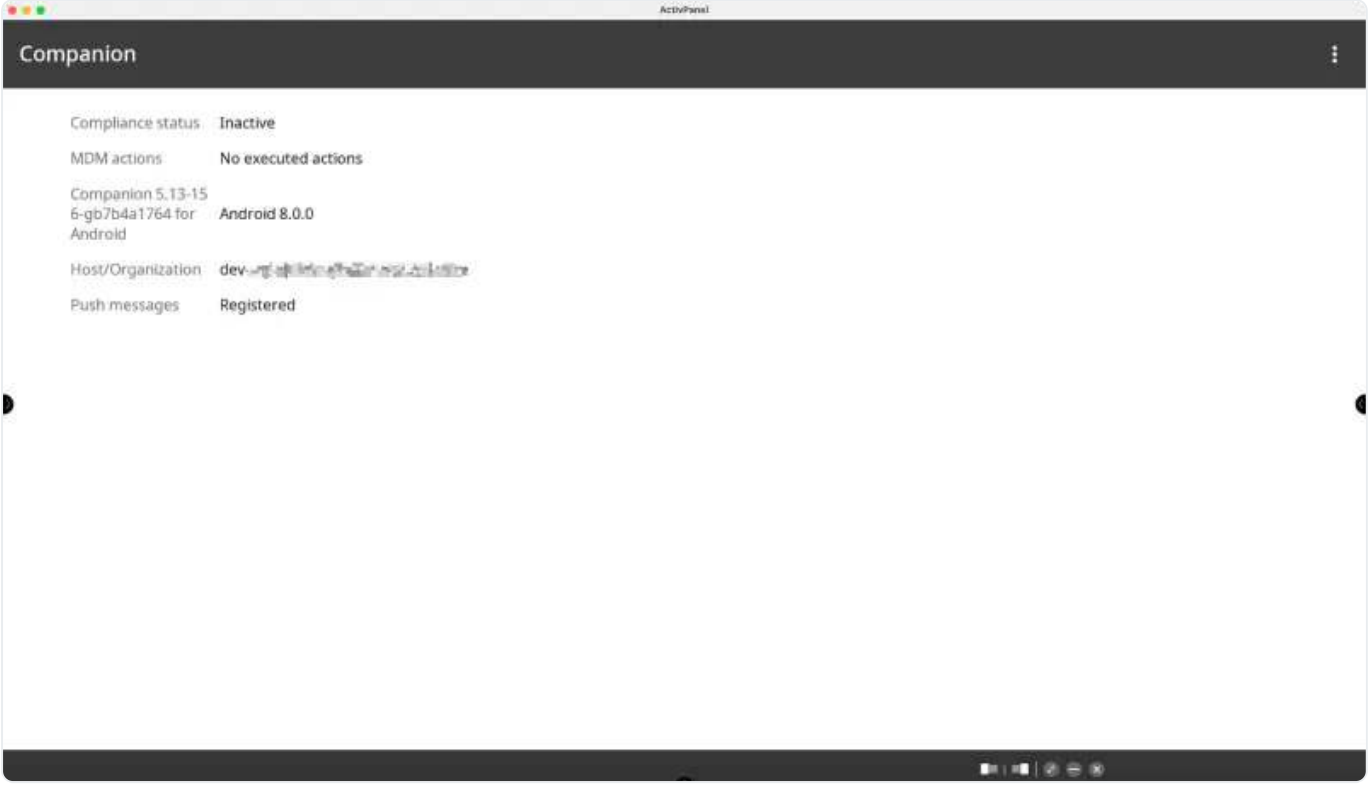
Eine Einschreibung für die Plattform Android erstellen und den Typ Dahua auswählen. Den Einschreibelink auf dem Gerät öffnen und den Anweisungen auf der Seite folgen.

Über den angezeigten Download-Button lässt sich der Relution Companion für Dahua herunterladen und installieren.

Nach erfolgreicher Installation des Companions zur Einschreibungsseite zurückkehren, um die Einschreibung zu starten.

Der Companion öffnet sich anschließend automatisch und fordert zur Bestätigung mehrerer Hinweise und Berechtigungen auf. Nach erfolgreicher Einschreibung erscheint ein entsprechender Bestätigungsbildschirm. Dieser sieht so oder so ähnlich aus.

Für Version 26.4.0



Anschließend den Bildschirmanweisungen folgen, bis die Einschreibung abgeschlossen ist.

Das Gerät sollte nun im Inventar des Relution Portals sichtbar sein.

Für Version 26.4.0

Unterstützte Aktionen

Auf Dahua-Whiteboards können über Relution folgende Aktionen ausgeführt werden:

Aktion	Beschreibung
Alarm auslösen →	
App entfernen →	
Datei an Gerät senden →	
Gerät auf Werkszustand zurücksetzen →	
Gerät neu starten →	Neustart oder Herunterfahren (Option Ausschalten)
Gerät vollständig sperren →	
Geräteinformationen aktualisieren →	
Nachricht senden →	
Relution Store App bereitstellen →	
Update des Betriebssystems →	

Für Version 26.4.0

Unterstützte Richtlinien

Folgende Richtlinien werden auf Dahua-Whiteboards unterstützt:

Richtlinie	Einschränkungen
EShare →	
App Konformität →	
Ethernet	

Herstellerspezifische Richtlinie

Die herstellerspezifische Richtlinie Dahua stellt folgende Einstellungen bereit:

Einstellung	Beschreibung
Helligkeit	Helligkeit auf einen festen Wert setzen (0–100, Standard 100)
Automatische Helligkeit einschalten	Helligkeit automatisch anpassen (Standard: aus)
Ausschaltzeit ohne Signal in Minuten	Zeit in Minuten ohne Eingangssignal, nach der das Whiteboard ausgeschaltet wird (mindestens 1, Standard 5)
Boot-Quelle	Aktive Quelle nach dem Hochfahren des Displays setzen
Aktuelle Quelle	Aktuelle Quelle setzen
USB-Verfügbarkeit	USB-Anschlüsse verfügbar machen (Standard: an)
Wake on LAN	Wake-on-LAN-Funktion aktivieren (Standard: an)
Stummschalten	Ton stummschalten (Standard: aus)
Lautstärke	Lautstärke auf einen festen Wert setzen (0–100, Standard 33)
Sprache	Gerätesprache setzen: Englisch, Deutsch oder Spanisch (Standard Deutsch)
Zeitzone	Zeitzone des Geräts setzen (Standard Europa/Paris)
Zeitpläne für das Ein- und Ausschalten	Bis zu 5 Zeitpläne für das automatische Ein- und Ausschalten

Für Boot-Quelle und Aktuelle Quelle stehen Nicht ändern (Standard), Android, HDMI 1–3, USB-C 1–2, VGA, OPS, DisplayPort, Component (YPbPr), AV und Letzte Quelle zur Auswahl.

heinekingmedia

Mit Relution ist es möglich, interaktive Whiteboards der Marke heinekingmedia zentral zu verwalten.

Unterstützte Produktserien und Modelle

Relution unterstützt folgende heinekingmedia-Produktserien:

- Digitale Tafel (DT-86A80-L20HM)
- Digitale Tafel Gen3 (DT-65A11-L30HM)

Einschreibung

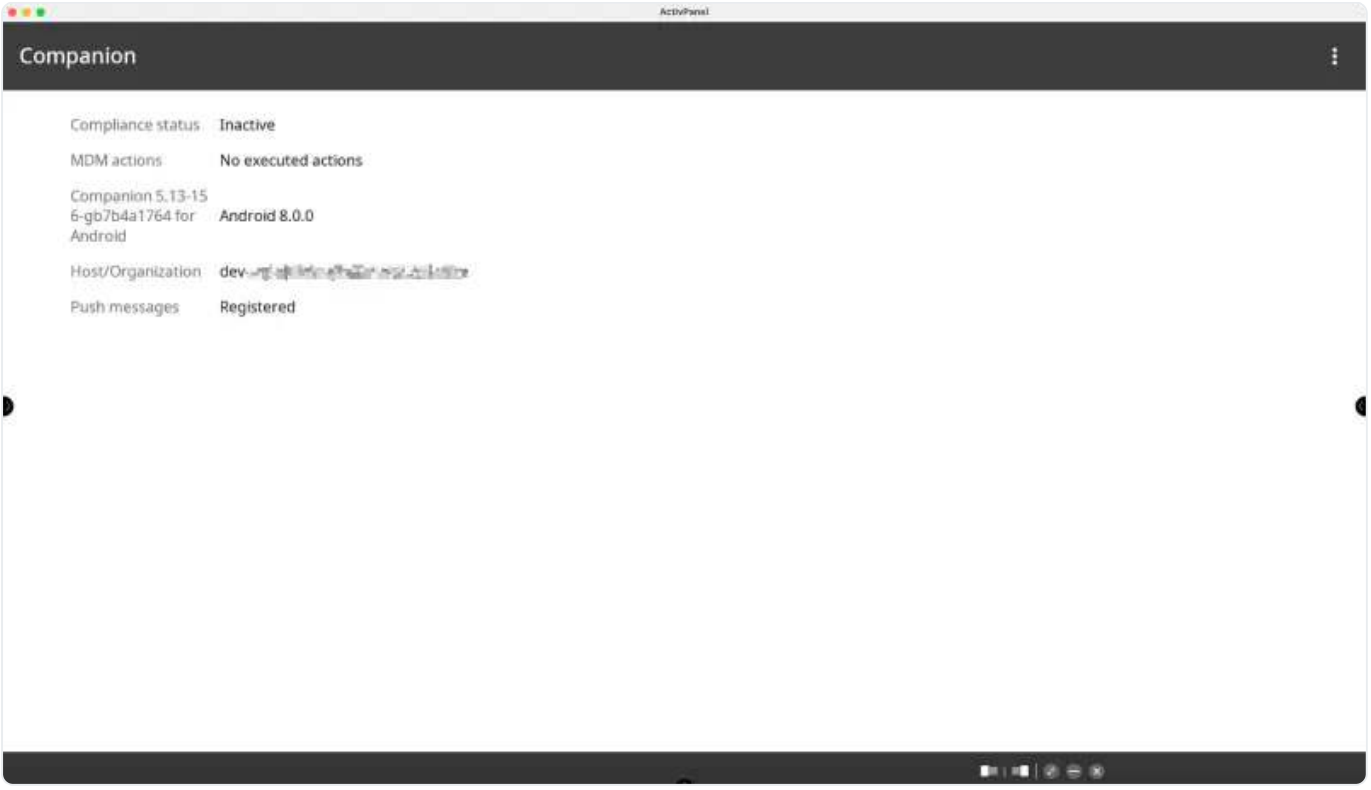
Eine Einschreibung für die Plattform Android erstellen und den Typ heinekingmedia auswählen. Den Einschreibelink auf dem Gerät öffnen und den Anweisungen auf der Seite folgen.

Über den angezeigten Download-Button lässt sich der Relution Companion für heinekingmedia herunterladen und installieren.

Nach erfolgreicher Installation des Companions zur Einschreibungsseite zurückkehren, um die Einschreibung zu starten.

Der Companion öffnet sich anschließend automatisch und fordert zur Bestätigung mehrerer Hinweise und Berechtigungen auf. Nach erfolgreicher Einschreibung erscheint ein entsprechender Bestätigungsbildschirm. Dieser sieht so oder so ähnlich aus.

Für Version 26.4.0



Anschließend den Bildschirmanweisungen folgen, bis die Einschreibung abgeschlossen ist.

Das Gerät sollte nun im Inventar des Relution Portals sichtbar sein.

Für Version 26.4.0

Unterstützte Aktionen

Auf heinekingmedia-Whiteboards können über Relution folgende Aktionen ausgeführt werden:

Aktion	Beschreibung
Alarm auslösen →	
App entfernen →	
Datei an Gerät senden →	
Gerät auf Werkszustand zurücksetzen →	
Gerät neu starten →	Neustart oder Herunterfahren (Option Ausschalten)
Geräteinformationen aktualisieren →	
Nachricht senden →	
Relution Store App bereitstellen →	
Update des Betriebssystems →	

Für Version 26.4.0

Unterstützte Richtlinien

Folgende Richtlinien werden auf heinekingmedia-Whiteboards unterstützt:

Richtlinie	Einschränkungen
Kiosk-Modus →	
Hotspot →	
EShare →	
App Konformität →	

Interaktive Whiteboard Konfiguration

Die Richtlinie Interaktive Whiteboard Konfiguration stellt folgende Einstellungen für heinekingmedia-Whiteboards bereit:

Einstellung	Beschreibung
Hardware-Tasten sperren	
Fernbedienung sperren	
Einstellungen sperren	Geräteeinstellungen sperren. Ist der Schalter aktiv, muss das Feld Pin zum Entsperren der Einstellungen (nur Ziffern) ausgefüllt werden. Das Portal kennzeichnet das Feld nur für Prowise und wende.interaktiv, ohne Eintrag lässt sich die Konfiguration aber nicht speichern.
Sperrbildschirm	Nur verfügbar, wenn Einstellungen sperren aktiviert ist. Sperrbildschirm aktivieren und eine numerische PIN setzen (Pflichtfeld Pin für den Sperrbildschirm). Wird Einstellungen sperren ausgeschaltet, wird auch der Sperrbildschirm deaktiviert.
Touch-Eingabe sperren	
USB-Anschlüsse sperren	
App-Installation blockieren	
App-Deinstallation blockieren	
Limitieren der maximalen Lautstärke	Einen Wert für die maximale Lautstärke setzen (Feld Die maximale Lautstärke in Prozent, 0–100, Standard 100)
Helligkeit	Helligkeit auf einen festen Wert setzen (0–100, Standard 100). Einen eigenen Schalter gibt es nicht, der Wert wird immer übertragen.
Sprache	Gerätesprache setzen: Englisch, Deutsch, Spanisch oder Chinesisch (Standard Deutsch)
Zeitzone	Zeitzone des Geräts setzen (Standard Europa/Paris)
Boot-Quelle	Aktive Quelle nach dem Hochfahren des Displays setzen: Android, AV, DisplayPort, HDMI 1–3, OPS, USB-C, VGA oder Letzte Quelle (Standard)
HDMI-Ausgang	Auflösung und Bildfrequenz setzen: Auto (Standard), 2k 60Hz, 4k 30Hz oder 4k 60Hz
URL der OTA-Aktualisierung	Adresse für Over-the-Air-Updates, nur HTTPS-URLs werden akzeptiert
Einschaltzeit setzen	Nach Aktivieren des Schalters Aus/An Wochentage und Uhrzeit für das automatische Einschalten des Displays setzen
Ausschaltzeit setzen	Nach Aktivieren des Schalters Aus/An Wochentage und Uhrzeit für das automatische Ausschalten des Displays setzen

Einstellung	Beschreibung
Ausgewählte Apps sperren	Nach Aktivieren des Schalters Aus/An Apps über ihre Paketnamen sperren und eine numerische PIN zum Entsperren dieser Apps setzen (Pflichtfeld PIN zum Entsperren von Apps)
System-Utilities	Konfiguration der Utilities: Mem clear, Hardware-Erkennung, App-Sperre, Sperrbildschirm, Home, Zurück, Menü, Bildschirm aus, Spotlight, WLAN, Quelle, Digitale Tafel, Stummschalten, Lautstärke, Helligkeit und Mehr. Ist der Schalter Aus/An aktiv, müssen genau fünf Utilities ausgewählt sein, sonst lässt sich die Konfiguration nicht speichern.
Seitliche Navigationsleiste	Elemente der seitlichen Navigationsleiste konfigurieren: Offene Apps, Quelle, Steuerung, Einstellungen, Einfrieren, Bildschirmfoto, Zeit, Kamera, Ordner, Helligkeit, Dunkelheit. Ist der Schalter Aus/An aktiv, müssen genau vier Elemente ausgewählt sein, sonst lässt sich die Konfiguration nicht speichern.

Für Version 26.4.0

i3-Technologies

Mit Relution ist es möglich, interaktive Whiteboards der Marke i3-Technologies zentral zu verwalten.

Unterstützte Produktserien und Modelle

Relution unterstützt folgende i3-Technologies-Produktserien:

- i3TOUCH E-ONE

Einschreibung

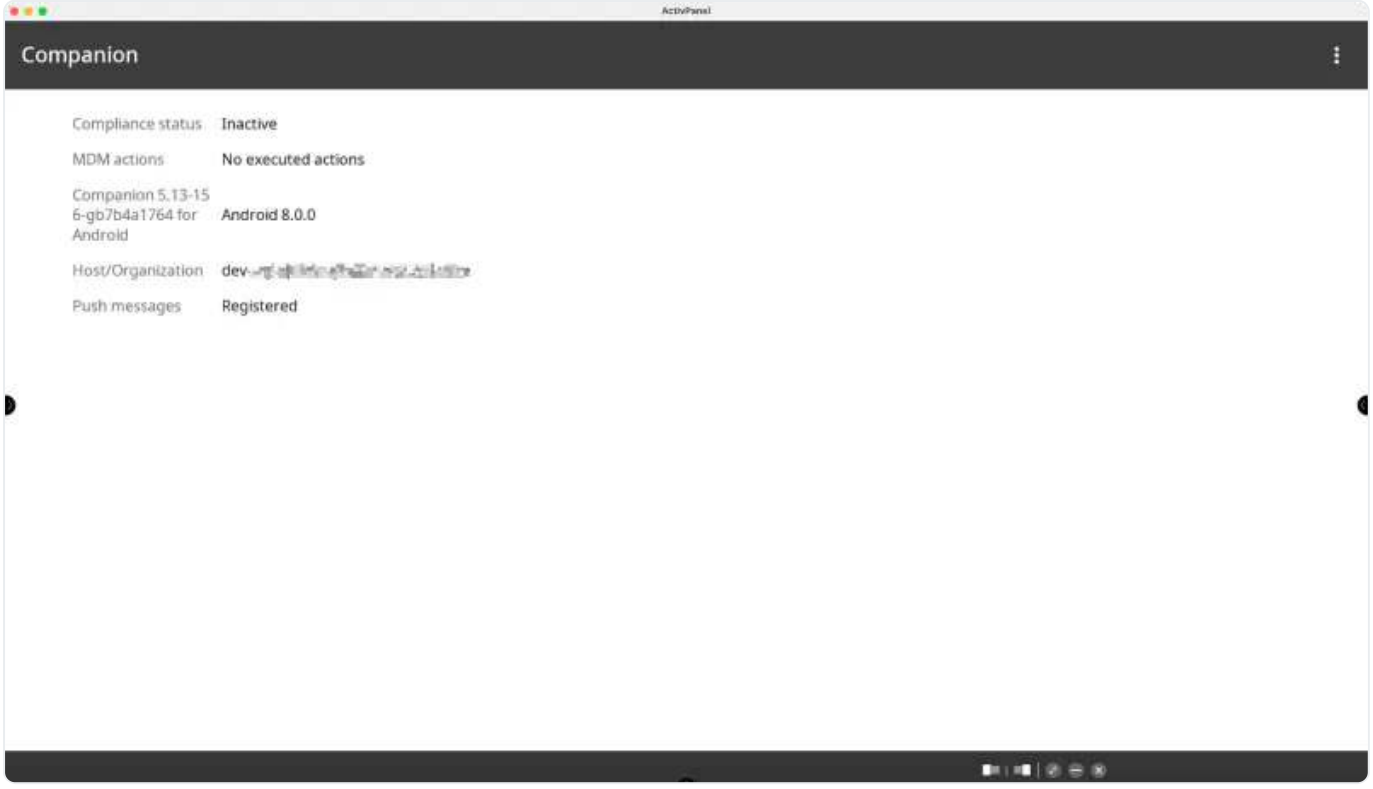
Eine Einschreibung für die Plattform Android erstellen und den Typ i3 auswählen.

Sicherstellen, dass der Relution Companion bereits vor der Einschreibung über den i3 Store installiert wurde.

Den Relution Companion öffnen und die Serveradresse sowie den Einschreibungscode eingeben.

Der Companion fordert mehrere Bestätigungen. Die angezeigten Hinweise und Berechtigungsabfragen bestätigen. Nach erfolgreicher Einschreibung erscheint ein entsprechender Bestätigungsbildschirm. Dieser sieht so oder so ähnlich aus.

Für Version 26.4.0



Anschließend den Bildschirmanweisungen folgen, bis die Einschreibung abgeschlossen ist.

Das Gerät sollte nun im Inventar des Relution Portals sichtbar sein.

Device Owner aktivieren

Die Integration benötigt Device-Owner-Berechtigungen auf dem Gerät. Um den Device Owner zu aktivieren, den Anweisungen für Android Debug Bridge Einrichtung und Verbindung → folgen.

Nachdem das Gerät verbunden wurde, den Geräteeigentümer-Modus durch Ausführen des Befehls aktivieren:

```
adb shell dpm set-device-owner
com.mwaysolutions.relution.i3/com.mwaysolutions.relution.receiver.MdmDeviceAdminReceive
r
```

Unterstützte Aktionen

Auf i3-Technologies-Whiteboards können über Relution folgende Aktionen ausgeführt werden:

Für Version 26.4.0

Aktion	Beschreibung
Alarm auslösen →	
App entfernen →	
Datei an Gerät senden →	
Gerät auf Werkszustand zurücksetzen →	
Gerät entsperren →	
Gerät neu starten →	Neustart oder Herunterfahren (Option Ausschalten)
Gerät vollständig sperren →	
Geräteinformationen aktualisieren →	
Nachricht senden →	
Relution Store App bereitstellen →	
Update des Betriebssystems →	

Unterstützte Richtlinien

Folgende Richtlinien werden auf i3-Technologies-Whiteboards unterstützt:

Richtlinie	Einschränkungen
Kiosk-Modus →	
Geplantes OTA-Update →	
Hotspot →	
App Konformität →	

Herstellerspezifische Richtlinie

Für Version 26.4.0

Die herstellerspezifische Richtlinie i3 stellt folgende Einstellungen bereit:

Einstellung	Beschreibung
Automatische Helligkeit einschalten	Helligkeit automatisch regeln
Helligkeit einstellen	Helligkeit auf einen festen Wert setzen. Nach dem Aktivieren wird das Feld Helligkeit (0–100) freigegeben.
Lautstärke einstellen	Lautstärke auf einen festen Wert setzen. Nach dem Aktivieren wird das Feld Lautstärke (0–100) freigegeben.
Sperrbildschirm-PIN aktivieren	PIN für den Sperrbildschirm im Feld Pin für den Sperrbildschirm festlegen (Pflichtfeld, 4–8 Ziffern)
Zeitpläne für das Ein- und Ausschalten	Bis zu 10 Zeitpläne für das automatische Ein- und Ausschalten

Promethean

Mit Relution ist es möglich, interaktive Whiteboards der Marke Promethean zentral zu verwalten.

Unterstützte Produktserien und Modelle

Relution unterstützt folgende Promethean-Produktserien:

- Active Panel 7 und Active Panel 7 Premium
- Active Panel 9 und Active Panel 9 Premium

Einschreibung

Eine Einschreibung für die Plattform Android erstellen und den Typ Promethean auswählen.

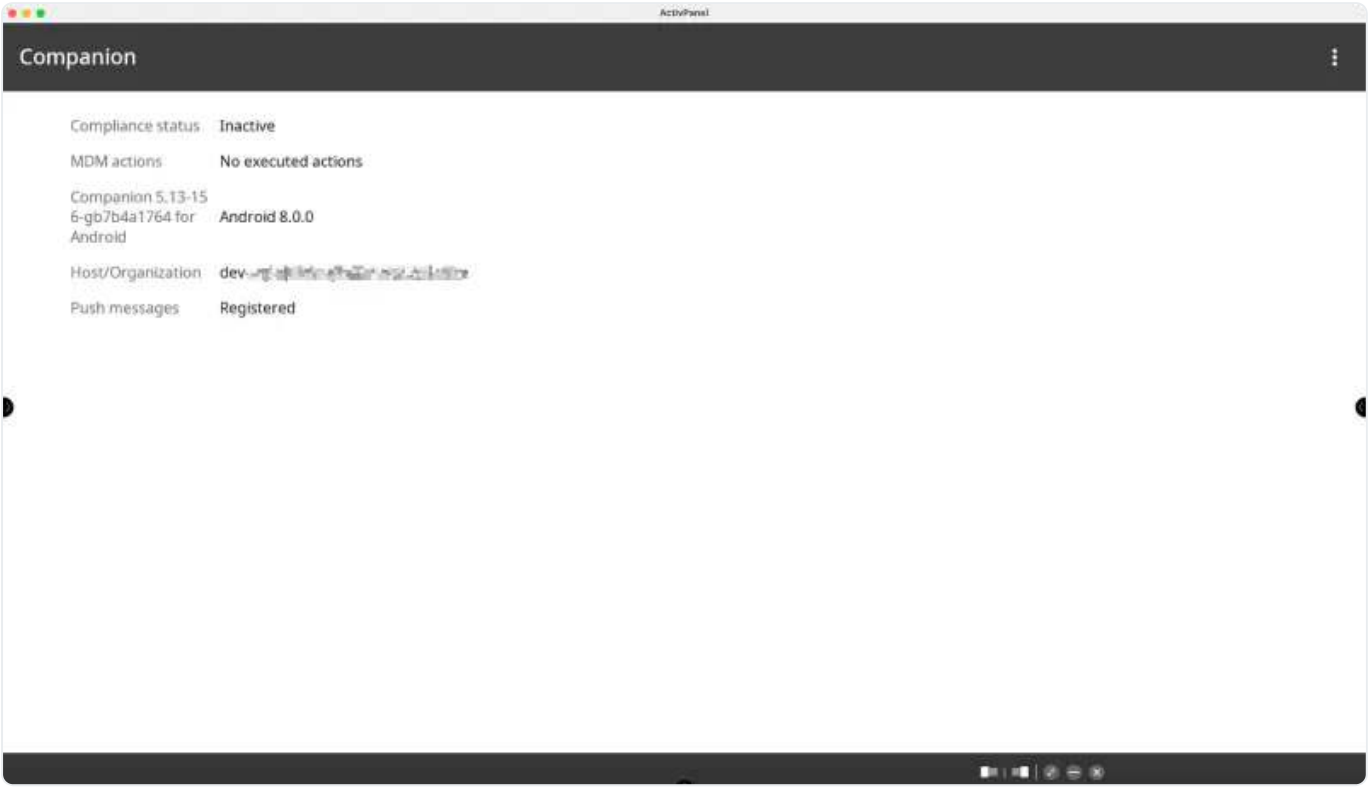
Sicherstellen, dass der Relution Companion bereits vor der Einschreibung über Promethean World installiert wurde.

Falls die Promethean World oder der Relution Companion nicht verfügbar sein sollten, empfiehlt sich eine Kontaktaufnahme mit dem persönlichen Promethean Ansprechpartner.

Den Relution Companion öffnen und die Serveradresse sowie den Einschreibungscode eingeben.

Der Companion fordert mehrere Bestätigungen. Die angezeigten Hinweise und Berechtigungsabfragen bestätigen. Nach erfolgreicher Einschreibung erscheint ein entsprechender Bestätigungsbildschirm. Dieser sieht so oder so ähnlich aus.

Für Version 26.4.0



Anschließend den Bildschirmanweisungen folgen, bis die Einschreibung abgeschlossen ist.

Das Gerät sollte nun im Inventar des Relution Portals sichtbar sein.

Für Version 26.4.0

Unterstützte Aktionen

Auf Promethean-Whiteboards können über Relution folgende Aktionen ausgeführt werden:

Aktion	Beschreibung
Alarm auslösen →	
App entfernen →	
Datei an Gerät senden →	
Gerät auf Werkszustand zurücksetzen →	
Gerät neu starten →	Neustart oder Herunterfahren (Option Ausschalten)
Gerät vollständig sperren →	Setzt eine PIN voraus, die am Gerät oder über die Einstellung ActivPanel Pin der herstellerspezifischen Richtlinie festgelegt ist
Geräteinformationen aktualisieren →	
Nachricht senden →	
Relution Store App bereitstellen →	
Shortcut entfernen →	
Shortcut hinzufügen →	
Update des Betriebssystems →	

Unterstützte Richtlinien

Folgende Richtlinien werden auf Promethean-Whiteboards unterstützt:

Richtlinie	Einschränkungen
Kiosk-Modus →	
WLAN →	
Hotspot →	Nur verfügbar für Active Panel 9 und Active Panel 9 Premium

Herstellerspezifische Richtlinie

Die herstellerspezifische Richtlinie Promethean stellt folgende Einstellungen bereit. Die Reihenfolge entspricht der Anordnung im Portal. Auswahlfelder stehen beim Anlegen auf Nicht ändern; in diesem Fall bleibt der Wert auf dem Whiteboard unverändert.

Für Version 26.4.0

Einstellung	Beschreibung
Helligkeit	Helligkeit auf einen festen Wert zwischen 0 und 100 setzen
Helligkeitsmodus	Mögliche Werte: Nicht ändern, Automatisch, Energieeinsparung, Augenschutz, Normal
Stift Ende	Modus des Stift-Endes festlegen: Stift (Standard) oder Radiergummi
Kontrast	Kontrast auf einen festen Wert zwischen 0 und 100 setzen. Nur verfügbar für Active Panel 7
Zeit, bis das Display in den Standby-Modus wechselt	Automatischer Wechsel in den Standby-Modus nach 3 Minuten bis 4 Stunden
Zeit, bis das Panel in den Ruhemodus wechselt	Automatischer Wechsel in den Ruhemodus nach 3 Minuten bis 8 Stunden
Aktivieren des Näherungssensors	Aufwachen bei Annäherung ein-/ausschalten. Nur verfügbar für Active Panel 7 und Active Panel 9 Premium
Verzögerungstimer für Näherungssensor aktivieren	Verzögerungstimer für Näherungssensor ein-/ausschalten
Verzögerungszeit des Näherungssensors	Mögliche Werte: Nicht ändern, 1 Minute, 5 Minuten, 10 Minuten
Bildschirm „Proximity Illuminate“ aktivieren	Bildschirmbeleuchtung bei Bewegung ein-/ausschalten
Proximity Reset Standby und Sleep-Timer aktivieren	Standby- und Ruhetimer bei Bewegung zurücksetzen
Blaues Licht reduzieren	Blaulichtfilter ein-/ausschalten
Quelle Erkennung	Automatische Quellenerkennung konfigurieren. Mögliche Werte: Nicht ändern, Automatisch, Manuell, Aus
Standard-Quelle	Standard-Quelle festlegen, z. B. die zuletzt genutzte Quelle, Home, HDMI 1–3, AV, DP, OPS, USB-C oder VGA
HDMI EDID-Modus	HDMI EDID-Modus auf EDID 1.4 oder EDID 2.0 setzen
Netzwerkeinstellungen anzeigen	Netzwerkeinstellungen auf dem Gerät ein-/ausblenden
Wake on LAN	Wake on LAN Funktion aktivieren
Aktivieren der Netzwerkerkennung mit AirPlay	AirPlay-Erkennungsprotokoll ein-/ausschalten
Aktivieren der Netzwerkerkennung mit Promethean	Proprietäres Erkennungsprotokoll von Promethean ein-/ausschalten
Aktivieren der Netzwerkerkennung mit WebRTC	WebRTC-Erkennungsprotokoll ein-/ausschalten

Einstellung	Beschreibung
Aktivieren der Netzwerkerkennung über WLAN Direct	Aktivieren/Deaktivieren des WLAN Direct-Erkennungsprotokolls
Miracast über Infrastruktur aktivieren	Miracast über Infrastruktur ein-/ausschalten. Deaktivieren, wenn Aktivieren der Netzwerkerkennung über WLAN Direct ausgeschaltet ist.
IPv6 aktivieren	IPv6 ein-/ausschalten. Auf OPS nicht verfügbar
Lautstärke	Lautstärke auf einen festen Wert zwischen 0 und 100 setzen. Nicht einstellbar, solange Stummschaltung aktivieren eingeschaltet ist
Stummschaltung aktivieren	Lautstärke stummschalten
Panel-Lautsprecher aktivieren	Panel-Lautsprecher ein-/deaktivieren
Eingebaute Lautsprecher aktivieren	Panel-Lautsprecher einbeziehen oder nicht. Nur aktivieren, wenn Line-Out-Modus auf Line-out steht und Panel-Lautsprecher aktivieren aktiviert ist.
Bass	Basspegel zwischen 0 und 100
Balance	Balance zwischen 0 und 100
Klanghöhen	Höhenpegel zwischen 0 und 100
Mitteltöner	Mitteltonpegel zwischen 0 und 100
Line-Out-Modus	Mögliche Werte: Nicht ändern, Kopfhörer, Line-out
Subwoofer aktivieren	Subwoofer ein-/ausschalten. Nur aktivieren, wenn Panel-Lautsprecher aktivieren aktiviert ist.
Panel-Modus	Mögliche Werte: Nicht ändern, Vollbild, Keine Anzeige, Eingeschränktes Display
Aktivieren von Benutzern und Profilen	Verwaltung lokaler Benutzer auf dem Gerät ein-/ausschalten. Nur verfügbar für Active Panel 7
Vereinheitlichtes Menü aktivieren	Vereinheitlichtes Menü (Unified Menu) ein-/ausblenden
Registerkarte „Menü anzeigen“ aktivieren	Registerkarte „Menü“ ein-/ausblenden
Home-Quelle aktivieren	Home-Quelle ein-/ausschalten
Apps freigeben	Nicht-System-Apps im Launcher ein- oder ausblenden
App-Einstellungen anzeigen	App-Einstellungen auf dem Gerät ein-/ausblenden
Installation von Apps aus einer anderen Quelle aktivieren	Installation von Apps aus anderen Quellen (Sideloading) erlauben oder unterbinden
Google Play aktivieren	Google Play auf dem Gerät ein-/ausschalten. Nur verfügbar für Active Panel 7

Einstellung	Beschreibung
Werksreset aktivieren	Zurücksetzen auf Werkseinstellungen am Gerät erlauben oder unterbinden
Einstellungen sperren	Zugriff auf die Einstellungen des Panels und deren Änderung am Gerät verhindern
OTA-Update aktivieren	Firmware-Updates über das Netzwerk (OTA) erlauben oder unterbinden
Lokale Aktualisierung einschalten	Lokale Firmware-Updates erlauben oder unterbinden
Bildschirmfreigabe bei Aktualisierung neu starten	Bei aktivierter Option startet Screen Share neu, sobald sich eine der Netzwerkerkennungen über AirPlay, Promethean oder WebRTC ändert. Andernfalls übernimmt Screen Share die Änderungen beim nächsten Start
ActivPanel Pin anwenden	Aktiviert die Verwaltung der PIN. Nur verfügbar für Active Panel 9 und Active Panel 9 Premium. Bleibt das Feld ActivPanel Pin bei aktivem Schalter leer, wird die PIN auf dem Whiteboard gelöscht
ActivPanel Pin	PIN mit 4 bis 16 Ziffern (nur 0–9). Nur bearbeitbar, wenn ActivPanel Pin anwenden aktiviert ist
Aktivierte Passwörter anzeigen	Anzeige von Passwörtern ein-/ausschalten. Standardmäßig aktiviert
Systemsperre ausblenden	Systemsperre ein-/ausblenden
Die Identität setzt voraus, dass der Benutzer, der sich anmeldet, zu der registrierten Organisation des Panels gehört	

Prowise

Mit Relution ist es möglich, interaktive Whiteboards der Marke Prowise zentral zu verwalten.

Unterstützte Produktserien und Modelle

Relution unterstützt folgende Prowise-Produktserien:

- Touchscreen
- Touchscreen Ultra

Einschreibung

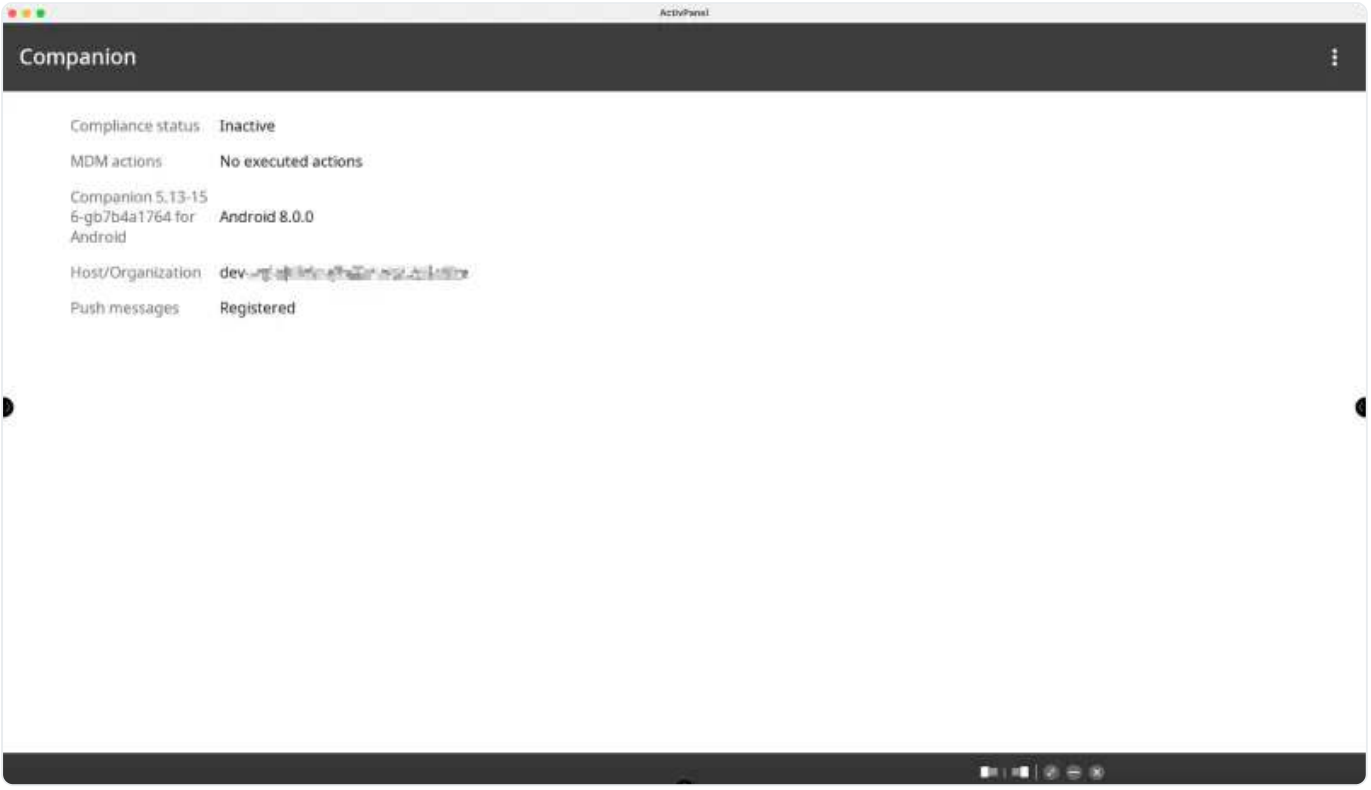
Eine Einschreibung für die Plattform Android erstellen und den Typ Prowise auswählen.

Sicherstellen, dass der Relution Companion bereits vor der Einschreibung über den Prowise Store installiert wurde.

Den Relution Companion öffnen und die Serveradresse sowie den Einschreibungscode eingeben.

Der Companion fordert mehrere Bestätigungen. Die angezeigten Hinweise und Berechtigungsabfragen bestätigen. Nach erfolgreicher Einschreibung erscheint ein entsprechender Bestätigungsbildschirm. Dieser sieht so oder so ähnlich aus.

Für Version 26.4.0



Anschließend den Bildschirmanweisungen folgen, bis die Einschreibung abgeschlossen ist.

Das Gerät sollte nun im Inventar des Relution Portals sichtbar sein.

Für Version 26.4.0

Unterstützte Aktionen

Auf Prowise-Whiteboards können über Relution folgende Aktionen ausgeführt werden:

Aktion	Beschreibung
Alarm auslösen →	
App aus dem Prowise App Store installieren →	
App entfernen →	
Datei an Gerät senden →	
Gerät neu starten →	Neustart oder Herunterfahren (Option Ausschalten)
Gerät vollständig sperren →	Setzt ein Passwort oder eine PIN voraus, die lokal am Gerät oder, falls vorhanden, über die Konfiguration festgelegt ist
Geräteinformationen aktualisieren →	
Nachricht senden →	
Prowise-Update installieren →	

Für Version 26.4.0

Nicht verfügbar sind auf Prowise-Whiteboards unter anderem Gerät auf Werkszustand zurücksetzen, Relution Store App bereitstellen, Update des Betriebssystems sowie das Hinzufügen und Entfernen von Shortcuts. App-Installationen und Updates laufen über die beiden Prowise-Aktionen.

Unterstützte Richtlinien

Folgende Richtlinien werden auf Prowise-Whiteboards unterstützt:

Richtlinie	Einschränkungen
Kiosk-Modus →	
App Konformität →	

Interaktive Whiteboard Konfiguration

Die Richtlinie Interaktive Whiteboard Konfiguration stellt folgende Einstellungen für Prowise-Whiteboards bereit:

Einstellung	Beschreibung
Bildschirmfreigabedienste deaktivieren	Reflect, AirPlay, Chromecast und Miracast deaktivieren. Der Schalter wählt alle vier Dienste aus; einzelne Dienste lassen sich darunter per Kontrollkästchen wieder abwählen
Einstellungen sperren	Sperrt die Einstellungen auf dem Whiteboard. Bei aktivem Schalter ist Pin zum Entsperren der Einstellungen ein Pflichtfeld, das nur Ziffern annimmt
Sperrbildschirm	Nur wählbar, wenn Einstellungen sperren aktiviert ist
USB-Anschlüsse sperren	
Helligkeit	Helligkeit auf einen festen Wert zwischen 0 und 100 setzen (Standard: 100). Der Wert wird mit jeder Konfiguration übertragen
Ausgewählte Apps sperren	Über den Schalter Aus/An wird eine Liste von Apps gesperrt
Eingangskanäle deaktivieren	Liste der Videoeingänge, die auf dem Whiteboard deaktiviert werden

Für Version

SMART

Mit Relution ist es möglich, interaktive Whiteboards der Marke SMART zentral zu verwalten.

Unterstützte Produktserien und Modelle

Relution unterstützt folgende SMART-Produktserien:

- MX (IDX55-4)

Einschreibung

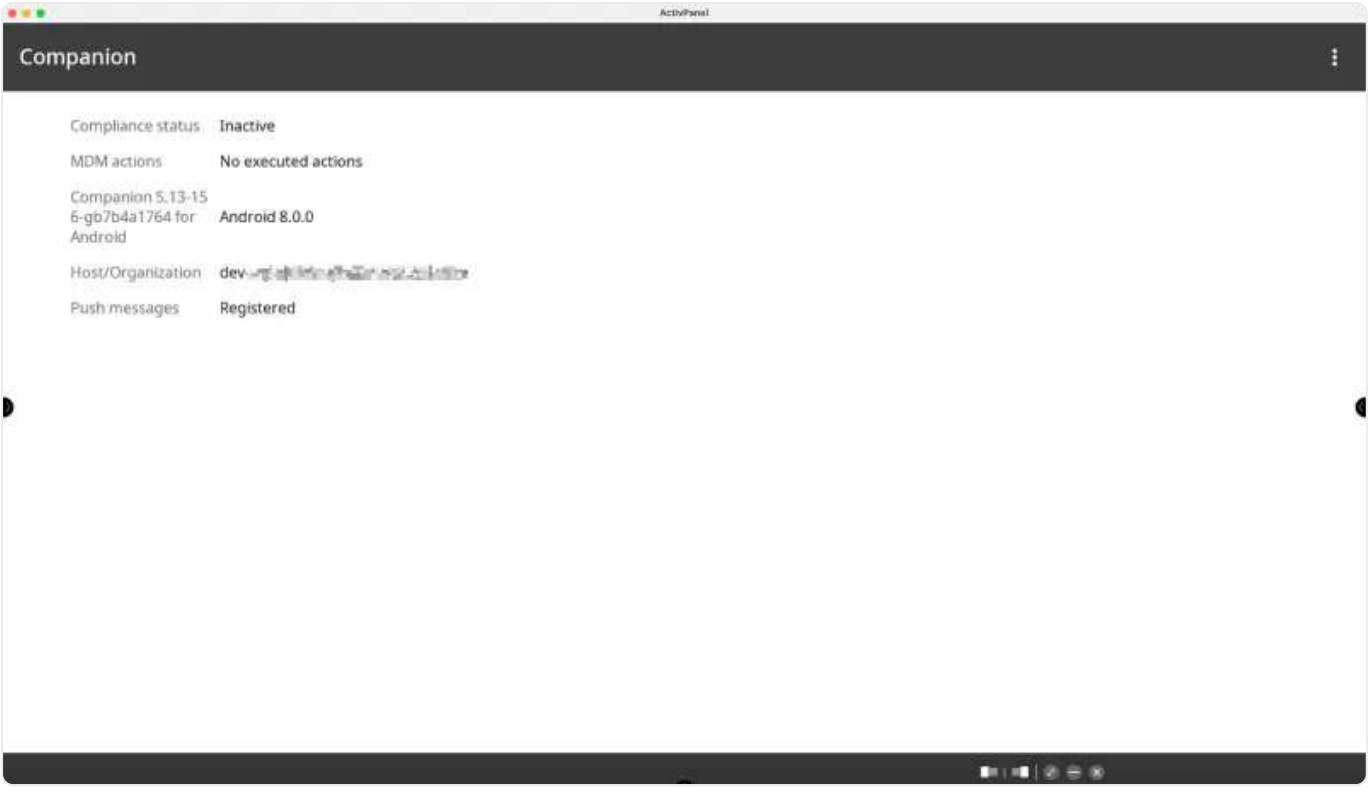
Eine Einschreibung für die Plattform Android erstellen und den Typ SMART auswählen. Den Einschreibelink auf dem Gerät öffnen und den Anweisungen auf der Seite folgen.

Über den angezeigten Download-Button lässt sich der Relution Companion für SMART herunterladen und installieren.

Nach erfolgreicher Installation des Companions zur Einschreibungsseite zurückkehren, um die Einschreibung zu starten.

Der Companion öffnet sich anschließend automatisch und fordert zur Bestätigung mehrerer Hinweise und Berechtigungen auf. Nach erfolgreicher Einschreibung erscheint ein entsprechender Bestätigungsbildschirm. Dieser sieht so oder so ähnlich aus.

Für Version 26.4.0



Anschließend den Bildschirmanweisungen folgen, bis die Einschreibung abgeschlossen ist.

Das Gerät sollte nun im Inventar des Relution Portals sichtbar sein.

Für Version 26.4.0

Unterstützte Aktionen

Auf SMART-Whiteboards können über Relution folgende Aktionen ausgeführt werden:

Aktion	Beschreibung
Alarm auslösen →	
App entfernen →	
Datei an Gerät senden →	
Gerät neu starten →	Neustart oder Herunterfahren (Option Ausschalten)
Geräteinformationen aktualisieren →	
Nachricht senden →	
Relution Store App bereitstellen →	

Unterstützte Richtlinien

Folgende Richtlinien werden auf SMART-Whiteboards unterstützt:

Richtlinie	Einschränkungen
App Konformität →	

Herstellerspezifische Richtlinie

Die herstellerspezifische Richtlinie SMART stellt folgende Einstellungen bereit:

26.4.0

Einstellung	Beschreibung
Boot Quelle	Aktive Quelle nach dem Hochfahren des Displays setzen: Android, AV, DP, HDMI 1–3, USB-C 1–2, PC oder VGA. Standard: Nicht ändern
Automatische Helligkeit einschalten	Automatische Helligkeit ein-/ausschalten
Helligkeit	Helligkeit auf einen festen Wert zwischen 0 und 100 setzen (Standard: 100). Der Wert wird mit jeder Konfiguration übertragen
Zeit, bis das Display in den Standby-Modus wechselt	Automatischer Wechsel in den Standby-Modus nach 1, 5 oder 30 Minuten bzw. 1, 1,5, 2, 5 oder 10 Stunden; alternativ Nie
Stummschalten	Lautstärke stummschalten
Lautstärke	Lautstärke auf einen festen Wert zwischen 0 und 100 setzen (Standard: 33). Der Wert wird mit jeder Konfiguration übertragen
Sprache	Systemsprache: Englisch, Deutsch (Standard) oder Spanisch
App-Store aktivieren	App-Store ein-/ausschalten. Standardmäßig aktiviert
Automatisches Datum und Uhrzeit aktivieren	Automatische Datums- und Zeiteinstellung ein-/ausschalten
Bluetooth einschalten	Bluetooth ein-/ausschalten

ViewSonic

Mit Relution ist es möglich, interaktive Whiteboards der Marke ViewSonic zentral zu verwalten.

Unterstützte Produktserien und Modelle

Relution unterstützt folgende ViewSonic-Produktserien:

- CDExx30
- IFP6550-5
- IFP6552-1ANEP

Einschreibung

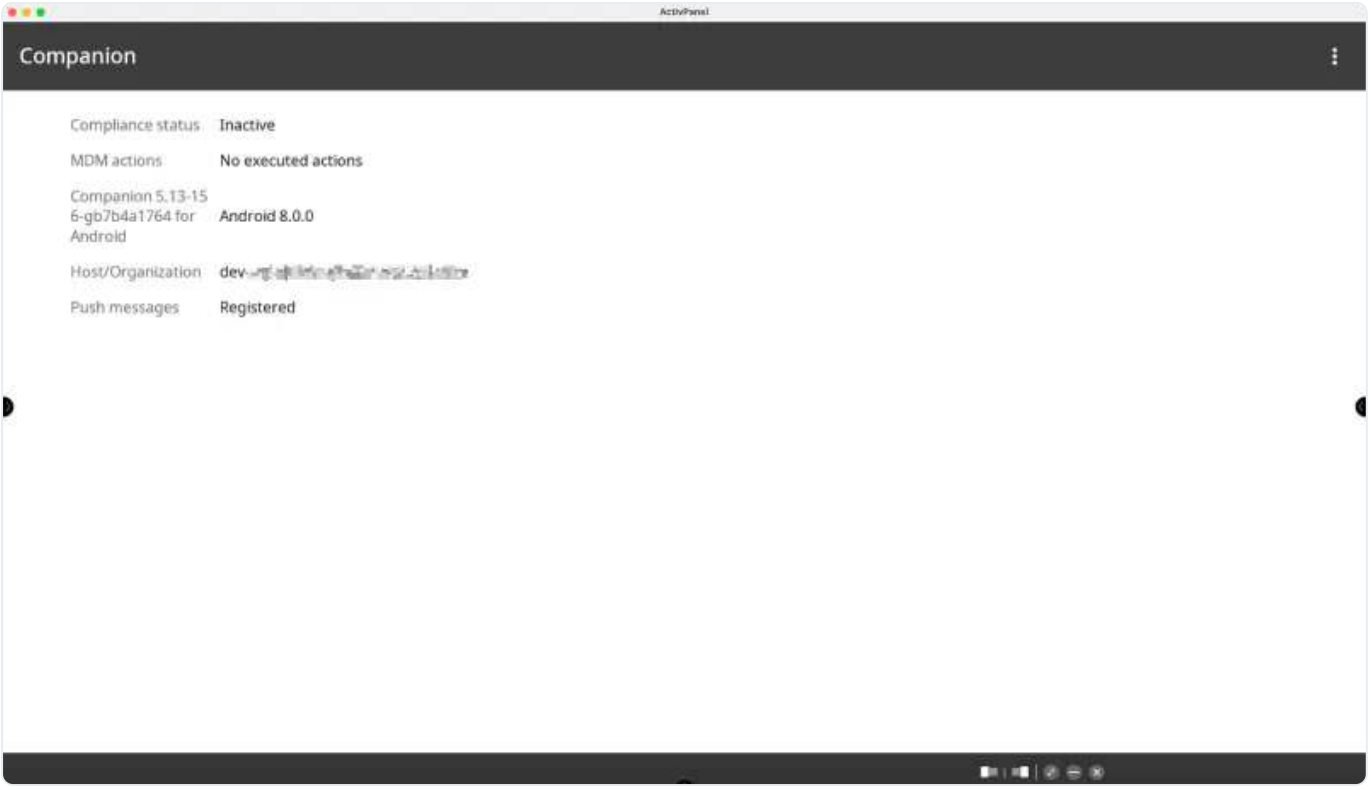
Eine Einschreibung für die Plattform Android erstellen und den Typ ViewSonic selektieren. Den Einschreibelink auf dem Gerät öffnen und den Anweisungen auf der Seite folgen.

Über den angezeigten Download-Button lässt sich der Relution Companion für ViewSonic herunterladen und installieren.

Nach erfolgreicher Installation des Companions zur Einschreibungsseite zurückkehren, um die Einschreibung zu starten.

Der Companion öffnet sich anschließend automatisch und fordert zur Bestätigung mehrerer Hinweise und Berechtigungen auf. Nach erfolgreicher Einschreibung erscheint ein entsprechender Bestätigungsbildschirm. Dieser sieht so oder so ähnlich aus.

Für Version 26.4.0



Anschließend den Bildschirmanweisungen folgen, bis die Einschreibung abgeschlossen ist.

Das Gerät sollte nun im Inventar des Relution Portals sichtbar sein.

Für Version 26.4.0

Unterstützte Aktionen

Auf ViewSonic-Whiteboards können über Relution folgende Aktionen ausgeführt werden:

Aktion	Beschreibung
Alarm auslösen →	
App entfernen →	
Datei an Gerät senden →	
Gerät auf Werkszustand zurücksetzen →	
Gerät neu starten →	Neustart oder Herunterfahren (Option Ausschalten)
Geräteinformationen aktualisieren →	
Nachricht senden →	
Relution Store App bereitstellen →	
Update des Betriebssystems →	

Für Version 26.4.0

Unterstützte Richtlinien

Folgende Richtlinien werden auf ViewSonic-Whiteboards unterstützt:

Richtlinie	Einschränkungen
App Konformität →	

Herstellerspezifische Richtlinie

Die herstellerspezifische Richtlinie ViewSonic stellt folgende Einstellungen bereit:

Einstellung	Beschreibung
Aktuelle Quelle	Aktuelle Quelle setzen: Nicht ändern (Standard), Android, HDMI 1–3, USB-C 1–2 oder VGA
Helligkeit aktivieren	Helligkeit auf einen festen Wert (0–100) setzen (nur CDExx30)
Automatische Hintergrundbeleuchtung	Hintergrundbeleuchtung automatisch regeln (nur IFP6550, IFP6552)
Hintergrundbeleuchtung aktivieren	Hintergrundbeleuchtung auf einen festen Wert (0–100) setzen (nur IFP6550, IFP6552)
Eye Care aktivieren	
Stummschalten	
Lautstärke	Lautstärke auf einen festen Wert (0–100) setzen, Standard 33
Aktivieren des Sperrbildschirm PINs	Sperrbildschirm-PIN aus genau 4 Ziffern setzen (Pflichtfeld bei aktivierter Option)
Menü sperren	
Hardware-Tasten sperren	
Touch-Eingabe sperren	
Einstellungen sperren	Ein Passwort zum Entsperren der Einstellungen setzen (Feld Passwort zum Entsperren der Einstellungen, Pflichtfeld bei aktivierter Option)
Automatisches Datum und Uhrzeit aktivieren	
Zeitzone	
Sprache	
Einschaltzeit setzen	Wochentage und Uhrzeit für das automatische Einschalten des Displays setzen
Ausschaltzeit setzen	Wochentage und Uhrzeit für das automatische Ausschalten des Displays setzen
Eco-Modus	Aktiviert oder deaktiviert den Energiesparmodus des Displays (Aktiviert, Deaktiviert). Bei deaktiviertem Eco-Modus verwendet das Display standardmäßig die Energiespar-Stufe 1.
Energy Star	Energy-Star-Modus des Displays aktivieren oder deaktivieren (Aktiviert, Deaktiviert)
Standby-Modus	Standby-Verhalten des Displays festlegen: Ruhezustand oder Schlafmodus
Standby ohne Signal	Zeit, nach der das Display ohne Eingangssignal in den Standby wechselt: Aus, 5, 15 oder 30 Minuten

Einstellungen, die nur für bestimmte Modelle gelten, sind im Portal mit einem Modell-Badge gekennzeichnet.

Für Eco-Modus, Energy Star, Standby-Modus und Standby ohne Signal ist standardmäßig Nicht ändern ausgewählt. Die jeweilige Einstellung am Display bleibt dann unverändert.

Für Version 26.4.0

VS

Mit Relution ist es möglich, interaktive Whiteboards der Marke VS zentral zu verwalten.

Unterstützte Produktserien und Modelle

Relution unterstützt folgende VS-Produktserien:

- VS-S-E1
- VS-S-E3

Einschreibung

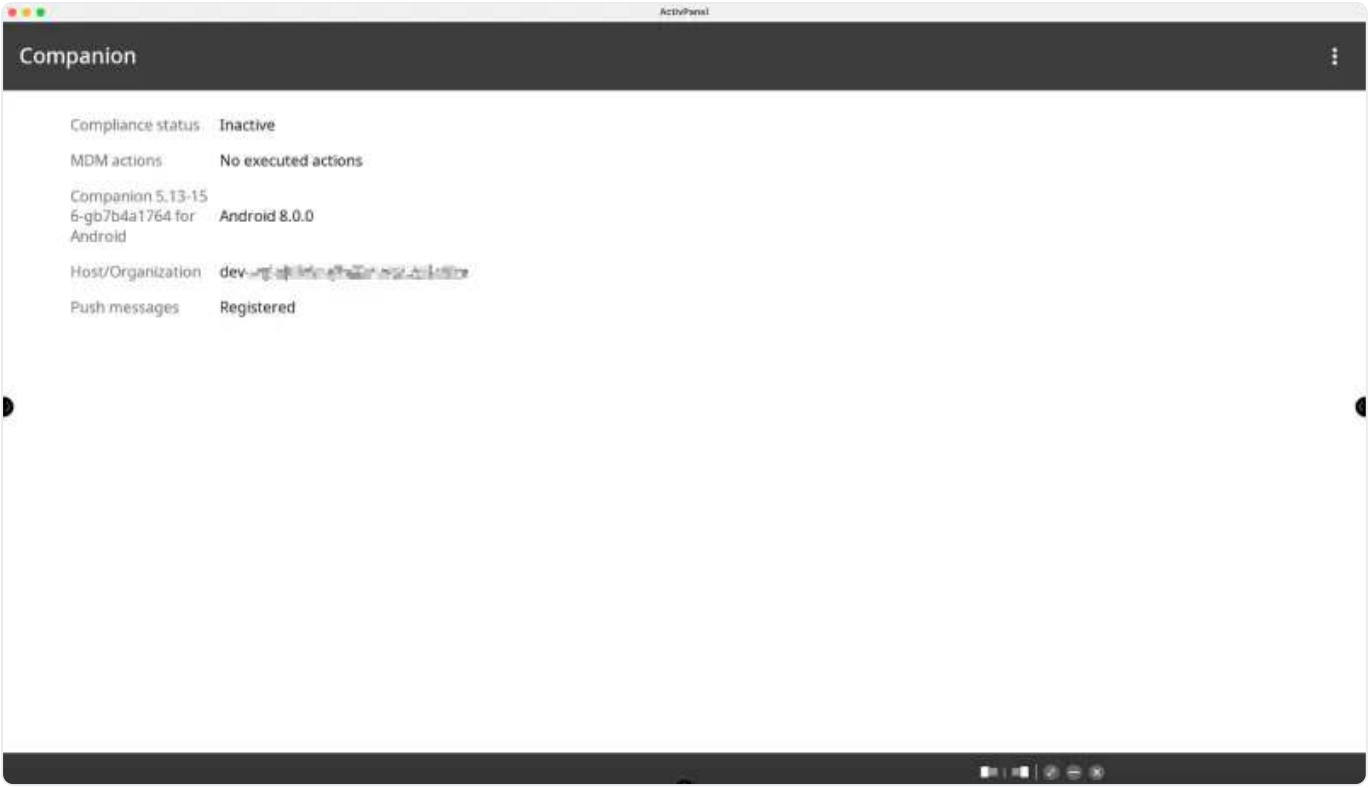
Eine Einschreibung für die Plattform Android erstellen und den Typ VS selektieren. Den Einschreibelink auf dem Gerät öffnen und den Anweisungen auf der Seite folgen.

Über den angezeigten Download-Button lässt sich der Relution Companion für VS herunterladen und installieren.

Nach erfolgreicher Installation des Companions zur Einschreibungsseite zurückkehren, um die Einschreibung zu starten.

Der Companion öffnet sich anschließend automatisch und fordert zur Bestätigung mehrerer Hinweise und Berechtigungen auf. Nach erfolgreicher Einschreibung erscheint ein entsprechender Bestätigungsbildschirm. Dieser sieht so oder so ähnlich aus.

Für Version 26.4.0



Anschließend den Bildschirmanweisungen folgen, bis die Einschreibung abgeschlossen ist.

Das Gerät sollte nun im Inventar des Relution Portals sichtbar sein.

Für Version 26.4.0

Unterstützte Aktionen

Auf VS-Whiteboards können über Relution folgende Aktionen ausgeführt werden:

Aktion	Beschreibung
Alarm auslösen →	
App entfernen →	
Datei an Gerät senden →	
Gerät auf Werkszustand zurücksetzen →	
Gerät neu starten →	Neustart oder Herunterfahren (Option Ausschalten)
Gerät vollständig sperren →	
Geräteinformationen aktualisieren →	
Nachricht senden →	
Relution Store App bereitstellen →	
Update des Betriebssystems →	

Für Version 26.4.0

Unterstützte Richtlinien

Folgende Richtlinien werden auf VS-Whiteboards unterstützt:

Richtlinie	Einschränkungen
App Konformität →	

Herstellerspezifische Richtlinie

Die herstellerspezifische Richtlinie VS stellt folgende Einstellungen bereit:

Einstellung	Beschreibung
Helligkeit	Helligkeit auf einen festen Wert (0–100) setzen, Standard 100
Eye Care aktivieren	
Touch-Eingabe sperren	
Boot-Quelle	Aktive Quelle nach dem Hochfahren des Displays setzen: Nicht ändern (Standard), Android, HDMI 1–3, USB-C 1–2 oder VGA
Aktuelle Quelle	Aktuelle Quelle setzen, Auswahl wie bei Boot-Quelle
Keine Signalabschaltung	Schaltet das Display aus, wenn nach der eingestellten Zeit kein Signal empfangen wird
Kein Signal Ausschaltzeit	Zeit ohne Signal bis zum Ausschalten (1 Minute bis 1 Stunde, Standard 5 Minuten); nur bei aktivierter Option Keine Signalabschaltung
Anschalten, wenn die Quelle angeschlossen wird	Standardmäßig aktiviert
Quellalias zulassen	Nach Aktivierung können Aliase für Android, HDMI1–HDMI4, PC und VGA1 vergeben werden
Ethernet aktivieren	Standardmäßig aktiviert
Wake on LAN	
Stummschalten	
Lautstärke	Lautstärke auf einen festen Wert (0–100) setzen, Standard 33
Aktivieren des Sperrbildschirm PINs	Sperrbildschirm-PIN mit genau 4 Stellen setzen (Pflichtfeld bei aktivierter Option); ein Neustart des Geräts kann erforderlich sein, damit die Änderung wirksam wird
Sprache	Gerätesprache setzen, Standard Deutsch
Automatische OTA-Updates aktivieren	
Installation aus unbekannten Quellen zulassen	Erlaubt die Installation von unbekannten Quellen, einschließlich von USB-Sticks; standardmäßig aktiviert
Einschaltzeit setzen	Wochentage und Uhrzeit für das automatische Einschalten des Displays setzen
Ausschaltzeit setzen	Wochentage und Uhrzeit für das automatische Ausschalten des Displays setzen
Zeit, bis das Display in den Standby-Modus wechselt	Nicht ändern, Nie (Standard), 15 Minuten, 30 Minuten, 1 Stunde, 1,5 Stunden oder 2 Stunden

wende.interaktiv

Mit Relution ist es möglich, interaktive Whiteboards der Marke wende.interaktiv zentral zu verwalten.

Unterstützte Produktserien und Modelle

Relution unterstützt die galneoscreen-Produktserie mit den folgenden Modellen:

- galneoscreen V2
- galneoscreen V3
- galneoscreen V4
- galneoscreen V5

Diese Modelle werden ausschließlich in Kombination mit den folgenden Android-Versionen unterstützt:

- Android 8
- Android 9
- Android 11
- Android 14 (eingeschränkter Funktionsumfang)

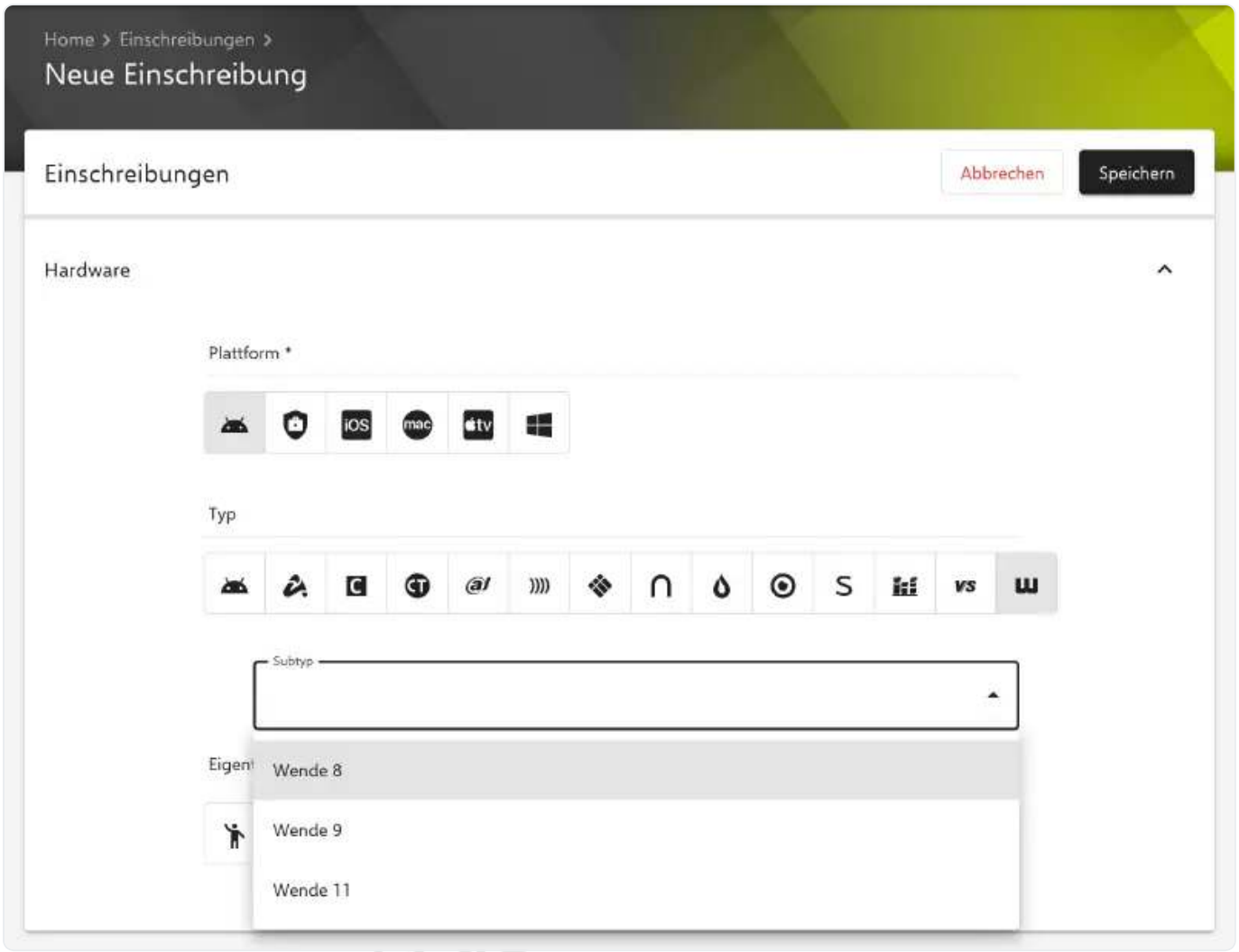
Für Version 26.4.0

Einschreibung erstellen

Eine Einschreibung für die Plattform Android erstellen und den Typ Wende selektieren. Abhängig von der Android-Version des einzuschreibenden Modells anschließend den entsprechenden Subtyp Wende 8, Wende 9 oder Wende 11 auswählen.

Die folgende Tabelle gibt eine Übersicht darüber, welcher Subtyp für welche Android-Version zu verwenden ist:

Android-Version	Einschreibe-Subtyp	Bereitstellung des Relution Companions
Android 8	Wende 8	Relution
Android 9	Wende 9	Relution
Android 11	Wende 11	Relution
Android 14	Wende 11	wende.interaktiv



Whiteboard einschreiben

Für jede Einschreibung wird ein individueller Einschreibelink erzeugt. Den Link auf dem Gerät öffnen und den Anweisungen auf der Seite folgen.

Geräte mit Android-Version 8, 9 oder 11: Für Geräte mit Android Version 8, 9 oder 11 stellt Relution automatisch die passende Companion-Version bereit, basierend auf dem zuvor gewählten Einschreibe-Subtyp.

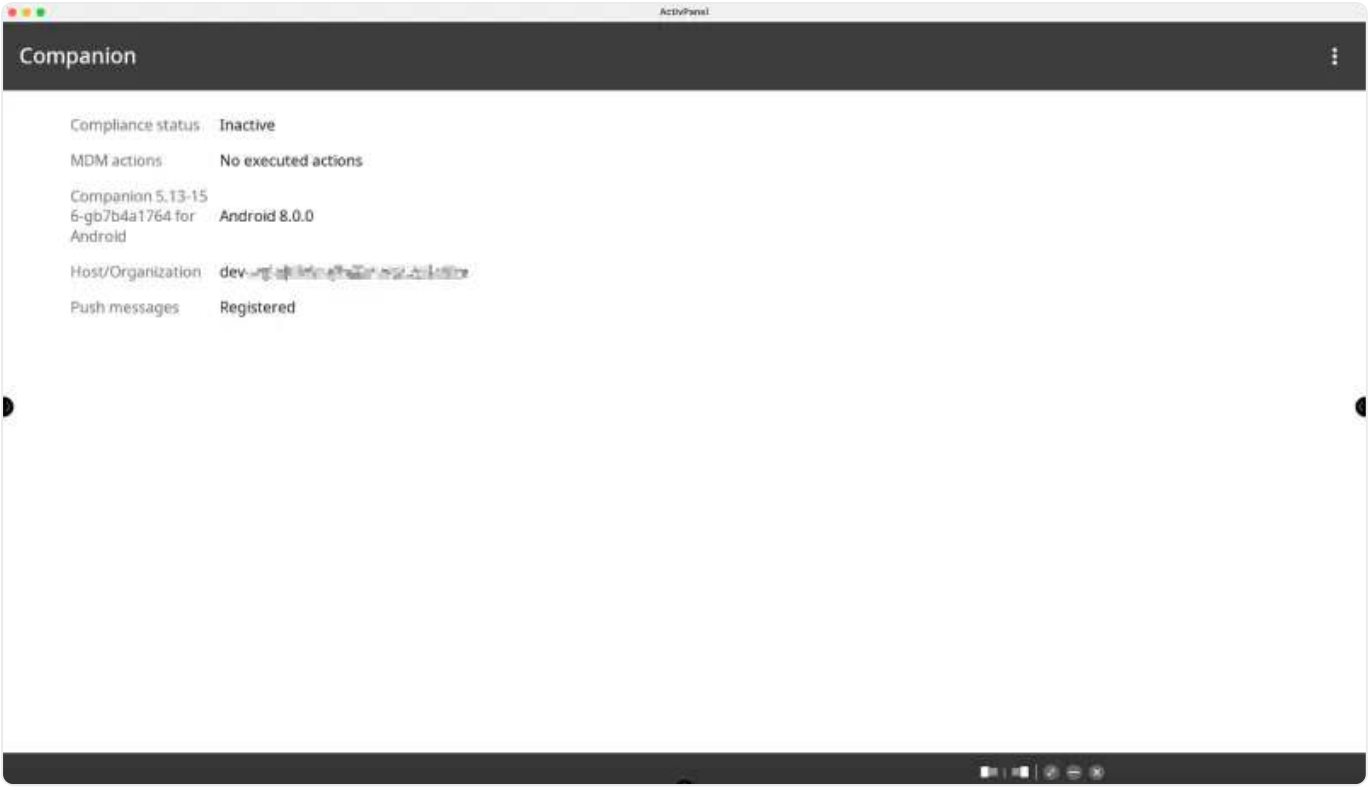
Über den angezeigten Download-Button lässt sich der Relution Companion für das entsprechende Whiteboard-Modell herunterladen und direkt auf dem Gerät installieren.

Geräte mit Android-Version 14: Die Einschreibung von Geräten mit Android 14 erfordert die Installation einer speziellen Version des Relution Companion für Wende 11.

> Diese Version muss unbedingt vor der Einschreibung aktiv bei wende.interaktiv angefordert werden.

Nach erfolgreicher Installation des Companions zur Einschreibeseite zurückkehren, um den Einschreibevorgang zu starten.

Der Relution Companion startet im Anschluss automatisch und fordert zur Bestätigung mehrerer Hinweise und Berechtigungen auf. Nach erfolgreicher Einschreibung erscheint ein entsprechender Bestätigungsbildschirm. Dieser sieht so oder so ähnlich aus.



Anschließend den weiteren Bildschirmanweisungen folgen, bis die Einschreibung abgeschlossen ist.

Das Gerät erscheint danach automatisch im Inventar des Relution Portals.

Für Version 26.4.0

Update des Relution Companions

Der Relution Companion wird je nach Einschreibetyp und Android-Version entweder automatisch über Relution aktualisiert oder benötigt ein manuelles Update, das bei wende.interaktiv angefordert werden kann. Die folgende Übersicht zeigt, ob ein Update automatisch erfolgt oder manuell durchgeführt werden muss.

Einschreibe-Subtyp	Android-Version	Update-Typ
Wende 8	Android 8	Automatisch
Wende 9	Android 9	Automatisch
Wende 11	Android 11	Automatisch
Wende 11	Android 14	Manuell (bereitgestellt durch wende.interaktiv)

Welche Companion-Version Relution aktuell für Wende 8, Wende 9 und Wende 11 bereitstellt, ist unter `Einstellungen` → `Relution Client Apps` → `Wende companion` einsehbar.

Unterstützte Aktionen

Auf wende.interaktiv-Whiteboards können über Relution folgende Aktionen ausgeführt werden:

Aktion	Beschreibung
Alarm auslösen →	
App entfernen →	
Datei an Gerät senden →	
Gerät auf Werkszustand zurücksetzen →	
Gerät neu starten →	Neustart oder Herunterfahren (Option Ausschalten)
Gerät orten	
Gerät vollständig sperren →	
Geräteinformationen aktualisieren →	
Nachricht senden →	
Relution Store App bereitstellen →	
Shortcut hinzufügen →	Verfügbar auf Wende 8 und Wende 9
Update des Betriebssystems →	

Unterstützte Richtlinien

Folgende Richtlinien werden auf wende.interaktiv-Whiteboards unterstützt:

Richtlinie	Einschränkungen
Kiosk-Modus →	Verfügbar auf Wende 11
EShare →	
App Konformität →	

Interaktive Whiteboard-Konfiguration

Mit der Richtlinie Interaktive Whiteboard Konfiguration können folgende Einstellungen für wende.interaktiv-Whiteboards zentral bereitgestellt werden:

Einstellung	Beschreibung
Hardware-Tasten sperren	
Fernbedienung sperren	
Einstellungen sperren	Eine PIN (nur Ziffern) zum Entsperren der Einstellungen setzen (Feld Pin zum Entsperren der Einstellungen, Pflichtfeld bei aktivierter Option)
Touch-Eingabe sperren	
Helligkeit	Helligkeit auf einen festen Wert setzen
Einschaltzeit setzen	Wochentage und Uhrzeit für das automatische Einschalten des Displays setzen
Ausschaltzeit setzen	Wochentage und Uhrzeit für das automatische Ausschalten des Displays setzen
Ausgewählte Apps sperren	

Update des Betriebssystems

Die Aktion Update installieren (Dialogtitel Update des Betriebssystems) ermöglicht es, ein bestimmtes Softwareupdate auf einem ausgewählten Gerät zu installieren.

Die Aktion steht für Android Classic Whiteboards aller Hersteller außer CTOUCH, Newline, Prowise und SMART zur Verfügung. Für Prowise-Whiteboards gibt es stattdessen die Aktion Prowise-Update installieren →.

Im Dialog wird lediglich die Version in der Liste Folgende Updates sind für dieses Gerät verfügbar: ausgewählt. Es können nur Updates ausgewählt werden, die vom Gerät selbst als verfügbar gemeldet wurden. Meldet das Gerät keine Updates, bleibt die Liste leer und die Aktion kann nicht ausgeführt werden.

Sind Konfigurationen aktiv, die Betriebssystem-Updates verzögern, installiert das Gerät die neueste für es verfügbare Version. Diese kann älter sein als die ausgewählte Version. Ist ein Sperrcode aktiviert, muss dieser vor dem Start eingegeben werden.

Gerät entsperren

Die Aktion Gerät entsperren (im Portal: Entsperre Gerät) ermöglicht es, das Gerät aus der Ferne zu entsperren, ohne eine PIN einzugeben. Sie hebt typischerweise eine Sperre durch die Aktion Gerät vollständig sperren → auf.

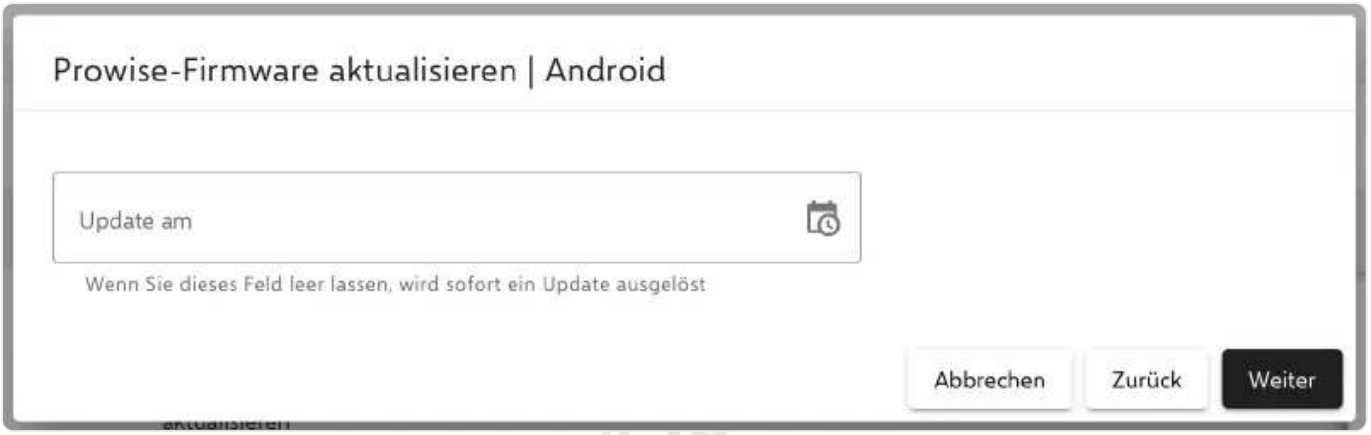
Die Aktion steht nur für Whiteboards von CTOUCH, i3-Technologies und Newline zur Verfügung. Alle anderen Geräte werden am Gerät selbst mit dem Passwort entsperrt.

Prowise-Update installieren

Die Aktion Prowise-Update installieren (Dialogtitel Prowise-Firmware aktualisieren) ermöglicht es, das neueste verfügbare Update auf einem ausgewählten Prowise-Whiteboard → zu installieren. Die Aktion steht nur für Prowise-Whiteboards zur Verfügung und ersetzt dort die Aktion Update installieren.

Optional lassen sich im Feld Update am ein Datum und eine Uhrzeit für das Update auswählen. Bleibt das Feld leer, wird das Update sofort ausgelöst.

Wird die Aktion erneut gesendet, solange eine frühere Aktion dieses Typs noch nicht an das Gerät zugestellt ist, wird die frühere Aktion abgebrochen. Die Aktion lässt sich außerdem als Aktion einer Gerätegruppe hinterlegen.



Für Versi

App aus dem Prowise App Store installieren

Die Aktion App aus dem Prowise App Store installieren installiert eine App aus dem Prowise App Store auf einem Prowise-Whiteboard →. Die Aktion steht nur für Prowise-Whiteboards zur Verfügung und ersetzt dort die Aktion Relution Store App bereitstellen.

Die App wird über ihren Paketnamen bestimmt. Im ersten Schritt wird die Quelle gewählt, im zweiten Schritt genau eine App:

- Relution App Store App: Auswahl einer nativen Android-App aus dem Relution App Store.
- Google Play Store App: Suche im öffentlichen Google Play Store.
- Interner Name einer App: manuelle Eingabe des Paketnamens im Feld Interner Name.

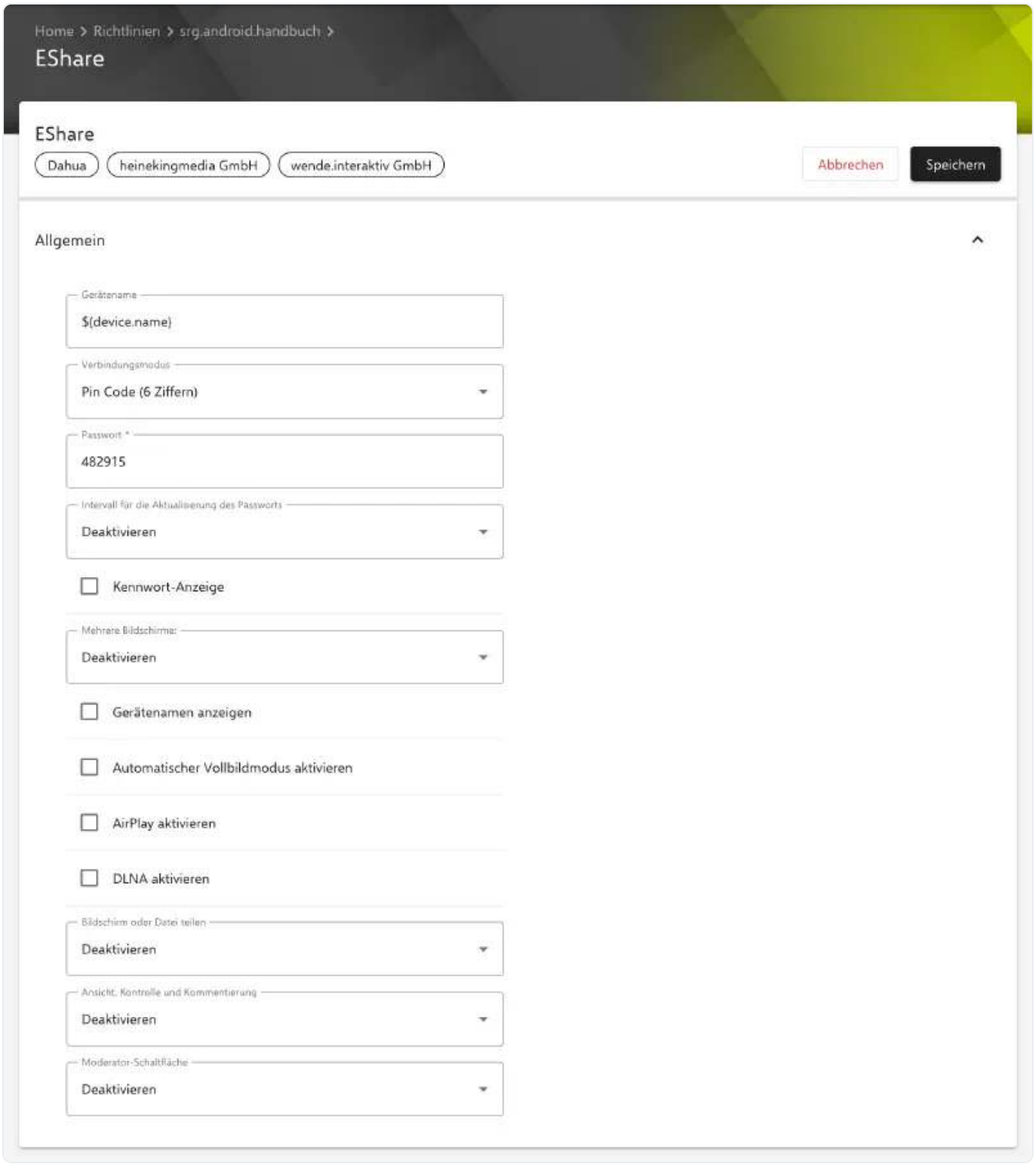
Relution übergibt nur den Paketnamen an den Relution Companion auf dem Whiteboard. Das Whiteboard installiert dann die passende App aus dem Prowise App Store, sofern sie dort verfügbar ist. Ist die App im Prowise App Store nicht vorhanden, wird sie nicht installiert.

EShare

EShare ist eine plattformübergreifende Software für die drahtlose Bildschirmübertragung und Zusammenarbeit zwischen verschiedenen Geräten. Sie ermöglicht unter anderem Bildschirmspiegelung, Dateiübertragung und Fernsteuerung.

Die Richtlinie EShare ermöglicht es, die Einstellungen für EShare auf Whiteboards zu konfigurieren und zu verwalten. Im Portal ist sie für Whiteboards von Dahua →, heinekingmedia → und wende.interaktiv → gekennzeichnet.

Für Version 26.4.0



Konfiguration

Die folgenden Optionen stehen zur Konfiguration von EShare zur Verfügung:

- Gerätename: Den Namen des Geräts festlegen. Vorbelegt ist der Platzhalter `${device.name}`, sodass ohne Änderung der Gerätename aus Relution verwendet wird.
- Verbindungsmodus: Gerätename, Pin Code (6 Ziffern) oder Buchstaben (8 Zeichen) wählen. Bei Pin Code (6 Ziffern) und Buchstaben (8 Zeichen) stehen zusätzlich zur Verfügung:
  - Passwort: Pflichtfeld; ohne Passwort lässt sich die Konfiguration nicht speichern.
  - Intervall für die Aktualisierung des Passworts: Deaktivieren, 10 Minuten, 30 Minuten, 1 Stunde oder 1 Tag.
  - Kennwort-Anzeige
- Mehrere Bildschirme: Deaktivieren oder 2, 4, 6 bzw. 9 Bildschirme auswählen.
- Gerätenamen anzeigen: Die Anzeige des Gerätenamens aktivieren/deaktivieren.
- Automatischen Vollbildmodus aktivieren
- AirPlay aktivieren
- DLNA aktivieren
- Bildschirm oder Datei teilen: Bildschirm- oder Dateifreigabe deaktivieren, alle Optionen zulassen oder nur mit Genehmigung zulassen.
- Ansicht, Kontrolle und Kommentierung: Alle Optionen deaktivieren, alle erlauben, nur Ansicht oder nur mit Genehmigung zulassen.
- Moderator-Schaltfläche: Anzeigeoption wählen: Deaktivieren, immer anzeigen, nur auf dem Startbildschirm oder automatisch.

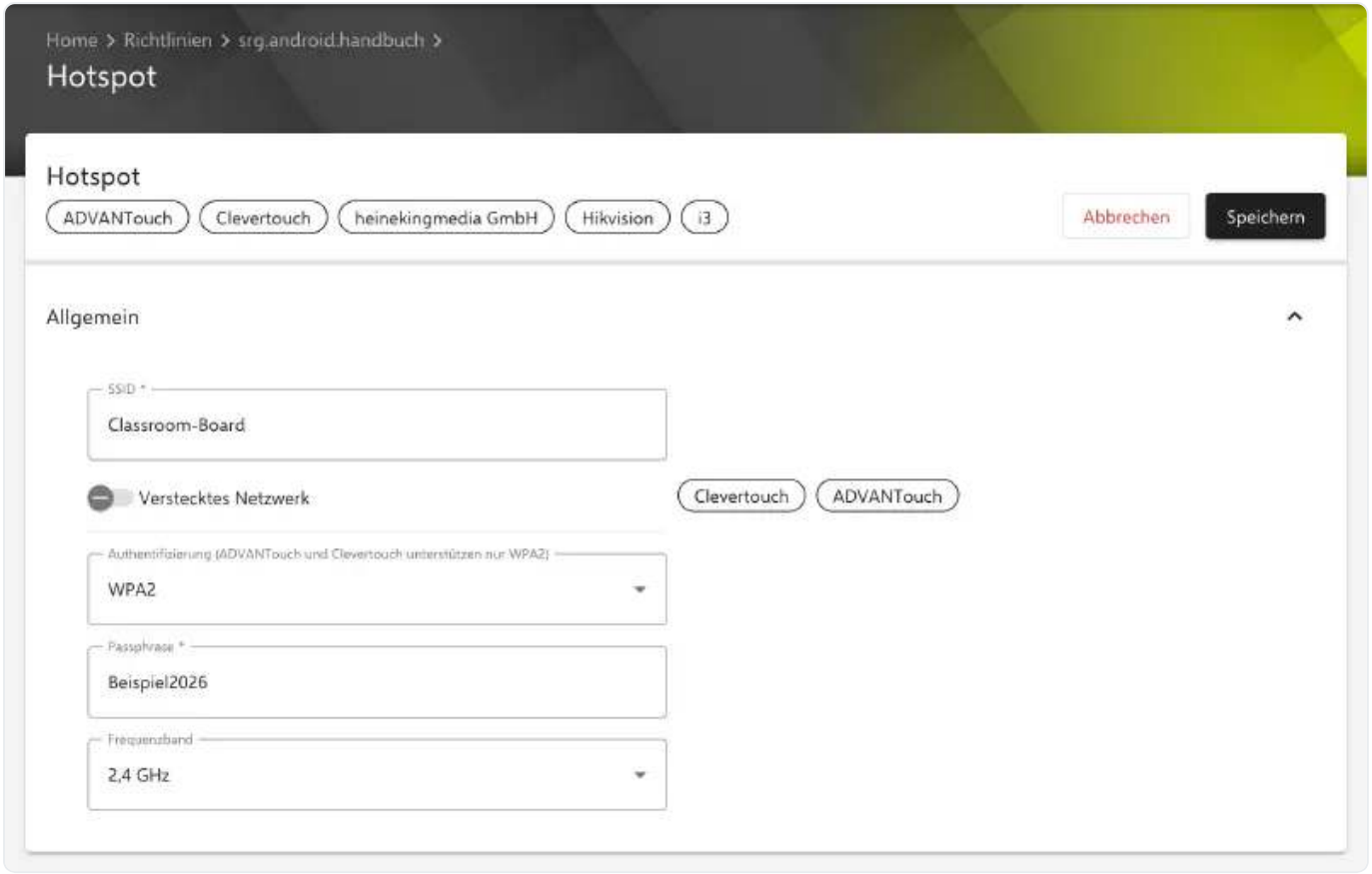
Bei einer neuen Konfiguration ist der Verbindungsmodus Gerätename voreingestellt, alle Kontrollkästchen sind deaktiviert, und Mehrere Bildschirme, Bildschirm oder Datei teilen, Ansicht, Kontrolle und Kommentierung sowie Moderator-Schaltfläche stehen auf Deaktivieren.

Lässt sich die Konfiguration auf dem Gerät nicht anwenden, wird für das Gerät der Compliance-Verstoß EShare-Konfiguration angezeigt.

Für Version 26.4.0

Hotspot

Die Richtlinie Hotspot ermöglicht es, die Einstellungen für WLAN-Hotspots auf Geräten remote zu konfigurieren und zu verwalten. Im Portal ist sie für Whiteboards von ADVANTouch →, Clevertouch →, heinekingmedia →, i3-Technologies → und Hikvision gekennzeichnet.



Konfiguration

Die folgenden Optionen stehen zur Konfiguration des WLAN-Hotspots zur Verfügung:

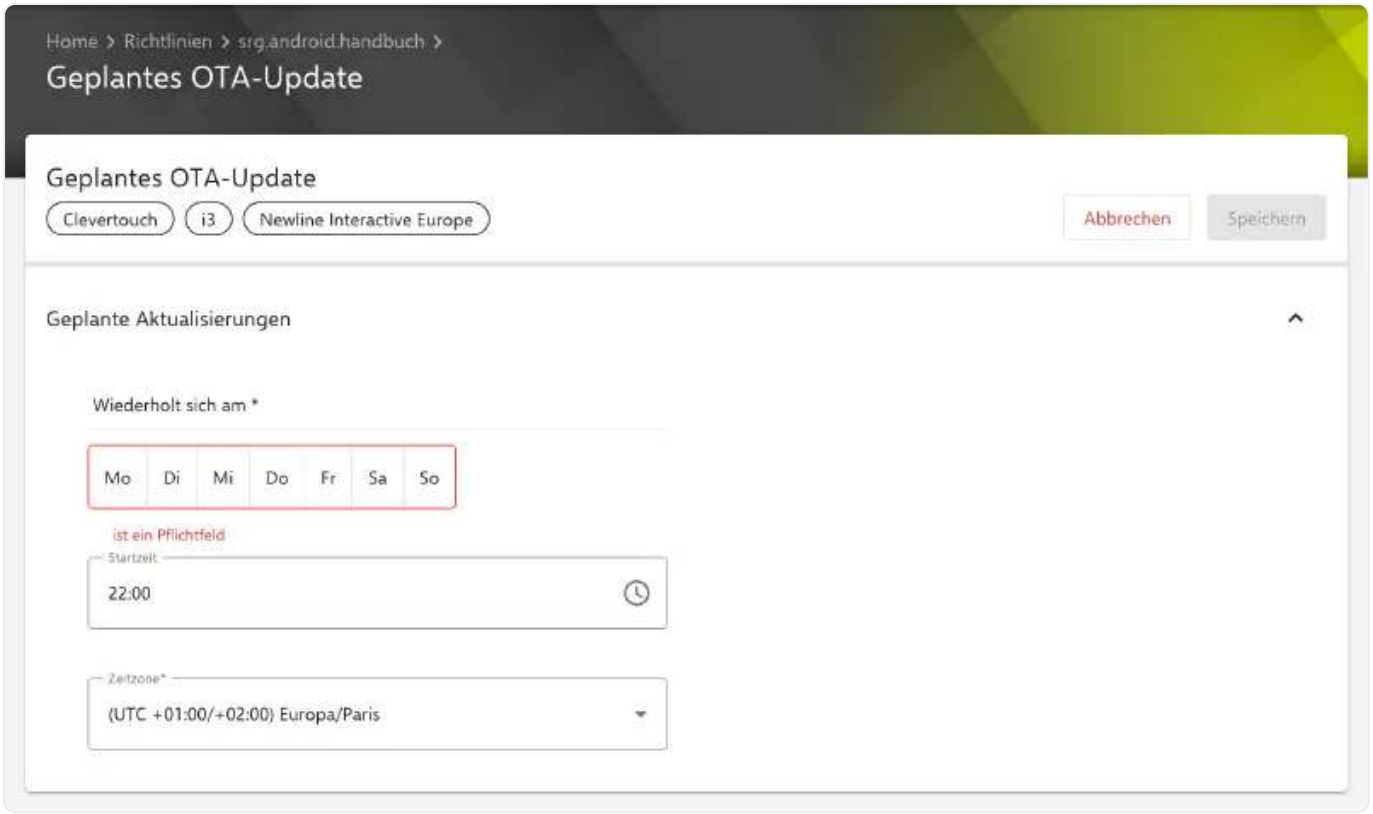
- SSID: Der sichtbare Name des WLAN-Hotspots zur Identifikation durch andere Geräte (Pflichtfeld).
- Verstecktes Netzwerk: Deaktiviert die sichtbare Übertragung der SSID, sodass der Hotspot nicht in der Liste der verfügbaren Netzwerke angezeigt wird. Die Option ist im Portal nur für Clevertouch und ADVANTouch gekennzeichnet und standardmäßig deaktiviert.
- Authentifizierung: Keine (offenes Netzwerk) oder WPA2 (Standard). ADVANTouch und Clevertouch unterstützen nur WPA2.
- Passphrase: Passwort für den Zugriff auf den Hotspot. Das Feld erscheint nur bei WPA2, ist dann ein Pflichtfeld und muss 8 bis 63 Zeichen lang sein.
- Frequenzband: Funkbereich des Hotspots, 2,4 GHz (Standard) oder 5 GHz.

Lässt sich die Konfiguration auf dem Gerät nicht anwenden, wird für das Gerät der Compliance-Verstoß Hotspot-Konfiguration angezeigt.

Geplantes OTA-Update

Die Richtlinie Geplantes OTA-Update ermöglicht es, Firmware-Updates auf interaktiven Whiteboards außerhalb der Nutzungszeiten automatisch durchzuführen.

Die Konfiguration wird für Whiteboards von Clevertouch →, i3-Technologies → und Newline unterstützt. Je Richtlinie ist eine Konfiguration dieses Typs möglich.



Funktionsweise

Im Abschnitt Geplante Aktualisierungen wird der Beginn des Update-Fensters festgelegt:

- Wiederholt sich am: Wochentage, an denen das Update-Fenster beginnt (Mehrfachauswahl, mindestens ein Tag erforderlich). Bei einer neuen Konfiguration ist kein Tag vorausgewählt.
- Startzeit: Uhrzeit, zu der das Update-Fenster an den gewählten Tagen beginnt (Standard 22:00). Die Startzeit gilt für alle gewählten Wochentage.
- Zeitzone: Zeitzone, in der die Startzeit gilt (Standard Europa/Paris). Maßgeblich ist diese Zeitzone, nicht die Ortszeit des Geräts; bei Standorten in mehreren Zeitzonen ist das zu berücksichtigen.

Zum festgelegten Zeitpunkt prüft der Relution Companion, ob ein Firmware-Update für das Gerät verfügbar ist. Ist ein Update verfügbar, wird es automatisch und ohne Benutzerinteraktion installiert.

Wann werden keine Updates installiert?

Firmware-Updates werden nicht installiert, wenn das Gerät zur geplanten Uhrzeit ausgeschaltet ist. Wird das Gerät beispielsweise erst am nächsten Morgen eingeschaltet und wurde das Update-Fenster verpasst, wartet der Relution Companion bis zum nächsten definierten Zeitfenster, um das Update durchzuführen. So wird sichergestellt, dass Updates ausschließlich zu den vorgesehenen Zeiten erfolgen.

Für Version 26.4.0

Device Owner (Companion)

Mit der Funktion Device Owner für den Relution Companion gibt es die Möglichkeiten zur erweiterten Verwaltung von Android-Geräten. Dazu gehören folgende Funktionen:

- Apps ohne Benutzerinteraktion installieren und deaktivieren (Richtlinien-Konfiguration App Konformität →).
- Kiosk-Modus ohne Benutzerinteraktion aktivieren (Richtlinien-Konfiguration Kiosk-Modus →).
- Aktion Gerät neu starten →.

Anleitungen zur Android Debug Bridge Einrichtung und Verbindung sind hier zu finden: Android Debug Bridge Einrichtung →

Relution Companion herunterladen

Relution Companion →

Relution Companion App auf dem Gerät installieren

Das kann entweder manuell oder über die Android Debug Bridge (ADB) gemacht werden.

rsion 26.4.0

```
adb install Relution-normal-release.apk
```

Device Owner nach der Installation aktivieren

```
adb shell dpm set-device-owner
com.mwaysolutions.relution/com.mwaysolutions.relution.receiver.MdmDeviceAdminReceiver
```

Der Befehl gilt für den allgemeinen Relution Companion mit dem Paketnamen `com.mwaysolutions.relution`. Herstellerspezifische Companion-Varianten tragen einen eigenen Paketnamen (z. B. `com.mwaysolutions.relution.i3` oder `com.mwaysolutions.relution.advantouch`); der passende Befehl steht dann im jeweiligen Herstellerartikel, etwa i3-Technologies → oder ADVANTouch →.

Gerät neu einschreiben

Anschließend wird das Gerät in Relution neu eingeschrieben. Dazu wird eine Einschreibung für die Plattform Android mit dem Typ des jeweiligen Herstellers erstellt und auf dem Gerät im Relution Companion verwendet. Das Vorgehen ist im Abschnitt zur Einschreibung des jeweiligen Herstellerartikels beschrieben, siehe Hersteller →.

Für Version 26.4.0

Android Debug Bridge Einrichtung

Entwickleroptionen auf dem Gerät aktivieren

Es ist möglich, dass die Freischaltung der Entwickleroptionen beim Hersteller angefordert werden muss.

- Einstellungen öffnen.
- Info zum Gerät öffnen (kann je nach Hersteller variieren).
- 7x auf Buildnummer tippen (aktiviert die Entwickler-Optionen).
- Einen Schritt zurück und in die Entwickler-Optionen wechseln.
- Die Option USB Debugging suchen und aktivieren.

Enthält die dem Gerät zugewiesene Richtlinie die Konfiguration Restriktionen → mit aktivierter Option USB Debugging verbieten (bei neuen Konfigurationen voreingestellt), kann USB-Debugging auf dem Gerät gesperrt sein.

Android Debug Bridge (ADB) laden und installieren

Mac →
Windows →
Linux →

Für Version 26.4.0

Android Debug Bridge (ADB) starten

```
adb start-server
```

Mit dem Gerät verbinden

```
adb connect <IP-Adresse>
```

Etwaige Vertrauensmeldung bestätigen, die das Gerät anzeigt.

EDLA Geräte einschreiben

Mit Relution ist es möglich, interaktive Whiteboards die EDLA zertifiziert sind über Android Enterprise zu verwalten.

Einschreibung

Das Gerät wird als vollverwaltetes Android Enterprise Gerät → eingeschrieben. Als Einschreibevariante dient die Variante mittels DPC-Identifier →.

> Ab Relution 5.33 lässt sich bei der Einschreibung festlegen, ob nicht wesentliche vorinstallierte System-Apps während der Einrichtung deaktiviert werden oder aktiviert bleiben. Hierfür gibt es beim Anlegen der Einschreibung unter Einschreibungsoptionen im Abschnitt Compliance den Schalter System-Apps aktiviert lassen. Er ist standardmäßig deaktiviert. Für die Einschreibung von Whiteboards muss der Schalter aktiviert werden.

Relution übernimmt den Schalter ausschließlich in den QR-Code der Einschreibung. Der DPC-Identifier enthält ihn nicht; bei der Einschreibung per DPC-Identifier hat der Schalter daher keine Wirkung, siehe Optionen der Einschreibung →. Vorinstallierte Apps, die nach der Einschreibung deaktiviert sind, lassen sich nachträglich freigeben, siehe Vorinstallierte Apps →.

EDLA Erweiterungen

Für Version 26.4.0

Für bestimmte interaktive Whiteboards stehen Erweiterungen zur Verfügung, die den allgemeinen Funktionsumfang durch whiteboard-spezifische Funktionen ergänzen. Einen Überblick gibt EDLA Erweiterungen →.

Hardware-Plattform CVTE

Mit Relution ist es möglich, interaktive Whiteboards der Hardware-Plattform CVTE zentral zu verwalten.

Unterstützte Produktserien und Modelle der Basiskonfiguration

Relution unterstützt folgende Hersteller und Produktserien:

- Heinekingmedia DT-75-C10HM

Unterstützte Produktserien und Modelle mit Bytello Share

Die folgenden Hersteller und Produktreihen unterstützen die Konfiguration von Bytello Share Screensharing-Diensten:

- Heinekingmedia DT-75-C10HM

Für Version 26.4.0

Einschreibung

Die Einschreibung erfolgt wie unter EDLA Geräte einschreiben → beschrieben.

Unterstützte Aktionen

Es stehen die Android Enterprise Aktionen → zur Verfügung, einschließlich Gerät herunterfahren. Diese Aktion fährt das Whiteboard vollständig herunter. Bei Android Enterprise wird sie nur von bestimmten Whiteboards unterstützt; das Portal kennzeichnet sie mit den unterstützten Herstellern, darunter heinekingmedia (HKM).

Unterstützte Richtlinien

Neben der Konfiguration CVTE OEM-Konfiguration werden alle Android-Enterprise-Konfigurationen unterstützt.

Relution CVTE OEMConfig App

Um die Zusatzfunktionen der Whiteboards über Android Enterprise bereitzustellen, muss die Relution CVTE OEMConfig App auf dem Gerät installiert und konfiguriert sein.

Konfiguration

Eine Richtlinie mit einer CVTE OEM-Konfiguration erstellen, um die Relution CVTE OEMConfig App zu konfigurieren.

Die Konfiguration installiert die Relution CVTE OEMConfig App mit dem Installationstyp Installation erzwungen auf dem Gerät, aktualisiert sie mit hoher Priorität und erteilt ihr die benötigten Berechtigungen. Benutzer können die App nicht entfernen. Eine separate Verteilung über die Konfiguration Apps verwalten ist nicht erforderlich und auch nicht möglich: Ist die App dort eingetragen, lässt sich die Konfiguration nicht speichern, und das Portal verweist auf die CVTE OEM-Konfiguration.

In den Werten der Konfiguration können Platzhalter verwendet werden; das Formular zeigt die verfügbaren Platzhalter an.

Die App meldet außerdem zusätzliche Geräteinformationen an Relution, etwa IP- und MAC-Adresse, Firmware- und Systemversion sowie den Status von Ethernet, Hotspot und Wake-on-LAN.

Konfiguration der Bytello Share Screensharing-Dienste

Die folgenden Apps zur Konfiguration Apps verwalten → hinzufügen:

Version 26.4.0

Name	Interner Name	Installationstyp
ScreensharePro	com.seewo.screensharepro.server	Vorinstalliert
Bytello ScreensharePro	com.bytello.screensharepro.server	Vorinstalliert

Einstellungsmöglichkeiten

Die Relution CVTE OEMConfig App bietet folgende Einstellungen:

Einstellung	Beschreibung
Lautstärke	Systemlautstärke einstellen (0-100)
Stummschalten	Audioausgang stummschalten aktivieren/deaktivieren
Soundmodus	Auswählen zwischen Standard, Film, Unterricht, Meeting, Benutzerdefiniert
Audio-Balance	Balance zwischen linkem/rechtem Kanal einstellen (0-100)
Bass	Tieftöne anpassen (0-100)
Höhen	Höhen anpassen (0-100)
Helligkeit	Bildschirmhelligkeit einstellen (0-100)
Bildmodus	Standard, Dynamisch, Lebendig, Weich, Benutzerdefiniert, Einzelhandel
Schärfe	Bildschärfe anpassen (0-100)
Kontrast	Kontraststufen einstellen (0-100)
Farbton	Farbtemperatur anpassen (0-100)
Sättigung	Farbintensität einstellen (0-100)
Automatischer Lichtsensor	Anpassung an Umgebungslicht aktivieren
Blaulichtfilter	Augenbelastung bei schwachem Licht reduzieren
Touch aktivieren	Touchscreen-Funktionalität konfigurieren
Werkzeugleistentyp	Auswahl zwischen Floating Bar, Slide Bar oder System Bottom Bar
Automatischer Standby	Inaktivitäts-Timeout einstellen (0-240 Minuten)
Standby bei keinem Signal	Automatisches Herunterfahren bei fehlendem Eingangssignal (0-7200 Sekunden)
Augenschutzmodus	Blaulichtreduzierung aktivieren
Wake-on-Source	Automatisches Einschalten bei verbundener Quelle
Wake-on-LAN	Netzwerk-Wake-Funktion konfigurieren
Touch-Eingabe	Touch-Funktionalität aktivieren/deaktivieren
OEM-Sperre	Unbefugte Änderungen an Einstellungen verhindern
Ethernet	Kabelgebundene Netzwerkverbindung verwalten

Einstellung	Beschreibung
Hotspot	Drahtlosen Zugangspunkt konfigurieren
Gerätesichtbarkeit	Netzwerkerkennung bei Freigabe steuern
Freigabeerlaubnis	Bestätigung für Freigabesitzungen erforderlich machen
Chromecast	Google Cast-Protokoll aktivieren
AirPlay	Apple Screen Mirroring aktivieren
Miracast	Windows Wireless Display aktivieren
Webcast	Browserbasierte Freigabe aktivieren
Autostart	Freigabedienst beim Start ausführen
HID-Touch	USB-Touchsteuerung aktivieren
DLNA	Media-Server-Funktionen konfigurieren
Gerätename	Benutzerdefinierten Netzwerknamen festlegen
Code-Aktualisierung	PIN-Aktualisierungsintervall festlegen
Fenstergröße	Größe des schwebenden Bedienfelds steuern
Automatische Updates	Automatische Firmware-Updates konfigurieren
Update-Überprüfung	Authentizitätsprüfung für Updates aktivieren
Debug-Modus	Entwicklerdiagnostik aktivieren
Sprache	Systemsprache einstellen (Englisch, Französisch, Deutsch, Italienisch, Spanisch, Türkisch)
Zeitplan	Automatisierte Ein-/Ausschaltzeiten erstellen mit: Täglicher/Wöchentlicher Wiederholung, Spezifischen Zeiteinstellungen, Mehrfachaufgabenunterstützung
Quellenalias	Eingangsquellen umbenennen (HDMI/DP/VGA)
Eingangsquelle erzwingen	Startkanal für Eingangsquelle festlegen

Bytello Share-Optionen

Die Relution CVTE OEMConfig App bietet auch die folgenden Konfigurationsoptionen, wenn Bytello Share ebenfalls verfügbar ist:

Einstellung	Beschreibung
Gerätesichtbarkeit im Netzwerk	Sichtbarkeit des Geräts im Netzwerk aktivieren oder deaktivieren.
Genehmigung erforderlich	Alle Geräte zur Bildschirmfreigabe benötigen eine Genehmigung
Chromecast aktivieren	Chromecast-Unterstützung aktivieren/deaktivieren
Airplay aktivieren	Airplay-Unterstützung aktivieren/deaktivieren
Miracast aktivieren	Miracast-Unterstützung aktivieren/deaktivieren
Webcast aktivieren	Webcast-Unterstützung aktivieren/deaktivieren
Automatischer Start beim Booten	Automatischer Start der Bildschirmfreigabe beim Booten des Geräts
HID-Touch-Steuerung	HID-Touch-Control-Unterstützung aktivieren/deaktivieren
DLNA aktivieren	DLNA-Unterstützung aktivieren/deaktivieren
Gerätename	Namen für dieses Gerät festlegen
Code-Aktualisierungszeit	Zeitintervall für die Codeaktualisierung festlegen (Minuten)
Größe des schwebenden Fensters	Setzt die Größe des schwebenden Steuerfensters (Normal, Mini, Geschlossen)
Einstellungen der Systemleiste	Sichtbarkeit der Systemleiste (Sichtbar, Versteckt)

Newline

Mit Relution ist es möglich, interaktive Whiteboards von Newline zentral zu verwalten.

Unterstützte Produktserien und Modelle

- TT-7523QA (Lyra Pro)
- TT-6523QCA+ (Elara Pro)

Einschreibung

Die Einschreibung erfolgt wie unter EDLA Geräte einschreiben → beschrieben.

Unterstützte Aktionen

Es stehen die Android Enterprise Aktionen → zur Verfügung, einschließlich Gerät herunterfahren. Diese Aktion fährt das Whiteboard vollständig herunter. Bei Android Enterprise wird sie nur von bestimmten Whiteboards unterstützt; das Portal kennzeichnet sie mit den unterstützten Herstellern, darunter Newline.

Für Version 26.4.0

Relution Newline OEMConfig App

Um die Zusatzfunktionen der Whiteboards über Android Enterprise bereitzustellen, muss die Relution Newline OEMConfig App auf dem Gerät installiert und konfiguriert sein.

Konfiguration

Eine Richtlinie mit der Konfiguration Newline OEMConfig erstellen, um die Relution Newline OEMConfig App zu konfigurieren.

Die Konfiguration ist ab Relution 5.34.0 verfügbar.

Die Konfiguration installiert die Relution Newline OEMConfig App mit dem Installationstyp Installation erzwungen auf dem Gerät, aktualisiert sie mit hoher Priorität und erteilt ihr die benötigten Berechtigungen. Benutzer können die App nicht entfernen. Eine separate Verteilung über die Konfiguration Apps verwalten ist nicht erforderlich und auch nicht möglich: Ist die App dort eingetragen, lässt sich die Konfiguration nicht speichern, und das Portal verweist auf die Konfiguration Newline OEMConfig.

In den Werten der Konfiguration können Platzhalter verwendet werden; das Formular zeigt die verfügbaren Platzhalter an.

Einstellungsmöglichkeiten

Die Relution Newline OEMConfig App bietet folgende Einstellungen:

Für Version 26.4.0

Einstellung	Beschreibung
Soundausgabe	Aktuelle Soundausgabe einstellen
Lautstärke	Systemlautstärke einstellen (0–100)
Stummschalten	System stumm/aktiv schalten
Wake on lan	Wake on lan aktivieren oder deaktivieren
Wake on Wireless	Wake on Wireless (WoWLAN) aktivieren oder deaktivieren
Wi-Fi	Wi-Fi-Konnektivität aktivieren oder deaktivieren
Ethernet	Ethernet aktivieren oder deaktivieren
Hotspot	Hotspot aktivieren oder deaktivieren
Ethernet tethering	Ethernet-Tethering aktivieren oder deaktivieren
Proxy-Konfiguration	Netzwerk-Proxy-Einstellungen konfigurieren, einschließlich Host, Port und Ausschlussliste
Proxy Host	Proxy-Server-Hostname oder IP-Adresse
Proxy Port	Proxy-Server-Portnummer (1–65535)
Proxy Ausschlussliste	Kommagetrennte Liste von Hosts, die den Proxy umgehen
Helligkeit	Helligkeitswert einstellen (0–100). Bildmodus muss auf CUSTOM/USER eingestellt sein.
Bildmodus	Bildmodus einstellen
Schriftgröße	Schriftgröße einstellen
Startquelle	Startquellenkonfiguration einstellen
Automatische Quellenumschaltung	Automatische Quellenumschaltung aktivieren oder deaktivieren
CEC automatisches Einschalten	CEC automatisches Einschalten aktivieren oder deaktivieren
CEC automatisches Ausschalten	CEC automatisches Ausschalten aktivieren oder deaktivieren
HDMI/DP EDID Typ	HDMI/DisplayPort EDID-Version einstellen
Signalquelle Aufwachen	Aufwachen bei Erkennung neuer Signalquelle aktivieren oder deaktivieren
Debug-Modus	Debug-Modus aktivieren oder deaktivieren
24-Stunden-Zeitformat	24-Stunden-Zeitformat aktivieren oder deaktivieren

Einstellung	Beschreibung
Linke Toolbar	Linke Toolbar aktivieren oder deaktivieren
Rechte Toolbar	Rechte Toolbar aktivieren oder deaktivieren
Schnelleinstellungen	Zugriff auf Schnelleinstellungen aktivieren oder deaktivieren
Einschaltdatum/-zeit	Geplante Einschaltzeit konfigurieren
Ausschaltdatum/-zeit	Geplante Ausschaltzeit konfigurieren
Energiesparzeit	Energiesparzeit aktivieren. Deaktivieren, um nie einzustellen.
Energiesparzeit (Minuten)	Energiesparzeit in Minuten. Übliche Werte sind 30, 60, 90, 120
Power-Button-Verhalten	Power-Button-Aktion konfigurieren (Sleep vs Power Off)
Tap Wake	Bildschirm durch Antippen aktivieren oder deaktivieren
Augenschutz Schreiben	Schreiborientierten Augenschutzmodus aktivieren oder deaktivieren
Adaptive Helligkeit	Automatische Helligkeitsanpassung für Augenschutz aktivieren oder deaktivieren
Blaulichtfilter	Blaulichtfilter aktivieren oder deaktivieren
Blaulichtfilter Stufe	Blaulichtfilter-Intensitätsstufe einstellen (0-100)
Geräte-Logo	Herstellerlogo anzeigen/ausblenden
UI-Theme	Zwischen Newline Q oder Z Theme-Varianten wählen
Automatische Dateibereinigung	Intervall für automatische Dateibereinigung einstellen
Android OS (Warnung: kann nur im Händlermenü wieder aktiviert werden)	Android OS aktivieren oder deaktivieren (Warnung: kann nur im Händlermenü wieder aktiviert werden)
USB-Sperre	USB-Port-Sperre aktivieren oder deaktivieren
Menü-Sperre	Systemmenü-Zugriff aktivieren oder deaktivieren
Einstellungs-Sperre	Einstellungsänderungen aktivieren oder deaktivieren
App-Installation deaktivieren	App-Installation aktivieren oder deaktivieren
Front-Power-Button-Sperre	Front-Power-Button-Funktionalität aktivieren oder deaktivieren
Front-Panel-Buttons-Sperre	Front-Panel-Buttons aktivieren oder deaktivieren
Touch-Sperre	Touch-Sperre aktivieren oder deaktivieren
Signalquelle Touch-Sperre	Signalquelle Touch-Sperre einstellen
Wi-Fi-Einstellungs-Sperre	Wi-Fi-Konfigurationsänderungen aktivieren oder deaktivieren

Einstellung	Beschreibung
Ethernet-Einstellungs-Sperre	Ethernet-Konfigurationsänderungen aktivieren oder deaktivieren
Launcher-Icons-Sperre	Launcher-Icon-Änderungen aktivieren oder deaktivieren
Admin-Modus-Passwort	Admin-Modus-Passwort setzen (mind. 6 Zeichen)
Theme & Hintergrund-Sperre	Änderungen an Geräte-Theme und Hintergrundeinstellungen verhindern
Blockierte URLs	URLs blockieren
Lokales OTA	Lokale Firmware-Updates aktivieren oder deaktivieren
OTA-Hintergrunddownload	OTA-Hintergrunddownloads aktivieren oder deaktivieren
OTA-Benachrichtigungen	OTA-Update-Benachrichtigungen aktivieren oder deaktivieren

Für Version 26.4.0

Vorinstallierte Apps

Um vorinstallierte Apps gezielt freizugeben, wird der jeweilige Package-Name der App benötigt. Eine vollständige Liste aller vorinstallierten Apps, die nach der Einschreibung in Android Enterprise nicht mehr verfügbar sind, lässt sich ermitteln, indem das Gerät auf die Werkseinstellungen zurückgesetzt und der vollständige Geräte-Setup-Prozess durchgeführt wird, ohne das Gerät in Android Enterprise einzuschreiben.

> Ob nicht wesentliche vorinstallierte System-Apps bei der Einschreibung deaktiviert werden, legt der Schalter System-Apps aktiviert lassen der Einschreibung fest. Relution übernimmt ihn nur in den QR-Code, nicht in den DPC-Identifier, siehe EDLA Geräte einschreiben →.

Sobald das Gerät vollständig eingerichtet und einsatzbereit ist, per Android Debug Bridge → mit dem Gerät verbinden. Anschließend folgenden Befehl ausführen, um eine Liste aller installierten Packages zu exportieren:

```
adb shell cmd package list packages > list1.txt
```

Das Gerät danach erneut auf die Werkseinstellungen zurücksetzen und in Android Enterprise einschreiben.

Nach der erfolgreichen Einschreibung wieder mit dem Gerät per ADB verbinden und folgenden Befehl ausführen:

für Version 26.4.0

```
adb shell cmd package list packages > list2.txt
```

Nun lassen sich beide Dateien miteinander vergleichen.

Alle Apps, welche in der Datei `list1.txt` vorkommen, jedoch in `list2.txt` fehlen, müssen mit dem Installationstyp Vorinstalliert der Konfiguration Apps verwalten hinzugefügt werden.

In der Konfiguration Apps verwalten öffnet Hinzufügen den Dialog App auswählen. Dort wird als Quelle die Option App manuell hinzufügen ausgewählt. Im nächsten Schritt werden Name (Anzeigename der App) und Interner Name (Package-Name) eingetragen. Der interne Name entspricht dem Eintrag aus der Datei `list1.txt`, der hinzugefügt werden soll – jedoch ohne den Präfix `package:`. Beispiel: Soll der Eintrag `package:io.relution.files` hinzugefügt werden, ist als interner Name `io.relution.files` anzugeben.

Die App erscheint anschließend mit dem Installationstyp Installation erzwungen in der Liste. In der Spalte Installationstyp wird Vorinstalliert ausgewählt.

Manuelle Einschreibung

Ab Relution-Version 5 lassen sich Windows 10/11-Geräte einschreiben und ohne ein Microsoft- bzw. `Azure AD`-Konto verwalten. Voraussetzung für die Einschreibung ist ein lokaler Benutzer. Dieser Benutzer muss über administrative Berechtigungen verfügen und darf nach der Einschreibung nicht gelöscht werden.

Geräte sollten mit einer eindeutigen ID ausgestattet sein. Relution erkennt ein Gerät bei der Einschreibung an seiner Windows-Geräte-ID und behandelt eine Einschreibung mit einer bereits bekannten ID als erneute Einschreibung desselben Geräts. Insbesondere bei der Vorkonfiguration über ein Image sollte deshalb darauf geachtet werden, dass die Geräte vom MDM unterschieden werden können.

Neben der manuellen Einschreibung stehen für Windows-Geräte die Einschreibung über Autopilot → und das Bulk Enrollment → mit einem Bereitstellungspaket zur Verfügung.

> Die Windows 10/11 Home-Edition unterliegt bei der Verwaltung diversen Einschränkungen. Es stehen nicht alle Verwaltungsmöglichkeiten zur Verfügung. Einschränkungen der Windows Home Edition →

Unterstützte Windows-Versionen

- Windows 10/11 Home
- Windows 10/11 Professional
- Windows 10/11 Education
- Windows 10/11 Enterprise

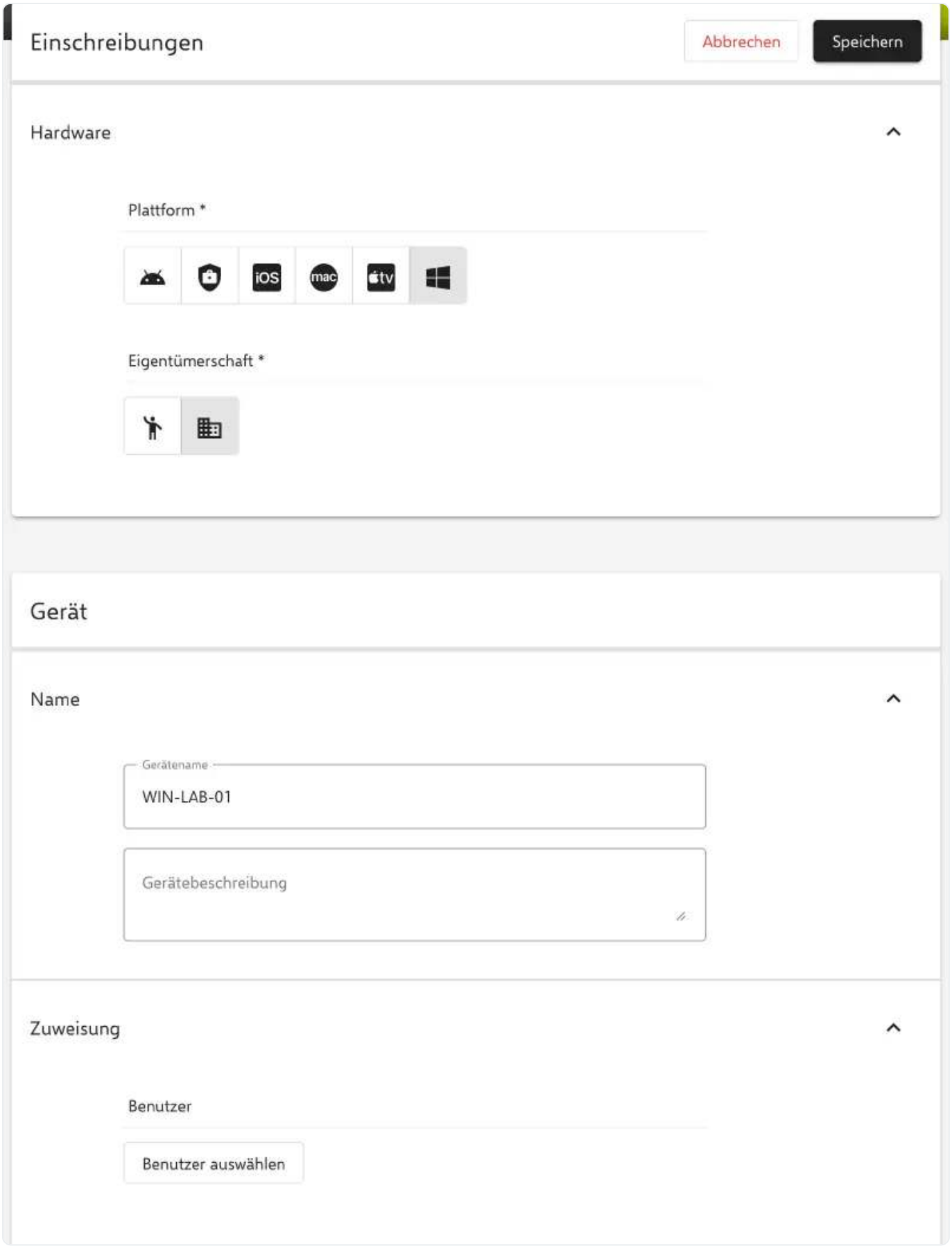
Für Version 26.4.0

Nicht unterstützte Windows-Versionen

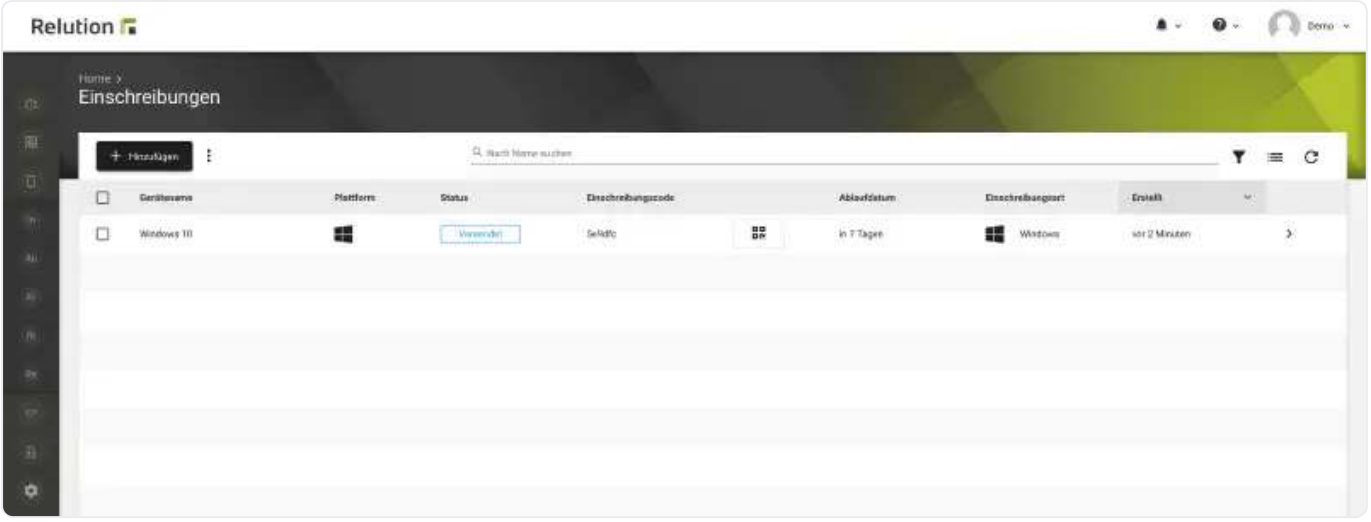
- Windows 10/11 Enterprise LTSC
- Windows 10/11 IoT Enterprise
- Windows 10/11 IoT Enterprise LTSC

Windows-Geräte manuell einschreiben

Um ein Windows 10/11-Gerät einzuschreiben, muss eine neue Einschreibung in Relution angelegt werden. Die Einschreibung wird unter `Geräte` → `Einschreibungen` über Hinzufügen angelegt; in der globalen Organisation steht der Menüpunkt nicht zur Verfügung. Im Abschnitt Hardware wird unter Plattform Windows ausgewählt und die Eigentümerschaft festgelegt. Optional wird unter Gerätename ein Name vorgegeben (nur Buchstaben, Ziffern und Bindestriche); bleibt das Feld leer, wird der Name automatisch generiert. Unter Zuweisung kann ein Benutzer ausgewählt werden, über Gültig bis ein Ablaufdatum.


Einschreibungen
Abbrechen
Speichern
Hardware
Plattform *
iOS
mac
tv
Eigentümerschaft *
Gerät
Name
Gerätename
WIN-LAB-01
Gerätebeschreibung
Zuweisung
Benutzer
Benutzer auswählen

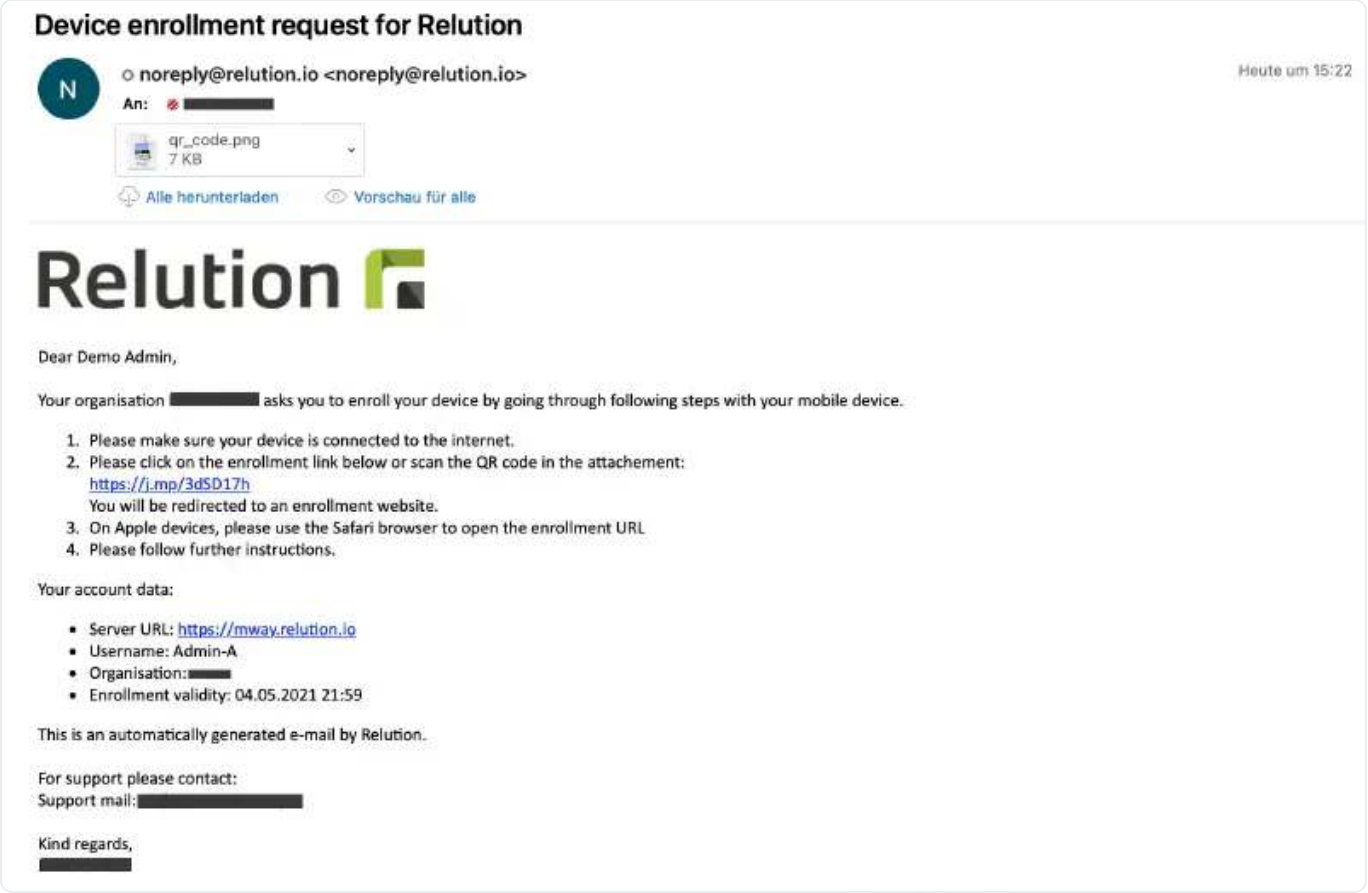
Anschließend wird die Einschreibung unter Einschreibungen aufgeführt – mit dem Status Versendet, sofern die Einschreibungsinformationen per E-Mail oder SMS verschickt wurden, andernfalls mit dem Status Erstellt. Nach der Einschreibung eines Geräts wechselt eine nicht mehrfach verwendbare Einschreibung in den Status Eingeschrieben und kann nicht erneut verwendet werden.



Einschreibeinformationen erhalten

Für Version 26.4.0

Die benötigten Einschreibeinformationen können beim Anlegen der Einschreibung im Bereich Benachrichtigung per E-Mail, per SMS oder über beide Kanäle versendet werden. Voraussetzung ist, dass der jeweilige Kanal unter `Einstellungen` → `Benachrichtigungen` aktiviert ist. Für den Versand per E-Mail muss der Einschreibung ein Benutzer mit E-Mail-Adresse zugewiesen sein, für den Versand per SMS muss eine Telefonnummer angegeben sein. Benutzer, die den einzuschreibenden Geräten zugewiesen sind, erhalten beispielsweise folgende E-Mail mit allen relevanten Informationen:



Device enrollment request for Relution

N ○ noreply@relution.io <noreply@relution.io> Heute um 15:22

An: [redacted]

qr_code.png 7 KB

Alle herunterladen Vorschau für alle

Relution

Dear Demo Admin,

Your organisation [redacted] asks you to enroll your device by going through following steps with your mobile device.

1. Please make sure your device is connected to the internet.
2. Please click on the enrollment link below or scan the QR code in the attachement:
   https://j.mp/3dSD17h
   You will be redirected to an enrollment website.
3. On Apple devices, please use the Safari browser to open the enrollment URL
4. Please follow further instructions.

Your account data:

- Server URL: https://mway.relution.io
- Username: Admin-A
- Organisation: [redacted]
- Enrollment validity: 04.05.2021 21:59

This is an automatically generated e-mail by Relution.

For support please contact:
Support mail: [redacted]

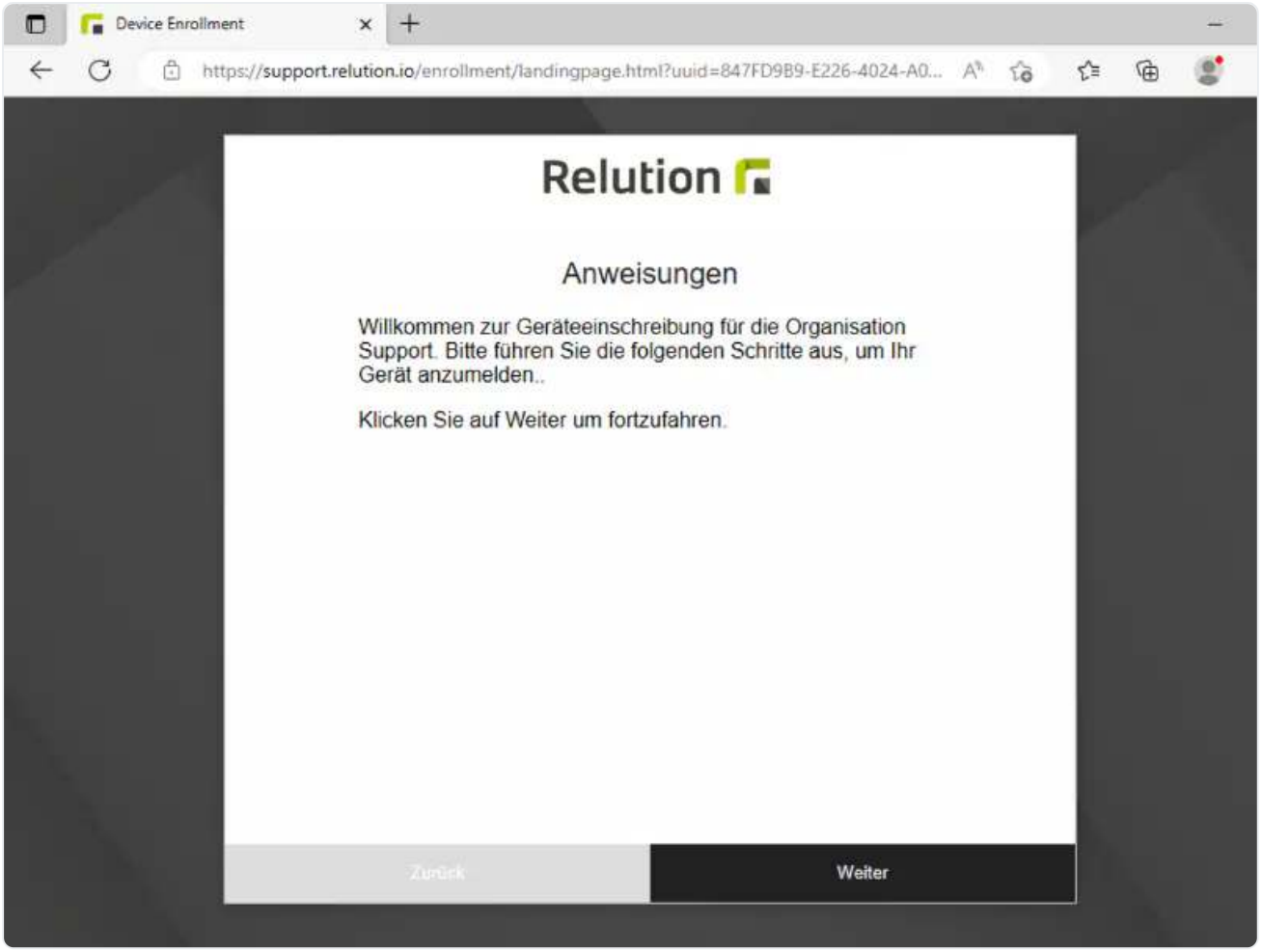
Kind regards,
[redacted]

Der Einschreibungslink in der E-Mail führt automatisch zum Einschreibeprozess auf dem Windows 10/11-Gerät.

Für Version 26.4.0

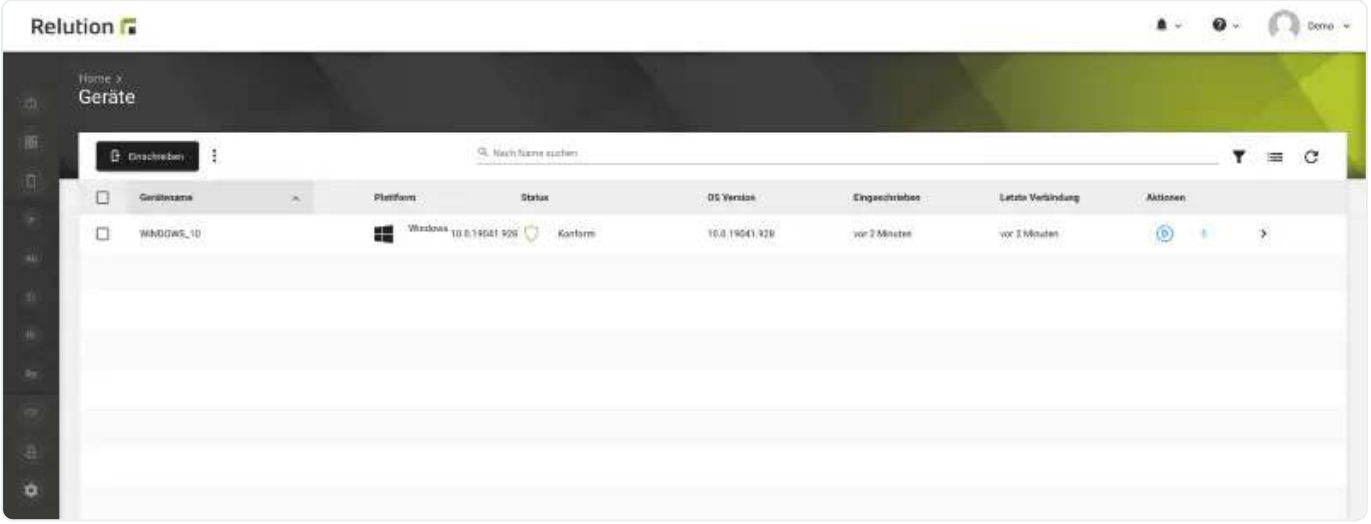
Einschreibung auf Windows 10/11-Geräten durchführen

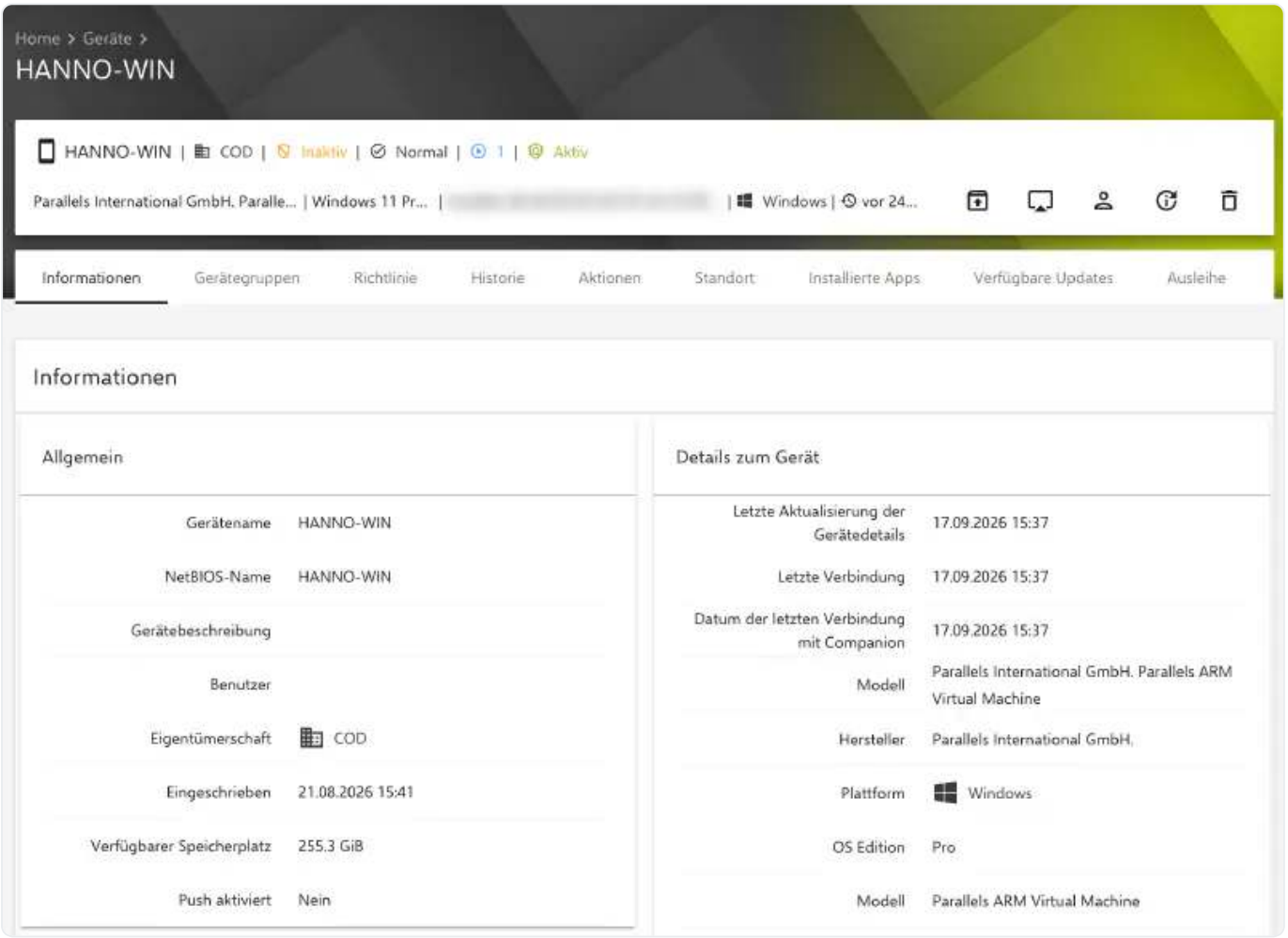
1. Den in der Einschreibung angezeigten Link im Browser des einzuschreibenden Geräts öffnen.



2. Auf Weiter und anschließend auf Einschreibung klicken. Der Browser versucht nun die Einstellungsapp zu öffnen. Auf Öffnen klicken.

3. Alle weiteren Abfragedialoge bestätigen. Das Gerät ist im Anschluss eingeschrieben und kann mit Relution verwaltet werden.



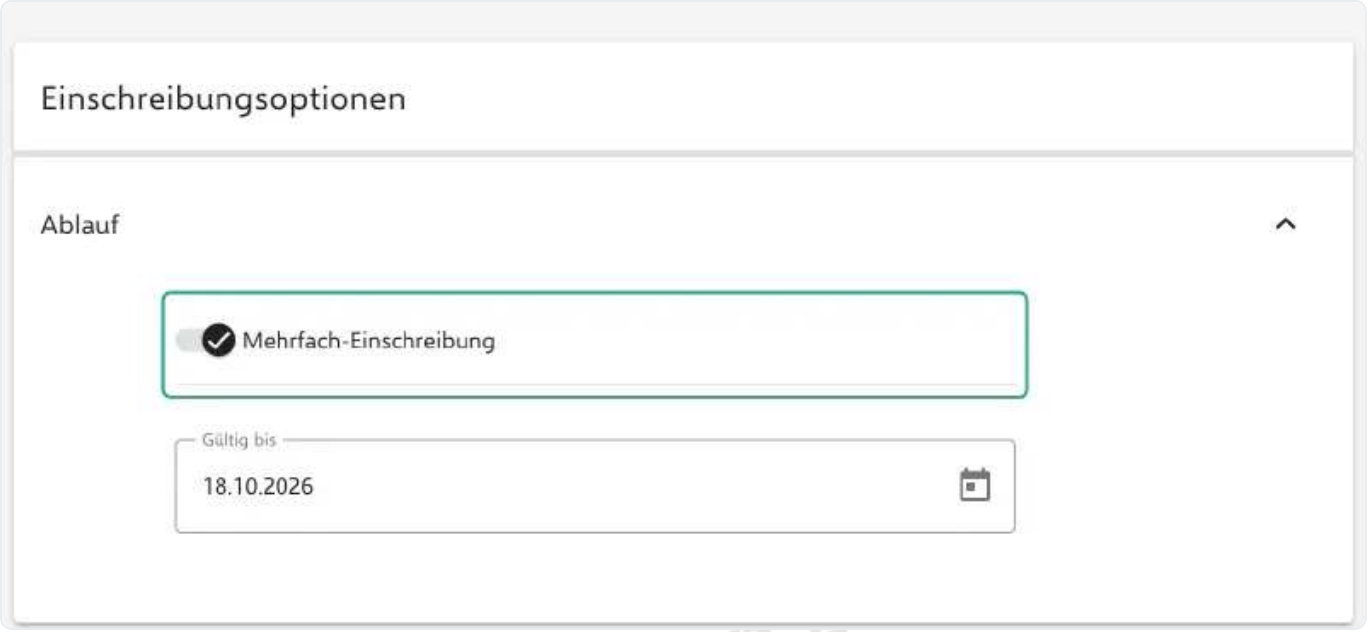


Mehrfach-Einschreibung von Windows 10/11-Geräten

Relution unterstützt das `Bulk-Enrollment` als eine effiziente Methode, um eine große Anzahl von Windows 10/11-Geräten einzuschreiben, die von einem MDM-Server verwaltet werden sollen, ohne dass ein erneutes Image der Geräte erforderlich ist.

Dafür wird beim Anlegen der Einschreibung im Bereich Einschreibungsoptionen im Abschnitt Ablauf der Schalter Mehrfach-Einschreibung aktiviert. Die Einschreibung kann dann für mehrere Geräte verwendet werden. Allein durch den Schalter erfolgt jedoch noch keine Masseneinschreibung: Der erzeugte Einschreibungscode wird anschließend im Windows Configuration Designer in ein Bereitstellungspaket (`ppkg`) übernommen. Das Bulk Enrollment ist für Windows 10/11 Professional, Enterprise und Education verfügbar. Bulk Enrollment →

Die Aktion Multi-Einschreibung im Kontextmenü der Einschreibungsliste legt dagegen mehrere einzelne Einschreibungen für ausgewählte Benutzer gleichzeitig an und ist hierfür nicht gemeint.



Für Version 2

Weitere Details sind in der Microsoft-Dokumentation zu Massenregistrierung zu finden:

Windows Provisioning Tool →

Das Konto auf dem Gerät, mit dem das Gerät registriert wurde, darf nicht gelöscht werden.

Bulk Enrollment

Bei der Registrierung und Einrichtung einer großen Anzahl von Windows 10/11-Geräten entsteht durch einen manuellen Einschreibeprozess ein nicht unerheblicher Aufwand. Das `Windows Bulk Enrollment`, auch Masseneinschreibung genannt, stellt eine effiziente Möglichkeit dar, viele Windows 10/11-Geräte schnell einzuschreiben, ohne die Einschreibungen über die Systemeinstellungen auf jedem einzelnen Gerät abschließen zu müssen. Die massenhafte Registrierung von Windows 10/11-Geräten ist für die Versionen Professional, Enterprise und Education verfügbar. Die Einschreibung einzelner Geräte ist unter Manuelle Einschreibung → beschrieben.

Windows Configuration Designer (WCD)

Um `Windows Bulk Enrollment` durchführen zu können, wird das Tool `Windows Configuration Designer` (WCD) benötigt, das aus dem Microsoft Store → heruntergeladen werden kann. Alternativ lässt sich das WCD-Tool über das Windows Assessment and Deployment Kit (ADK) → herunterladen und ist dann auch in anderen Sprachen verfügbar.

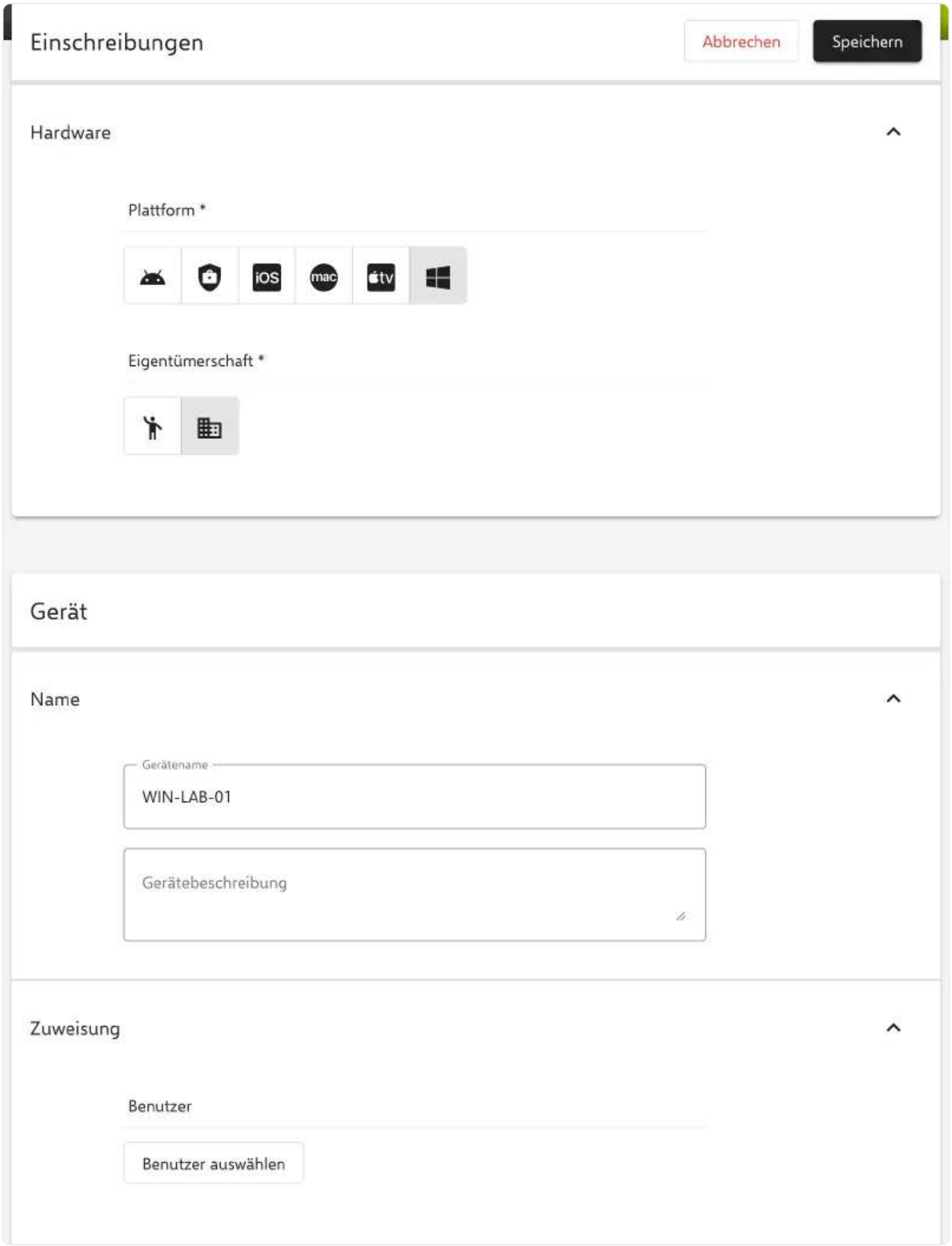
Mit dem WCD-Tool lassen sich Bereitstellungspakete, sogenannte `Provisioning Packages`, erzeugen, die für die Ausführung von Masseneinschreibungen benötigt werden. Das Dateiformat von Bereitstellungspaketen ist eine `ppkg`-Datei. Dies ist ein Container für eine Sammlung von Konfigurationseinstellungen. Das `Bulk Enrollment` wird nicht mit einem `Azure AD`-Konto oder `Windows Autopilot` durchgeführt. Die Registrierung erfolgt über eine `ppkg` Datei, diese kann nach der Inbetriebnahme des Gerätes mit einem Administrator Konto ausgeführt werden. Alternativ kann die `ppkg` in ein Windows Image eingearbeitet werden; das Vorgehen ist in folgender Anleitung beschrieben. Windows Bulk ppkg Image →

> Die ppkg darf nicht wie eine auto/unattend.xml auf einem USB-Stick bei der Installation vom OS verwendet werden. Bei der Installation des OS wird ein Temp-Admin verwendet, dieser und die Einschreibung würden nach einiger Zeit verworfen werden.

Für Version 26.4.0

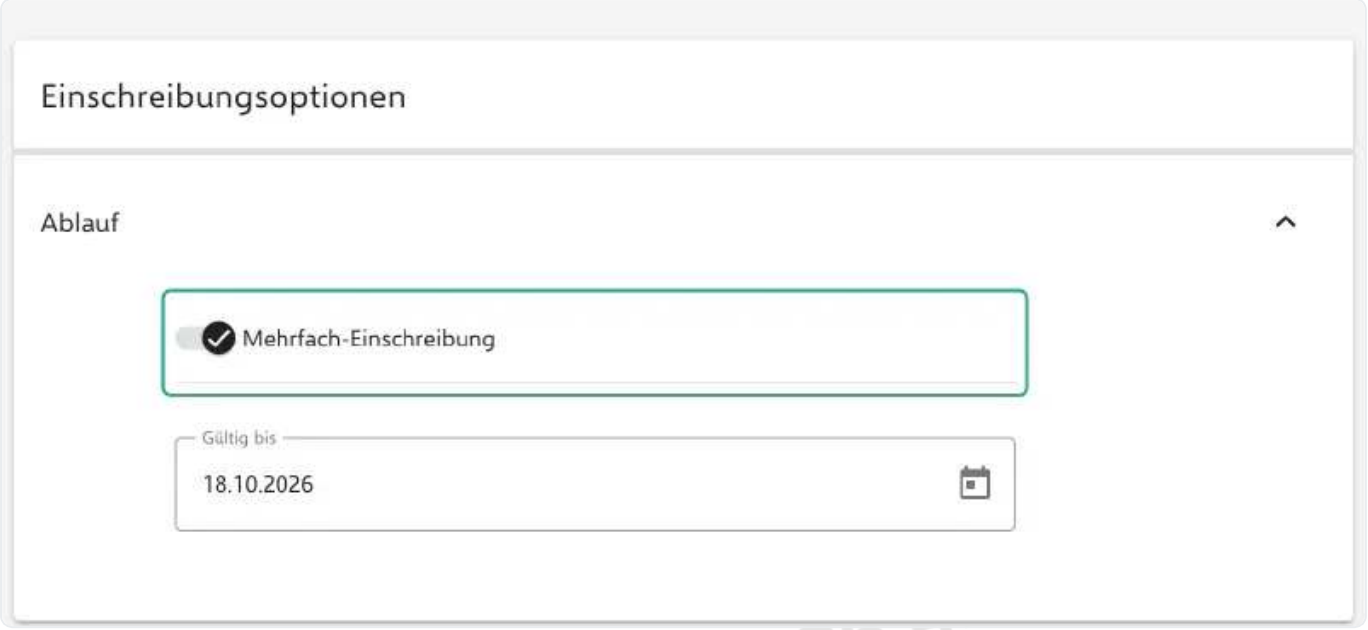
Vorbereitung der Einschreibung in Relution

Für die Masseneinschreibung von Windows 10/11-Geräten muss in Relution eine manuelle Einschreibung angelegt werden. Sie wird unter `Geräte` → `Einschreibungen` über Hinzufügen erstellt. Im Abschnitt Hardware wird unter Plattform Windows ausgewählt. Einschreibungscodes anderer Plattformen werden bei der Windows-Einschreibung abgelehnt.


Einschreibungen
Abbrechen
Speichern
Hardware
Plattform *
iOS
mac
tv
Eigentümerschaft *
Gerät
Name
Gerätename
WIN-LAB-01
Gerätebeschreibung
Zuweisung
Benutzer
Benutzer auswählen

Die Einstellungen der Einschreibung gelten für alle Geräte, die mit dem Bereitstellungspaket eingeschrieben werden. Ist unter Zuweisung ein Benutzer ausgewählt, werden alle Geräte diesem Benutzer zugewiesen; ohne Benutzer werden die Geräte keinem Benutzer zugeordnet.

Im Bereich Einschreibungsoptionen wird im Abschnitt Ablauf die Option Mehrfach-Einschreibung aktiviert. Nur so lässt sich die erzeugte Einschreibung für mehrere Windows 10/11-Geräte verwenden. Die Option kann nach dem Anlegen nicht mehr geändert werden. Über Gültig bis kann optional ein Ablaufdatum gesetzt werden.



Für Version 26.4

Nach dem Speichern wird der Einschreibungscode im Bereich Einschreibungs-Information der Einschreibung mit einer Schaltfläche zum Kopieren angezeigt; in der Einschreibungsliste steht er in der Spalte Einschreibungscode. Er wird im weiteren Prozess bei der Erstellung des Bereitstellungspaketes über das WCD-Tool benötigt.

Der Einschreibungscode wird fest in das Bereitstellungspaket übernommen. Nach Ablauf des Datums unter Gültig bis schlagen Einschreibungen mit diesem Paket fehl, bis die Einschreibung in der Einschreibungsliste über Einschreibung(en) verlängern verlängert wird. Wird die Einschreibung gelöscht, kann das Bereitstellungspaket nicht mehr verwendet werden; es muss dann mit dem Einschreibungscode einer neuen Einschreibung neu erzeugt werden.

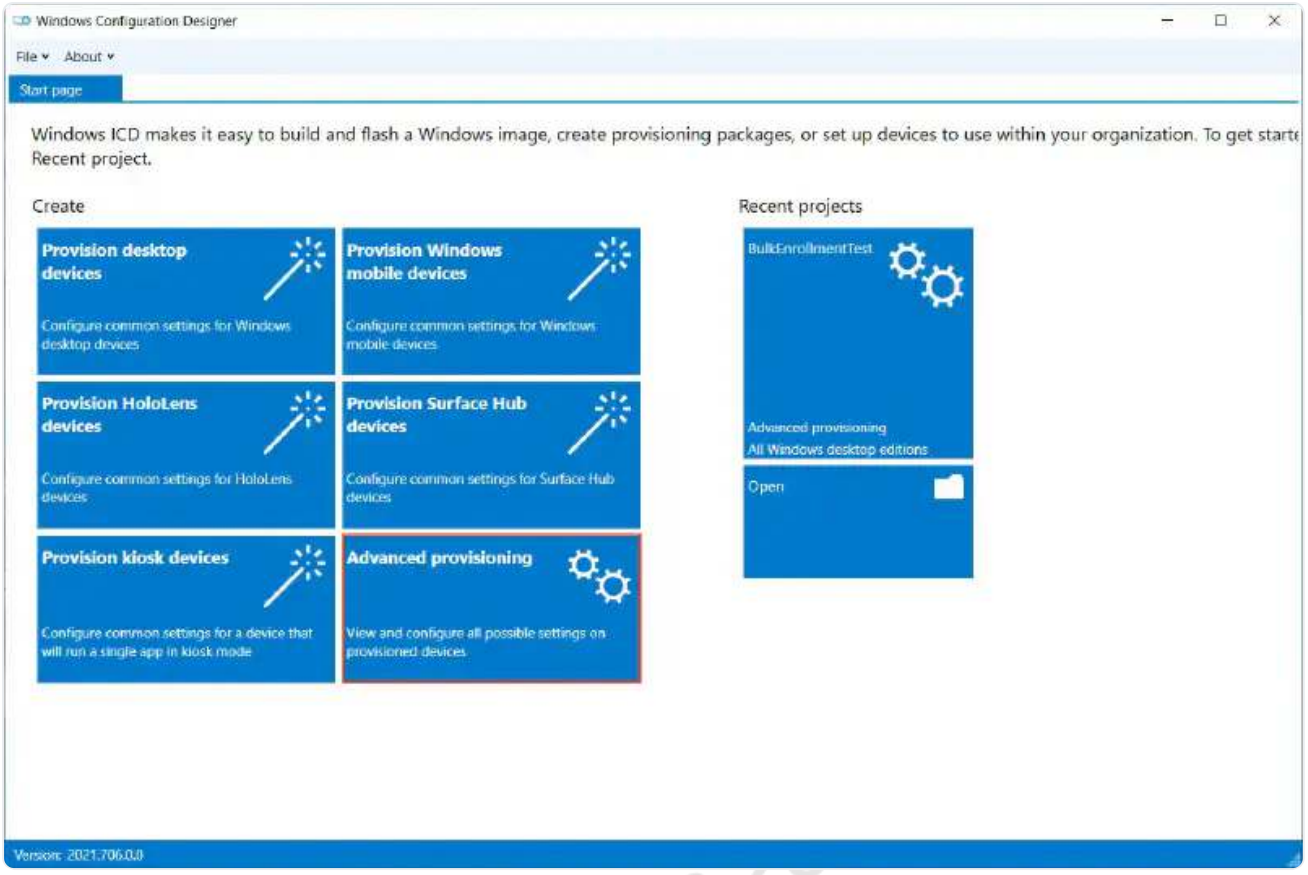
Die Aktion Multi-Einschreibung im Kontextmenü der Einschreibungsliste legt dagegen mehrere einzelne Einschreibungen für ausgewählte Benutzer an und wird für dieses Verfahren nicht benötigt.

Erstellen von Bereitstellungspaketen mit Windows Configuration Designer (WCD)

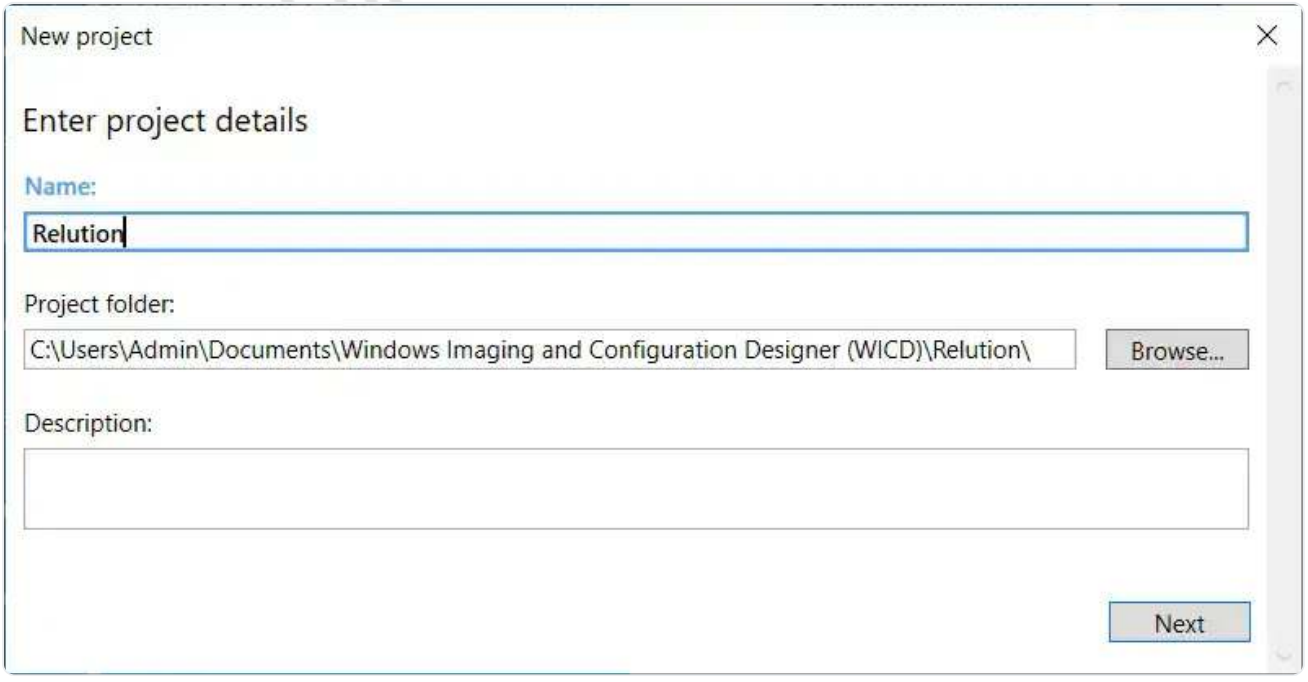
Folgende Schritte werden nach dem Download und der Installation des WCD-Tools durchgeführt, um ein Bereitstellungspaket zu erstellen:

Für Version 26.4.0

1. In der Startansicht die Kachel Verwenden der erweiterten Bereitstellung wählen.

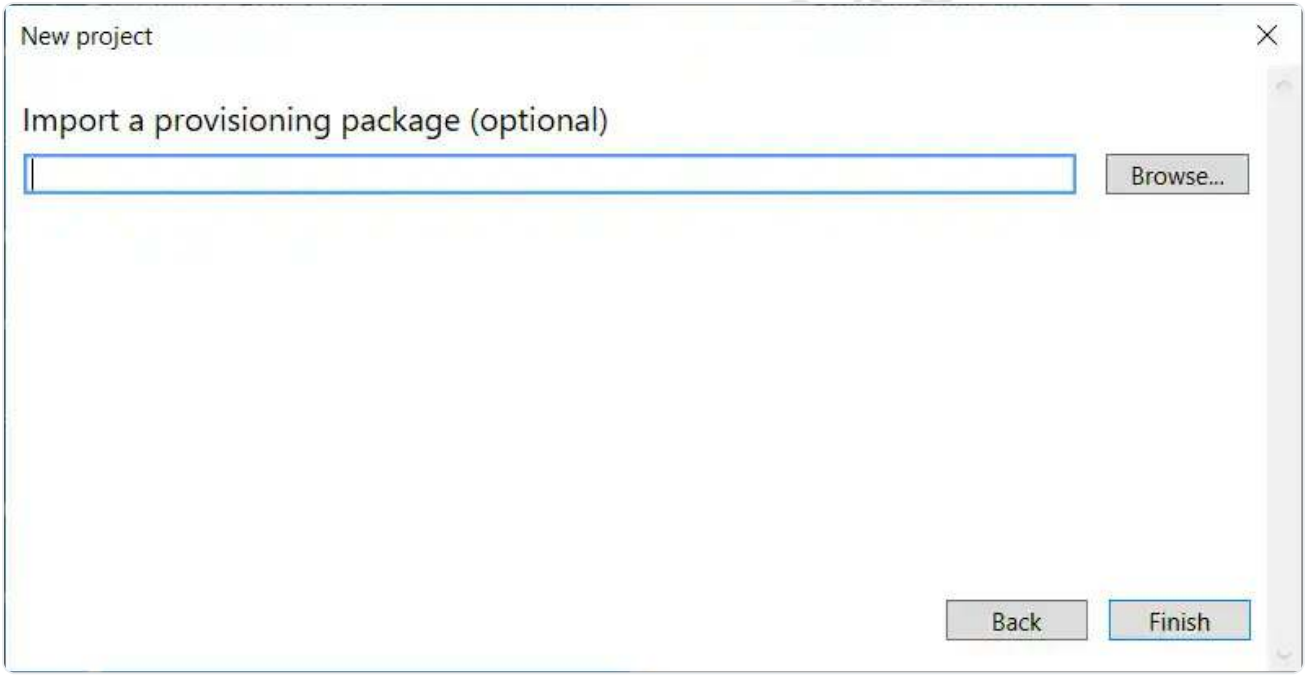


2. Einen Projektnamen angeben und auf Weiter klicken.



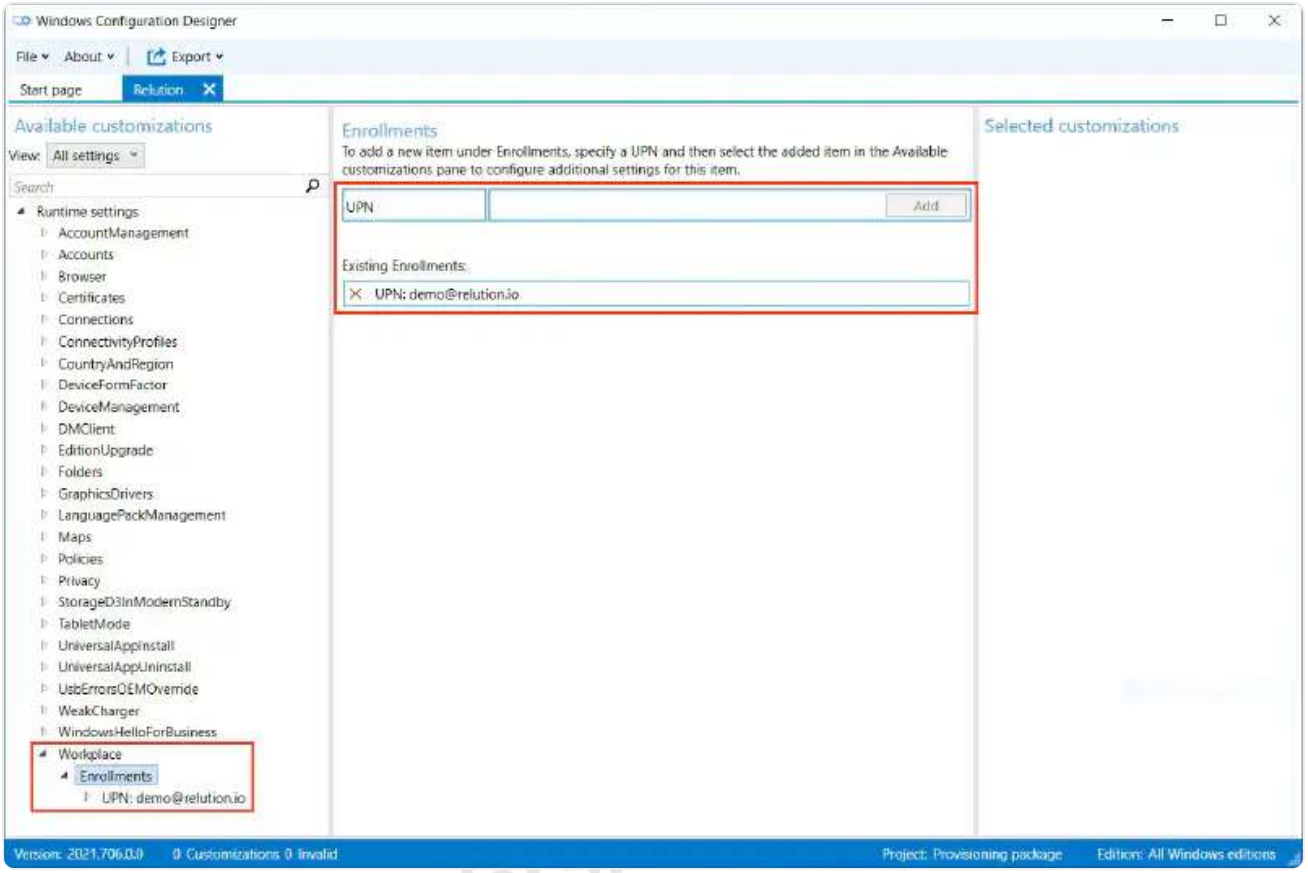
3. Alle Windows Desktop Editionen wählen und Weiter klicken.

4. Import eines Bereitstellungspakets (optional) überspringen und mit Fertigstellen bestätigen.



5. Den Menüpunkt Laufzeiteinstellungen und anschließend Workplace im linken Navigationsbereich erweitern und auf Einschreibungen klicken.

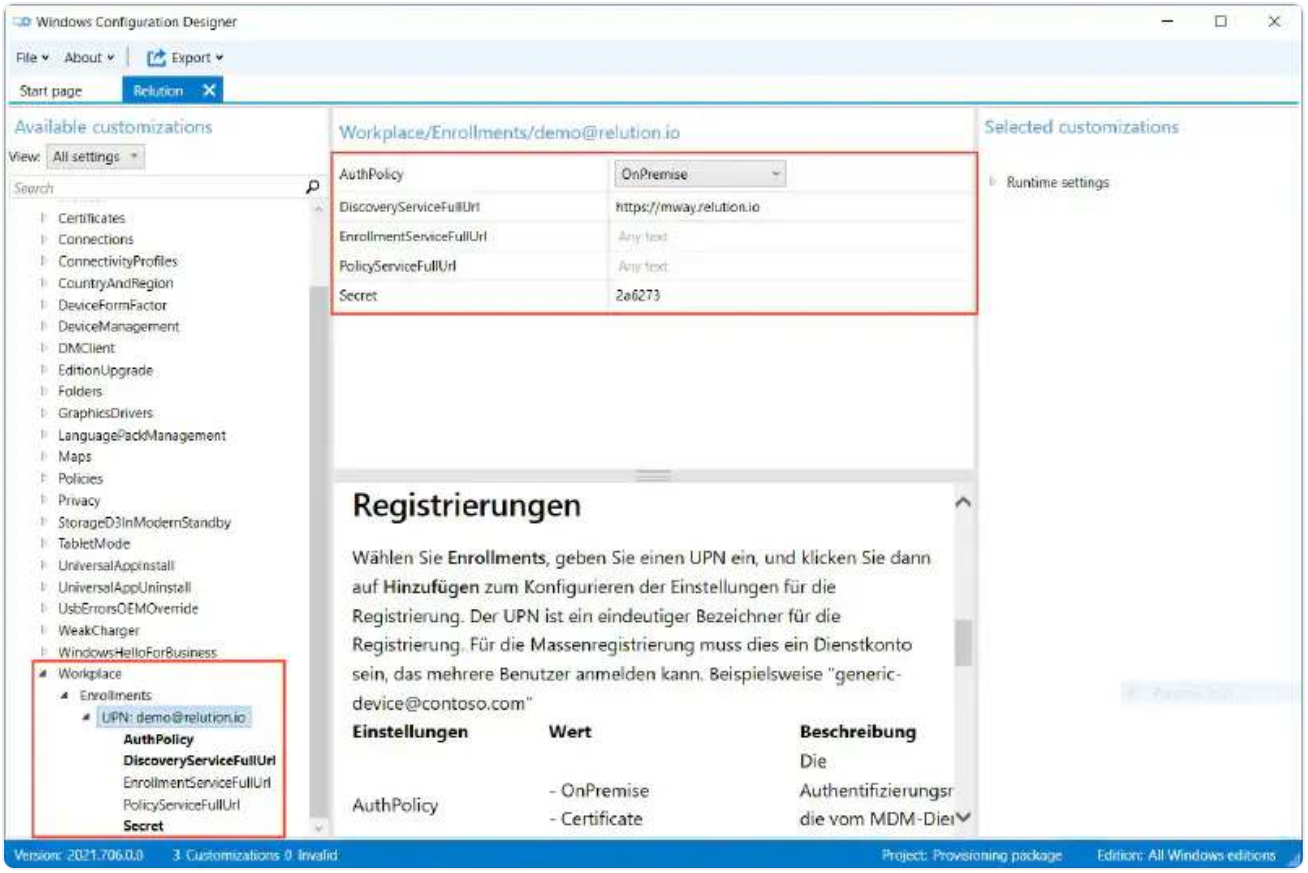
6. Unter Einschreibungen eine UPN im Format einer E-Mail-Adresse eintragen und hinzufügen. Relution wertet diesen Wert bei der Einschreibung nicht aus. Organisation und Benutzerzuordnung ergeben sich aus der Einschreibung in Relution, deren Einschreibungscode unten als `Secret` eingetragen wird.



Für Vers

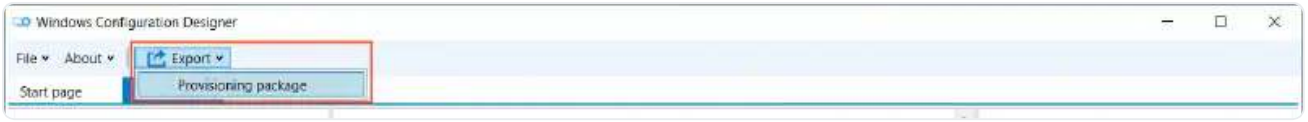
7. Den neu angelegten Eintrag mit der UPN im linken Navigationsbereich erweitern und die Eingabe folgender Informationen für die restlichen Einstellungen durchführen:

   - `AuthPolicy` – `OnPremise` auswählen.
   - `DiscoveryServiceFullUrl` – Angabe der entsprechenden Domain des verwendeten Relution-Servers.
   - `EnrollmentServiceFullUrl` – Optional.
   - `PolicyServiceFullUrl` – Optional.
   - `Secret` Eingabe des Einschreibungscodes aus Relution.

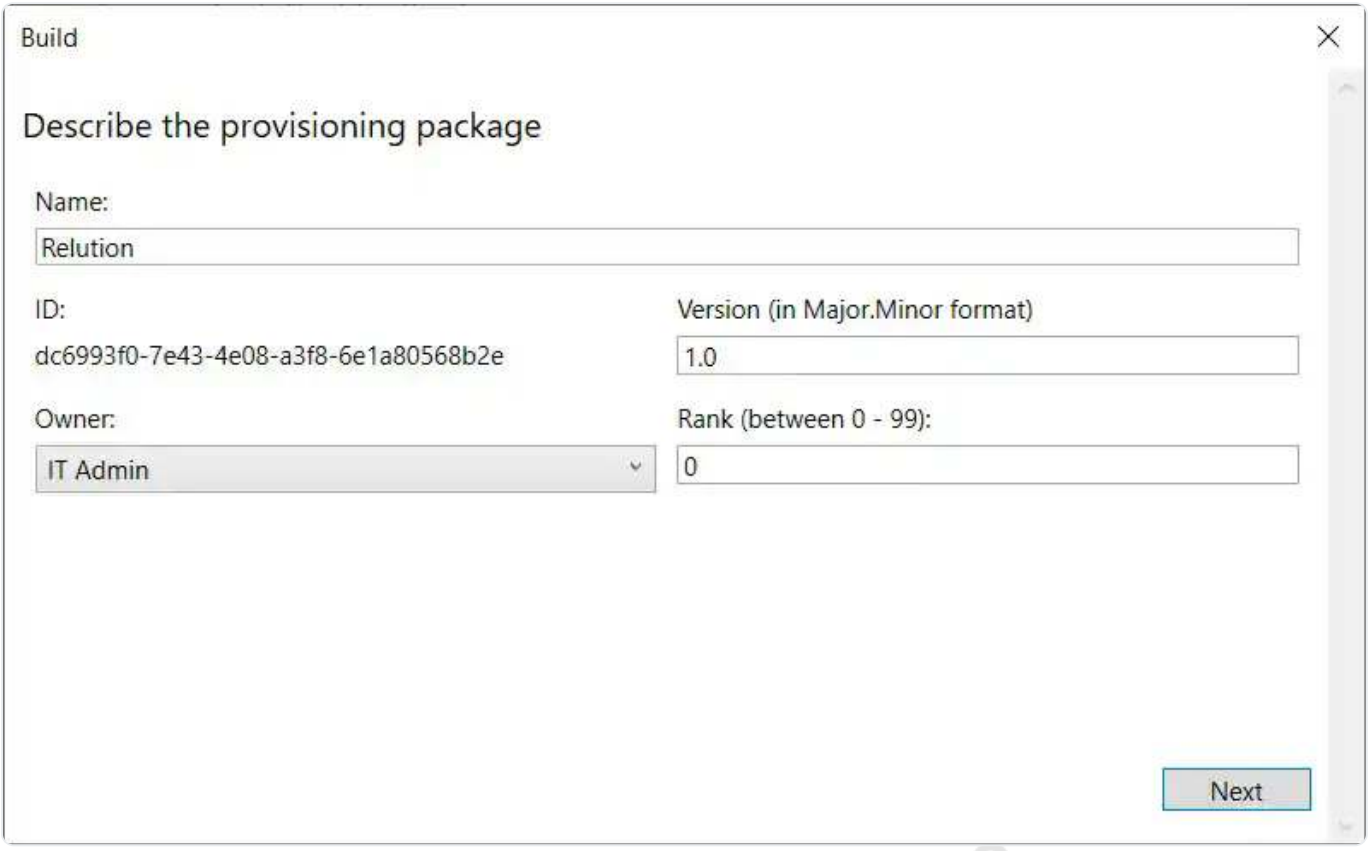


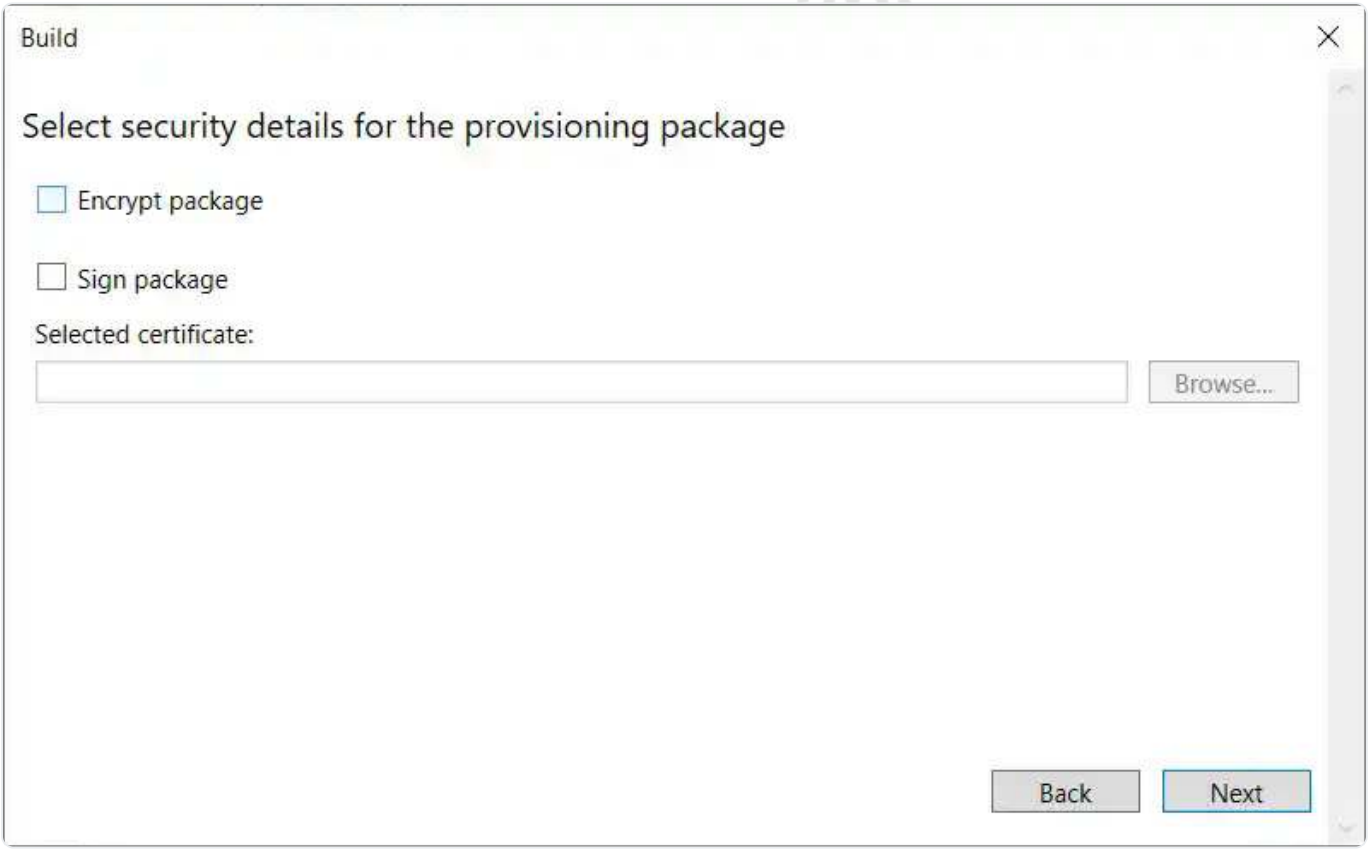
8. Nach Eingabe aller Einstellungen im Hauptmenü `Datei` → `Speichern` wählen.

9. Anschließend im Hauptmenü `Exportieren` → `Bereitstellungspaket` wählen.



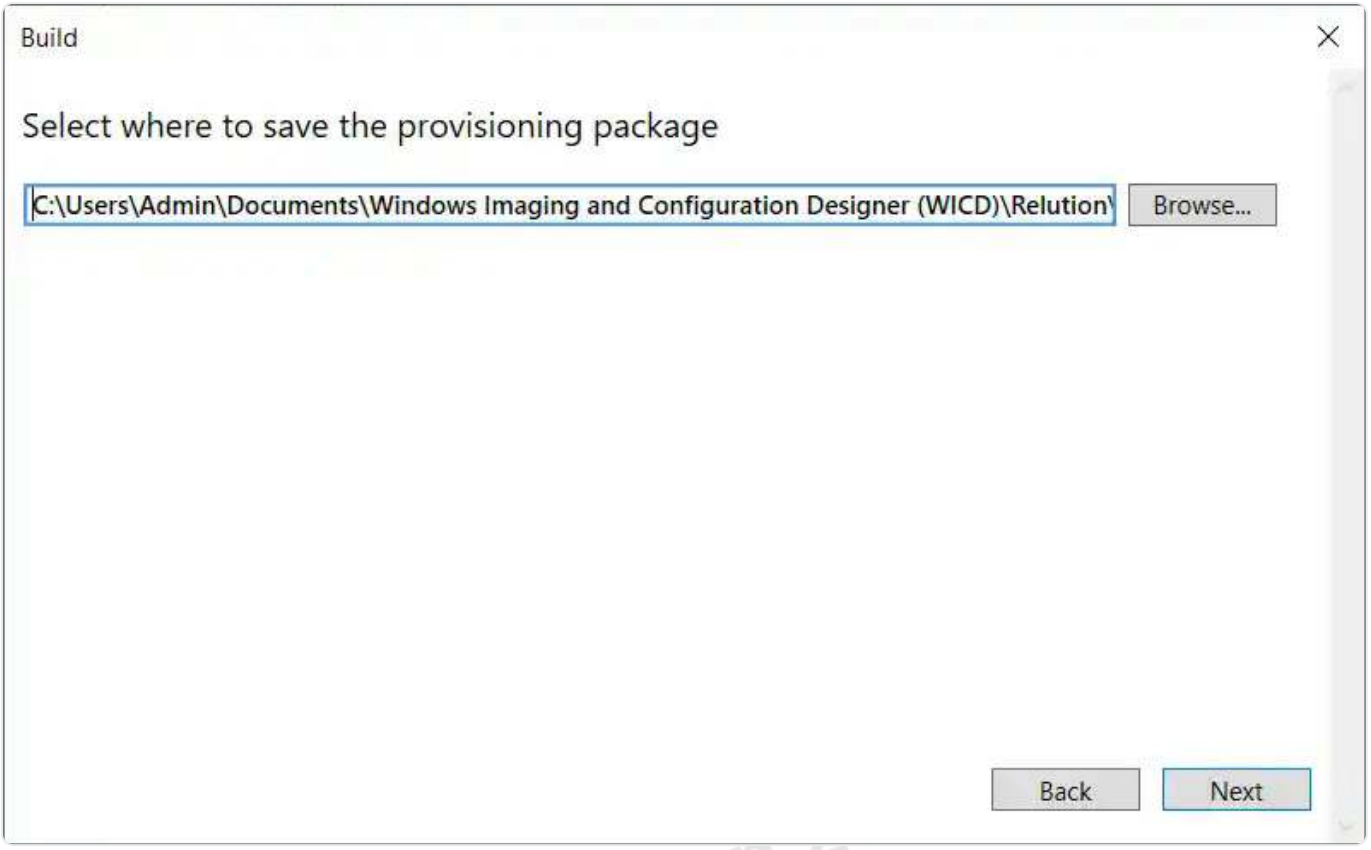
10. Im anschließenden Dialog die Werte für das Paket angeben, den Speicherort für die Paketausgabe wählen und auf Erstellen klicken.

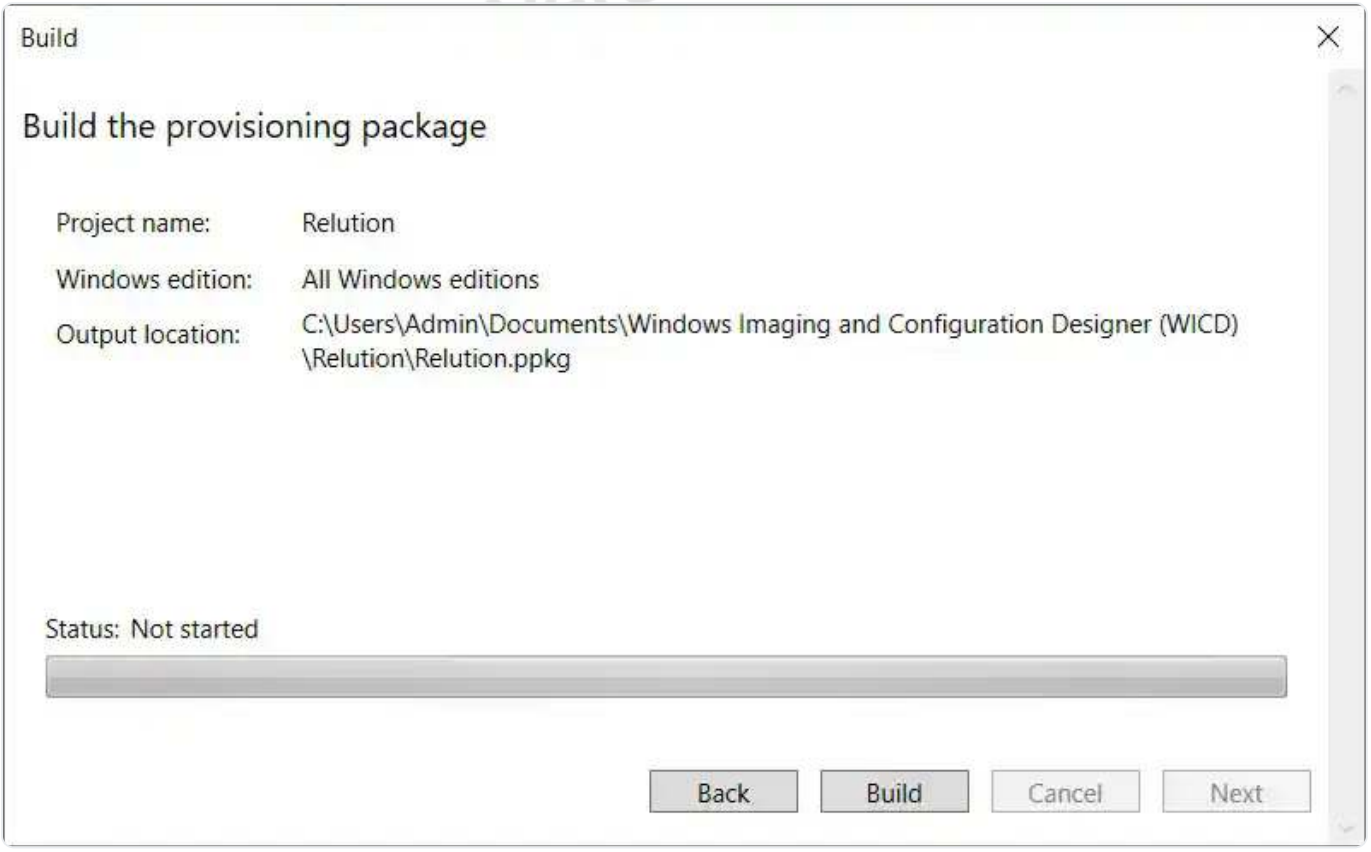


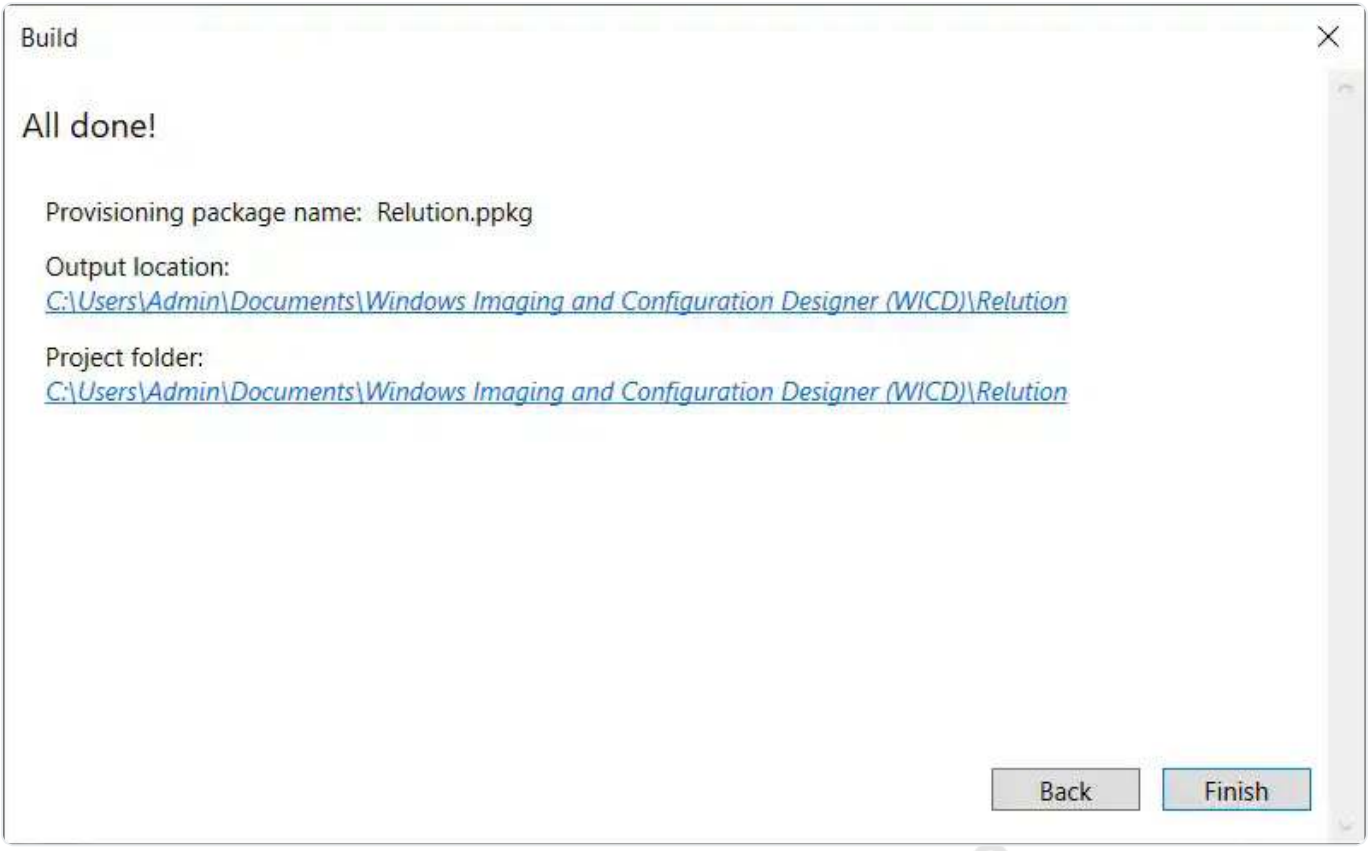


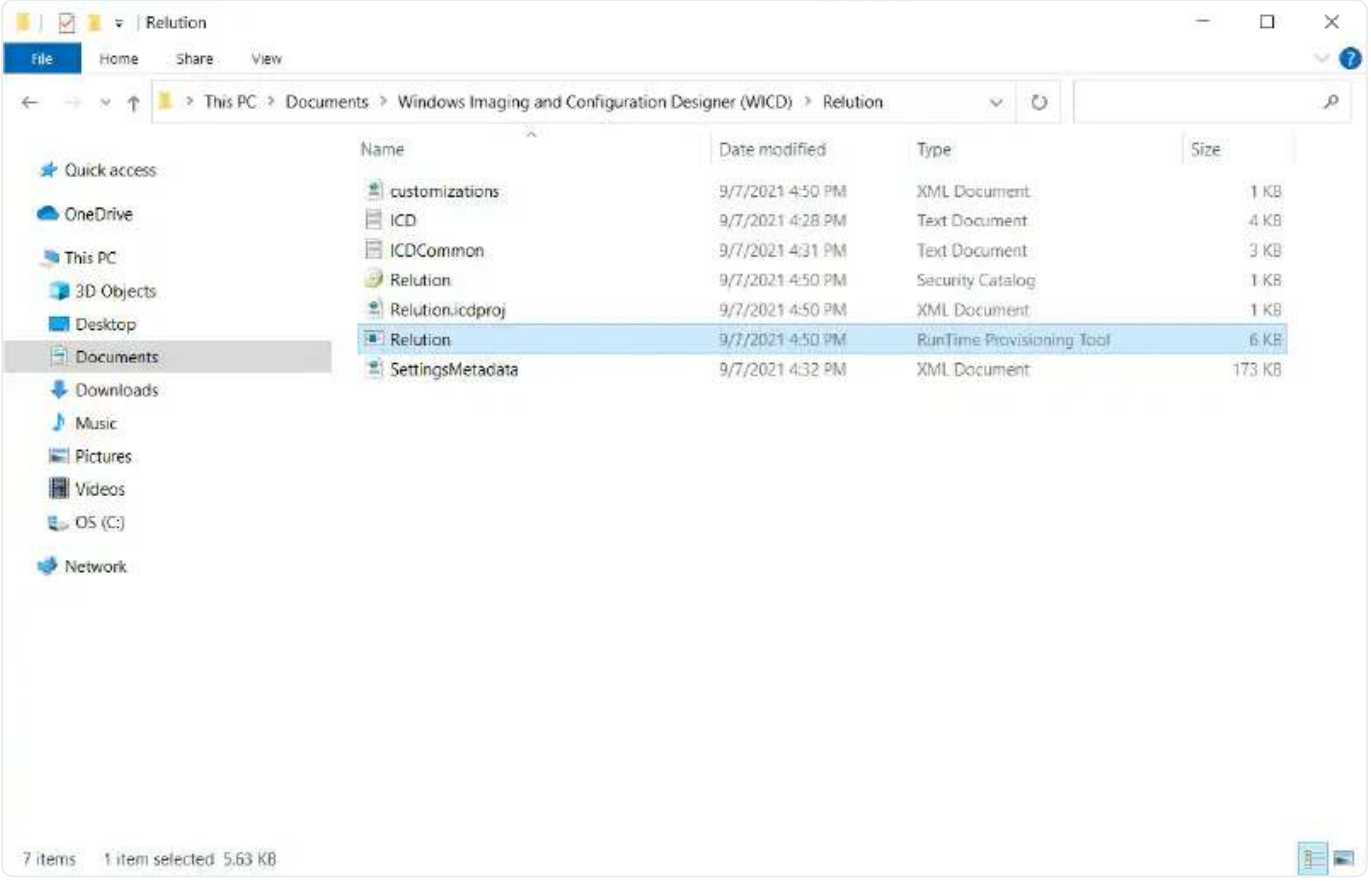
Das Bereitstellungspaket sollte geschützt (verschlüsselt und/oder signiert) werden. Dies bietet einen zusätzlichen Schutz, falls ein USB-Stick oder eine SD-Karte verloren geht. Die Verschlüsselung schützt vor unbefugten Zugriffen auf

die `ppkg`-Datei.






Build
All done!
Provisioning package name: Relution.ppkg
Output location:
C:\Users\Admin\Documents\Windows Imaging and Configuration Designer (WICD)\Relution
Project folder:
C:\Users\Admin\Documents\Windows Imaging and Configuration Designer (WICD)\Relution
Back
Finish

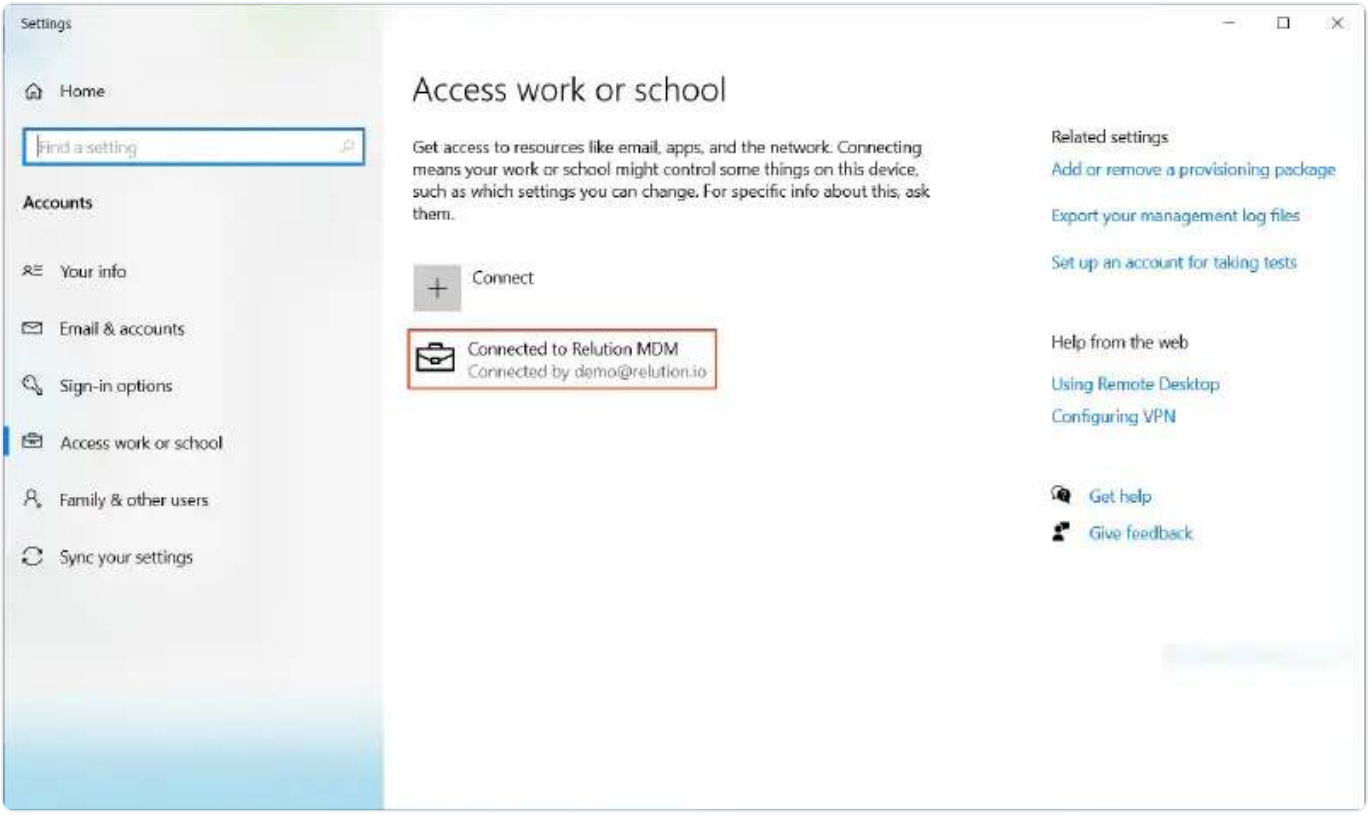

Relution
File
Home
Share
View
This PC > Documents > Windows Imaging and Configuration Designer (WICD) > Relution
Quick access
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
OS (C:)
Network
Name
Date modified
Type
Size
customizations 9/7/2021 4:50 PM XML Document 1 KB
ICD 9/7/2021 4:28 PM Text Document 4 KB
ICDCommon 9/7/2021 4:31 PM Text Document 3 KB
Relution 9/7/2021 4:50 PM Security Catalog 1 KB
Relution.icdproj 9/7/2021 4:50 PM XML Document 1 KB
Relution 9/7/2021 4:50 PM RunTime Provisioning Tool 6 KB
SettingsMetadata 9/7/2021 4:32 PM XML Document 173 KB
7 items
1 item selected 5.63 KB

Anwendung von Bereitstellungspaketen auf Windows 10/11-Geräten

Es reicht völlig aus, die ppkg-Datei mit einem Doppelklick auf dem Gerät zu öffnen und die Dialoge zu bestätigen. Das Gerät ist im Anschluss automatisch eingeschrieben. Auch hier benötigt der Benutzer administrative Berechtigungen, um die Einschreibung auszuführen.

Überprüfen des Bereitstellungspaketes auf eingeschriebenen Windows 10/11-Geräten

Unter `Systemeinstellungen` unter `Geschäfts- oder Schulkonto zugreifen` wird die Verbindung mit dem Relution MDM-Server angezeigt.



Das Konto auf dem Gerät, mit dem das Gerät registriert wurde, darf nicht gelöscht werden.

Autopilot

`Windows Autopilot` ist ein cloudbasiertes Angebot von Microsoft, mit dem sich neue Windows 10/11-Geräte automatisiert einrichten lassen, um sie für den produktiven Einsatz vorzubereiten. Die Windows 10/11-Geräte müssen dabei nicht neu installiert werden, `Windows Autopilot` bedient sich aus dem bereits vorhandenem `Image` auf den Geräten. Relution unterstützt die automatische Einschreibung über `Windows Autopilot` und so lassen sich Windows 10/11-Geräte über diesen Weg schnell und einfach in Relution inventarisieren.

Voraussetzungen für die Nutzung von Windows Autopilot

> Aktuell nur bei eigenem Relution Server möglich.

`Windows Autopilot` kann mit Windows 10/11 Professional, Enterprise oder Education ab der Version 1709 verwendet werden. Für die Nutzung werden eine `Microsoft Entra ID`-Umgebung, eine `Microsoft Entra ID P1 oder P2`-Lizenz sowie eine `Microsoft Intune Plan 1`-Lizenz benötigt. Für die Einrichtung in Microsoft Entra müssen Benutzer über Administratorrechte verfügen, beispielsweise die Rolle `Globaler Administrator`. Laut der Microsoft Dokumentation sollte die `Microsoft Intune Plan 1` Lizenz nicht benötigt werden, allerdings hat sich gezeigt, dass ohne diese Intune nicht verwendbar ist, nur dafür wird diese benötigt.

Bei der Inbetriebnahme der Windows 10/11-Geräte ist eine Internetverbindung zwingend erforderlich, damit die automatische Registrierung und Einrichtung durchgeführt werden kann.

Lizenzanforderungen →

Für Version 26.4.0

Funktionsweise bei der Inbetriebnahme von Windows 10/11-Geräten

Beim Start der `Out Of The Box Experience` (OOBE) der Windows 10/11-Geräte erkennt das System bei einer bestehenden Netzwerkverbindung automatisch, dass es über `Windows Autopilot` konfiguriert werden soll. Die Geräte übermitteln ihre ID an Microsoft und prüfen, ob es in `Autopilot` für eine `Entra ID`-Umgebung registriert wurde. Anschließend müssen sich die Benutzer mit ihren Zugangsdaten auf der Microsoft-Anmeldeseite anmelden. Durch die Anmeldung wird die Einschreibung in Relution durchgeführt und ein Benutzerkonto für die `Entra ID`-Benutzer auf den Geräten angelegt.

Vorteile von Windows Autopilot

`Windows Autopilot` hat zum Ziel, neue Windows 10/11-Geräte nicht mehr umständlich einzeln mit einem intern erstellten `Image` bespielen zu müssen, sondern die Geräte sollen sich möglichst selbständig in vorkonfigurierte Geräte verwandeln. Das minimiert den Aufwand für die `Image`-Erstellung und reduziert die erforderliche Zeit für die physische Registrierung und Bereitstellung der Geräte. Entra muss hierzu nur einmal eingerichtet werden und die automatische Registrierung funktioniert solange, bis das definierte Gültigkeitsdatum des `Geheimen Clientschlüssel` abläuft (siehe Microsoft Entra ID verknüpfen →).

Entra Join

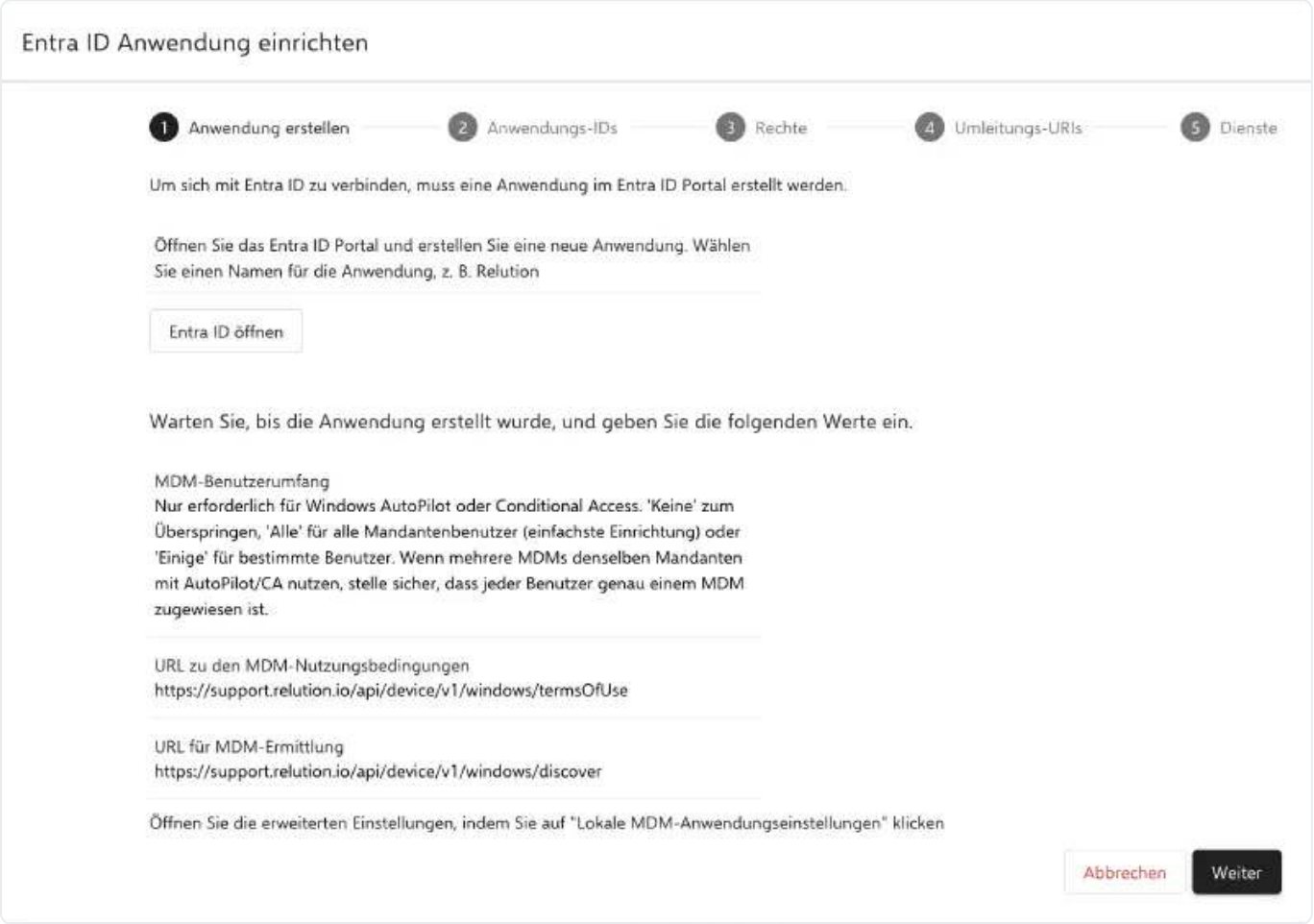
Im Unterschied zu `Windows Autopilot` dient `Entra Join` nicht der automatischen Ersteinrichtung eines Geräts, sondern der Verbindung des Geräts mit der Unternehmensumgebung. `Windows Autopilot` wird genutzt, um neue Geräte automatisiert bereitzustellen und einzurichten, während `Entra Join` das Gerät mit dem Benutzer von `Microsoft Entra ID` verbindet.

Diese benutzerbezogene Alternative zu Windows Autopilot ermöglicht es den eigenen Entra Benutzern, jedes Windows Gerät einzuschreiben. Dazu wird das Gerät über `Einstellungen` → `Konten` → `Auf Arbeits- oder Schulkonto zugreifen` → `Verbinden` → `Dieses Gerät mit Microsoft Entra ID verknüpfen` mit Entra ID verknüpft, anschließend erfolgt die Anmeldung mit den Microsoft-Benutzerdaten. Werden im Dialog Verbinden direkt die Anmeldedaten eingegeben, wird das Gerät nur in Entra ID registriert (ohne Verknüpfung). Dieser Ablauf wird von Relution nicht unterstützt und mit einer Fehlermeldung abgebrochen.

Hinzufügen der MDM Anwendung in Entra

Die MDM-Anwendung wird im Rahmen der Verknüpfung von Relution mit Entra ID → angelegt: Unter `Einstellungen` → `Benutzerverwaltung` → `Entra ID` liefert der erste Schritt Anwendung erstellen der Relution-Anleitung die benötigten Angaben. Danach wird die Verknüpfung mit Anwendungs-ID und Verzeichnis-ID dieser Anwendung im Schritt Anwendungs-IDs fortgesetzt. Es kann entweder die bestehende MDM-Anwendung in Microsoft Entra verwendet werden oder eine angelegt werden und mit den Angaben aus der Relution-Anleitung vollständig konfiguriert werden.

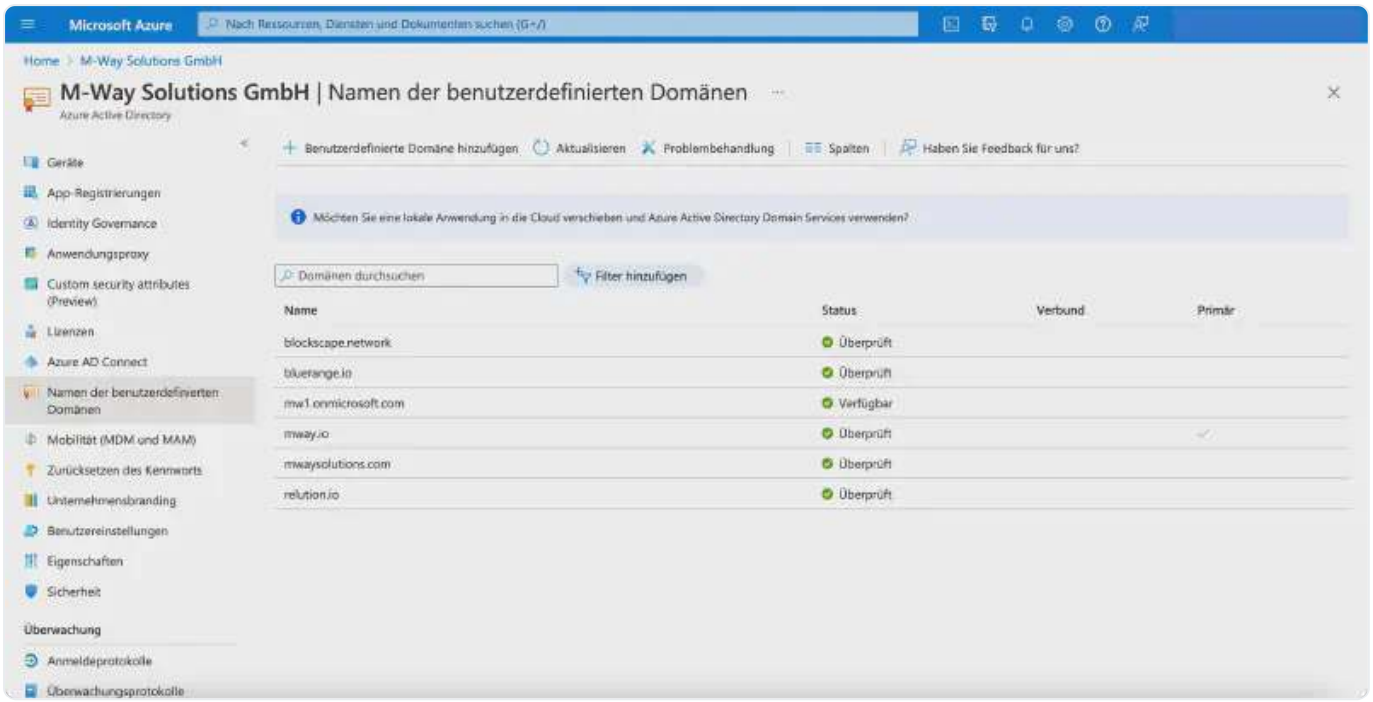
Für Version 26.4.0



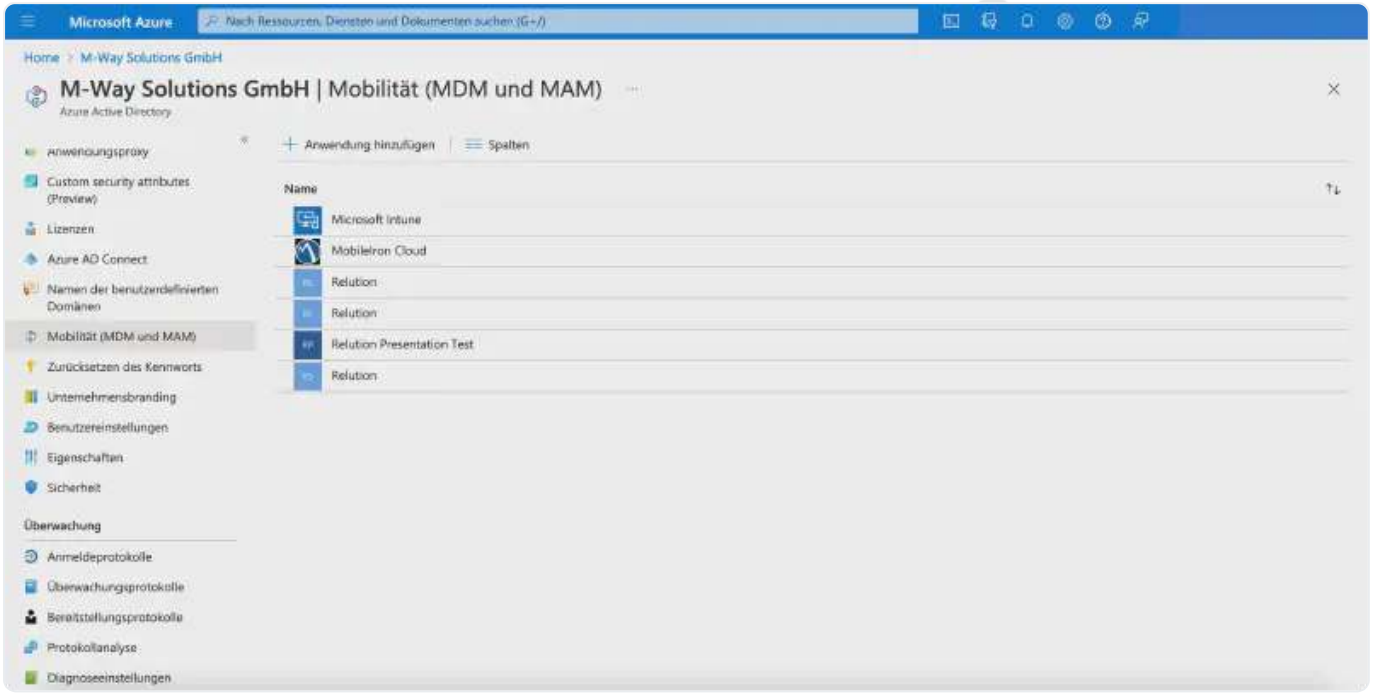
Für Version

Die Domäne des entsprechenden Relution-Servers in `Microsoft Entra ID` unter `Namen der benutzerdefinierten Domänen` hinzufügen. Dies kann einige Zeit in Anspruch nehmen. Weitere Informationen sind in der Microsoft-Dokumentation zu finden.

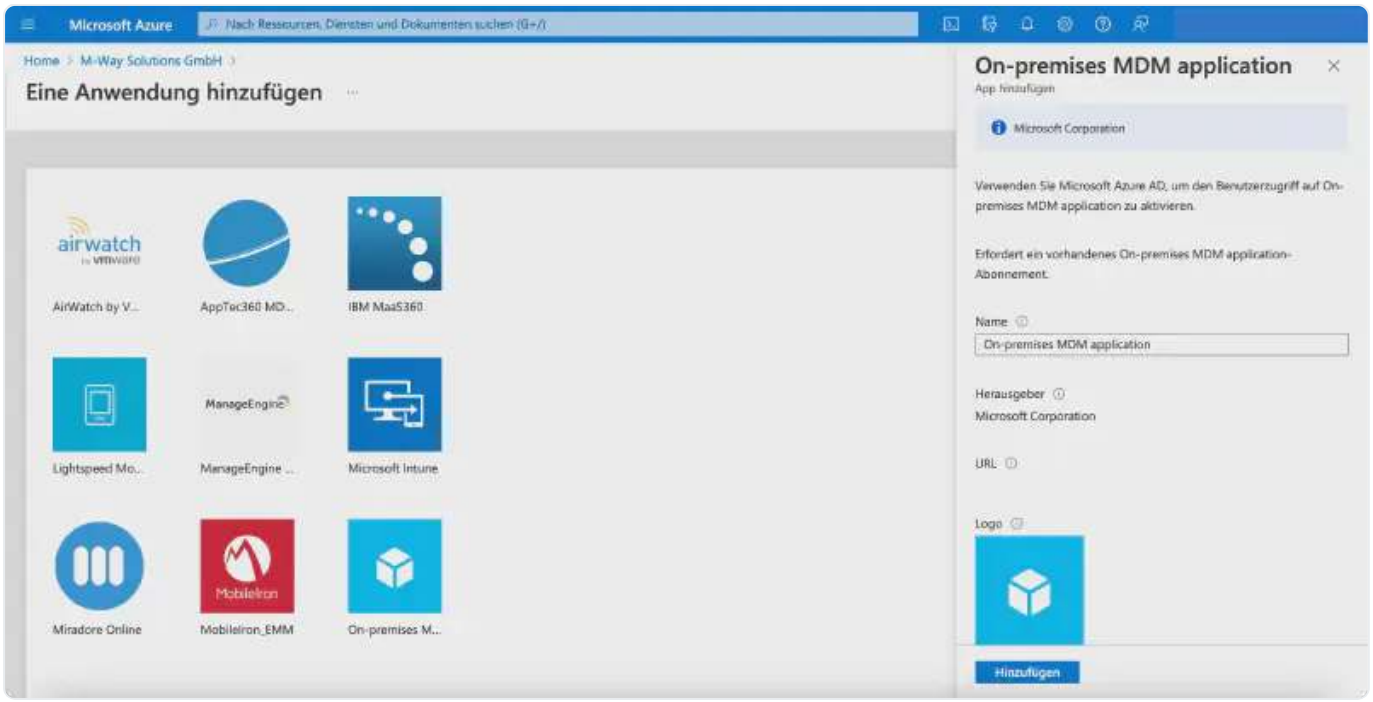
Microsoft Dokumentation →



Unter `Mobilität (MDM und MAM)` wird anschließend die gewünschte MDM-Anwendung hinzugefügt und aktiviert:



1. Die Kachel `On-Premises MDM Applikation` unten rechts wählen.
2. Einen Namen vergeben.
3. Auf `Hinzufügen` klicken.



Nun wird die neue MDM-Anwendung mit den Angaben der Relution-Anleitung konfiguriert:

1. Für `MDM-Benutzerbereich` die gewünschte Einstellung wählen.
2. Die URL zu den `MDM-Nutzungsbedingungen` aus Relution eintragen:

   ```
   https://serverurl/api/device/v1/windows/termsOfUse
   ```

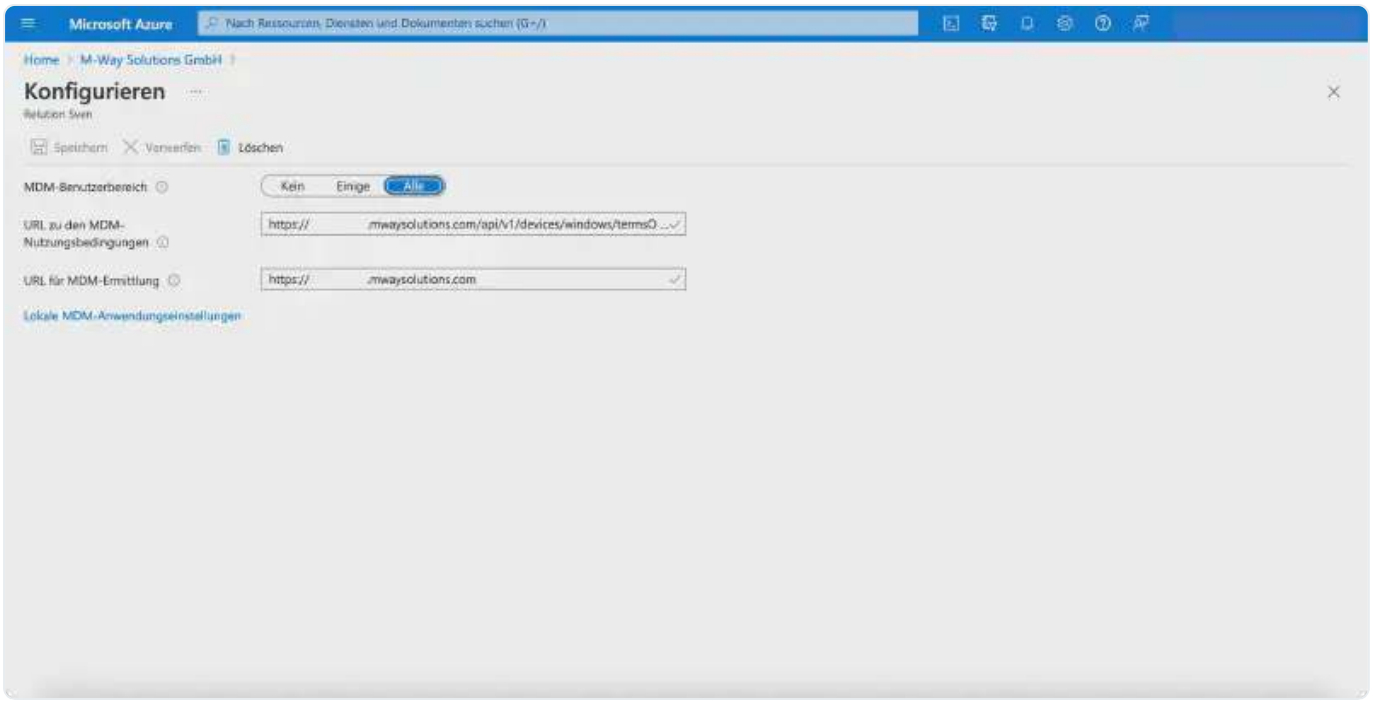
   Microsoft fragt diese URL vor jeder Einschreibung ab. Es wird keine Webseite aufgerufen.

3. Die URL für MDM-Ermittlung eintragen:

   ```
   https://serverurl/api/device/v1/windows/discover
   ```

4. Auf `Speichern` klicken.

Version 26.4.0

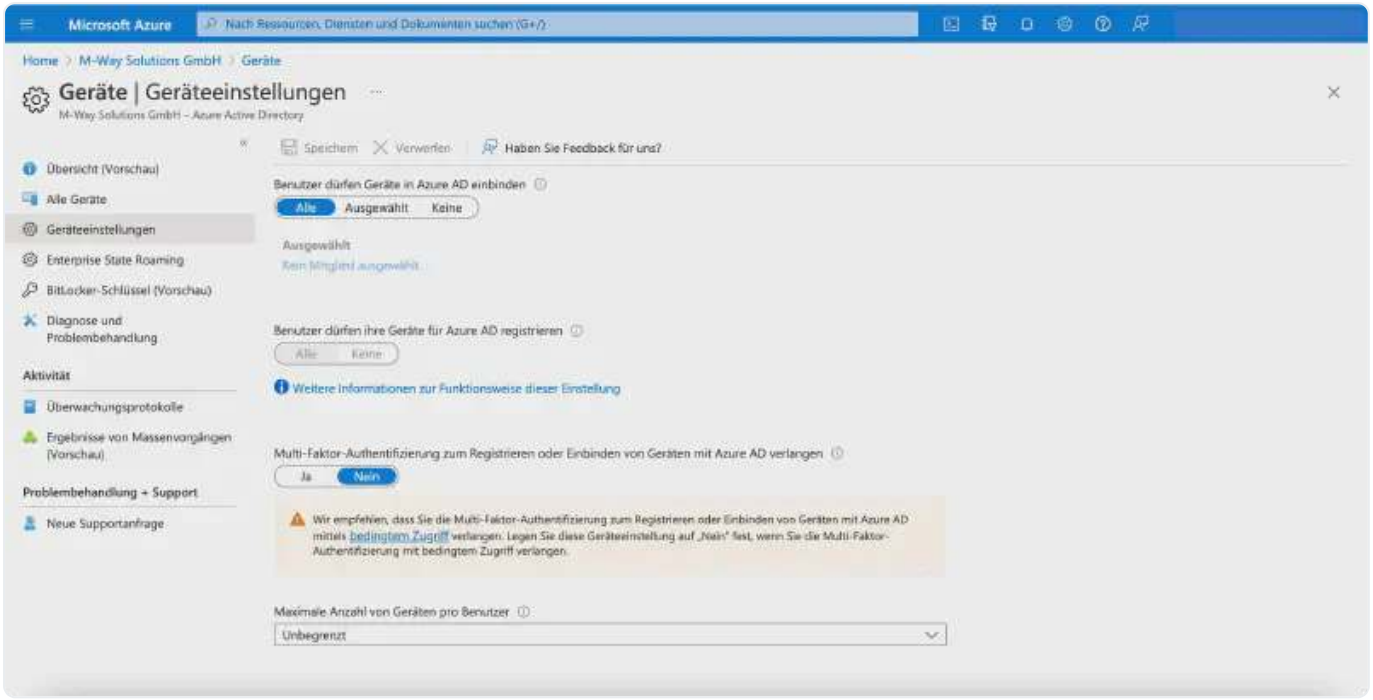


Überprüfen der Entra-Standardeinstellungen und Abschließen der Einrichtung

Für Version 26.4.0

Nach Abschluss der Verknüpfung von Entra ID mit Relution → ist zu prüfen, ob unter `Geräte` → `Geräteeinstellungen` folgende Punkte konfiguriert wurden, um somit Entra Join zu ermöglichen. Für Windows Autopilot kann dieser Schritt übersprungen werden.

- Alle Benutzer dürfen Geräte in `Microsoft Entra ID` einbinden.
- Alle Benutzer dürfen ihre Geräte für `Microsoft Entra ID` registrieren.
- Maximale Anzahl von Geräten pro Benutzer sollte beachtet werden.



Hinzufügen von Windows 10/11-Geräten

Diese Schritte ersetzen die früher notwendigen Schritte im Microsoft Store for Business.

Neue Geräte können über einen Partner beschafft und registriert werden. Über diesen Weg werden die Geräte automatisch in das Intune Portal und in `Microsoft Entra ID` hinterlegt und müssen nicht selbst manuell eingepflegt werden.

Bereits in Betrieb genommene Geräte lassen sich manuell hinzufügen. Dazu wird eine `CSV`-Datei benötigt, die per PowerShell-Skript auf den Geräten erzeugt wird. Anschließend wird die CSV-Datei im Intune-Portal → hochgeladen und das Gerät kann zurückgesetzt werden.

Die Datei kann mit diesem Script mittels Powershell erzeugt werden:

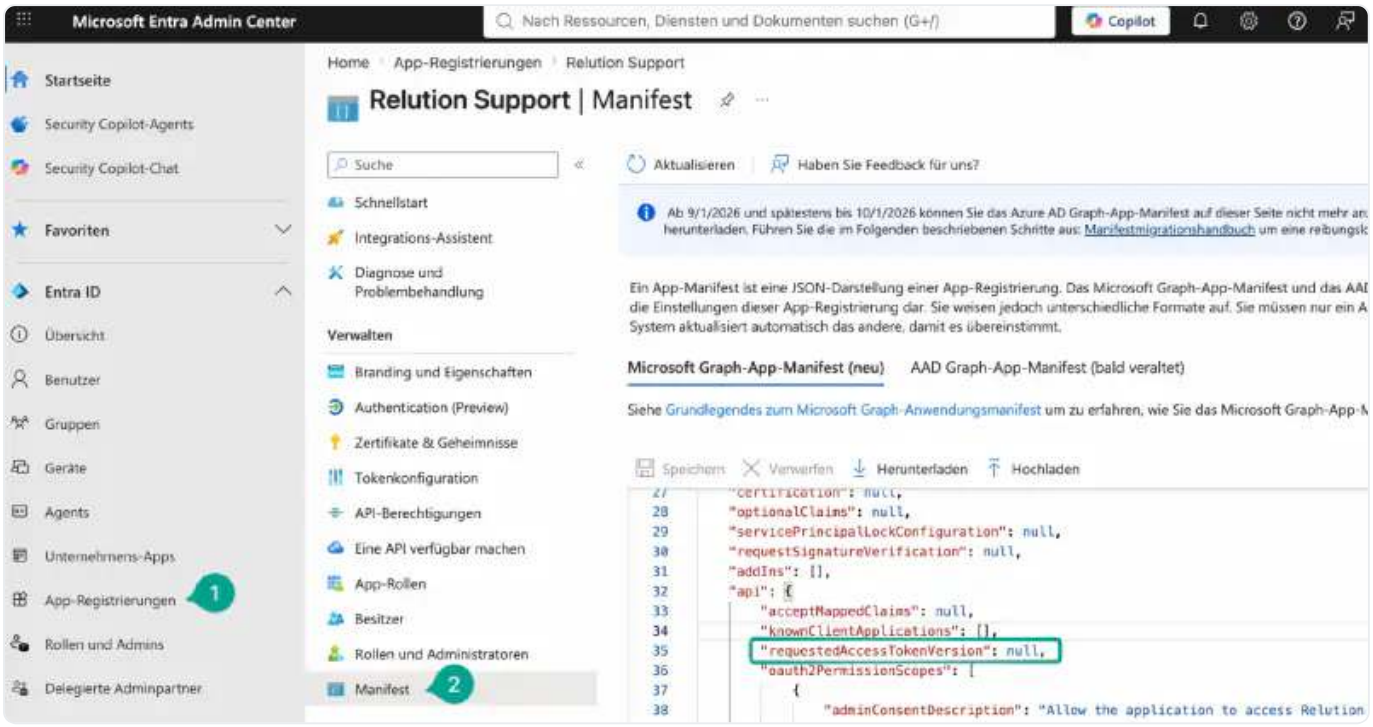
```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
New-Item -Type Directory -Path "C:\HWID"
Set-Location -Path "C:\HWID"
$env:Path += ";C:\Program Files\WindowsPowerShell\Scripts"
Set-ExecutionPolicy -Scope Process -ExecutionPolicy RemoteSigned
Install-Script -Name Get-WindowsAutopilotInfo
Get-WindowsAutopilotInfo -OutputFile AutopilotHWID.csv
```

Die Powershell muss als Administrator ausgeführt werden.

Die Datei muss dann unter `Geräte` → `Registrierung` (Suche, Ergebnis auswählen) → nach unten scrollen → `Geräte` → `Importieren` hochgeladen werden.

Die Geräte erscheinen anschließend in der Geräteliste und müssen mit einem konfigurierten Profil verknüpft werden.

> Wurde die Entra ID-Anwendung nach dem 1. Juli 2026 erstellt, ist gegebenenfalls eine zusätzliche Anpassung erforderlich, falls Geräte während der OOBE den Fehler anzeigen, dass keine Verbindung zur URL der MDM-Nutzungsbedingungen hergestellt werden kann. In diesem Fall wird im Manifest der Anwendung der Eintrag `requestedAccessTokenVersion` auf `null` gesetzt (`"requestedAccessTokenVersion": null,`).



Vorbereitung der Out Of The Box Experience (OOBE) bei Microsoft

Für Version 26.4.0

Nun muss noch ein Profil erzeugt werden.

Dazu wieder in die Suche der Funktionen wechseln. Also links auf `Geräte` → `Registrierung` (Suche) → nach unten scrollen → `Bereitstellungsprofile` klicken.

1. Auf Profil erstellen klicken.
2. Windows PC wählen.
3. Einen Namen vergeben.
4. Weiter klicken.
5. Erneut auf Weiter klicken.
6. Entweder Gruppe hinzufügen oder Alle Geräte hinzufügen wählen.
7. Auf Weiter klicken.
8. Auf Erstellen klicken.

Die Geräte sind nun mit dem Profil verknüpft.

Hinterlegte Windows 10/11-Geräte in Relution synchronisieren

Unter `Geräte` → `Auto-Einschreibungen` werden die Windows 10/11-Geräte über die Schaltfläche Geräte synchronisieren in Relution hinzugefügt. Voraussetzung ist, dass in der Entra-ID-Verknüpfung die Option Autopilot Geräte synchronisieren aktiviert ist (Schritt Dienste der Relution-Anleitung). Die Geräte dürfen zu diesem Zeitpunkt noch nicht eingeschrieben sein.

Im selben Schritt befindet sich die Option Autopilot-Registrierung aktivieren, die für Windows Autopilot aktiviert bleiben sollte. Bei einer neuen Verknüpfung sind beide Optionen standardmäßig aktiviert.

Zusätzlich synchronisiert Relution die Autopilot-Geräte automatisch, standardmäßig alle 24 Stunden. Geräte, die nicht mehr in Windows Autopilot registriert sind, werden dabei aus den Auto-Einschreibungen entfernt.

Erst wenn Windows 10/11-Geräte in der Übersicht erscheinen, kann eine automatische Einschreibung über Windows Autopilot durchgeführt werden.

Automatische Einschreibung von Windows 10/11-Geräten in Relution

Für Version 26.4.0

Nach Zurücksetzen der Geräte oder bei erstmaliger Inbetriebnahme wird im OOBE die Netzwerkverbindung hergestellt. Sobald dies geschehen ist, kommunizieren die Geräte mit Microsoft und laden das `Autopilot`-Profil herunter.

Daraufhin erscheint der Anmeldebildschirm für das Microsoft-Konto. Nachdem Benutzer ihre Anmeldedaten eingegeben haben, findet die Kommunikation mit Relution statt. Es wird zunächst der Nutzungsbedingungs-Endpunkt aufgerufen, und daraufhin findet die Einschreibung in Relution statt.

Voraussetzung ist, dass in Relution genau ein Benutzer existiert, dessen E-Mail-Adresse dem Entra-Anmeldenamen (UPN) entspricht, und dass für das Gerät eine Auto-Einschreibung vorhanden ist. Ist der Auto-Einschreibung ein Benutzer zugewiesen, kann nur dieser die Einschreibung durchführen. Anschließend erscheinen die Windows 10/11-Geräte im Geräteinventar der Organisation dieses Benutzers und können über Windows-Richtlinienkonfigurationen und Aktionen weiter konfiguriert werden.

Wird ein über Windows Autopilot eingeschriebenes Gerät in Relution gelöscht, lässt es sich über dieselbe Auto-Einschreibung erneut einschreiben, auch wenn es sich noch im Papierkorb befindet.

Das Konto auf dem Gerät, mit dem das Gerät registriert wurde, nicht löschen.

Verfügbare Aktionen

Mit Relution können IT-Administratoren eine Vielzahl von Remote-Aktionen auf Windows-Geräten ausführen. Diese Funktionen unterstützen die zentrale Verwaltung, erhöhen die Sicherheit und vereinfachen die Bereitstellung sowie das Troubleshooting im Unternehmens- oder Bildungsumfeld. Die Aktionen lassen sich gezielt auf ein einzelnes Gerät oder über die Mehrfachauswahl in der Geräteliste auf mehrere Geräte gleichzeitig anwenden. Zusätzlich können sie über die Mitgliedschaft in Gerätegruppen ereignis- oder zeitgesteuert ausgelöst werden: Aktionen mit Gerätegruppen →

Der Aktionsdialog wird unter `Geräte` → `Inventar` über Aktion anwenden geöffnet, entweder für die in der Liste ausgewählten Geräte oder in der Detailansicht eines Geräts. Nachfolgend sind alle aktuell unterstützten Geräteaktionen für Windows-Geräte in Relution aufgeführt:

Für Version 26.4.0

Geräteaktionen

Aktion	Beschreibung
App entfernen	Funktion: Deinstallation ausgewählter Apps vom Gerät. Entfernen lassen sich MSI-, EXE- und WinGet-Apps aus dem Relution Store. Laut Hinweis im Aktionsdialog erfolgt die Deinstallation nur für den aktuell verwalteten Benutzer; für andere Benutzer bleiben die Apps sichtbar und nutzbar. Einsatzbereich: Entfernung veralteter oder unerwünschter Apps von verwalteten Windows-Unternehmensgeräten. Voraussetzung: Relution Companion; ab Windows 10 Version 1511, nicht für Windows Home.
Benutzerkonten hinzufügen	Funktion: Hinzufügen neuer lokaler Benutzerkonten zum Gerät. Je Konto werden Benutzername und Passwort angegeben; über den Schalter Administrator erhält das Konto Administratorrechte. Erfüllt das Passwort die Komplexitätsanforderungen des Geräts nicht, wird das Konto nicht angelegt. Einsatzbereich: Einrichtung zusätzlicher Nutzerprofile, z. B. für wechselnde Benutzer in Bildungseinrichtungen oder Unternehmen. Voraussetzung: Ab Windows 10 Version 1803, nicht für Windows Home.
Bitlocker aktivieren	Funktion: Aktiviert BitLocker auf einem oder mehreren Laufwerken und startet die Verschlüsselung. Je Laufwerk werden der Laufwerksbuchstabe (z. B. `C:`) und der Schutzschlüssel angegeben: Wiederherstellungspasswort oder TPM (nur für das Betriebssystem-Laufwerk). Mit Nur genutzter Speicherplatz wird nur der belegte Speicherplatz statt des gesamten Laufwerks verschlüsselt. Einsatzbereich: Schutz sensibler Daten durch Laufwerksverschlüsselung. Zusatzinformation: Wird Wiederherstellungspasswort als Schutzschlüssel gewählt, wird das Passwort automatisch erzeugt und in den Gerätedetails in Relution gespeichert. Voraussetzung: Relution Companion.
Bitlocker deaktivieren	Funktion: Deaktiviert BitLocker (Verschlüsselung) auf einem oder mehreren Laufwerken. Einsatzbereich: Entfernt den Schutz vom Gerät, indem die angegebenen Laufwerke entschlüsselt werden. Voraussetzung: Relution Companion.
Gerät auf Werkszustand zurücksetzen	Funktion: Zurücksetzen des Geräts auf Werkszustand und Löschen aller Daten. Einsatzbereich: Neuaufsetzen eines Geräts vor der Weitergabe oder bei Problemen. Achtung: Dieser Vorgang löscht sämtliche Daten unwiderruflich! Voraussetzung: Ab Windows 10 Version 1709, auch für Windows Home.
Gerät neu starten	Funktion: Führt einen Neustart des Geräts durch. Einsatzbereich: Übernahme von Änderungen nach Installationen oder Konfigurationen, Behebung von Problemen.
Gerät orten	Funktion: Ermittelt den aktuellen Standort des Geräts. Einsatzbereich: Auffinden verloren gegangener oder gestohlener Geräte. Hinweis: Aktive Internetverbindung und aktivierte Ortungsdienste erforderlich.
Gerät Scannen	Funktion: Startet einen Sicherheits-Scan des Geräts mit dem integrierten Microsoft Defender, um nach Schadsoftware und Sicherheitsbedrohungen zu suchen. Über Scan Typ wird zwischen Schnell Scan und Vollständiger Scan gewählt. Einsatzbereich: Gewährleistung der Sicherheit von Unternehmensgeräten, Erkennung und Beseitigung potenzieller Bedrohungen, Überprüfung der Einhaltung von Sicherheitsrichtlinien.

Aktion	Beschreibung
	Hinweis: Microsoft Defender ist die in Windows integrierte Antiviren-Software. Voraussetzung: Ab Windows 10 Version 1809, auch für Windows Home.
Geräteinformationen aktualisieren	Funktion: Aktualisierung der in Relution gespeicherten Geräteinformationen. Einsatzbereich: Sicherstellung aktueller Geräteinformationen in Relution.
Office 365 installieren	Funktion: Installation von Office 365 for Business auf dem Gerät. Mit Office 365 Installation wird eine Konfiguration XML hochgeladen, die im Microsoft 365 Apps Admin Center (`config.office.com`) erstellt wird. Mit Office-Installationsdaten löschen werden die Installationsdaten auf dem Gerät entfernt, damit eine fehlgeschlagene Installation erneut versucht werden kann; optional wird dabei die installierte Office-Suite deinstalliert, ohne dass Dateien verloren gehen. Einsatzbereich: Einfache Bereitstellung von Office 365 auf Unternehmensgeräten. Voraussetzung: Ab Windows 10 Version 1703, nicht für Windows Home.
Passwort zurücksetzen (Windows)	Funktion: Setzt das Passwort eines lokalen Benutzerkontos auf dem Gerät auf ein neues Passwort. Angegeben werden der Benutzername und das neue Passwort. Einsatzbereich: Unterstützung bei vergessenen oder gesperrten Passwörtern. Voraussetzung: Relution Companion.
PowerShell-Skript ausführen	Funktion: Ausführung eines in Relution verwalteten PowerShell-Skripts auf dem Gerät. Optional werden Argumente für die Befehlszeile, Umgebungsvariablen und eine Zeitüberschreitung (in Minuten) festgelegt. Einsatzbereich: Automatisierung komplexer Aufgaben und Konfigurationen. Hinweis: PowerShell-Kenntnisse erforderlich. Voraussetzung: Relution Companion; ab Windows 10 Version 1511, nicht für Windows Home.
Relution Store App bereitstellen	Funktion: Bereitstellung einer App aus dem Relution Store auf dem Gerät. Zur Auswahl stehen App vom Microsoft Store installieren, MSI-App installieren, Exe installieren und Winget-App installieren; für jeden Typ ist eine eigene Berechtigung erforderlich. Die Apps werden systemweit installiert, WinGet-Apps dagegen für den angemeldeten Benutzer. Einsatzbereich: Einfache Verteilung von Unternehmens-Apps auf Windows-Geräten. Voraussetzung: Ab Windows 10 Version 1511, nicht für Windows Home. MSI-, EXE- und WinGet-Apps erfordern den Relution Companion.

Voraussetzungen

Mehrere Aktionen werden ausschließlich vom Relution Companion für Windows → ausgeführt: App entfernen, Bitlocker aktivieren, Bitlocker deaktivieren, Passwort zurücksetzen (Windows), PowerShell-Skript ausführen sowie die Bereitstellung von MSI-, EXE- und WinGet-Apps über Relution Store App bereitstellen.

Einige Aktionen setzen eine Mindestversion und Edition von Windows voraus. Der Aktionsdialog kennzeichnet die unterstützten Editionen mit Badges. Auf Windows Home stehen App entfernen, Benutzerkonten hinzufügen, Office 365 installieren, PowerShell-Skript ausführen und Relution Store App bereitstellen nicht zur Verfügung: Einschränkungen der Windows Home Edition →

Verfügbare Konfigurationen

Eine Richtlinie ist eine Sammlung einer oder mehrerer Konfigurationen. Jede Richtlinie kann auf einem oder auf mehreren Geräten gleichzeitig angewendet werden. Zudem können mit jedem Gerät eine oder mehrere Richtlinien verknüpft sein.

Für Version 26.4.0

Verfügbare Konfigurationen

Konfiguration	Beschreibung
Antivirus	Verwaltung der Antivirus-Einstellungen
App Konformität	Verwaltung appspezifischer Einschränkungen (ab Windows 10 Version 1511, nicht für Windows Home)
App-Kontrolle →	Verwaltung von Windows Defender Application Control (WDAC)-Richtlinien (ab Windows 10 Version 1903, nicht für Windows Home)
Benutzerdefinierte CSP →	Zusammenfassung beliebiger CSP-Einstellungen in einer Konfiguration
Bitlocker →	Konfiguration der Festplattenverschlüsselung (Enterprise und Education ab Windows 10 Version 1703, Pro ab Version 1809, nicht für Windows Home)
BranchCache	Konfiguration des BranchCache-Inhaltscachings (ab Windows 10 Version 2004, nicht für Windows Home)
E-Mail	Hinzufügen von E-Mail-Konfigurationen für mehrere Benutzer
Exchange →	Verwaltung von Exchange-Konten
Gerätename →	Konfiguration des Gerätenamens
Globale Proxies	Konfiguration globaler Proxies (ab Windows 10 Version 1703, nicht für Windows Home)
Hintergrundbild	Verwaltung des Hintergrundbilds (ab Windows 10 Version 1709, nicht für Windows Home)
Passwort →	Verwaltung der Passwortrichtlinien
Remotedesktopdienst	Verwaltung des Remotedesktopdienstes
Restriktionen →	Verwaltung der Geräterestriktionen
Script →	Automatische Skriptausführung nach Ereignissen oder Zeitplänen über den Relution Companion
Shared PC →	Verwaltung der Windows-Richtlinie für Shared PC
Sicherheitsoptionen für lokales Gerät	Verwaltung der Richtlinien für lokale Gerätesicherheitsoptionen
Startmenü	Personalisierung des Startmenüs (ab Windows 10 Version 1703, nicht für Windows Home)
VPN →	Verwaltung von VPN-Einstellungen (ab Windows 10 Version 1607, auch für Windows Home)
Windows Companion →	Verhalten des Relution Companion für Windows: Logging, App-Handling, Server-Kommunikation und automatischer Gerätebenutzerwechsel

Konfiguration	Beschreibung
Windows Firewall →	Verwaltung der Windows-Firewall-Einstellungen (ab Windows 10 Version 1709, nicht für Windows Home)
Windows Hello →	Verwaltung der Windows-Hello-Konfiguration
Windows Kiosk-Modus →	Verwaltung der Kiosk-Modus-Einstellungen
Windows Lizenzierung	Verwaltung der Windows-Lizenzierungsrichtlinie
Windows Office →	Bereitstellung von Microsoft Office über eine extern erzeugte Konfigurations-XML (ab Windows 10 Version 1703, nicht für Windows Home)
Windows Update →	Verwaltung der Windows-Update-Richtlinie (ab Windows 10 Version 1607, nicht für Windows Home)
WLAN →	Verwaltung der WLAN-Einstellungen
Zertifikat →	Auswahl eines Zertifikats, das standardmäßig auf dem Gerät installiert wird

Die Konfigurationen App-Kontrolle, Benutzerdefinierte CSP, E-Mail, Exchange, Script, VPN, WLAN und Zertifikat können mehrfach in einer Richtlinie angelegt werden, alle übrigen jeweils nur einmal. Ist eine nur einmal erlaubte Konfiguration bereits in der Richtlinie enthalten, wird sie im Auswahldialog nicht mehr angeboten.

Im Auswahldialog weisen Badges auf die unterstützten Windows-Editionen und die jeweilige Mindestversion hin; die Angaben in Klammern geben diese Badges wieder. Weitere Einschränkungen der Home-Edition beschreibt der Artikel Einschränkungen der Windows Home Edition →

Die Konfigurationen Script und Windows Companion werden vom Relution Companion für Windows → umgesetzt.

Für Version 26.4.0

App-Kontrolle

Seit der Version `5.24.0` ist in Relution die Konfiguration App-Kontrolle verfügbar. Hiermit lassen sich Windows Defender Anwendungssteuerungs-Richtlinien (WDAC-Richtlinien) auf Windows-Geräten anwenden. Diese definieren, welchen Anwendungen vertraut wird, sodass nur diese auf dem Gerät ausgeführt werden können. Die Konfiguration wird auf Windows Pro, Enterprise und Education ab Version 1903 unterstützt.

Microsoft stellt alle notwendigen Informationen über WDAC-Richtlinien in deren Dokumentation → bereit.

Generierung der WDAC-Richtlinie

Die Konzeption und Erstellung der WDAC-Richtlinien erläutert Microsoft im Entwurfshandbuch →.

Es wird empfohlen, jegliche WDAC-Richtlinien ausgiebig zu testen, bevor diese über Relution an Produktiv-Geräte ausgerollt werden.

> Es muss sichergestellt werden, dass die *Relution Windows Companion* Applikation durch die festgelegten Regeln nicht blockiert oder eingeschränkt wird.

Für Version 26.4.0

Erstellung der benötigten WDAC-Richtlinie Datei

Für die Generierung können der WDAC Assistent → und die Beispiel Basisrichtlinien → verwendet werden.

Wird für die Generierung das WDAC-Assistenten-Tool verwendet, erzeugt dieses zwei Dateien: eine XML-Datei und eine CIP-Datei. Die MDM-Schnittstelle benötigt die Richtlinie als Binär-Datei. Die CIP-Datei liegt bereits in diesem Binärformat vor und kann direkt in Relution hochgeladen werden. Die XML-Datei muss zuerst in eine Binär-Datei umgewandelt werden; wie das geht, wird in den folgenden Abschnitten erläutert.

XML-Datei

Die WDAC-Richtlinien XML-Datei enthält zwei Informationen, die für das erfolgreiche Anwenden der Konfiguration auf den Windows Geräten über Relution entscheidend sind.

AllowAll.xml

File | C:/Windows/schemas/CodeIntegrity/ExamplePolicies/AllowAll.xml

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<SiPolicy xmlns="urn:schemas-microsoft-com:sipolicy" PolicyType="Base Policy">
   <VersionEx>1.0.3.0</VersionEx>
   <PolicyID>{31351756-3F24-4963-8380-4E7602335AAE}</PolicyID>
   <BasePolicyID>{31351756-3F24-4963-8380-4E7602335AAE}</BasePolicyID>
   <PlatformID>{2E07F7E4-194C-4D20-B7C9-6F44A6C5A234}</PlatformID>
 ▶<Rules>
   ...
   </Rules>
   <!-- EKUS -->
   <EKUs/>
   <!-- File Rules -->
 ▶<FileRules>
   ...
   </FileRules>
   <!-- Signers -->
   <Signers/>
   <!-- Driver Signing Scenarios -->
 ▶<SigningScenarios>
   ...
   </SigningScenarios>
   <UpdatePolicySigners/>
   <CiSigners/>
   <HvciOptions>0</HvciOptions>
 ▶<Settings>
   ...
   </Settings>
 </SiPolicy>
```

Für Version

Die `<PolicyID>` ist eine GUID, welche diese WDAC-Richtlinie eindeutig identifiziert. Sie wird daher für das Anwenden, Aktualisieren und Löschen der Konfiguration verwendet.

Die `<VersionEx>` wird als Versionierung für die WDAC-Richtlinie verwendet. Für jede Aktualisierung einer WDAC-Richtlinie muss `<VersionEx>` daher erhöht werden. Ist die Version kleiner als die zuletzt angewendete, lehnt Windows die Richtlinie ab und das Update der Konfiguration über Relution schlägt fehl.

Konvertierung der XML-Datei

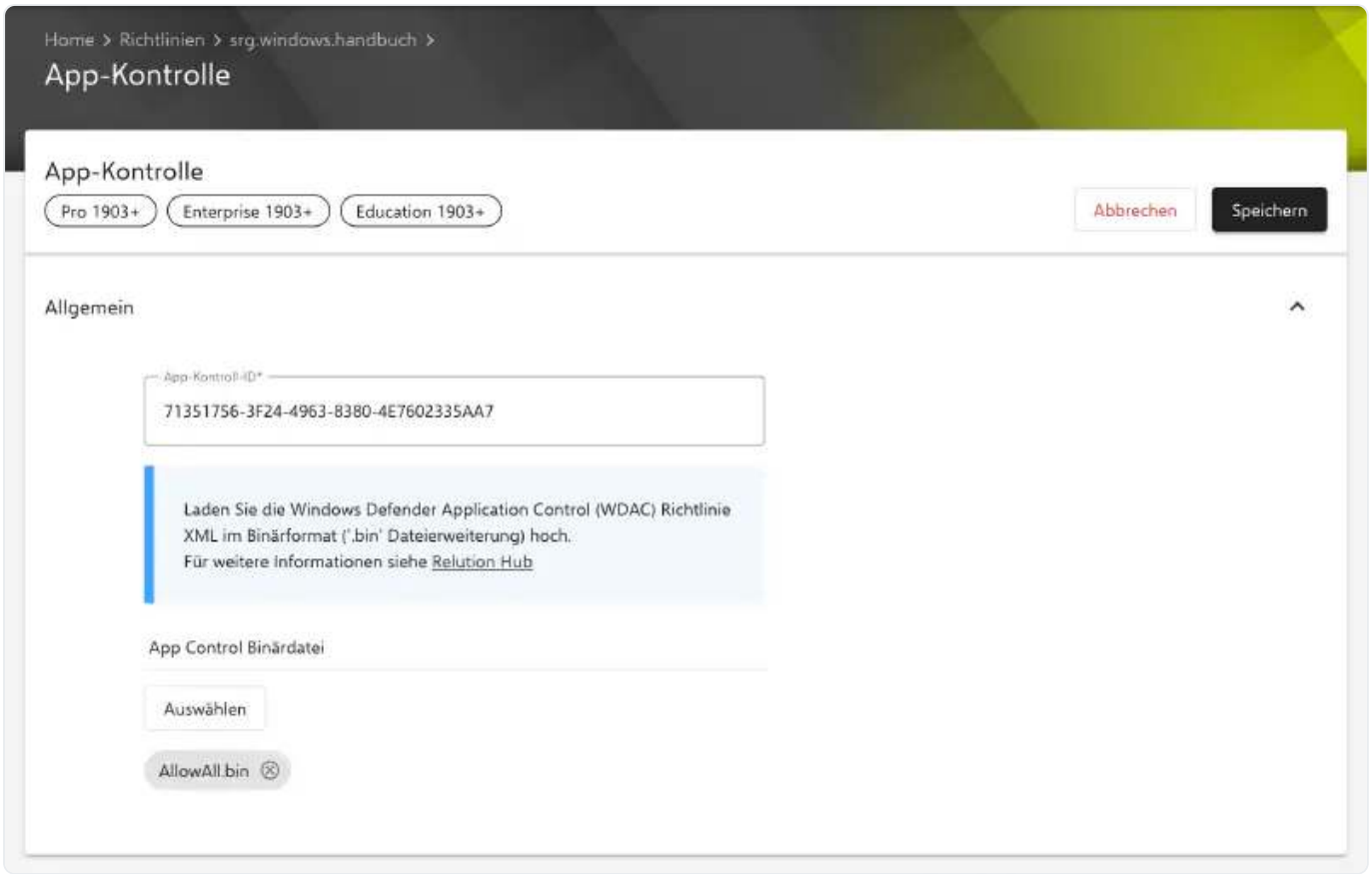
Die XML-Datei muss in eine Binär-Datei umgewandelt werden. Dies kann mit dem ConvertFrom-CIPolicy → PowerShell-Befehl gemacht werden.

Beispiel:

```
ConvertFrom-CIPolicy -XmlFilePath .\AllowAll.xml -BinaryFilePath .\AllowAll.bin
```

Die dadurch generierte Binär-Datei kann in der Konfiguration App-Kontrolle in Relution hochgeladen werden.

Konfiguration App-Kontrolle



Die Konfiguration App-Kontrolle besteht aus zwei Pflichtfeldern:

- Feld App-Kontroll-ID: Damit die Konfiguration erfolgreich auf dem Gerät angewendet werden kann, muss die App-Kontroll-ID denselben Wert wie die `<PolicyID>` aus der WDAC-Richtlinie enthalten, jedoch ohne die geschweiften Klammern. Erwartet wird eine GUID im Format `XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX`, andere Eingaben werden als ungültig markiert.
  - Beispiel:
    - PolicyID in der WDAC-Richtlinie: `<PolicyID>{31351756-3F24-4963-8380-4E7602335AAE}</PolicyID>`
    - App-Kontroll-ID in der Konfiguration: `31351756-3F24-4963-8380-4E7602335AAE`
  - Es ist nicht möglich, die eingetragene App-Kontroll-ID nach dem erstmaligen Speichern zu ändern. Es ist jedoch möglich, mehrere (sich ergänzende) Konfigurationen App-Kontrolle zu erstellen und auf einem Gerät anzuwenden.
- Feld App Control Binärdatei: Upload der WDAC-Richtlinie im Binärformat, siehe Generierung der WDAC-Richtlinie →. Der Hinweis im Formular nennt die Dateiendung `.bin`. Relution prüft die Dateiendung jedoch nicht, sodass auch die CIP-Datei des WDAC-Assistenten ohne Umbenennen hochgeladen werden kann.

Aktualisierung

Damit eine neue Version der Konfiguration App-Kontrolle erfolgreich auf dem Gerät angewendet werden kann, muss die `<PolicyID>` in der WDAC-Richtlinie denselben Wert wie die App-Kontroll-ID der Konfiguration und die `<VersionEx>` einen höheren Wert aufweisen als in der vorherigen Version.

Löschen

Damit das Löschen einer WDAC-Richtlinie auf dem Gerät angewendet wird, ist ein Neustart des Geräts erforderlich.

Microsoft empfiehlt einen Workaround, sodass die App-Einschränkungen auch ohne Neustart entfernt werden, siehe Microsoft Dokumentation →.

Löschen einer unsignierten WDAC-Richtlinie

In Relution kann das Entfernen ohne Neustart daher folgendermaßen umgesetzt werden:

1. Erstellung einer *Allow-All* WDAC-Richtlinie
   - Die `<PolicyID>` muss der App-Kontroll-ID entsprechen
   - Die `<VersionEx>` muss höher sein als in der vorherigen Version
2. Konvertierung der XML-Datei in das benötigte Binär-Format
3. Erstellung einer neuen Richtlinien-Version in Relution
   - Hochladen der neuen Binär-Datei der *Allow-All* WDAC-Richtlinie in der Konfiguration App-Kontrolle
4. Veröffentlichung der neuen Richtlinien-Version
   - Dadurch werden die bestehenden Einschränkungen von dem Gerät entfernt
5. Entfernen der Richtlinie von dem Gerät
   - Dies löscht die Konfiguration App-Kontrolle von dem Gerät. Allerdings ist dies erst nach dem Neustart aktiv.

Löschen einer signierten WDAC-Richtlinie

Das Entfernen einer signierten WDAC-Richtlinie (ohne benötigten Neustart) kann in Relution daher folgendermaßen umgesetzt werden:

1. Erstellung einer signierten WDAC-Richtlinie, welche unsignierte WDAC-Richtlinien erlaubt
   - Die `<PolicyID>` muss der App-Kontroll-ID entsprechen
   - Die `<VersionEx>` muss höher sein als in der vorherigen Version
2. Konvertierung der XML-Datei in das benötigte Binär-Format
3. Erstellung einer neuen Richtlinien-Version in Relution
   - Hochladen der neuen Binär-Datei der signierten WDAC-Richtlinie (die unsignierte WDAC-Richtlinien erlaubt) in der Konfiguration App-Kontrolle
4. Veröffentlichung der neuen Richtlinien-Version
   - Dadurch können unsignierte WDAC-Richtlinien auf dem Gerät angewendet werden
5. Löschen einer unsignierten WDAC-Richtlinie →

Für Version 26.4.0

Benutzerdefinierte CSP

Die MDM-Schnittstelle nutzt zur Verwaltung von Windows-Geräten Richtlinien des Konfigurationsdienstanbieters (Configuration Service Provider, CSP). Diese werden mithilfe des SyncML Protokolls →, einem speziellen XML-Format, auf dem Gerät angewendet, gelöscht oder abgefragt. Eine Liste verfügbarer CSP-Richtlinien ist in der offiziellen Microsoft MDM Dokumentation → enthalten.

Mit der Konfiguration Benutzerdefinierte CSP können beliebige CSP-Richtlinien in einer oder mehreren Konfigurationen dieses Typs zusammengeführt und auf Windows-Geräten angewendet werden. Die über die MDM-Schnittstelle verfügbaren Funktionen sind dadurch nur noch durch die von Microsoft angebotenen CSP-Richtlinien begrenzt. Microsoft erweitert diese Richtlinien kontinuierlich. Eine Übersicht der aktuellen Neuerungen ist in der offiziellen Microsoft-Dokumentation → zu finden.

Wichtige Anmerkungen

Bei der Arbeit mit der Konfiguration Benutzerdefinierte CSP wird die Konfiguration nicht von Relution implementiert, daher übernimmt Relution keine Haftung für eventuelle Schäden. Die verwendeten CSPs sollten vor der Anwendung auf einem Gerät sorgfältig geprüft werden. Weitere Hinweise sind unter Best Practices → zu finden.

Es besteht die Möglichkeit, dass die verwendeten CSPs auch von Relution selbst genutzt werden. In diesem Fall kann es zu Wechselwirkungen kommen, die von Relution bereitgestellte Konfigurationen beeinträchtigen oder überschreiben.

Für Version 26.4.0

Funktionsweise

Beim Einsatz von CSP-Richtlinien sind die folgenden Besonderheiten des SyncML-Protokolls zu beachten.

Allgemein

Nicht jede CSP-Richtlinie lässt sich auf jedem Gerät anwenden. Die Verfügbarkeit hängt von der *Betriebssystem-Version* und der *Edition* ab. Die entsprechenden Informationen sind den jeweiligen CSP-Richtlinien zu entnehmen. Wird ein Gerät nicht unterstützt, schlägt die Anwendung der Richtlinie fehl.

Die CSP-Richtlinien können im Geräte- oder Benutzer-Kontext → angewendet werden. Dabei ist zu beachten, dass der Benutzerkontext nur für den Benutzer gilt, mit dem die Einschreibung durchgeführt wurde. Daher wird empfohlen, CSP-Richtlinien ausschließlich im Gerätekontext zu verwenden.

Die CSP-Richtlinien unterstützen nicht alle SyncML-Befehle. Es kann vorkommen, dass bestimmte CSP-Richtlinien beispielsweise nur für die Abfrage (`Get`-Befehl) verfügbar sind.

Beispiel: Um Cortana auf einem Gerät zu erlauben oder zu blockieren (in der Relution Konfiguration *Restriktionen* bereits enthalten), kann der folgende CSP verwendet werden: Richtlinien CSP/Benutzerfreundlichkeit/AllowCortana →.

- Dieser CSP ist ab *Version 1507* und für *alle Editionen* anwendbar.
- Es wird ausschließlich der Gerätekontext unterstützt.
- Unterstützte SyncML-Abfragen erlaubt: Hinzufügen (`Add`), Löschen (`Delete`), Abrufen (`Get`), Ersetzen (`Replace`).

Add und Replace

Das SyncML-Protokoll weist einige Besonderheiten auf, die bei der Anwendung von Konfigurationen berücksichtigt werden müssen.

Manche CSP-Richtlinien müssen bei erstmaliger Anwendung mit dem `Add`-Befehl hinzugefügt werden. Bei späteren Aktualisierungen kann dieser `Add`-Befehl dann fehlschlagen. In solchen Fällen muss stattdessen der Befehl `Replace` verwendet werden. Weitere Hinweise sind unter Best Practices → zu finden.

Delete

Das Löschen einer CSP-Richtlinie kann direkt auf der jeweiligen CSP-Richtlinie erfolgen. In manchen Fällen ist der `Delete`-Befehl auch auf einem übergeordneten oder auch *Root*-Knoten möglich. Dabei werden alle untergeordneten CSP-Richtlinien unterhalb ebenfalls entfernt.

Schlägt das Löschen fehl, bleiben die betreffenden CSP-Richtlinien auf dem Gerät weiterhin aktiv. In diesem Fall muss das Feld SyncML löschen angepasst und die Richtlinie erneut angewendet sowie anschließend korrekt entfernt werden.

Atomic und Sequence

Mit dem `Sequence`-Befehl lassen sich mehrere CSP-Richtlinien gruppieren und in einer definierten Reihenfolge ausführen. Schlägt eine einzelne Richtlinie fehl, werden die übrigen dennoch angewendet. Dies kann zu unerwünschtem Verhalten führen, weshalb fehlerhafte Richtlinien gegebenenfalls manuell entfernt werden müssen.

Wird das SyncML hingegen innerhalb eines `Atomic`-Befehls ausgeführt, führt ein Fehler bei einer einzelnen Richtlinie zum Abbruch und Rollback der gesamten Konfiguration. Die Richtlinien werden entweder vollständig oder gar nicht angewendet. Der `Atomic`-Befehl ist daher vorzuziehen und wird aktuell ausschließlich unterstützt.

Für Version 26.4.0

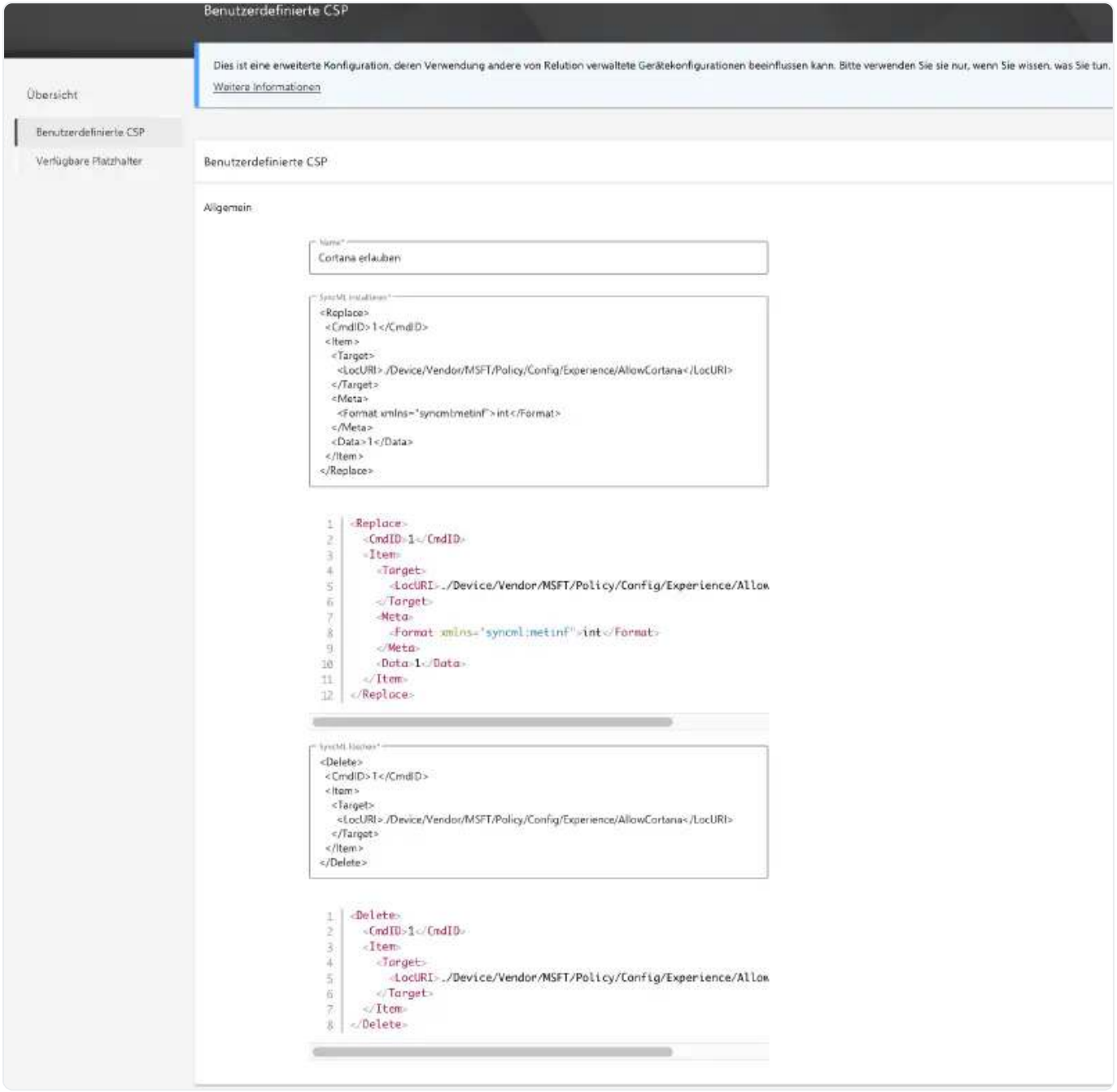
In Relution

Um eine benutzerdefinierte Konfiguration auf Windows-Geräten anzuwenden, wird unter `Geräte` → `Richtlinien` in einer Windows-Richtlinie die Konfiguration Benutzerdefinierte CSP hinzugefügt. Nach dem Veröffentlichen der Richtlinie wird die Konfiguration auf die Geräte der Gerätegruppen angewendet, denen die Richtlinie zugewiesen ist (siehe Richtlinien →).

Für eine funktionierende Anwendung sind zwei SyncML-Befehle erforderlich: im Feld SyncML installieren ein Befehl zum Anwenden bzw. Aktualisieren der Konfiguration und im Feld SyncML löschen ein Befehl zum Entfernen der Konfiguration vom Gerät. Bei mehrfacher Veröffentlichung ist darauf zu achten, dass der Befehl in SyncML installieren bei Bedarf angepasst wird.

Die Konfiguration Benutzerdefinierte CSP enthält folgende Eigenschaften (alle sind Pflichtfelder):

Eigenschaft	Beschreibung
Name	Bezeichnung der Konfiguration (maximal 255 Zeichen)
SyncML installieren	Das auszuführende SyncML, wenn die Konfiguration auf dem Gerät angewendet wird
SyncML löschen	SyncML-Inhalt, der beim Entfernen der Konfiguration vom Gerät ausgeführt wird



Damit Relution die Konfiguration erfolgreich auf dem Gerät anwenden und das Ergebnis auswerten kann, wird das eingegebene SyncML automatisch ergänzt.

- Enthält das angegebene SyncML `<Format>` - oder `<Type>`-Element, wird dieses automatisch um den erforderlichen *Namespace erweitert*. Dies geschieht beim Speichern der Konfiguration.
- Das SyncML wird bei der Auslieferung automatisch in einen `Atomic`-Block eingebettet. Dies ist notwendig, um die Antwort des Geräts eindeutig der jeweiligen Konfiguration zuordnen zu können.
- Zusätzlich wird das SyncML bei der Auslieferung um die erforderlichen Container `SyncBody`, `SyncHdr` und `SyncML` erweitert, sodass es konform an das Gerät gesendet werden kann. Dies geschieht erst bei Auslieferung der Konfiguration.

> Die Felder SyncML installieren und SyncML löschen dürfen nur die Befehle selbst enthalten (z. B. `<Replace>`, `<Add>`, `<Delete>`), ohne die Elemente `SyncML`, `SyncHdr` oder `SyncBody`. Enthält das SyncML eines dieser Elemente oder ist es kein gültiges SyncML, wird die Konfiguration beim Speichern abgelehnt. Vollständige SyncML-Nachrichten aus der Microsoft-Dokumentation müssen daher vorher auf die Befehle gekürzt werden.

In beiden SyncML-Feldern können Platzhalter verwendet werden, einschließlich Platzhaltern für Zertifikate. Die verfügbaren Platzhalter werden im Bereich Verfügbare Platzhalter unterhalb der Konfiguration angezeigt und bei der Auslieferung durch die Werte des jeweiligen Geräts bzw. Benutzers ersetzt (siehe Erweiterte Platzhalter →).

Bei jeder Änderung der Richtlinien eines Geräts, etwa nach dem Veröffentlichen einer neuen Richtlinien-Version, sendet Relution das SyncML aus SyncML installieren aller zugewiesenen Konfigurationen Benutzerdefinierte CSP erneut, auch wenn die Konfiguration selbst unverändert ist. Anders als bei anderen Windows-Konfigurationen wird der Zustand auf dem Gerät vorher nicht abgefragt. Ein `Add`-Befehl kann dadurch bei späteren Auslieferungen fehlschlagen (siehe Best Practices →).

Schlägt die Anwendung auf dem Gerät fehl, meldet Relution am Gerät einen Compliance-Verstoß vom Typ Benutzerdefinierte CSP-Konfiguration.

Für Version 26.4.0

Beispiele

Richtlinien CSP/Benutzerfreundlichkeit/AllowCortana →

- Cortana zulassen

SyncML installieren:

```
<Replace>
  <CmdID>1</CmdID>
  <Item>
    <Target>
      <LocURI>./Device/Vendor/MSFT/Policy/Config/Experience/AllowCortana</LocURI>
    </Target>
    <Meta>
      <Format>int</Format>
    </Meta>
    <Data>1</Data>
  </Item>
</Replace>
```

- Cortana blockieren

SyncML installieren:

```
<Replace>
  <CmdID>1</CmdID>
  <Item>
    <Target>
      <LocURI>./Device/Vendor/MSFT/Policy/Config/Experience/AllowCortana</LocURI>
    </Target>
    <Meta>
      <Format>int</Format>
    </Meta>
    <Data>0</Data>
  </Item>
</Replace>
```

- CSP-Richtlinie *AllowCortana* von Gerät entfernen

SyncML löschen:

```
<Delete>
  <CmdID>1</CmdID>
  <Item>
    <Target>
      <LocURI>./Device/Vendor/MSFT/Policy/Config/Experience/AllowCortana</LocURI>
    </Target>
  </Item>
</Delete>
```

Best Practices

- Eine *Aktualisierung der Konfiguration* kann über eine neue Richtlinien-Version erfolgen (ggf. mit angepasstem SyncML installieren).
- Sollte das Löschen fehlschlagen, bleiben die betroffenen CSP-Richtlinien auf dem Gerät aktiv. In diesem Fall ist eine Anpassung von SyncML löschen erforderlich, gefolgt von einem erneuten Anwenden und anschließendem Entfernen der Richtlinie.
- Es wird empfohlen, den `Replace`-Befehl anstelle von `Add` zu verwenden - außer die entsprechende CSP-Richtlinie unterstützt `Replace` bei der Erstanwendung nicht.
- Falls `Replace` bei der erstmaligen Anwendung einer CSP-Richtlinie nicht zulässig ist, sollte die Konfiguration zunächst mit `Add` angewendet werden. Anschließend sollte SyncML installieren auf `Replace` umgestellt und eine neue Richtlinien-Version auf das Gerät ausgerollt werden.
- Es wird dringend empfohlen, das gewünschte Verhalten *ausgiebig auf geeigneten Testgeräten zu testen*. Mindestens folgende Szenarien sollten getestet werden:
  - Erstmaliges Anwenden der Konfiguration
  - Aktualisierung der Konfiguration
  - Löschen der Konfiguration

Beispielrichtlinien

Ein umfangreiches Beispiel für benutzerdefinierte Richtlinien wurde im Relution Community Board veröffentlicht: Relution Community Board - Custom CSP →.

Vielen Dank an die Community für den wertvollen Beitrag.

Für Version 26.4.0

Gerätename

Ab `Relution Server Version 5.33` kann der Gerätename für Windows-Geräte über die Richtlinie Gerätename vergeben werden. Der Name wird im Pflichtfeld Name im Abschnitt Allgemein eingetragen. Benutzer- und Geräteplatzhalter sind möglich; die verfügbaren Platzhalter zeigt das Portal unterhalb der Konfiguration im Bereich Verfügbare Platzhalter an. Pro Richtlinie ist eine Gerätename-Konfiguration möglich.

Hinweise

> Nachdem der Gerätename angepasst wurde, muss das Gerät neu gestartet werden, damit der neue Name wirksam wird. Bis zum Neustart wird bei jeder Aktion Geräteinformationen aktualisieren noch der alte Name angezeigt. Der Gerätename darf nur Buchstaben, Ziffern und Bindestriche enthalten. Dies gilt auch für Platzhalter.

Relution setzt zuerst die Platzhalter ein und entfernt dann alle Zeichen außer Buchstaben (a–z, A–Z, ohne Umlaute), Ziffern und Bindestrichen, auch aus den eingesetzten Werten. Bindestriche am Anfang und Ende werden ebenfalls entfernt. Der eingegebene und der auf dem Gerät gesetzte Name können daher voneinander abweichen, z. B. wird aus `Müller PC_01` der Name `MllerPC01`. Der Gerätename sollte nach dem Einsetzen der Platzhalter höchstens 63 Zeichen lang sein.

Weitere Funktionen wie Teilzeichenfolgen, Standardwerte für leere Felder oder das Ersetzen von Umlauten sind im Artikel Erweiterte Platzhalter → beschrieben.

Wird die Konfiguration oder die Richtlinie vom Gerät entfernt, bleibt der zuletzt gesetzte Gerätename erhalten.

Für Version 26.4.0

Restriktionen anwenden

Um sicherzustellen, dass Windows 10/11-Geräte nur in Übereinstimmung mit festgelegten Restriktionen verwendet werden, können Einschränkungen in der Richtlinienkonfiguration Restriktionen definiert und auf eingeschriebenen Windows-Geräten angewendet werden.

Verfügbare Kategorien

Die Konfiguration ist in folgende Gruppen gegliedert:

- Konten
- App Management
- Kamera
- Verbindungen
- Experience
- System
- Einstellungen
- WLAN
- Stromversorgung (Abschnitte Akku und Netzbetrieb)
- Datenschutz

Neben jeder Option zeigt das Portal an, für welche Windows-Editionen und ab welcher Windows-Version sie gilt. Einstellungen, die die Edition oder Version eines Geräts nicht unterstützt, überträgt Relution nicht an dieses Gerät. Die meisten Restriktionen gelten nur für Windows Pro, Enterprise und Education (siehe Einschränkungen der Windows Home Edition →).

Für Version 26.4.0

Über das Download-Symbol oben im Formular (Restriktionen als CSV-Datei exportieren) lassen sich die eingestellten Werte einschließlich noch nicht gespeicherter Änderungen als CSV-Datei herunterladen.

MDM-Verbindung vor Entfernung schützen

Damit Windows-10/11-Geräte (Pro, Enterprise, Education) im eigenen System verbleiben und die Verbindung zu Relution aufrechterhalten wird, lässt sich mittels Restriktion verhindern, dass das MDM-Profil durch den Benutzer entfernt wird. Die Löschoption wird dabei zwar weiterhin angezeigt, hat jedoch keine Funktion mehr.

- Entfernen von MDM Verbindung aus Relution erlauben (Gruppe Experience) – Wenn deaktiviert, wird sichergestellt, dass Benutzer verbundene Geräte nicht manuell vom MDM-Server trennen können. Eine Abmeldung durch den MDM-Server bleibt weiterhin möglich.
- Zurücksetzen des Geräts auf Werkszustand durch den Benutzer zulassen (Gruppe System) – Wenn deaktiviert, wird verhindert, dass auf den Geräten ein Factory Reset durchgeführt werden kann. Dies würde die Einschreibung auf den Geräten und die Verbindung zum MDM-Server löschen.

Beide Optionen sind standardmäßig aktiviert. Der Schutz greift also erst, wenn sie in der Konfiguration ausdrücklich deaktiviert werden.

Beide Optionen werden nur auf Windows 10/11 Pro, Enterprise und Education angewendet. Auf Geräten mit Windows Home überträgt Relution sie nicht, sodass sich diese Geräte trotz Restriktion weiterhin vom MDM-Server trennen oder auf den Werkszustand zurücksetzen lassen (siehe Einschränkungen der Windows Home Edition →).

Durch Kombination beider Optionen wird die MDM-Steuerung eingeschriebener Windows-10/11-Geräte (Pro, Enterprise, Education) sowie etwaige Konfigurationen und Funktionsbeschränkungen abgesichert.

Windows Hello

Mit Relution kann Windows Hello for Business in einer Richtlinie für Windows-Geräte konfiguriert werden. Windows Hello ermöglicht Benutzern die Anmeldung per PIN, Gesichtserkennung oder Fingerabdruck anstelle eines Kennworts.

Konfiguration

- Mandanten-ID – ID des Entra-ID-Mandanten im GUID-Format, Pflichtfeld.
- Ein Trusted Platform Module (TPM) wird genutzt – schränkt die Bereitstellung auf Geräte mit nutzbarem TPM ein. Standardmäßig aktiviert.

PIN-Richtlinie

- Minimale PIN-Länge und Maximale PIN-Länge (jeweils 4–127 Zeichen, Standard: 4) – die maximale Länge darf nicht kleiner sein als die minimale. Ohne Anpassung gilt damit eine feste PIN-Länge von 4 Zeichen.
- Kleinbuchstaben in PIN, Großbuchstaben in PIN, Sonderzeichen in PIN – jeweils Erlaubt (Standard), Erforderlich oder Nicht Erlaubt
- PIN Ablaufzeit und PIN Ablaufzeit (Tage) – erzwingt einen PIN-Wechsel nach 1–730 Tagen (ab Windows 1511). Der Schalter ist standardmäßig deaktiviert, die PIN läuft dann nicht ab; bei Aktivierung sind 5 Tage voreingestellt.
- Vorherige PINs speichern und Anzahl der vorherigen PINs – verhindert die Wiederverwendung der letzten 1–50 PINs (ab Windows 1511). Standardmäßig aktiviert mit 5 PINs; bei deaktiviertem Schalter wird kein PIN-Verlauf geführt.

Für Version 26.4.0

Biometrie und Wiederherstellung

- Erlaubt biometrische Authentifizierung – aktiviert Anmeldung per Gesicht oder Fingerabdruck (ab Windows 1511). Standardmäßig aktiviert.
- Erweitertes Anti-Spoofing wird verwendet, sofern es verfügbar ist – zusätzlicher Schutz bei der Gesichtserkennung (ab Windows 1511). Standardmäßig aktiviert.
- Aktiviert PIN-Wiederherstellung – ermöglicht das Zurücksetzen einer vergessenen PIN (ab Windows 1703). Standardmäßig aktiviert.
- Zertifikat für Authentifizierung von lokalen Ressourcen – Windows Hello for Business verwendet ein Zertifikat für die Anmeldung an lokalen Ressourcen. Bei aktivierter Option richtet Windows Hello die PIN erst ein, wenn das Gerät ein Zertifikat vom Verwaltungsserver erhalten hat, z. B. über die Konfiguration Zertifikate → mit dem Speicherort des Zertifikatsschlüssel Windows Hello für Unternehmen. Standardmäßig aktiviert. Ohne eine solche Zertifikatsverteilung wird keine PIN eingerichtet; in diesem Fall ist die Option zu deaktivieren.

Optionen mit Versionsangabe werden nur an Geräte ab der jeweiligen Windows-Version übertragen.

> Windows Hello for Business erfordert eine Anbindung an Microsoft Entra ID. Die konkreten Mindestanforderungen an Hardware (TPM-Version) und Windows-Version sollten anhand der Microsoft-Dokumentation → geprüft werden.

WLAN

Mit Relution können WLAN-Netzwerke zentral auf Windows-Geräten eingerichtet werden, ohne dass Benutzer die Zugangsdaten selbst eingeben müssen.

Konfiguration

- Netzwerk SSID – Pflichtfeld, maximal 32 Zeichen, ohne führende oder abschließende Leerzeichen, muss innerhalb der Richtlinienversion eindeutig sein.
- Verstecktes Netzwerk – für Netzwerke, die ihre SSID nicht senden (standardmäßig deaktiviert).
- Netzwerk automatisch beitreten – standardmäßig aktiviert.
- Authentifizierungstyp: Offen (Standard), Persönlicher WPA, Persönlicher WPA2, Persönliches WPA3, Firmenweiter WPA, Firmenweiter WPA2, Firmenweiter WPA3, Firmenweiter WPA3 192-Bit
- Verschlüsselungstyp – bei WPA und WPA2 (persönlich oder firmenweit) wahlweise AES (Standard) oder TKIP; bei Persönliches WPA3 und Firmenweiter WPA3 fest AES, bei Firmenweiter WPA3 192-Bit fest GCMP-256; bei Offen entfällt das Feld.
- Passwort – Netzwerkschlüssel bei den persönlichen Authentifizierungstypen, maximal 64 Zeichen. Das Portal zeigt das Feld auch bei Offen an, dort wird es aber nicht übertragen. Bleibt es leer, wird kein Schlüssel übertragen.
- Übergangsmodus – nur bei Persönliches WPA3

Weisen mehrere Richtlinien einem Gerät WLAN-Konfigurationen mit derselben Netzwerk SSID zu, wird nur die Konfiguration aus der Richtlinie mit der höchsten Priorität angewendet.

Für Version 26.4.0

Enterprise-Authentifizierung (EAP)

Bei den firmenweiten Authentifizierungstypen erscheint der Abschnitt Verschlüsselungseinstellungen. Mindestens ein EAP-Typ muss ausgewählt sein. Sobald ein EAP-Typ gewählt ist, erscheint zusätzlich der Abschnitt Vertrauen mit den vertrauenswürdigen Servernamen und Zertifikaten.

- EAP Types akzeptieren – TLS, TTLS und/oder PEAP
- Identitätszertifikat – nur bei TLS/TTLS; dort Pflicht. Zwei Optionen stehen zur Wahl:
  - Zertifikat wählen – ein manuell hochgeladenes Zertifikat (siehe Zertifikatsverwaltung →) oder eine Zertifikatsvorlage, z. B. der Built-In CA →.
  - Benutzerdefiniertes Zertifikat verwenden – das Benutzerzertifikat aus dem Profil des Benutzers, der dem Gerät zugewiesen ist (siehe Benutzerzertifikate →). Das optionale Feld Zertifikatsname wählt ein bestimmtes Zertifikat anhand des Namens aus, wenn der Benutzer mehrere besitzt, und kann Platzhalter enthalten. Bleibt es leer, wird das am längsten gültige Zertifikat verwendet.
- Innerer Authentifizierungstyp – bei TTLS: PAP, CHAP, MSCHAP oder MSCHAPv2 (Pflichtfeld); sobald PEAP gewählt ist, nur MSCHAPv2 (optional)
- Innere Authentifizierung – Textfeld, nur bei TTLS ohne PEAP; Pflichtfeld bei PAP, CHAP oder MSCHAP
- Anonymer Benutzername – bei TTLS/PEAP, optional
- Server Zertifikat von Nutzer anfragen – nur bei PEAP. Ist die Option aktiv, wird das Serverzertifikat nicht automatisch geprüft, und Windows darf beim Benutzer nachfragen, wenn die Zertifizierungsstelle nicht gefunden wird.
- Vertrauenswürdige Servernamen
- Vertrauenswürdige Zertifikate – Mehrfachauswahl von Zertifikaten (PKCS#1 oder PKCS#12) aus der Zertifikatsverwaltung →

Windows Update

Mit Relution lässt sich das Update-Verhalten von Windows-Geräten zentral steuern. Die Richtlinie steht ab Windows 10 Version 1607 für die Editionen Pro, Enterprise und Education zur Verfügung.

Automatisches Update

- Verhalten bei automatischen Updates: automatisch installieren und neu starten (Standard), zu gegebener Zeit installieren und neu starten, ohne Nutzerkontrolle installieren und neu starten, automatisch installieren und zur Planung des Neustarts auffordern, Benachrichtigung vor Download oder automatische Updates vollständig ausschalten.
- Bei „zu gegebener Zeit“: Häufigkeit der Update Installation (ab Version 1709) mit Jede Woche (Standard) oder einer oder mehreren bestimmten Wochen des Monats (erste bis vierte Woche); Jede Woche schließt die Auswahl einzelner Wochen aus. Dazu Zeitpunkt (0–23 Uhr, Standard 3 Uhr) und Tag (Standard: jeden Tag), an dem das Update installiert wird.
- Scannen nach App-Updates von Microsoft Update (standardmäßig aus)

Allgemein

Für Version 26.4.0

- Updates mit Nicht-Microsoft-Signatur akzeptieren (nur aus einem Intranet-Updatedienst, signiert mit einem Zertifikat aus „Vertrauenswürdige Herausgeber“; standardmäßig aus)
- Downloads über getaktete Netzwerke erlauben (ab 1709, standardmäßig aus)
- Benachrichtigungen für automatische Neustarts aktivieren (standardmäßig aus) und Zeitraum für Erinnerungen (15, 30, 60, 120 oder 240 Minuten, Standard 15; ab 1703)
- Zeitraum für Neustart-Warnungen (2, 4, 8, 12 oder 24 Stunden, Standard 4) und für unmittelbare Warnungen (15, 30 oder 60 Minuten, Standard 15; jeweils ab 1703)
- Automatische Wartung/Wake-up (ab 1903, standardmäßig an)
- Dual-Scan erlauben (ab 1709, standardmäßig an)
- Kulanzzeitraum vor der Deadline (0–7 Tage, Standard 2; ab 1903), kein automatischer Neustart außerhalb der Nutzungszeit, bis Deadline und Kulanzzeitraum abgelaufen sind (ab 1903, standardmäßig aus)
- WSUS-Server-URL sowie alternative URL; beide müssen gültige `http`- oder `https`-URLs sein
- Windows-Zielversion (ab 1803) und Produkt-Version (ab 2004, nur in Kombination mit der Zielversion wirksam); für die Produkt-Version schlägt das Portal `Windows 10`, `10`, `Windows 11` und `11` vor

Benutzerschnittstelle

Ab Version 1809: Zugriff auf Windows Update bzw. das Pausieren von Updates für Endbenutzer erlauben (beides standardmäßig an).

Nutzungszeit (Active Hours)

- Start und Ende der Nutzungszeit (0–23 Uhr, Standard 8 bis 17 Uhr), maximale Spanne 18 Stunden. Die Nutzungszeit darf über Mitternacht reichen; liegt das Ende vor dem Start, gilt es für den Folgetag.

Qualitäts-Updates

- Auto-Neustart-Deadline (2–30 Tage, Standard 7; ab 1703)
- Pause-Startdatum (ab 1703): Ab dem gewählten Datum werden Qualitäts-Updates für 35 Tage pausiert.
- Deadline in Tagen (0–30, Standard 7; ab 1903)
- Verschiebung in Tagen (0–365 Tage)

Feature-Updates

- Auto-Neustart-Deadline (2–30 Tage, Standard 7; ab 1809)
- Deinstallations-Zeitraum (2–60 Tage, Standard 10; ab 1803)
- Verschiebung in Tagen (0–365 Tage)
- Deadline in Tagen (0–30, Standard 7; ab 1903)
- Pause-Startdatum (ab 1703): Ab dem gewählten Datum werden Feature-Updates für 35 Tage pausiert.

Für Version 26.4.0

Exchange

Mit Relution lässt sich ein Exchange-ActiveSync-Konto zentral auf Windows-Geräten einrichten.

Konfiguration

Die Konfiguration ist in die Abschnitte Allgemein, Kontoeinstellungen (im Portal: Konto Einstellungen), Synchronisationseinstellungen und Logging-Einstellungen gegliedert. Kontoname, E-Mail-Adresse, Benutzername und Exchange Host sind Pflichtfelder; Exchange Domäne und Passwort sind optional.

Allgemein

- Secure Mail Gateway verwenden: Wird diese Funktion aktiviert, werden die URL und Domäne des Secure Mail Gateway → anstelle der Exchange-URL und Exchange-Domäne auf die Geräte verteilt. Dadurch kommunizieren die Geräte über das Secure Mail Gateway mit dem Exchange Server. Exchange Host und Exchange Domäne werden dann automatisch gesetzt und sind nicht bearbeitbar; als Domäne dient der eindeutige Name der Organisation. Enthält der Benutzername ein `@`, überträgt Relution ihn im Format `<Domäne>\<Benutzername>`. Die Option ist nur verfügbar, wenn das Secure Mail Gateway in den Einstellungen konfiguriert und aktiviert ist. Ist Windows oder eine Windows-Version in den Secure-Mail-Gateway-Einstellungen gesperrt, zeigt das Formular eine Warnung.
- Exchange Host – Pflichtfeld, ohne Protokoll (ohne `https://`).
- Exchange Domäne – optional.
- Exchange Server verwendet SSL für die Authentifizierung – Standardmäßig aktiviert.

Für Version 26.4.0

Kontoeinstellungen

- Kontoname – Pflichtfeld.
- E-Mail-Adresse – Pflichtfeld, unterstützt Platzhalter wie `${user.email}`; über E-Mail Adresse des Benutzers verwenden wird die E-Mail-Adresse des zugewiesenen Benutzers übernommen.
- Benutzername – Pflichtfeld. Wahlweise Manuell eingeben oder den Benutzernamen (`${user.name}`) bzw. die E-Mail-Adresse (`${user.email}`) des zugewiesenen Benutzers verwenden. Der Benutzername kann nach dem Erstellen der Konfiguration nicht mehr geändert werden.
- Passwort – optional, wird verschlüsselt gespeichert und nach dem Speichern nicht mehr im Klartext angezeigt.

Wird ein Platzhalter verwendet, muss dem Gerät ein Benutzer zugewiesen sein.

Synchronisationseinstellungen

- E-Mails, Kontakte, Kalender und Aufgaben synchronisieren – jeweils einzeln aktivierbar, standardmäßig alle aktiviert.
- Synchronisationszeitraum für E-Mails: alle, 3 Tage, 1 Woche (Standard), 2 Wochen oder 1 Monat.
- Synchronisationsintervall: Push (Standard), manuell, alle 15 oder 30 Minuten oder stündlich.

Logging-Einstellungen

- Logging: Deaktiviert (Standard), Aktiviert oder Erweitert.

Windows Office

Mit Relution kann eine Microsoft-Office-Installation über eine zuvor erstellte Konfigurations-XML zentral auf Windows-Geräten bereitgestellt werden. Die Richtlinie steht ab Windows 10 Version 1703 für die Editionen Pro, Enterprise und Education zur Verfügung.

Konfiguration

Die Konfiguration besteht aus einer einzigen Datei:

- Konfiguration XML – Pflichtfeld, XML-Datei-Upload. Nach dem Hochladen zeigt das Formular den Inhalt der Datei zur Kontrolle an.

Diese XML-Datei wird nicht in Relution erstellt, sondern über das offizielle Microsoft-Tool config.office.com → generiert. Dort werden Lizenzierung, Update-Kanal, zu installierende Office-Apps und Sprachen festgelegt.

Installation und Deinstallation

Für Version 26.4.0

Die Installation läuft auf dem Gerät asynchron. Solange sie andauert, bleibt die Aktion Richtlinie ändern im Status Nicht jetzt.

- Bereits installierte Office-Suite: Relution vergleicht die Product ID (`<Product ID="…">`) der auf dem Gerät gemeldeten Installation mit der Product ID der neuen XML. Unterscheiden sie sich, wird die vorhandene Office-Suite zuerst vollständig deinstalliert und die neue Konfiguration erst in einem Folgeschritt installiert. Bei gleicher Product ID wird ohne vorherige Deinstallation direkt neu installiert.
- Entfernen der Konfiguration: Wird die Konfiguration oder die Richtlinie vom Gerät entfernt und meldet das Gerät eine Office-Installation, deinstalliert Relution Office vom Gerät.
- Fehler: Meldet das Gerät bei der Installation einen Fehler, entsteht der Compliance-Verstoß Die Windows Office-Konfiguration ist ungültig.

Die Geräteaktion Office 365 installieren sollte nicht zusätzlich zu dieser Richtlinie verwendet werden. Hinweise zu hängenden Installationen stehen unter Office Installation steckt fest →.

Passwort

Die Richtlinien-Konfiguration Passwort legt fest, welche Anforderungen ein Gerätepasswort auf verwalteten Windows-Geräten erfüllen muss und wie sich das Gerät bei Inaktivität oder fehlgeschlagenen Anmeldeversuchen verhält.

Sobald die Konfiguration zugewiesen ist, aktiviert Relution auf dem Gerät die Gerätesperre per Passwort. Diese Einstellung ist immer aktiv und lässt sich in der Konfiguration nicht abschalten.

Diese Einstellungen werden nicht auf alle Arten von Windows-Konten angewendet. Maßgeblich ist die offizielle Microsoft-Dokumentation zum jeweiligen CSP: DeviceLock-CSP →

Konfigurationsmöglichkeiten

- Einfache Passwörter erlauben — Legt fest, ob PINs oder Passwörter wie „1111“ oder „1234“ erlaubt sind. Standardmäßig aktiviert.
- Minimale Länge — Mindestanzahl an Zeichen des Passworts (4–16). Standardwert ist 4.
- Mindestqualität — Legt fest, ob ein Passwort numerisch (z. B. „1042“), alphanumerisch (z. B. „A42B“) oder frei wählbar sein soll. Standardwert ist Alphanumerisch.
- Minimales Kennwortalter (in Tagen) — Anzahl an Tagen, die ein Passwort mindestens verwendet werden muss, bevor es geändert werden kann (0–41). Standardwert ist 0 – Änderungen sofort erlauben. Ist ein maximales Alter gesetzt, muss der Wert kleiner als das maximale Alter sein.
- Maximales Alter (in Tagen) — Anzahl an Tagen, bis das Passwort abläuft (0–730). Standardwert ist 0 – Passwörter laufen nicht ab.
- Passworthistorie — Anzahl der zuletzt verwendeten Passwörter, die nicht wiederverwendet werden dürfen (0–24). Standardwert ist 0 – das aktuelle Passwort kann zu jedem beliebigen Passwort geändert werden, auch zum aktuellen. Mit dem Wert 1 kann der Benutzer das aktuelle Passwort nicht wiederverwenden; der Wert 5 legt fest, dass weder das aktuelle Passwort noch eines der letzten vier Passwörter wiederverwendet werden kann.
- Zeit zur Bildschirm-Sperrung — Zeit in Minuten (0–999), die das Gerät im Ruhezustand verbringen kann, bis es gesperrt wird und PIN oder Passwort eingegeben werden muss. Standardwert ist 0 – das Gerät wird nicht gesperrt.
- Anzahl fehlgeschlagener Passwortversuche bevor alle Daten gelöscht werden — Anzahl fehlgeschlagener Anmeldeversuche, nach der das Gerät in den BitLocker-Wiederherstellungsmodus versetzt wird (0–16). Die Daten sind dann nicht mehr zugänglich, lassen sich aber wiederherstellen; das Gerät wird nicht auf Werkseinstellungen zurückgesetzt. Voraussetzung ist ein aktiviertes BitLocker. Standardwert ist 0 – deaktiviert.

Das minimale Kennwortalter wird ab Windows 10 Version 1709 übertragen, das maximale Alter und die Passworthistorie ab Version 1511. Auf älteren Versionen werden diese Werte nicht gesetzt.

Für Version 26.4.0

Mindestqualität

Für die Mindestqualität stehen drei Werte zur Verfügung:

- Numerisch
- Alphanumerisch (Standard)
- Wahl durch Benutzer

Verwandte Themen

- BitLocker → — Laufwerksverschlüsselung und Wiederherstellungsschlüssel.
- Windows Hello → — biometrische Anmeldung und PIN-Richtlinien.

Für Version 26.4.0

Windows Kiosk-Modus

Mit der Richtlinien-Konfiguration Windows Kiosk-Modus wird ein Gerät auf eine einzelne Anwendung beschränkt. Die Richtlinie steht ab Windows 10 Version 1803 für die Editionen Pro, Enterprise und Education zur Verfügung. Typische Einsatzfälle sind Informationsterminals, Selbstbedienungsplätze und Prüfungsgeräte.

> Die ausgewählte App und der Kiosk-Browser werden nicht automatisch installiert. Beide sind separat über die App-Verteilung bereitzustellen, bevor die Konfiguration greift.

Benutzeranmeldung

Benutzeranmeldetyp legt fest, welches Konto im Kiosk-Modus läuft:

- Automatische Anmeldung (Standard): Das Gerät meldet sich automatisch mit einem Kiosk-Konto an, das Windows dafür bereitstellt.
- Lokaler Benutzer: Der Kiosk-Modus gilt für das Konto, das im Feld Benutzername eingetragen ist. Das Feld erscheint nur bei dieser Option und ist dann Pflicht. Eine automatische Anmeldung erfolgt nicht; der Kiosk-Modus greift, sobald sich das Konto anmeldet.

Für Version 26.4.0

Art der Anwendung

Art der Anwendung bestimmt, was im Kiosk-Modus angezeigt wird: Microsoft Edge-Browser (Standard), Kiosk-Browser oder Store-App. Die weiteren Felder hängen von dieser Auswahl ab und sind in den folgenden Abschnitten beschrieben. Beim Wechsel der Art entfernt Relution die Browser-Einstellungen der zuvor gewählten Art vom Gerät.

Microsoft Edge

Diese Felder erscheinen bei Microsoft Edge-Browser:

- Edge Kiosk URL – Adresse der Startseite, Pflichtfeld. Es muss eine gültige URL eingetragen werden.
- Microsoft Edge Kiosk-Modus-Typ – Multi-Tab (Standard) oder Ohne Tabs.
- Browser nach Inaktivitätszeit aktualisieren – Zeit in Minuten (0–1440). Bleibt das Feld leer, verwendet Relution bei Multi-Tab 5 Minuten und bei Ohne Tabs den Wert 0.

Kiosk-Browser

Diese Felder erscheinen bei Kiosk-Browser:

- Standard-Homepage-URL – Startseite des Kiosk-Browsers.
- Homebuttons anzeigen, Navigationsschaltflächen anzeigen und Schaltfläche Sitzung beenden – blenden die jeweiligen Schaltflächen im Kiosk-Browser ein.
- Browser nach Inaktivitätszeit aktualisieren – Zeit in Minuten (1–1440). Bleibt das Feld leer, setzt Relution keinen Wert.
- URLs zulassen (max. 500) – ohne Eintrag sind im Kiosk-Browser alle Websites erreichbar. Sobald mindestens eine URL eingetragen ist, sind nur noch die eingetragenen URLs erreichbar, alle anderen Websites werden gesperrt. Platzhalter (`*`) sind nicht zulässig, jeder Eintrag muss eine gültige URL sein.

Store-App

Bei Store-App wird über die Schaltfläche App auswählen die Windows-App aus dem Relution App Store gewählt, die im Kiosk-Modus angezeigt wird (Pflichtfeld).

Die App muss bereits auf dem Gerät installiert sein (siehe Hinweis oben). Ist sie nicht installiert, wird die Konfiguration auf dem Gerät nicht angewendet.

Verwandte Themen

- Shared PC → — Windows-Geräte für die gemeinsame Nutzung konfigurieren.
- Restriktionen → — weitere Einschränkungen für Windows-Geräte.

Für Version 26.4.0

VPN

Mit der Richtlinien-Konfiguration VPN werden VPN-Profile zentral auf verwaltete Windows-Geräte verteilt. Die Konfiguration deckt neben der eigentlichen Verbindung auch Authentifizierung, Namensauflösung, Split-Tunneling und Proxy-Einstellungen ab. Unterstützt werden Windows Home, Pro, Enterprise und Education ab Version 1607.

Das Formular ist in die Abschnitte Allgemein, Apps, DNS Einstellungen, Split tunneling und Proxy Konfiguration gegliedert.

> Der Profilname ist der eindeutige Bezeichner eines VPN-Profils auf dem Gerät. Er muss sich von jeder anderen VPN-Konfiguration innerhalb derselben Richtlinienversion unterscheiden; Groß- und Kleinschreibung werden dabei nicht unterschieden. Gelten für ein Gerät mehrere Richtlinien mit VPN-Konfigurationen desselben Profilnamens, wird nur die Konfiguration aus der Richtlinie mit der höheren Priorität angewendet.

Allgemein

Feld	Beschreibung
Profilname	Pflichtfeld. Name des VPN-Profils auf dem Gerät; ohne führende oder nachgestellte Leerzeichen
VPN Typ	Automatisch (Standard), L2TP, PPTP oder IKEv2. Der Typ bestimmt, welche Authentifizierungstypen zur Auswahl stehen
Servernamen	Pflichtfeld. Mindestens ein VPN-Server; mehrere Einträge sind möglich
Automatisch verbinden	Die VPN-Verbindung wird automatisch aufgebaut
Anmeldedaten speichern	Die Anmeldedaten für die VPN-Verbindung werden auf dem Gerät gespeichert

Authentifizierung

Das Feld Authentifizierungstyp bietet je nach VPN Typ folgende Optionen. Bei einem Wechsel des VPN Typs wird der Authentifizierungstyp zurückgesetzt.

Option	Verfügbar bei	Beschreibung
Keine	allen Typen	Standard. Im Profil wird keine Authentifizierungsmethode festgelegt
EAP	allen Typen	Authentifizierung über EAP; die EAP-Konfiguration wird im Feld EAP XML hinterlegt
Vorinstallierter Schlüssel	L2TP	Das Feld Vorinstallierter Schlüssel erscheint und ist dann Pflichtfeld; der Block Identitätszertifikat entfällt
Computerzertifikat	IKEv2	Authentifizierung des Geräts über ein Computerzertifikat; das Feld EAP XML entfällt

Beim VPN Typ L2TP ist entweder ein vorinstallierter Schlüssel oder ein Identitätszertifikat erforderlich (Zertifikat, Zertifikatsvorlage oder Benutzerzertifikat). Fehlt beides, wird die Konfiguration nicht gespeichert.

EAP XML

EAP wird nicht über einzelne Felder eingerichtet, sondern als XML-Konfiguration im Textfeld EAP XML. Über dem Feld verlinkt das Portal die Microsoft-Dokumentation zum Aufbau dieser Konfiguration: EAP-Konfiguration →.

Das Feld steht bei allen Kombinationen außer IKEv2 mit Computerzertifikat zur Verfügung. An das Gerät übertragen wird das XML nur beim Authentifizierungstyp EAP; bei Keine und Vorinstallierter Schlüssel wird es ignoriert.

Für Version 26.4.0

Identitätszertifikat

Außer beim Authentifizierungstyp Vorinstallierter Schlüssel wird unter Identitätszertifikat festgelegt, welches Zertifikat für die Verbindung verwendet wird:

- Benutzerdefiniertes Zertifikat verwenden: Verwendet das Benutzerzertifikat. Über das optionale Feld Zertifikatsname wird ein bestimmtes Zertifikat anhand des Namens ausgewählt, wenn der Benutzer mehrere Zertifikate dieses Typs besitzt; der Name kann Platzhalter enthalten. Bleibt das Feld leer, wird das am längsten gültige Zertifikat verwendet. Voraussetzung ist, dass dem Gerät ein Benutzer zugewiesen ist, für den ein Benutzerzertifikat existiert.
- Zertifikat wählen: Auswahl eines Zertifikats oder einer Zertifikatsvorlage aus der Zertifikatsverwaltung.

Das Zertifikat wird nur beim Authentifizierungstyp EAP zusammen mit dem VPN-Profil auf dem Gerät installiert.

IKEv2-Parameter

Beim VPN Typ IKEv2 lassen sich zusätzlich die Kryptografie-Parameter festlegen. Standardwert aller Felder ist Nicht konfiguriert.

- IKE SA-Parameter: Verschlüsselungsalgorithmus, Integritätsalgorithmus und Diffie-Hellman-Gruppe
- Untergeordnete SA-Parameter: Verschlüsselungsalgorithmus, Integritätsalgorithmus und Diffie-Hellman-Gruppe (PFS-Gruppe, zusätzlich mit der Option Übergeordnete Diffie-Hellman-Gruppe verwenden)

Es werden entweder alle sechs Werte oder keiner gesetzt; eine teilweise Angabe wird nicht gespeichert.

Apps

Feld	Beschreibung
Apps	Apps, deren Start die VPN-Verbindung automatisch aufbaut. Bei Desktop-Apps wird der Dateipfad zur App eingetragen, bei universellen (UWP) Apps der Name der Paketfamilie
Beschränkt die VPN Verbindung für diese Apps	Wenn aktiviert, läuft nur der Datenverkehr der unter Apps eingetragenen Apps über das VPN

DNS Einstellungen

Das Feld DNS suffix nimmt DNS-Suffixe auf, die zur DNS-Suchliste hinzugefügt werden, damit Kurznamen korrekt aufgelöst werden. Das erste Suffix der Liste wird zugleich als primäres verbindungsspezifisches DNS-Suffix der VPN-Schnittstelle verwendet.

Die Regeln für die Name-Resolution-Policy-Tabelle (NRPT) legen fest, wie DNS-Namen aufgelöst werden, während eine VPN-Verbindung besteht. Jede Regel gibt eine Domäne und die DNS-Server oder den Web-Proxy-Server an, die zur Auflösung dieser Domäne verwendet werden. Über Hinzufügen wird eine Regel mit folgenden Feldern angelegt:

Für Version 26.4.0

Feld	Beschreibung
Domäne	Pflichtfeld. Domäne, für die die Regel gilt
DNS-Server	Ein oder mehrere DNS-Server für diese Domäne
Proxy	Web-Proxy-Server für diese Domäne
Automatisch verbinden	Das Gerät verbindet sich automatisch mit dem VPN, wenn es eine Verbindung zu dieser Domäne herstellt
Persistent	Die Regel bleibt aktiv, auch wenn das VPN nicht verbunden ist

Split tunneling

Split-Tunneling wird über den Schalter Split tunneling aktiviert. Nur dann werden die Einträge unter Split-Tunneling Routen für die VPN-Verbindung an das Gerät übertragen, und nur der Datenverkehr zu diesen Zielen läuft über das VPN.

> Ist der Schalter Split tunneling deaktiviert, wird das Profil als Force Tunnel eingerichtet: Der gesamte Datenverkehr läuft über das VPN, eingetragene Routen werden ignoriert.

Jede Route wird über Hinzufügen als Zielpräfix in CIDR-Schreibweise eingetragen, als IPv4- oder IPv6-Adresse mit Präfixlänge (z. B. `10.22.0.0/16`). Die Präfixlänge (Subnetzmaske) muss größer als 0 sein.

Proxy Konfiguration

Das Feld Proxy Typ bestimmt, welche weiteren Felder erscheinen:

Option	Beschreibung
Keine	Standard. Für die VPN-Verbindung wird kein Proxy konfiguriert
Automatisch	Pflichtfeld Proxy-Konfigurations-URL: gültige URL des Proxy-Konfigurationsskripts
Manuell	Pflichtfelder Proxy-Server und Proxy-Server-Port (Wert 1–65535, vorbelegt mit 1)

Verwandte Themen

- Zertifikate → — Identitäts- und Vertrauenszertifikate bereitstellen.
- WLAN → — Netzwerkprofile für Windows-Geräte.

Windows Firewall

Die Richtlinien-Konfiguration Windows Firewall verwaltet die Windows-Firewall auf verwalteten Geräten. Sie besteht aus drei Teilen: globalen Eigenschaften, Einstellungen je Netzwerkprofil und einzelnen Firewallregeln.

Zum Speichern muss mindestens einer der drei Teile konfiguriert sein — globale Eigenschaften, ein Profil oder eine Firewallregel.

Eine Firewall-Konfiguration kann die Kommunikation zwischen Gerät und MDM-Server unterbrechen. Die Kommunikation mit dem MDM-Server und mit dem Windows-Benachrichtigungsdienst (WNS) darf nicht blockiert werden, sonst lässt sich das Gerät nicht mehr verwalten.

Globale Eigenschaften

Die globalen Eigenschaften gelten profilübergreifend für das gesamte Gerät und stehen im Abschnitt Allgemein. Sie werden über den Schalter Konfigurierung der globalen Einstellungen freigeschaltet; ohne ihn sind die folgenden Felder nicht bearbeitbar und werden nicht übertragen. Wird der Schalter deaktiviert, werden die zuvor übertragenen globalen Eigenschaften wieder vom Gerät entfernt.

Für Version 26.4.0

- Blockiert das statusbehaftete FTP (File Transfer Protocol)
- Leerlaufzeit für Sicherheitszuordnung vor Löschvorgang: Anzahl Sekunden ohne Netzwerkdatenverkehr, nach der eine Sicherheitszuordnung gelöscht wird (300–3600).
- Codierung vorinstallierter Schlüssel
- IPsec-Ausnahmen (Auswahl):
  - Keine
  - Neighbor Discovery-IPv6-Codes vom Typ ICMP
  - ICMP
  - Router Discovery-IPv6-Codes vom Typ ICMP
  - Sowohl IPv4- als auch IPv6-DHCP-Datenverkehr
- Überprüfung der Zertifikatssperrliste (Pflichtfeld, Standard: Deaktiviert):
  - Deaktiviert
  - Überprüfung der Zertifikatssperrliste nur bei gesperrtem Zertifikat fehlerhaft
  - Überprüfung der Zertifikatssperrliste bei jedem Fehler fehlerhaft
- Authentifizierungssatz opportunistisch pro Schlüsselerstellungsmodul abgleichen
- Aktiviert Paketwarteschlange (Standard: Deaktiviert):
  - Deaktiviert
  - Nur eingehende verschlüsselte Pakete in Warteschlange einreihen
  - Pakete nach der Entschlüsselung nur zu Weiterleitung in Warteschlange einreihen

Profileigenschaften

Für jedes Netzwerkprofil – Domänennetzwerk (Arbeitsbereichsnetzwerk), Öffentliches Netzwerk (nicht sichtbar) und Privates Netzwerk (sichtbar) – gibt es einen eigenen Abschnitt mit dem Schalter Konfiguration der Profileigenschaften. Erst wenn er aktiviert ist, lassen sich die folgenden Einstellungen bearbeiten und werden an das Gerät übertragen. Wird er deaktiviert, werden die zuvor übertragenen Einstellungen des Profils wieder vom Gerät entfernt.

- Aktiviert Firewall
  - Geschützt: nur auswählbar, wenn Aktiviert Firewall gesetzt ist; blockiert zusammen mit der Firewall den gesamten eingehenden Datenverkehr.
- Erlaubt die Standardaktion für eingehende Verbindungen (Standard: aktiviert)
- Erlaubt die Standardaktion für ausgehende Verbindungen (Standard: aktiviert)
- Deaktiviert eingehende Benachrichtigungen
- Deaktiviert geschützten Modus
  - Ausnahme für durch IPsec geschützte Pakete bei geschütztem Modus: nur auswählbar, wenn Deaktiviert geschützten Modus gesetzt ist.
- Deaktiviert Unicastantworten auf Multicastbroadcasts
- Firewall-Regeln für autorisierte Anwendungen aus dem lokalen Speicher (Standard: aktiviert)
- Firewall-Regeln für den globalen Port aus dem lokalen Speicher (Standard: aktiviert)
- Firewall-Regeln aus dem lokalen Speicher (Standard: aktiviert)
- IPsec-Regeln aus dem lokalen Speicher (Standard: aktiviert)

Werden die Standardaktionen für eingehende oder ausgehende Verbindungen nicht erlaubt, ist eine Firewallregel erforderlich, die die Verbindungen mit Relution zulässt. Andernfalls kann Relution das Gerät nicht mehr verwalten.

Für Version 26.4.0

Firewallregeln

Die Firewallregeln stehen in einer Liste mit den Spalten Regelname, Regelbeschreibung, Datenverkehrsrichtung und Regel aktiviert. Über Hinzufügen, Bearbeiten und Löschen werden Regeln angelegt, geändert oder entfernt. Je Konfiguration sind maximal 100 Firewallregeln möglich.

Je Regel lassen sich Anwendung, Ports und Netzwerktypen festlegen:

- Regelname (Pflichtfeld)
- Regelbeschreibung
- Regel aktiviert (Standard: aktiviert)
- Erlaubt Verbindung für diese Regel (Standard: aktiviert): legt fest, ob die Regel den Datenverkehr zulässt oder blockiert.
- EdgeTraversal-Einstellung aktiviert (Standard: deaktiviert)
- Datenverkehrsrichtung: Eingehend oder Ausgehend (Standard)
- Netzwerktypen (Pflichtfeld, Mehrfachauswahl):
  - Alle existierenden Netzwerksets und jegliche zukünftige Netzwerksets (Standard; schließt die übrigen Optionen aus)
  - Domäne
  - Privat
  - Öffentlich
- Paketfamilienname der Anwendung, Dateipfad der Anwendung und Windows-Dienst (Abschnitt Anwendung)
- Lokaler Adressbereich und Remote Adressbereich (Abschnitt IP-Adresse): IPv4- oder IPv6-Adressen, als einzelne Adresse oder als Bereich mit Untere Bereichsgrenze und Obere Bereichsgrenze
- IP Protokoll: Zahl von 0 bis 255, mit Vorschlagsliste (z. B. 6 - TCP, 17 - UDP)
- Lokaler Portbereich und Remote Portbereich: Ports von 1 bis 65535, als einzelner Port oder als Bereich
- Schnittstellen-Typen (Mehrfachauswahl, Standard: alle): Lokales Netzwerk, Drahtlosnetzwerke, Remotezugriff
- Lokale Benutzer-Authorisierungsliste: autorisierte lokale Benutzer im SDDL-Format; ohne Angabe gilt die Regel für alle Benutzer. Für Regeln, die auf einen Windows-Dienst zielen, ist keine Liste möglich.

Je Bereichsliste (Lokaler Portbereich, Remote Portbereich, Lokaler Adressbereich, Remote Adressbereich) sind maximal 20 Einträge möglich; Bereiche innerhalb einer Liste dürfen sich nicht überschneiden. Portbereiche stehen nur zur Verfügung, wenn als IP Protokoll 6 - TCP oder 17 - UDP gewählt ist.

Verwandte Themen

- VPN → — VPN-Profile für Windows-Geräte.
- Custom CSP → — Einstellungen, die keine eigene Konfiguration haben.

Für Version 26.4.0

Zertifikate installieren

Mit der Richtlinienkonfiguration Zertifikat für Windows lassen sich über Relution Zertifikate auf Windows 10/11-Geräten installieren. Je nach Zertifikatstyp lassen sich der Zertifikatsspeicher oder der Speicherort von Zertifikat und Schlüssel festlegen.

Zertifikate in Relution hochladen

Um Zertifikate über Relution verteilen zu können, müssen diese zuerst in den Zertifikatsspeicher von Relution hochgeladen werden (siehe auch Zertifikatsverwaltung →).

- Dazu in `Einstellungen` → `Zertifikate` gehen.
- Die Schaltfläche Hinzufügen klicken.
- Einen Namen vergeben, bei passwortgeschützten Zertifikatsdateien (z. B. PKCS#12) das Passwort eingeben und am Schluss die Zertifikatsdatei auswählen.
- Mit Speichern bestätigen.

Anwenden von Zertifikaten auf Windows 10/11-Geräten

Für Version 26.4.0

1. Im Relution-Portal zum Menüpunkt `Geräte` → `Richtlinien` navigieren und auf Hinzufügen klicken.
2. Eine Windows-Richtlinie erstellen und einen Namen vergeben. Auf Speichern klicken.
3. Nach Klick auf Hinzufügen anschließend die Option Zertifikat auswählen und mit Details hinzufügen fortfahren.
4. Unter Zertifikat die Option Zertifikat wählen und das im vorherigen Abschnitt hochgeladene Zertifikat auswählen. Die weiteren Optionen hängen vom Zertifikatstyp ab:
   - Zertifikat ohne privaten Schlüssel (PEM/DER): den Zertifikatsspeicher wählen (Standard: Automatisch).
   - PKCS#12-Zertifikat (.p12/.pfx), Zertifikatsvorlage oder Benutzerzertifikat: unter Speicherort des Zertifikats (im Portal: Speicherort der Zertifikats) zwischen Gerät (Standard) und Benutzer wählen, den Speicherort des Zertifikatsschlüssels (im Portal: Speicherort des Zertifikatsschlüssel) festlegen (TPM, TPM falls verfügbar, Software oder Windows Hello für Unternehmen; Standard: Software) und bei Bedarf Schlüssel ist exportierbar aktivieren. Der Schalter ist nur bei Software verfügbar.
5. Die Konfiguration speichern und die aktuelle Version der Richtlinie veröffentlichen.
6. Um die Richtlinie auf Windows 10/11-Geräten anzuwenden, die gewünschten Geräte über das Tab Geräte mit dieser Richtlinie hinzufügen. Die gewählten Zertifikate werden anschließend automatisch auf den Geräten installiert.

> Für die Installation von MSIX-Dateien muss als Zertifikatsspeicher die Option Vertrauenswürdige Stammzertifikate ausgewählt werden, und es muss ein aus dem PKCS#12-Container exportiertes einzelnes Zertifikat (PEM-Format) verwendet werden.

Bei Automatisch wählt Relution den Speicher anhand des Zertifikats: selbstsignierte CA-Zertifikate werden unter Vertrauenswürdige Stammzertifikate installiert, übrige CA-Zertifikate unter Zwischenzertifizierungsstellen und alle anderen Zertifikate unter Eigene Zertifikate. Wird der Zertifikatsspeicher einer bestehenden Konfiguration geändert, entfernt Relution das Zertifikat aus dem bisherigen Speicher.

Das Zertifikat einer bestehenden Konfiguration lässt sich nachträglich nicht mehr ändern. Für ein anderes Zertifikat wird eine neue Konfiguration angelegt. Konfigurationen, die mit einer Version vor Relution 5.25 erstellt wurden, lassen sich nicht mehr bearbeiten und müssen ebenfalls neu angelegt werden.

Zertifikate aus Zertifikatsvorlagen verteilen

Seit Relution 26.0 ist es zudem möglich, Zertifikate aus Zertifikatsvorlagen direkt auf Windows-Geräte zu verteilen. Die Vorlage (z. B. eine Vorlage der Built-In CA →) wird im Schritt 4 über Zertifikat wählen anstelle eines hochgeladenen Zertifikats ausgewählt. Anschließend gelten die Optionen für PKCS#12-Zertifikate (Speicherort des Zertifikats und des Schlüssels).

Benutzerzertifikate verteilen

Alternativ zu Zertifikat wählen kann unter Zertifikat die Option Benutzerdefiniertes Zertifikat verwenden gewählt werden. Installiert wird dann das Benutzerzertifikat aus dem Profil des Benutzers, der dem Gerät zugewiesen ist (siehe Benutzerzertifikate →). Das optionale Feld Zertifikatsname wählt ein bestimmtes Zertifikat anhand des Namens aus, wenn der Benutzer mehrere besitzt, und kann Platzhalter enthalten. Bleibt es leer, wird das am längsten gültige Zertifikat verwendet. Auch hier gelten die Optionen für PKCS#12-Zertifikate.

Für Version 26.4.0

Windows Shared PC

Mit der Richtlinienkonfiguration Windows Shared PC ermöglicht es Relution, Windows-10/11-Geräte benutzerübergreifend zu nutzen. Um einen jederzeit datenschutzkonformen Einsatz zu gewährleisten und die Löschung von benutzerspezifischen Daten auf den Geräten sicherzustellen, erlaubt Shared PC diverse datenrelevante Einstellungen und Beschränkungen.

Diese Funktion ist besonders nützlich im Schul-, Bildungs- und Forschungskontext sowie für öffentliche Einrichtungen und Unternehmen, die gemeinsam geteilte PCs jederzeit datenschutzkonform nutzen möchten, ohne dass jeder Benutzer einen eigenen Computer benötigt.

Die Konfiguration wird auf Windows 10/11 Pro, Enterprise und Education angewendet. Windows Home wird nicht unterstützt.

Wie wird die Richtlinienkonfiguration Windows Shared PC konfiguriert?

Um Shared PC erfolgreich auf einem Windows-Gerät auszuführen, wird zuerst unter dem Menüpunkt `Geräte` → `Richtlinien` eine neue Richtlinie hinzugefügt.

Sobald die Richtlinie angelegt ist, kann die Konfiguration Shared PC ausgewählt und in der Richtlinie hinzugefügt werden. Alternativ können bereits bestehende Richtlinien um die Konfiguration Shared PC ergänzt werden.

In der Konfiguration können folgende Einstellungen vorgenommen werden:

Für Version 26.4.0

- Erlaube, dass nur ein einziger Benutzer gleichzeitig angemeldet ist: Dieser Schalter aktiviert den Shared-PC-Modus des Geräts und ist standardmäßig eingeschaltet. Wird er deaktiviert, ist der Shared-PC-Modus auf dem Gerät ausgeschaltet.
- Konten, die sich anmelden können: Es wird festgelegt, ob sich nur Domänenkonten (Domäne) oder zusätzlich Gastkonten ohne Passwort (Gast und Domain, Standard) auf den Geräten anmelden können. Nach der Abmeldung aus dem Gast-Modus werden alle temporären Daten immer automatisch gelöscht.
- Automatisches Löschen von Konten nach Wartungen oder Abmeldungen: Wenn aktiviert, löscht Windows zwischengespeicherte Konten, um Speicherplatz freizugeben (standardmäßig deaktiviert). Unter Geben Sie an, wann Konten gelöscht werden stehen folgende Optionen zur Wahl:
  - Sofort löschen: Konten werden bei der Abmeldung gelöscht.
  - Löschen bei Speicherplatzschwelle: Konten werden gelöscht, sobald der freie Speicherplatz unter den Wert in Beginne mit dem Löschen von Konten, wenn der freie Speicherplatz knapp ist fällt. Das Löschen endet, sobald der Wert in Löschung von Konten stoppen, wenn ausreichend freier Speicherplatz vorhanden ist erreicht ist. Beide Werte werden in Prozent angegeben (0–100, Standard 25). Konten, die am längsten inaktiv sind, werden zuerst gelöscht.
  - Löschen bei Speicherplatz- oder Inaktivitätsschwelle (Standard): Wie zuvor, zusätzlich werden Konten nach der in Inaktive Tage nach der Löschung des Kontos angegebenen Anzahl inaktiver Tage gelöscht (Standard 30).
- Beschränken Sie den Zugriff auf lokalen Speicher: Bei Aktivierung dieser Einstellung verfügt der Nutzer lediglich über Zugriff auf eigene Daten (standardmäßig deaktiviert).
- Bildungsumgebung aktivieren: Die Online-Suche kann stark eingegrenzt und für gewisse Websites komplett gesperrt werden (standardmäßig deaktiviert).
- Anmeldung nach dem Standbymodus erforderlich: Wird bei einer aktiven Anmeldung das Gerät in den Standbymodus versetzt, ist eine erneute Anmeldung erforderlich. Die Einstellung ist standardmäßig aktiviert.
- Gehen Sie nach einer bestimmten Zeit in den Schlafmodus: Um den Akku zu schonen, wird im Feld Sekunden, bis der Standbymodus aktiviert wird festgelegt, nach welcher Zeit das Gerät in den Standbymodus wechselt (standardmäßig aktiviert, 300 Sekunden).
- Tageszeit, zu der die Wartung beginnt: Uhrzeit, zu der das tägliche Wartungsfenster von Windows beginnt (Standard: 00:00). In diesem Zeitraum führt Windows Wartungsaufgaben aus, z. B. das Löschen von Konten gemäß der eingestellten Löschoption.

Für Version 26.4.0

Auf Windows-Pro-Geräten setzt eine Hintergrundbild-Konfiguration eine aktivierte Bildungsumgebung voraus. Ist auf dem Gerät eine Shared-PC-Konfiguration angewendet, in der Bildungsumgebung aktivieren ausgeschaltet ist (Standard), kann kein Hintergrundbild konfiguriert werden. Ohne Shared-PC-Konfiguration aktiviert die Hintergrundbild-Konfiguration die Bildungsumgebung selbst.

Windows Skript Konfiguration

Für verwaltete Windows-Geräte steht in Relution eine Richtlinienkonfiguration für die Anwendung von PowerShell-Skripten zur Verfügung. Die Konfiguration heißt in der Auswahl Script und kann, wie gewohnt, in Windows Richtlinien hinzugefügt werden. Ausgeführt wird sie über den Windows Companion →, der dafür auf dem Gerät installiert sein muss.

Vorbereitend muss jedoch im Menü unter Skripte das zu verteilende Powershell Skript hinterlegt werden.

> Das Skript ist nicht von Relution implementiert, daher übernehmen wir keine Garantie für etwaige Schäden. Das Skript sollte vor der Anwendung auf einem Gerät sorgfältig inspiziert werden. Zudem kann Relution bei eventuell auftretenden Fehlern oder der Erstellung der Skripte keinen Support leisten.

Konfiguration der Richtlinie

Die Richtlinie bietet, neben der Auswahl des gewünschten Skripts, diverse weitere Konfigurationsmöglichkeiten. Mindestens eine der beiden Ausführungsarten (ereignisbasiert oder zeitbasiert) muss aktiviert sein.

Auszuführendes Skript

Hier muss das zuvor hinterlegte Skript ausgewählt werden. Es ist immer nur ein Skript pro Konfiguration wählbar; zur Auswahl stehen PowerShell-Skripte für Windows. Platzhalter im Skriptinhalt werden vor der Auslieferung für jedes Gerät ersetzt (siehe Erweiterte Platzhalter →).

Für Version 26.4.0

Ereignisbasierte Ausführung

Mit dem Schalter Skript für die folgenden Ereignisse auf dem Gerät ausführen wird die Ausführung des Skripts von bestimmten Ereignissen auf dem Gerät abhängig gemacht. Unter Geräteereignisse muss dann mindestens eines der folgenden Ereignisse gewählt werden:

- Gerätestart
- Benutzer hat sich angemeldet – optional beschränkt das Feld Beschränkt den Anmeldetrigger auf einen bestimmten Benutzer die Ausführung auf einen Benutzer. Unterstützt werden die SID des Benutzers sowie die Formate `Domain\Username` und `Username`. Bleibt das Feld leer, wird das Skript bei der Anmeldung jedes Benutzers ausgeführt.
- Benutzer hat sich abgemeldet – beim Herunterfahren bleiben nur wenige Sekunden für die Ausführung, danach bricht das Gerät sie ab.

Zeitbasierte Ausführung

Mit dem Schalter Skript in der folgenden Zeitspanne ausführen werden Skripte zu bestimmten Zeitpunkten auf dem Zielgerät regelmäßig ausgeführt. Pflichtangaben sind die Wochentage unter Wiederholt sich am, die Startzeit (Standard: 08:00) und die Zeitzone (Standard: Europe/Paris).

Ausführung limitieren

Die Ausführung des Skripts lässt sich unter bestimmten Umständen auch verhindern bzw. das Verhalten anpassen. Alle Optionen sind standardmäßig deaktiviert. Mögliche Konfigurationen sind:

- Ausführung im Akkubetrieb nicht zulassen
- Ausführung stoppen, wenn auf Batteriebetrieb umgeschaltet wird
- Weckt das Gerät für Skriptausführung auf
- Task zur Skriptausführung auf dem Gerät ausblenden
- Erlauben Sie, die Skriptausführung bei Bedarf zu starten – erlaubt den manuellen Start der Skriptausführung bei Bedarf.

Für Version 26.4.0

Windows Bitlocker

Mit Relution kann die BitLocker-Verschlüsselung in einer Richtlinie für Windows-Geräte konfiguriert werden. Details zu BitLocker und dessen Funktionsweise kann der Microsoft Dokumentation → entnommen werden.

Konfiguration

Die Konfiguration ist in vier Bereiche gegliedert: Basiseinstellungen, OS Datenträger, Verbaute Festplatten und Entfernbare Festplatten.

Für OS Datenträger, verbaute und entfernbare Festplatten werden jeweils der Verschlüsselungstyp (Vollständig, Nur genutzter Speicherplatz, Wahl durch Benutzer oder Nicht konfiguriert) und die Verschlüsselungsmethode (AES 128bit CBC, AES 256bit CBC, XTS 128bit AES oder XTS 256bit AES) festgelegt. Die Verschlüsselungsmethode muss in allen drei Bereichen gesetzt sein oder in allen drei auf Nicht konfiguriert stehen, sonst lässt sich die Richtlinie nicht speichern.

Änderungen an der Konfiguration wirken sich nicht auf Laufwerke aus, die bereits verschlüsselt sind oder gerade verschlüsselt werden.

Basiseinstellungen

Für Version 26.4.0

- Geräte Verschlüsselung erforderlich: Aktiviert die vollständige Verschlüsselung für OS-Laufwerke und verbaute Festplatten (Standard: aktiviert).
- Erlauben Sie Standardbenutzern, die BitLocker-Verschlüsselung unbeaufsichtigt zu aktivieren: Erlaubt die stille Verschlüsselung auch für Benutzer ohne Administratorrechte. BitLocker muss dafür für die stille Verschlüsselung konfiguriert sein.
- Warnung zu Festplatten Verschlüsselung von Drittanbietern anzeigen: Wirkt nur auf Geräten, die in Microsoft Entra ID eingebunden sind. Die Option wird automatisch deaktiviert und gesperrt, sobald die stille Verschlüsselung für Standardbenutzer aktiviert ist.

OS Datenträger

- Wiederherstellungsoptionen vor dem Start (Text bzw. URL auf dem Wiederherstellungsbildschirm vor dem Start, wenn das OS-Laufwerk gesperrt ist):
  - Standard Wiederherstellungs-Nachricht und -URL vor dem Start
  - Benutzerdefinierte Wiederherstellungs-URL vor dem Start
  - Benutzerdefinierte Wiederherstellungs-Nachricht vor dem Start
- Authentifizierung beim Starten erforderlich: Nach Aktivierung stehen zusätzlich folgende Einstellungen zur Verfügung:
  - Minimale PIN-Länge: 4 bis 20 Ziffern, Standard 6.
  - Trusted Platform Module (TPM) auf inkompatiblen Geräten: Erlaubt BitLocker ohne TPM. Dann ist ein Kennwort oder ein Startschlüssel auf einem USB-Laufwerk erforderlich.
  - TPM Start, TPM Start PIN, TPM Startschlüssel und TPM Start PIN und Startschlüssel: jeweils Nicht konfiguriert, Optional, Erforderlich oder Blockiert. Steht eine dieser Optionen auf Erforderlich, müssen die übrigen drei auf Blockiert stehen. Ist Trusted Platform Module (TPM) auf inkompatiblen Geräten nicht aktiviert, dürfen nicht alle vier blockiert sein.
  - Wiederherstellung konfigurieren mit:
    - Daten Wiederherstellung erlauben
    - Wiederherstellungspasswort erstellen
    - Wiederherstellungsschlüssel erstellen
    - Wiederherstellungsbildschirm während der BitLocker Einrichtung verbergen
    - Wiederherstellungsinformationen in Active Directory Domain Services speichern (wahlweise nur das Wiederherstellungspasswort oder Wiederherstellungspasswort und -schlüssel)
    - BitLocker Einrichtung deaktivieren bis Wiederherstellungsinformationen in Active Directory Domain Services gespeichert sind

Für Version 26.4.0

Verbaute Festplatten

- Verschlüsselung erforderlich: Nicht durch BitLocker geschützte verbaute Festplatten werden nur lesend eingebunden.
- Wiederherstellungsoptionen: Nach Aktivierung stehen zur Verfügung:
  - Wiederherstellungs-Agent erlauben
  - Wiederherstellungspasswort erstellen
  - Wiederherstellungsschlüssel erstellen
  - Wiederherstellungsbildschirm während der BitLocker Einrichtung verbergen
  - Wiederherstellungsinformationen in Active Directory Domain Services speichern (wahlweise nur das Wiederherstellungspasswort oder Wiederherstellungspasswort und -schlüssel)
  - BitLocker Einrichtung deaktivieren bis Wiederherstellungsinformationen in Active Directory Domain Services gespeichert sind

Für Wiederherstellungspasswort erstellen und Wiederherstellungsschlüssel erstellen stehen Erlaubt, Erforderlich (Standard) und Blockiert zur Auswahl. Für OS Datenträger und verbaute Festplatten gelten dabei dieselben Regeln:

- Passwort und Schlüssel dürfen nicht beide blockiert sein.
- Das Wiederherstellungspasswort darf nicht blockiert sein, wenn die Wiederherstellungsinformationen in Active Directory Domain Services gespeichert werden.
- Das Wiederherstellungspasswort darf nicht auf Erforderlich stehen, wenn der Wiederherstellungsbildschirm verborgen wird und die Speicherung in Active Directory Domain Services nicht aktiviert ist.
- Der Wiederherstellungsschlüssel darf nicht auf Erforderlich stehen, wenn bei den entfernbaren Festplatten Verschlüsselung erforderlich aktiviert ist.

Entfernbare Festplatten

- Verschlüsselung erforderlich: Nicht durch BitLocker geschützte entfernbare Festplatten werden nur lesend eingebunden.
- Schreibenden Zugriff auf Geräte verweigern, die in anderen Organisationen konfiguriert sind: Schreibzugriff erhalten nur Laufwerke, deren Kennungsfelder zu denen des Computers passen.

Für entfernbare Festplatten stehen keine Wiederherstellungsoptionen zur Verfügung.

Bitlocker-Informationen in den Gerätedetails

Ab Server 5.21 zeigt Relution in den Gerätedetails unter Bitlocker-Informationen je Laufwerk Volume, Volume Status, Schutzstatus und Zusätzliche Informationen an. Ist für ein Laufwerk ein Wiederherstellungspasswort vorhanden, wird es dort mit Zeitstempel unter Passwort für die Wiederherstellung gespeichert. Die Informationen werden erst nach Klick auf Anzeigen geladen.

Geräteverschlüsselung ohne Benutzerinteraktion

BitLocker kann auf dem Gerät unter bestimmten Voraussetzungen ohne Benutzeraktion aktiviert werden. Dies gilt auch für Nutzer mit Standard-Rechten.

Die Geräte müssen dafür folgende Voraussetzungen erfüllen:

- Version 1803 oder höher für Endbenutzer mit Administrator-Berechtigung
- Version 1809 oder höher für Endbenutzer mit Standard-Berechtigung
- Eingebunden in Microsoft Entra oder Microsoft Entra hybrid oder Aktivierung über die Aktion Bitlocker aktivieren in Relution (setzt den installierten Relution Companion für Windows → voraus)
- Mindestens TPM 1.2
- BIOS-Modus Einstellung: `Native UEFI`

Für Version 26.4.0

Microsoft Entra oder Microsoft Entra hybrid eingebundene Geräte

Sind Geräte in Relution eingeschrieben und zusätzlich in Microsoft Entra eingebunden (z.B. über Autopilot), dann kann die BitLocker Konfiguration wie folgt konfiguriert werden, damit die Geräte automatisiert verschlüsselt werden, sobald die Konfiguration auf dem Gerät angewendet wird.

Basiseinstellungen:

- Geräte Verschlüsselung erforderlich: Aktiviert
- Erlauben Sie Standardbenutzern, die BitLocker-Verschlüsselung unbeaufsichtigt zu aktivieren: Aktiviert

OS Datenträger:

- Verschlüsselungstyp: Vollständig
- Authentifizierung beim Starten erforderlich: Aktiviert
- TPM Start: Optional oder Erforderlich
- TPM Start PIN: Blockiert
- TPM Startschlüssel: Blockiert
- TPM Start PIN und Startschlüssel: Blockiert
- Wiederherstellung konfigurieren: Deaktiviert
  - Alternativ kann es auch aktiviert werden, dann müssen jedoch folgende Punkte ebenfalls konfiguriert werden:
  - Wiederherstellungspasswort erstellen: Erlaubt. Erforderlich lässt sich nur speichern, wenn zusätzlich Wiederherstellungsinformationen in Active Directory Domain Services speichern aktiviert ist.
  - Wiederherstellungsschlüssel erstellen: Erlaubt oder Erforderlich. Erforderlich ist nicht zulässig, wenn bei den entfernbaren Festplatten Verschlüsselung erforderlich aktiviert ist.
  - Wiederherstellungsbildschirm während der BitLocker Einrichtung verbergen: Aktiviert

Andere Einstellungsmöglichkeiten in der Konfiguration können je nach Bedarf gesetzt werden. Nicht unterstützte Einstellungen können jedoch zu Problemen bei der Aktivierung von BitLocker führen.

Mittels Aktion - Bitlocker aktivieren

Geräte, die nicht in Microsoft Entra oder Microsoft Entra hybrid eingeschrieben sind, können die BitLocker-Verschlüsselung ohne Endbenutzer Interaktion über die Aktion Bitlocker aktivieren starten. Dies funktioniert ebenfalls für Standardbenutzer.

Die Aktion wird ausschließlich vom Relution Companion für Windows → ausgeführt. Der Companion muss daher auf dem Gerät installiert sein.

In der Aktion werden je Laufwerk (Laufwerksbuchstabe mit Doppelpunkt, z. B. `C:`) der Schutzschlüssel und die Option Nur genutzter Speicherplatz festgelegt. Als Schutzschlüssel stehen TPM (nur für das Betriebssystem-Laufwerk) und Wiederherstellungspasswort zur Verfügung. Das Wiederherstellungspasswort wird von Windows erzeugt und erscheint in den Gerätedetails unter Bitlocker-Informationen. Mit der Aktion Bitlocker deaktivieren wird die Verschlüsselung für ausgewählte Laufwerke wieder aufgehoben.

Für Version 26.4.0

Es wird jedoch empfohlen, zunächst eine BitLocker Konfiguration auf dem Gerät anzuwenden, um z.B. die Verschlüsselungsmethode oder andere Einstellungen festzulegen, auch wenn dies für die automatische Aktivierung nicht zwingend erforderlich ist.

Compliance-Meldungen

Weicht der Zustand des Geräts von der BitLocker-Richtlinie ab, meldet Relution am Gerät einen Compliance-Verstoß mit der Beschreibung `BitLocker Configuration violated. Messages:` und einer Liste der von Windows gemeldeten Ursachen. Die Meldungen erscheinen nur auf Englisch. Für häufige Meldungen sind im Folgenden Lösungen beschrieben.

The BitLocker policy requires a TPM protector to protect the OS volume, but a TPM is not used

- Folgende Konfiguration im Bereich OS Datenträger anwenden:
  - Authentifizierung beim Starten erforderlich → Aktiviert
  - Trusted Platform Module (TPM) auf inkompatiblen Geräten → Aktiviert
  - TPM Start → Erforderlich
  - TPM Start PIN → Blockiert
  - TPM Startschlüssel → Blockiert
  - TPM Start PIN und Startschlüssel → Blockiert

The encryption method of the OS volume doesn't match the BitLocker policy

- Mit folgendem Befehl die Verschlüsselungsmethode am Gerät ermitteln:

```
manage-bde -status
```

- Ergebnis: AES oder XTS mit 128 oder 256 Bit
- Die ermittelte Methode in der Richtlinie im Bereich OS Datenträger im Feld Verschlüsselungsmethode konfigurieren (z. B. XTS 256bit AES). Die Verschlüsselungsmethode muss auch in den Bereichen Verbaute Festplatten und Entfernbare Festplatten gesetzt sein, sonst lässt sich die Richtlinie nicht speichern.

Für Version 26.4.0

The BitLocker policy requires a TPM-only protector for the OS volume, but TPM protection is not used

- Der Verschlüsselungstyp im Bereich OS Datenträger muss von Vollständig auf Nur genutzter Speicherplatz gesetzt werden.

Verwandte Themen

- Windows-Geräte manuell einschreiben → — Manuelle Einschreibung von Windows-Geräten.

Companion konfigurieren

Über die Richtlinienkonfiguration Windows Companion lässt sich das Verhalten des Relution Companion für Windows → auf verwalteten Windows-Geräten steuern. Die Konfiguration ist in vier Abschnitte unterteilt: Allgemein, Handhabung von Apps, Server-Kommunikation sowie Benutzerwechsel beim Anmelden.

Detaillevel der Log-Ausgabe

Legt fest, wie detailliert der Windows Companion Log-Einträge schreibt. Zur Auswahl stehen Kein, Kritisch, Fehler, Warnung, Informationen, Debug und Trace – mit jeder Stufe steigt die Ausführlichkeit der Protokollierung. Standardwert ist Informationen.

Maximaldauer für Aktionsausführung

Legt die maximale Dauer in Minuten fest, für die eine Aktion verarbeitet werden darf, bevor sie vom Windows Companion abgebrochen wird. Standardwert sind 45 Minuten, zulässig sind 15 bis 180 Minuten.

Für Version 26.4.0

Maximaldauer für App-Installationen

Legt die maximale Dauer in Minuten fest, für die eine App-Installation verarbeitet werden darf, bevor sie vom Windows Companion abgebrochen wird. Standardwert sind 45 Minuten, zulässig sind 1 bis 150 Minuten.

Maximaldauer für das Entfernen von Apps

Legt die maximale Dauer in Minuten fest, für die eine App-Deinstallation verarbeitet werden darf, bevor sie vom Windows Companion abgebrochen wird. Standardwert sind 45 Minuten, zulässig sind 1 bis 150 Minuten.

WinGet und seine Abhängigkeiten verwalten

Legt fest, ob WinGet und seine Abhängigkeiten, wie Microsoft VC Redistributable, vom Windows Companion verwaltet und automatisch aktualisiert werden. Die Option ist standardmäßig aktiviert. Ist sie deaktiviert, aktualisiert der Companion WinGet nicht mehr; ein fehlendes Microsoft VC Redistributable wird aber weiterhin installiert, damit WinGet-Befehle funktionieren.

Server-Kommunikation

Die Kommunikation zwischen dem Relution Companion und dem Relution Server ist notwendig, damit Relution richtig funktioniert. Eine Kommunikation wird entweder eingeleitet durch:

- den Server, der dem Companion mitteilt, die Kommunikation zu starten
- den Companion, wenn für einige Zeit keine Interaktion zwischen Server und Companion stattgefunden hat

Mit den folgenden Einstellungen lässt sich das Verhalten dieser Mechanik optimieren, auch wenn dies in der Regel nicht notwendig ist. Nach der unter Prüfintervall definierten Zeit startet der Companion die Kommunikation, wenn die letzte Kommunikation mit dem Server älter ist als die unter Dauer seit letzter Kommunikation angegebene Zeit.

Prüfintervall

Legt das Intervall in Minuten fest, in dem der Windows Companion prüft, ob eine Anfrage an den Relution Server erforderlich ist. Standardwert sind 180 Minuten, zulässig sind 15 bis 1.440 Minuten.

Dauer seit letzter Kommunikation

Definiert die Mindestzeit in Minuten, die der Windows Companion wartet, um die nächste Anfrage an den Relution Server auszuführen. Standardwert sind 120 Minuten, zulässig sind 15 bis 600 Minuten.

Für Version 26.4.0

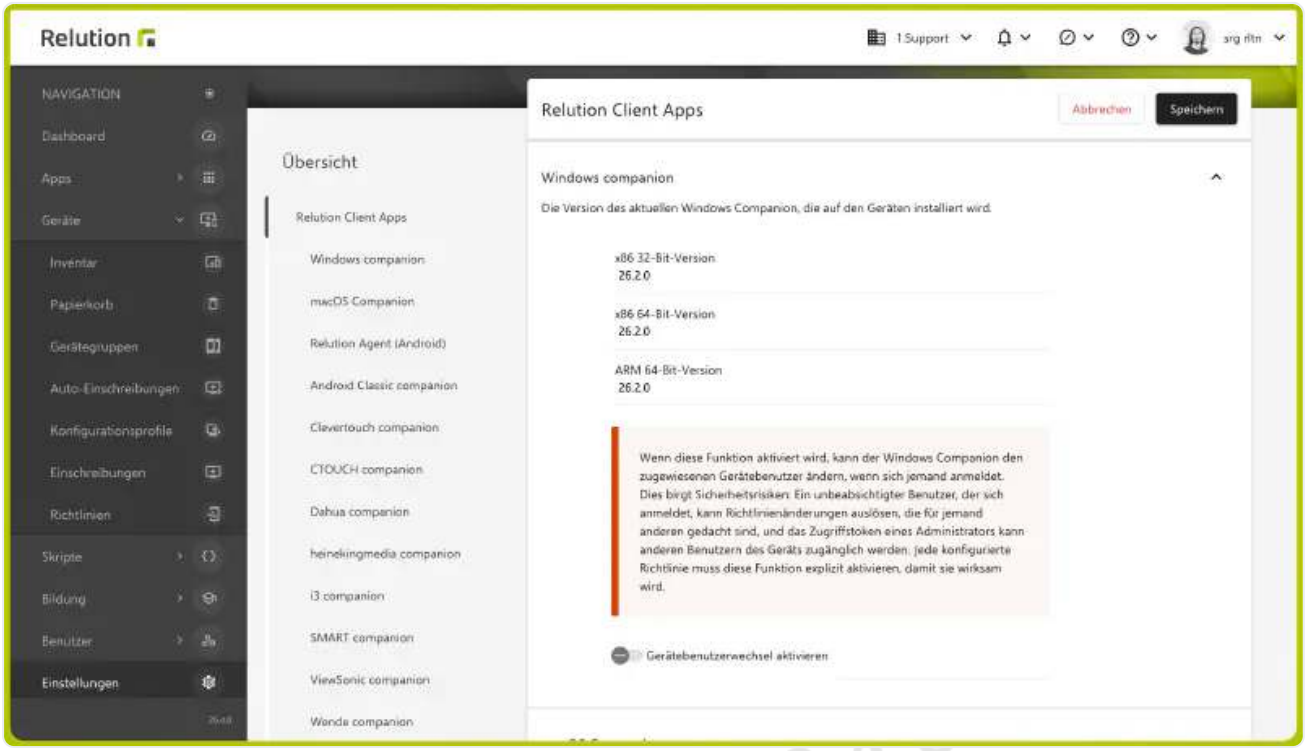
Benutzerwechsel beim Anmelden

Ab Version 26.4 kann der Relution Companion für Windows den einem Gerät in Relution zugewiesenen Benutzer automatisch aktualisieren, sobald sich eine andere Person am Windows-Gerät anmeldet. Das ist besonders für Geräte nützlich, die sich mehrere Personen teilen, z. B. im Klassenzimmer oder Großraumbüro: Der in Relution hinterlegte Gerätebenutzer entspricht so stets der Person, die aktuell tatsächlich am Gerät angemeldet ist.

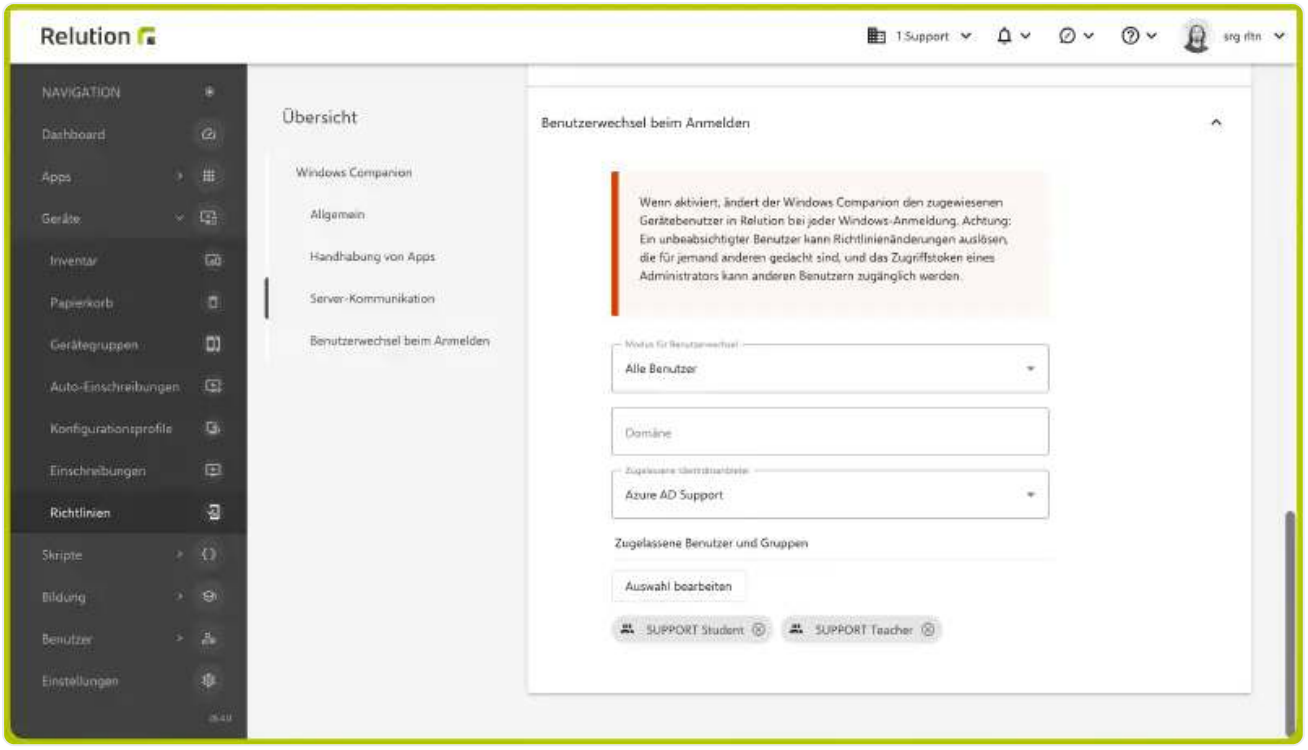
Aktivierung

Die Funktion muss an zwei Stellen aktiviert werden, bevor sie wirkt:

1. Organisationsweit unter `Einstellungen` → `Relution Client Apps` → `Windows companion` über den Schalter Gerätebenutzerwechsel aktivieren. Die Einstellung steht nur in Organisationen unterhalb der globalen Organisation zur Verfügung und setzt die Berechtigung für Relution Client Apps voraus.



2. Zusätzlich in jeder Richtlinie, die dies nutzen soll, im Abschnitt `Windows Companion` → `Benutzerwechsel beim Anmelden` über den Modus für Benutzerwechsel. Ist der Schalter auf Organisationsebene deaktiviert, lässt sich in der Richtlinie nur der Modus Deaktiviert speichern; wird der Schalter nachträglich ausgeschaltet, zeigen bestehende Richtlinien beim Öffnen einen entsprechenden Fehler.



Für Version 26.4.0

Wenn diese Funktion aktiviert wird, kann der Windows Companion den zugewiesenen Gerätebenutzer ändern, wenn sich jemand anmeldet. Dies birgt Sicherheitsrisiken: Ein unbeabsichtigter Benutzer, der sich anmeldet, kann Richtlinienänderungen auslösen, die für jemand anderen gedacht sind, und das Zugriffstoken eines Administrators kann anderen Benutzern des Geräts zugänglich werden. Jede konfigurierte Richtlinie muss diese Funktion explizit aktivieren, damit sie wirksam wird.

Modus für Benutzerwechsel

- Deaktiviert: Kein automatischer Benutzerwechsel.
- Nur Domänenbenutzer: Der Wechsel erfolgt nur, wenn der UPN der sich anmeldenden Person zu der im Feld Domäne angegebenen Domäne passt (ohne Beachtung der Groß-/Kleinschreibung) und die Person in Relution zu einem der unter Zugelassene Identitätsanbieter ausgewählten Anbieter gehört. Domäne und mindestens ein zugelassener Identitätsanbieter sind hierfür erforderlich. Voraussetzung ist mindestens ein aktiver Identitätsanbieter in der Organisation; ohne ihn ist das Feld Zugelassene Identitätsanbieter nicht auswählbar und die Richtlinie lässt sich in diesem Modus nicht speichern.
- Alle Benutzer: Domäne und Zugelassene Identitätsanbieter sind optional. Ist eine Domäne angegeben, erfolgt der Wechsel nur, wenn der UPN zu ihr passt (ohne Beachtung der Groß-/Kleinschreibung); sind Identitätsanbieter ausgewählt, muss die Person zu einem davon gehören. Bleiben beide Felder leer, wird nicht danach gefiltert.

In beiden aktiven Modi lässt sich der Wechsel zusätzlich über Zugelassene Benutzer und Gruppen (Schaltfläche Auswahl bearbeiten) einschränken. Zugelassen sind dann die ausgewählten Benutzer sowie Mitglieder der ausgewählten Gruppen. Bleibt das Feld leer, gilt keine zusätzliche Einschränkung.

Die Zuordnung erfolgt anhand des Windows-Anmeldenamens, der mit dem Benutzernamen in Relution innerhalb derselben Organisation abgeglichen wird. Ist die sich anmeldende Person in Relution nicht bekannt oder erfüllt sie die konfigurierten Bedingungen nicht, wird der zugewiesene Gerätebenutzer entfernt; es erfolgt jedoch keine Fehlermeldung auf dem Gerät. In den Gerätedetails wird bei jedem Wechsel das Feld Letzter verbundener Entra ID Benutzer aktualisiert; bei in Relution unbekannten Personen steht dort der Windows-Anmeldename im Format `Domäne\Benutzer`.

Für Version 26.4.0

Windows App Installation

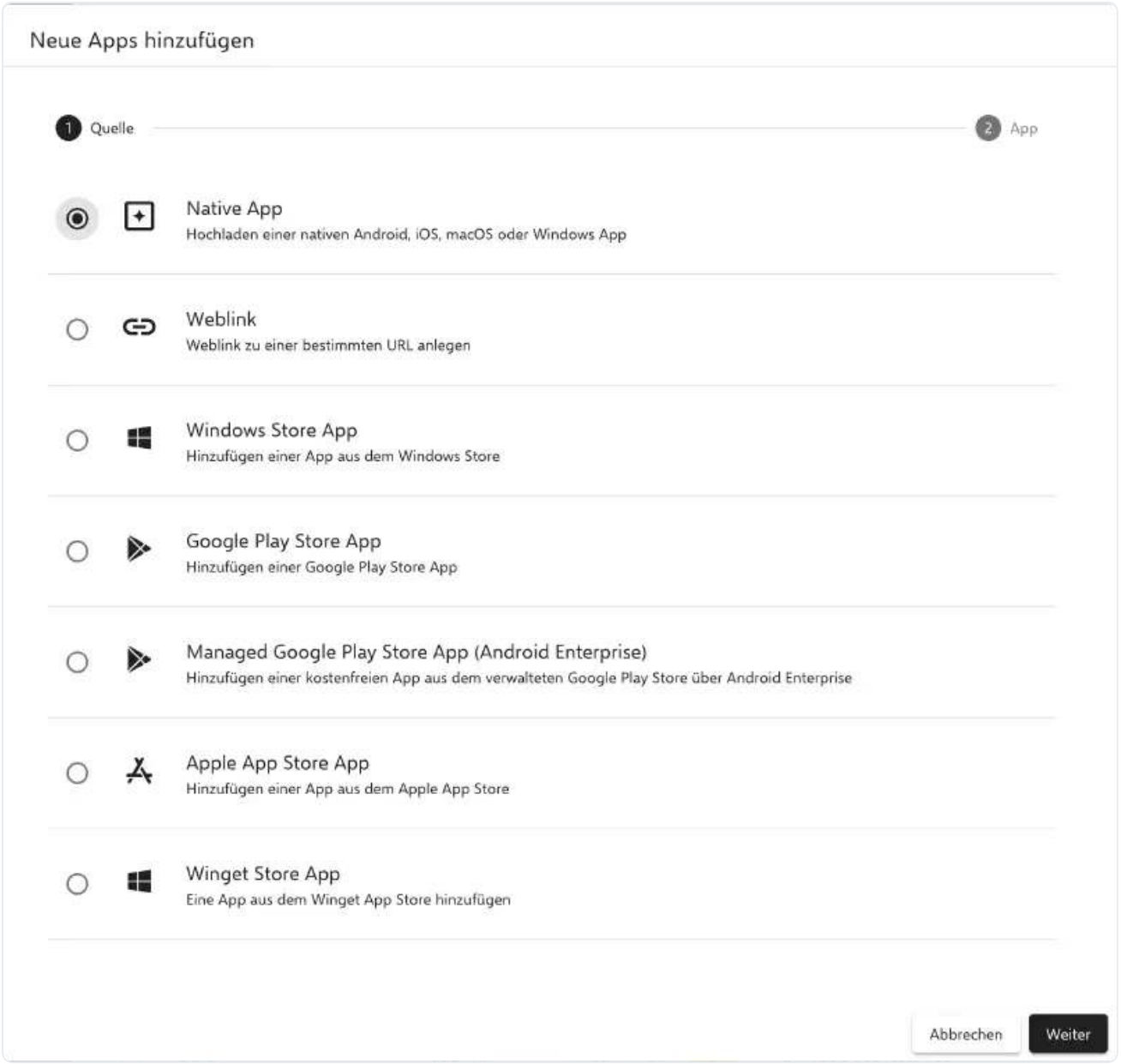
Klassische Apps (`.msi`- und `.exe`-Anwendungen) lassen sich über das Portal in den Relution App Store hochladen und auf allen durch Relution verwalteten Windows-Geräten installieren und wieder deinstallieren. Installation, Erkennung und Deinstallation übernimmt der Relution Companion auf dem Gerät; er muss deshalb auf den Zielgeräten installiert sein: Windows Companion →

Pakete im Format `.msix`, `.msixbundle`, `.appx` oder `.appxbundle` werden ebenfalls als Native App hochgeladen, benötigen aber weder Erkennungsregeln noch Parameter für die Installation: MSIX-Dateien erstellen →

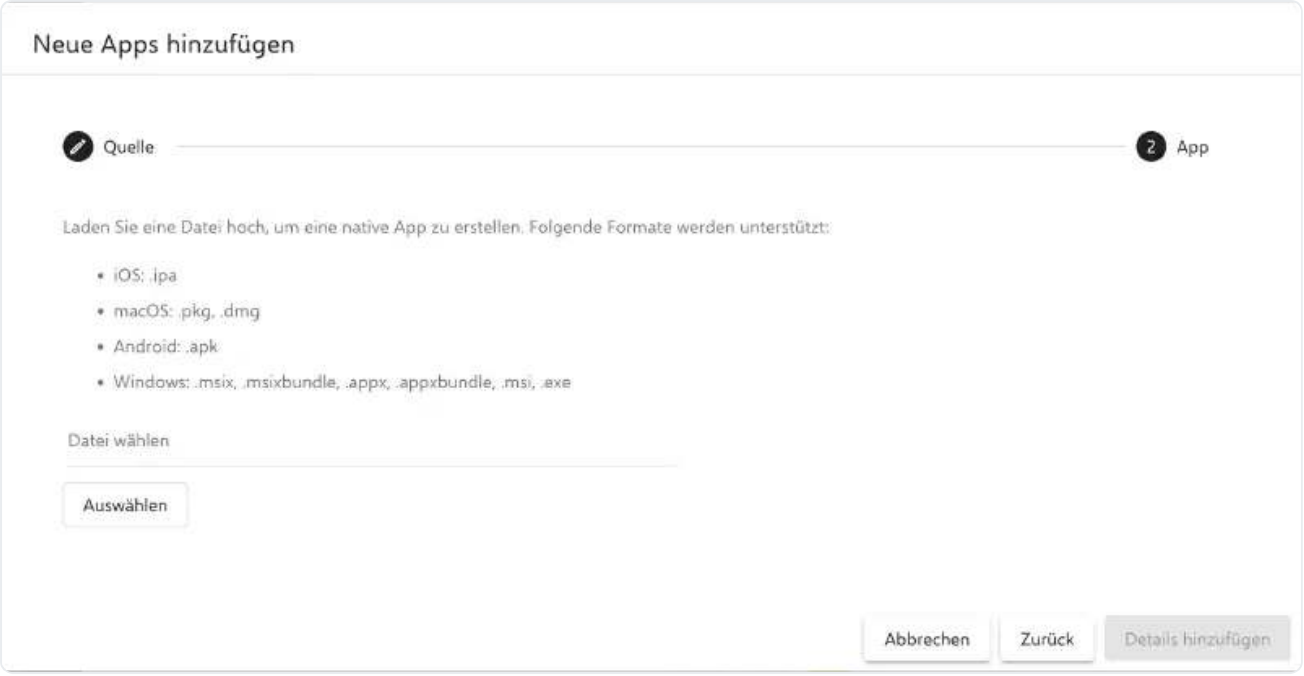
Nachfolgende Schritte müssen für eine erfolgreiche Installation eingehalten werden:

Für Version 26.4.0

1. Unter `Apps` → `App Store` wird über Hinzufügen die Option Native App gewählt.

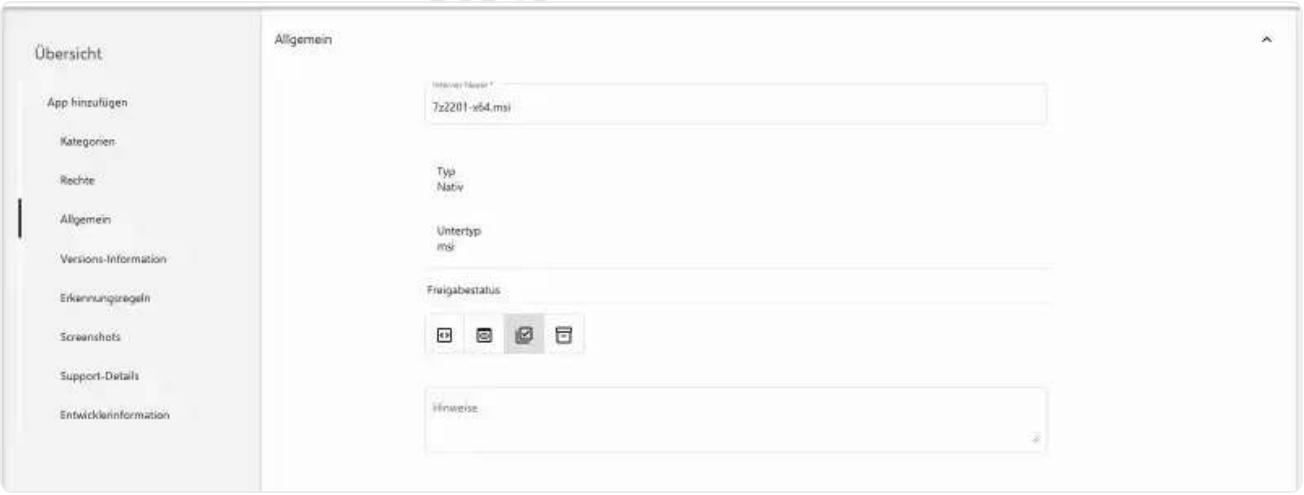


2. Im nächsten Schritt wird unter Datei wählen über die Schaltfläche Auswählen und den nativen Datei-Manager die entsprechende Datei im richtigen Format (`.msi` oder `.exe`) hochgeladen.



3. Nach dem Hochladen öffnet sich die App-Detailseite. Die benötigten Parameter müssen vom Administrator in Erfahrung gebracht und manuell eingepflegt werden. Mindestangaben sind der Versions-Name und mindestens eine Erkennungsregel, bei `.exe`-Apps zusätzlich die Pflichtfelder aus Schritt 4. Solange eine Pflichtangabe fehlt, lässt sich die App nicht speichern.

Version 26.4.0



4. Unter Versions-Information werden die Parameter für die Installation und Deinstallation gesetzt:
   - Bei `.msi`-Apps sind Parameter für die Installation und Parameter für die Deinstallation optional. Parameter für die Deinstallation lässt sich erst bearbeiten, wenn eine MSI-Erkennungsregel vorhanden ist (siehe Schritt 7).
   - Bei `.exe`-Apps sind Parameter für die Installation, Pfad zum Uninstaller (gültiger Windows-Pfad zum Deinstallationsprogramm) und Parameter für die Deinstallation Pflichtfelder. Mindestens der Parameter für eine Silent-Installation wird benötigt; Groß- und Kleinschreibung der Parameter kann eine Rolle spielen.

   Damit Installation und Deinstallation im Hintergrund und ohne manuellen Eingriff ablaufen, wird der zum Installer passende Silent-Parameter gesetzt, z. B. `/s` oder `/quiet`. Unter den Feldern zeigt das Portal eine Vorschau des daraus erzeugten Befehls, bei `.msi`-Apps etwa `msiexec /i <Dateiname> <Parameter>` für die Installation und `msiexec /x {<Produktcode>} <Parameter>` für die Deinstallation.

Details

Versions-Code *

1430988154

Versions-Name *

24.09

Groß- und Kleinschreibung kann Auswirkungen auf die Parameter für Installation und Deinstallation haben. Mindestens der Parameter für eine "Silent"-Installation wird benötigt.

Parameter für die Installation *

/S

```
1 | "7z-x64.exe" /S
```

Pfad zum Uninstaller *

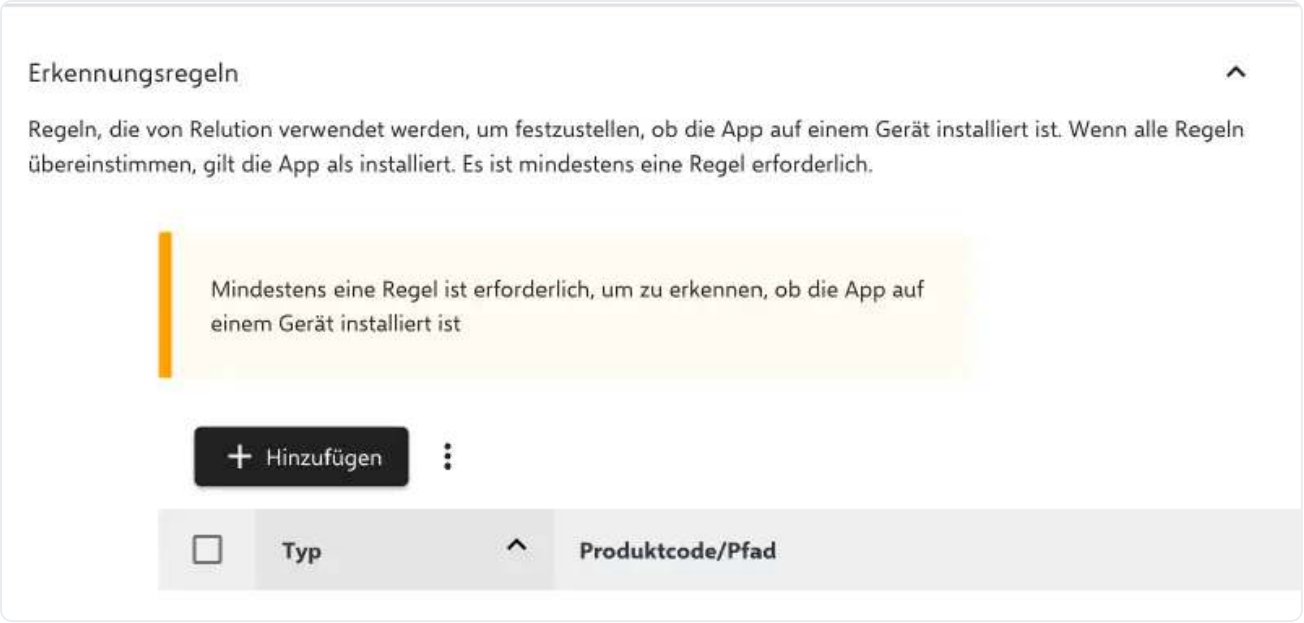
C:\Program Files\7-Zip\Uninstall.exe

Parameter für die Deinstallation *

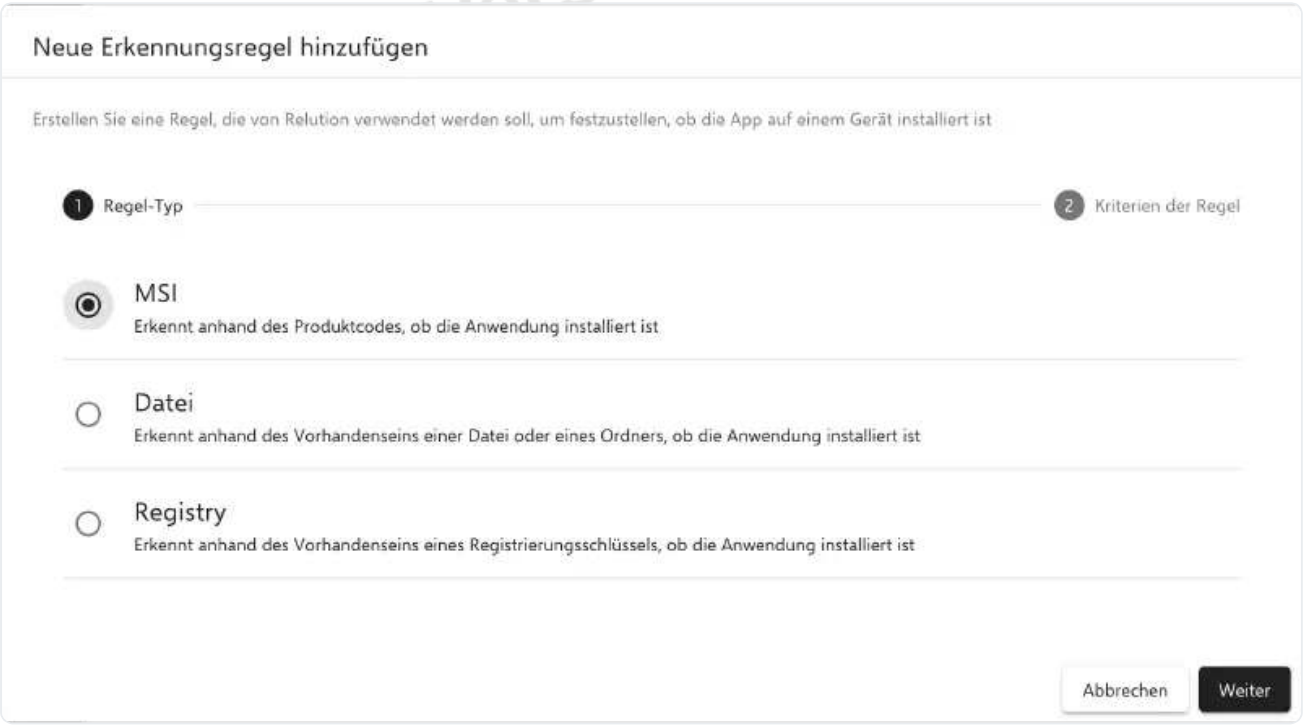
/S

```
1 | "C:\Program Files\7-Zip\Uninstall.exe" /S
```

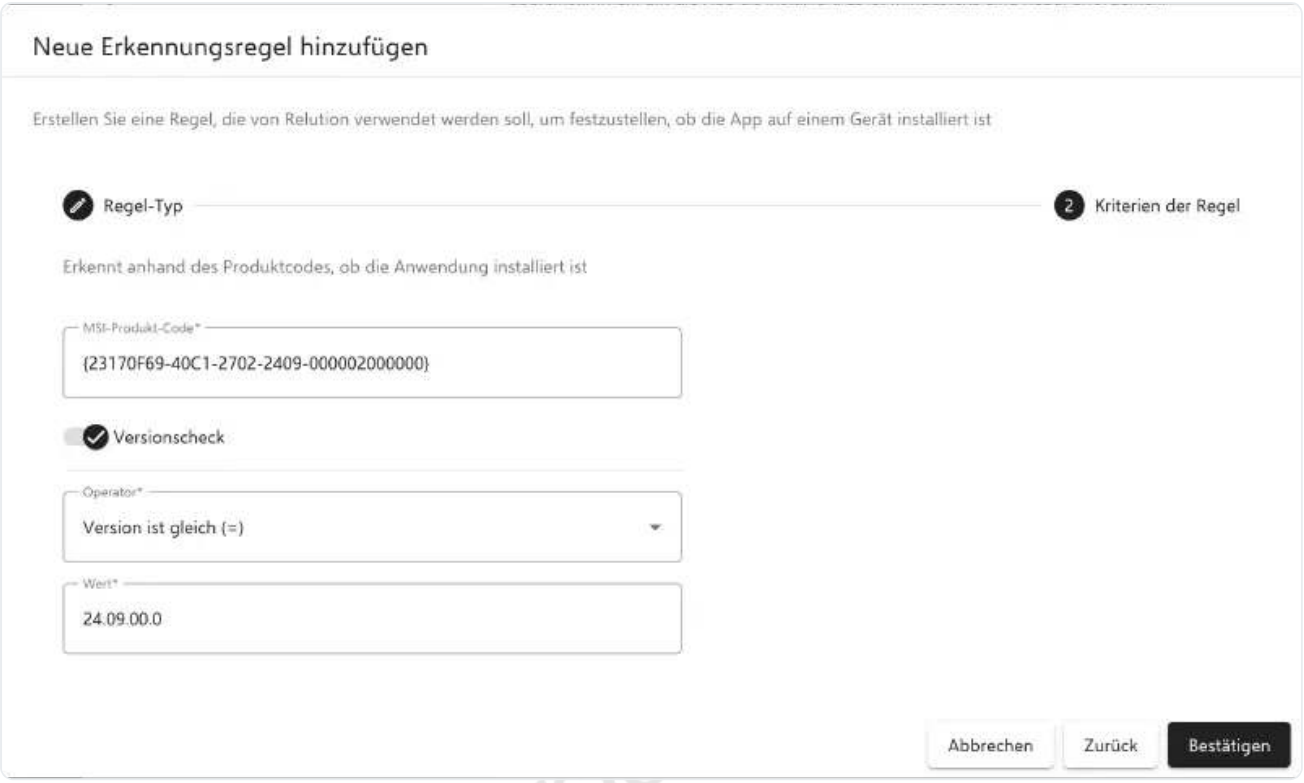
5. Im Anschluss werden Erkennungsregeln hinzugefügt, mit deren Hilfe der Relution Companion für Windows die Applikation eindeutig auf dem Windows-Rechner identifizieren kann.



6. Es stehen drei Erkennungsregeln zur Verfügung: MSI, Datei und Registry. Mindestens eine Regel ist erforderlich, um das Programm auf dem Windows-Gerät zu detektieren. Für `.msi`-Dateien ist die MSI-Erkennungsregel notwendig, damit das Programm deinstalliert werden kann. Bei `.exe`-Dateien eignen sich die beiden Erkennungsregeln Datei und Registry. Mehrere Erkennungsregeln lassen sich kombinieren; die App gilt nur dann als installiert, wenn alle Regeln zutreffen. Pro App ist eine MSI-Erkennungsregel möglich.

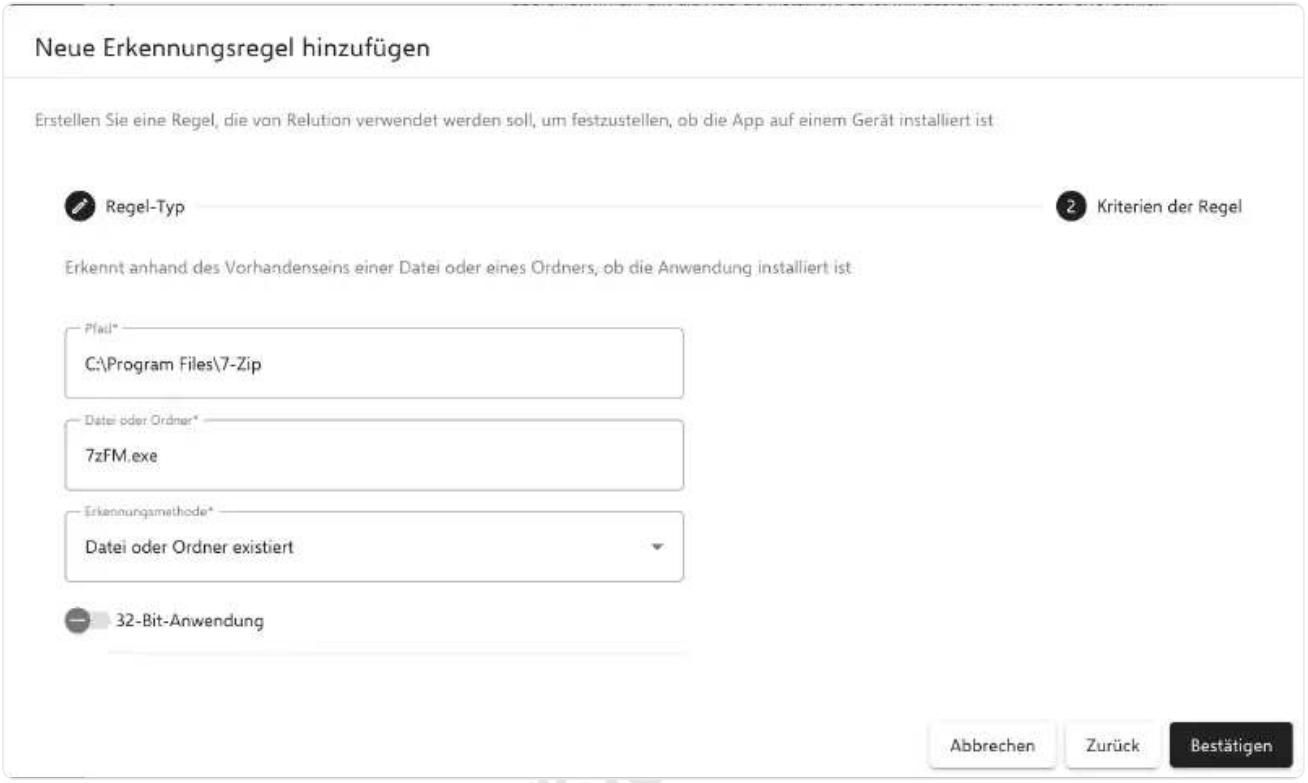


7. Für die MSI-Erkennungsregel wird der MSI-Produkt-Code der Applikation im Format `{AAAAAAAA-BBBB-CCCC-DDDD-EEEEEEEEEEEE}` eingetragen. Da es mehrere Versionen einer Applikation geben kann, lässt sich über den Schalter Versionscheck zusätzlich die Versionsnummer prüfen. Dazu wird im Feld Operator Version ist gleich (=) ausgewählt und im Feld Wert die Versionsnummer eingetragen. Mit Version ist nicht gleich (≠) trifft die Regel zu, wenn eine andere als die angegebene Version installiert ist.



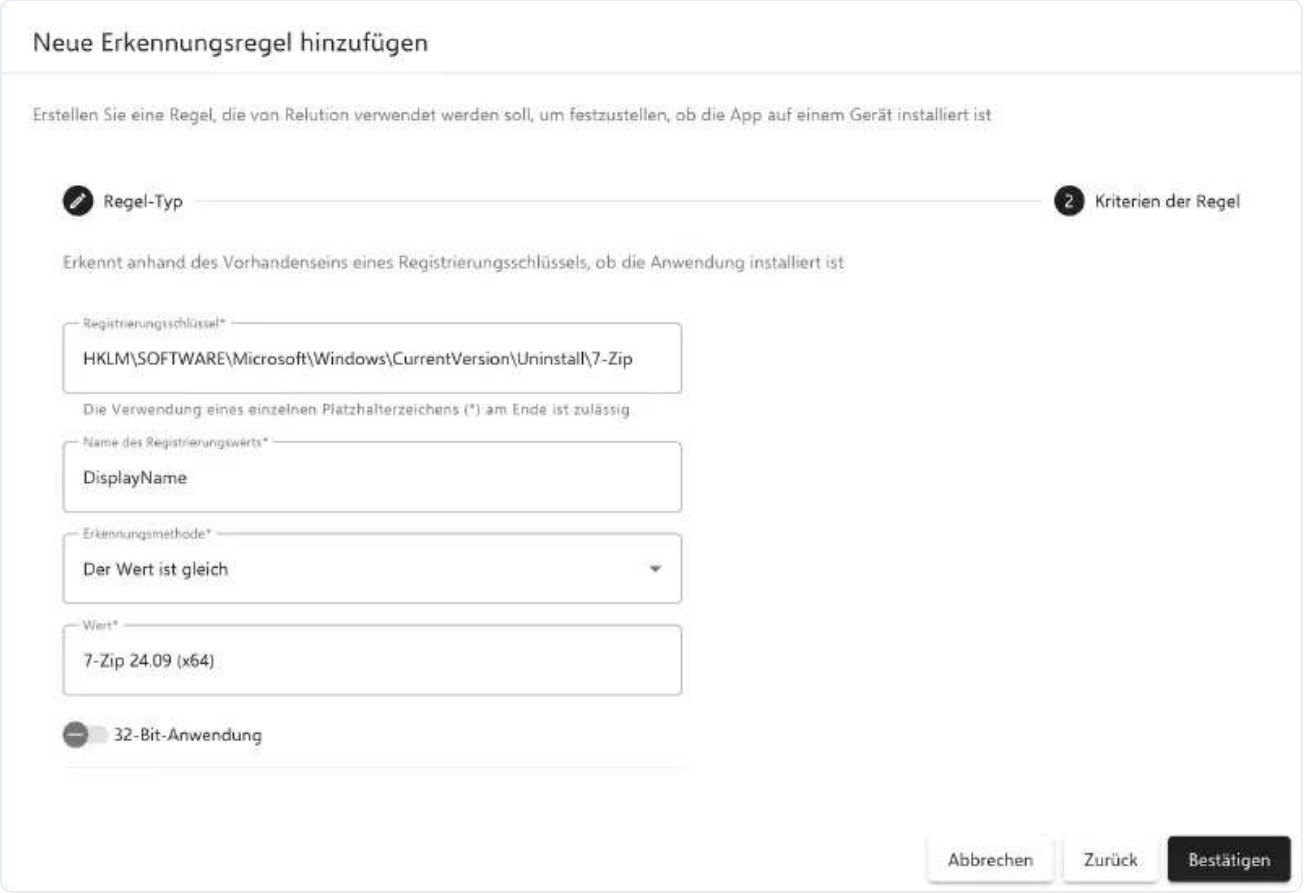
Für Versi

8. Die Datei-Erkennungsregel erkennt anhand des Vorhandenseins einer Datei oder eines Ordners, ob die Anwendung auf dem Windows-Gerät installiert ist. Dazu werden Pfad (z. B. `C:\Program Files\myApp`), Datei oder Ordner (z. B. `myApp.exe`) und die Erkennungsmethode (Datei oder Ordner existiert oder Datei oder Ordner existiert nicht) angegeben. Bei 32-Bit-Anwendungen wird der Schalter 32-Bit-Anwendung aktiviert; auf 64-Bit-Clients wird der Pfad dann automatisch angepasst, z. B. von `C:\Program Files` zu `C:\Program Files (x86)`.

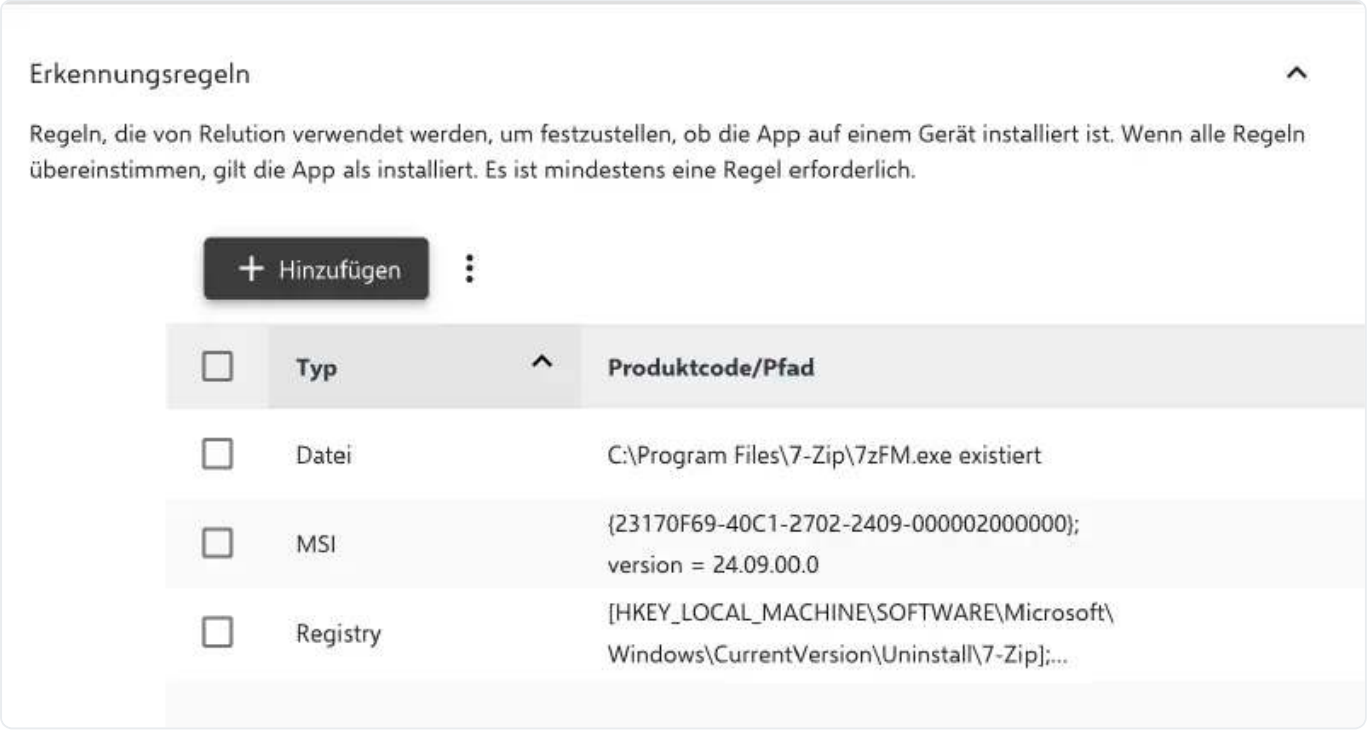


Für Versi

9. Die Registry-Erkennungsregel überprüft die Existenz der Applikation auf dem Windows-Gerät anhand eines Registrierungsschlüssels. Die Felder Registrierungsschlüssel, Name des Registrierungswerts und Erkennungsmethode werden manuell angegeben; am Ende des Registrierungsschlüssels ist ein einzelnes Platzhalterzeichen (`*`) zulässig. Der Name des Registrierungswerts ist frei wählbar, gängig ist z. B. `DisplayName` im Uninstall-Schlüssel der Anwendung. Als Erkennungsmethode stehen Ein Wert mit dem angegebenen Namen existiert (Standard), Ein Wert mit dem angegebenen Namen existiert nicht und Der Wert ist gleich zur Auswahl. Das Feld Wert ist nur bei Der Wert ist gleich aktiv. Um die Anwendung eindeutig auf dem Windows-Gerät zu detektieren, empfiehlt sich Der Wert ist gleich; der benötigte Wert ergibt sich aus der installierten Applikation. Der Schalter 32-Bit-Anwendung passt den Registrierungsschlüssel bei 32-Bit-Anwendungen auf 64-Bit-Clients automatisch an, z. B. von `HKLM\SOFTWARE\Microsoft` zu `HKLM\SOFTWARE\WOW6432Node\Microsoft`.



Nach Hinzufügen der benötigten Erkennungsregeln kann die Applikation gespeichert werden.



Anschließend lässt sich die Native App über den Relution App Store auf allen verwalteten Windows-Geräten installieren und wieder deinstallieren.

Deinstallation von Windows Store Apps

Für Version 26.4.0

Windows Store Apps lassen sich nicht über die Oberfläche deinstallieren. Daher ist es notwendig, diese per PowerShell-Skript lokal oder über Relution zu entfernen. Nachfolgend die allgemeinen Schritte:

App lokal am Gerät suchen

```
Get-AppxPackage -Name *<AppName>* -AllUsers
```

App über Script deinstallieren

```
Get-AppxPackage -Name *<AppName>* -AllUsers | Remove-AppxPackage -AllUsers
```

Das Provisioning-Paket der App kann dabei auf dem Gerät verbleiben. Um die App restlos zu entfernen, muss zunächst das Provisioning-Paket abgefragt und der PackageFullName ermittelt werden.

```
Get-AppxProvisionedPackage -Online | Select PackageName
```

Und anschließend vollständig gelöscht werden:

```
Remove-AppxProvisionedPackage -Online -PackageName <PackageFullName>
```

Empfehlung: WinGet verwenden

Wenn möglich, sollte WinGet genutzt werden. Hierüber stehen deutlich mehr Apps zur Verfügung und die Deinstallation ist einfacher: WinGet →

Für Version 26.4.0

WinGet

Ab Relution 5.26 ist es möglich den WinGet Paket-Manager → für die Anwendungsbereitstellung auf Windows Geräten zu verwenden.

Die Abschnitte Limitierungen und Bekannte Probleme beschreiben wichtige Einschränkungen.

Voraussetzungen

1. Der WinGet Client muss auf dem Gerät installiert sein. Er ist standardmäßig auf allen Windows 11 Versionen und auf Windows 10 ab Version 2004 (Mai 2020 Update) verfügbar.
2. Die Anwendung Microsoft Visual C++ Redistributable muss auf dem Gerät installiert sein, siehe Limitierungen →.
3. Relution Server Version 5.26 oder höher
4. Windows Companion Version 1.11 oder höher
5. WinGet Version 1.6 oder höher

Unterstützte Features

Für Version 26.4.0

Vor dem breiten Einsatz sollte jede WinGet App auf einem Testgerät geprüft werden.

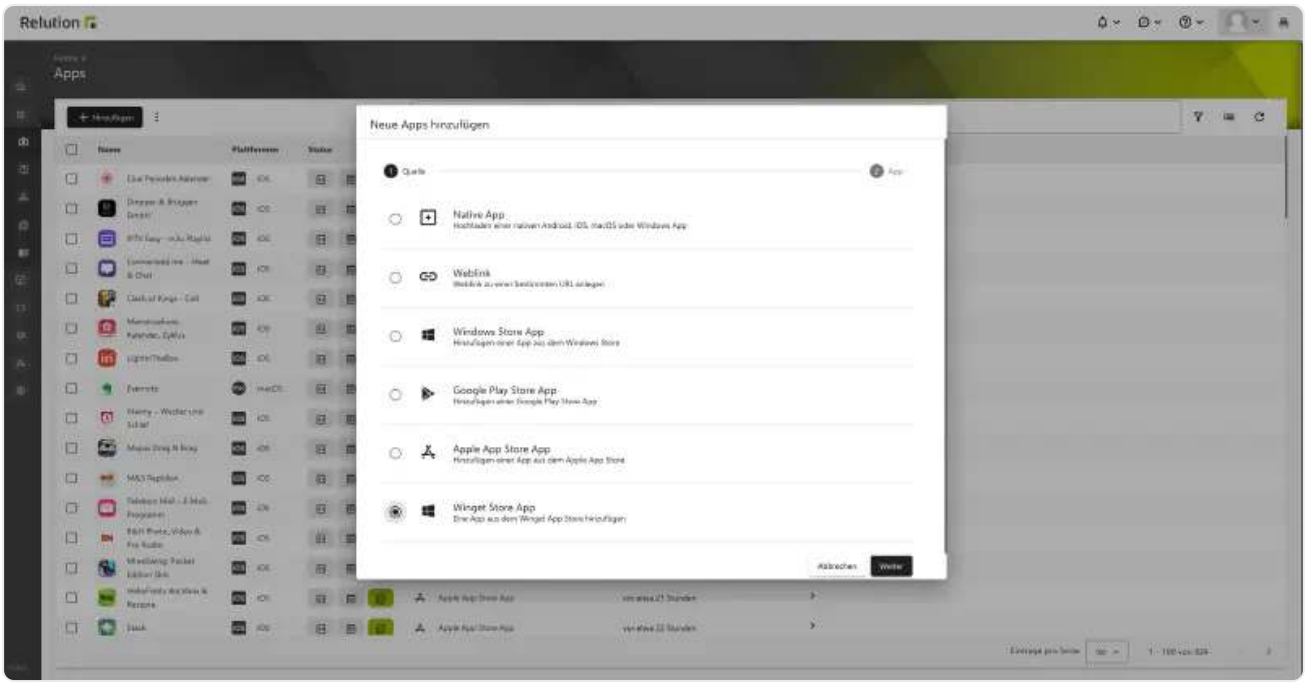
Die Abschnitte Limitierungen → und Bekannte Probleme → enthalten weitere Details.

- Suchen und Hinzufügen von WinGet Anwendungen in den Relution AppStore
- Bereitstellung von WinGet Anwendungen mittels Aktion, App Konformität und Auto-Deployments
- Anzeigen von installierten WinGet Apps in der installierten App Liste eines Geräts
- Entfernen von WinGet Apps mittels Aktion
- Automatische Aktualisierung von WinGet Apps auf den Geräten

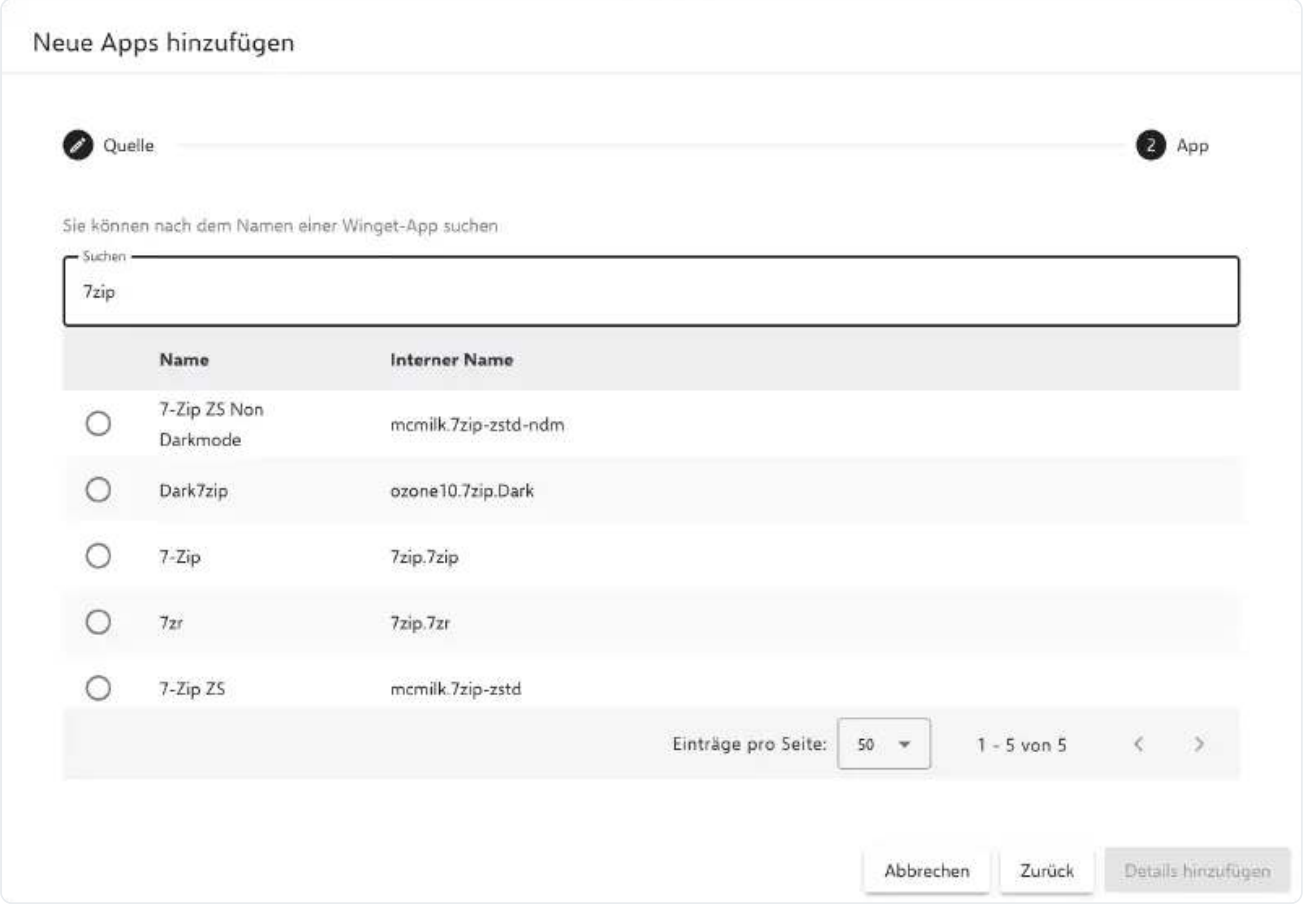
Hinzufügen von WinGet apps in den Relution AppStore

WinGet Apps müssen in den Relution AppStore hinzugefügt werden, bevor diese auf Geräten angewendet werden können.

1. Unter `Apps` → `App Store` öffnet die Schaltfläche Hinzufügen den Dialog Neue Apps hinzufügen. Als Quelle wird Winget Store App gewählt.

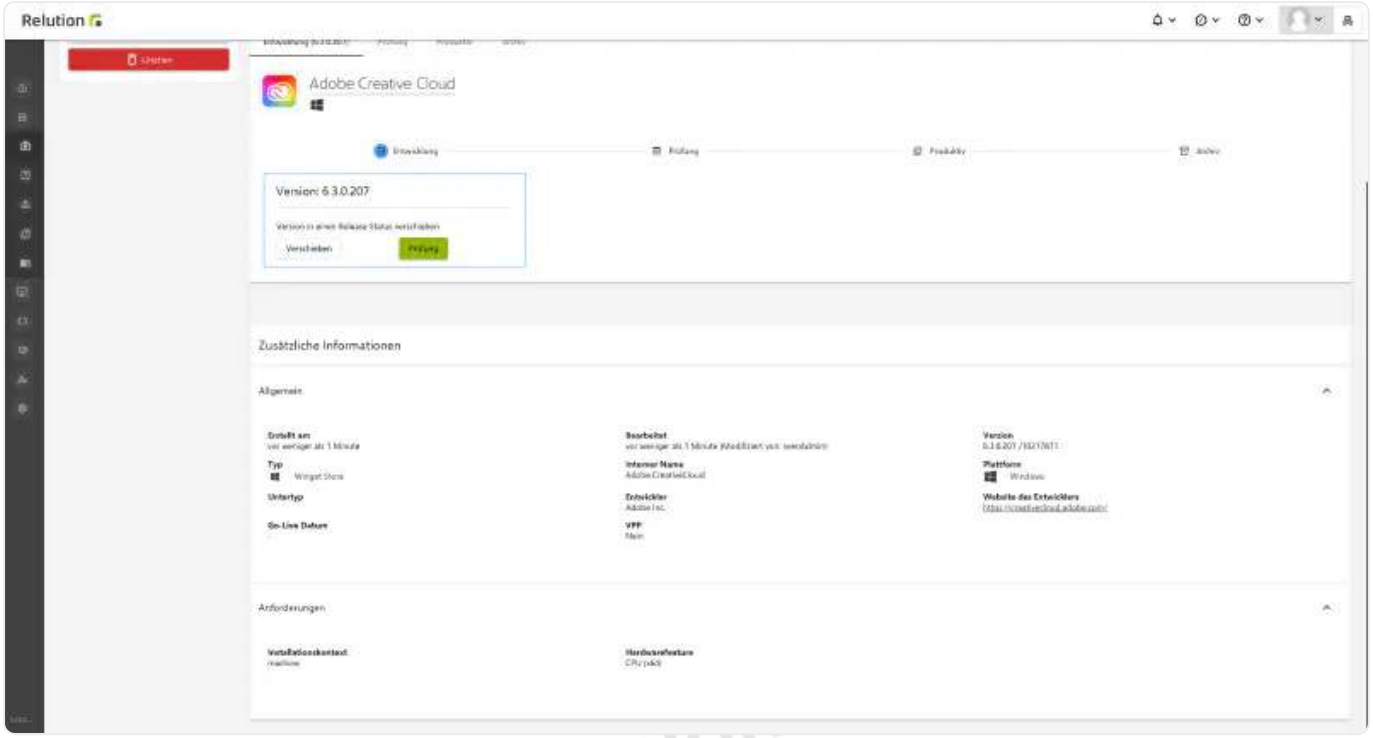


2. Die WinGet App wird über ihren Namen gesucht, ausgewählt und mit Details hinzufügen in den Relution AppStore übernommen.



3. Da WinGet-Manifeste kein Icon enthalten, übernimmt Relution nach Möglichkeit das Favicon der Herausgeber-Webseite als App-Icon. Ein bereits vorhandenes, z. B. manuell hochgeladenes Icon wird dabei nicht ersetzt. In den App-Details einer WinGet App ist nur das Icon bearbeitbar, alle anderen Felder werden automatisch aus dem Store gelesen.

Die WinGet App Details können zusätzliche Informationen wie den Installationsbereich enthalten, falls diese Informationen von der WinGet app bereitgestellt werden.



Für Version

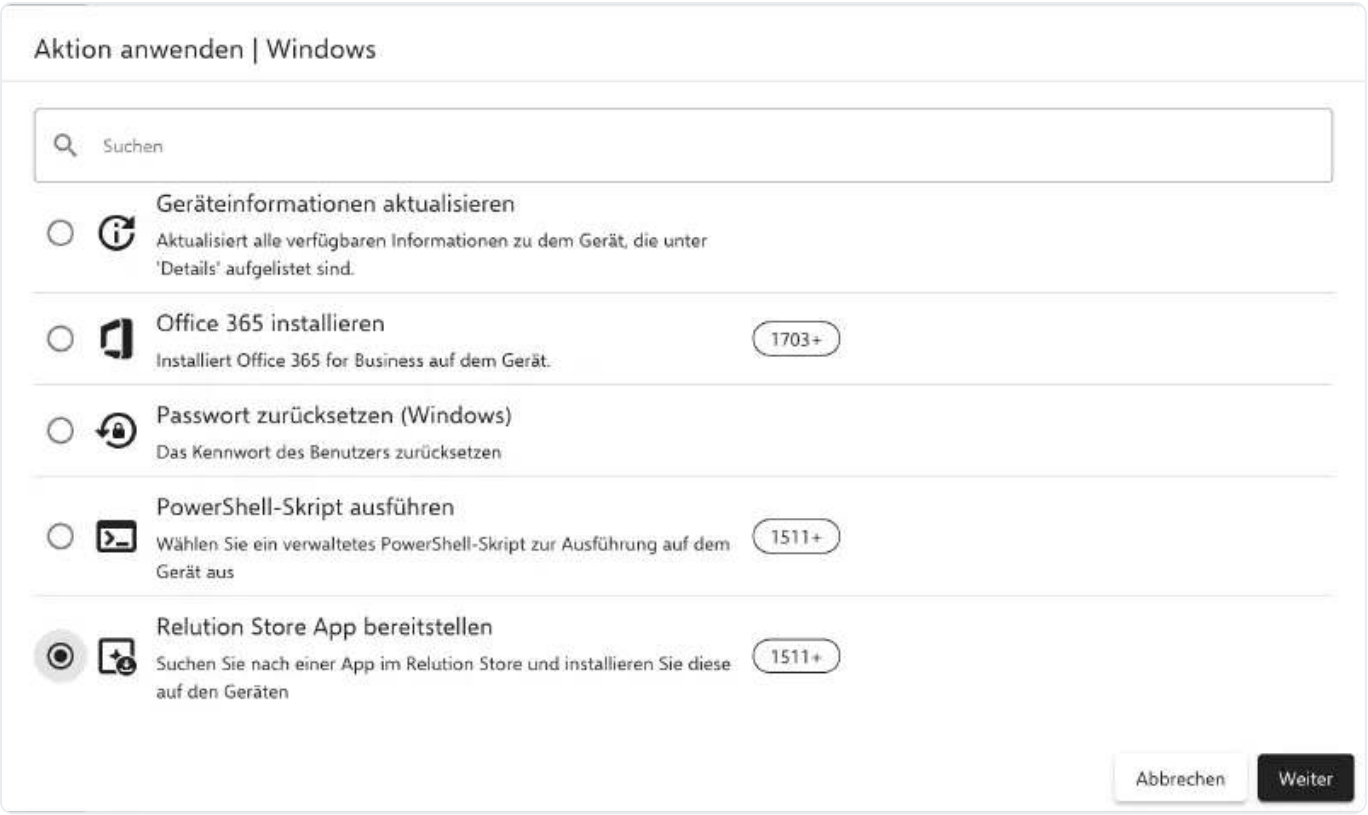
Bereitstellen von WinGet Apps

Nachdem die WinGet App zum Relution AppStore hinzugefügt wurde und eine Version im Status Produktiv hat, kann sie auf Windows Geräten bereitgestellt werden.

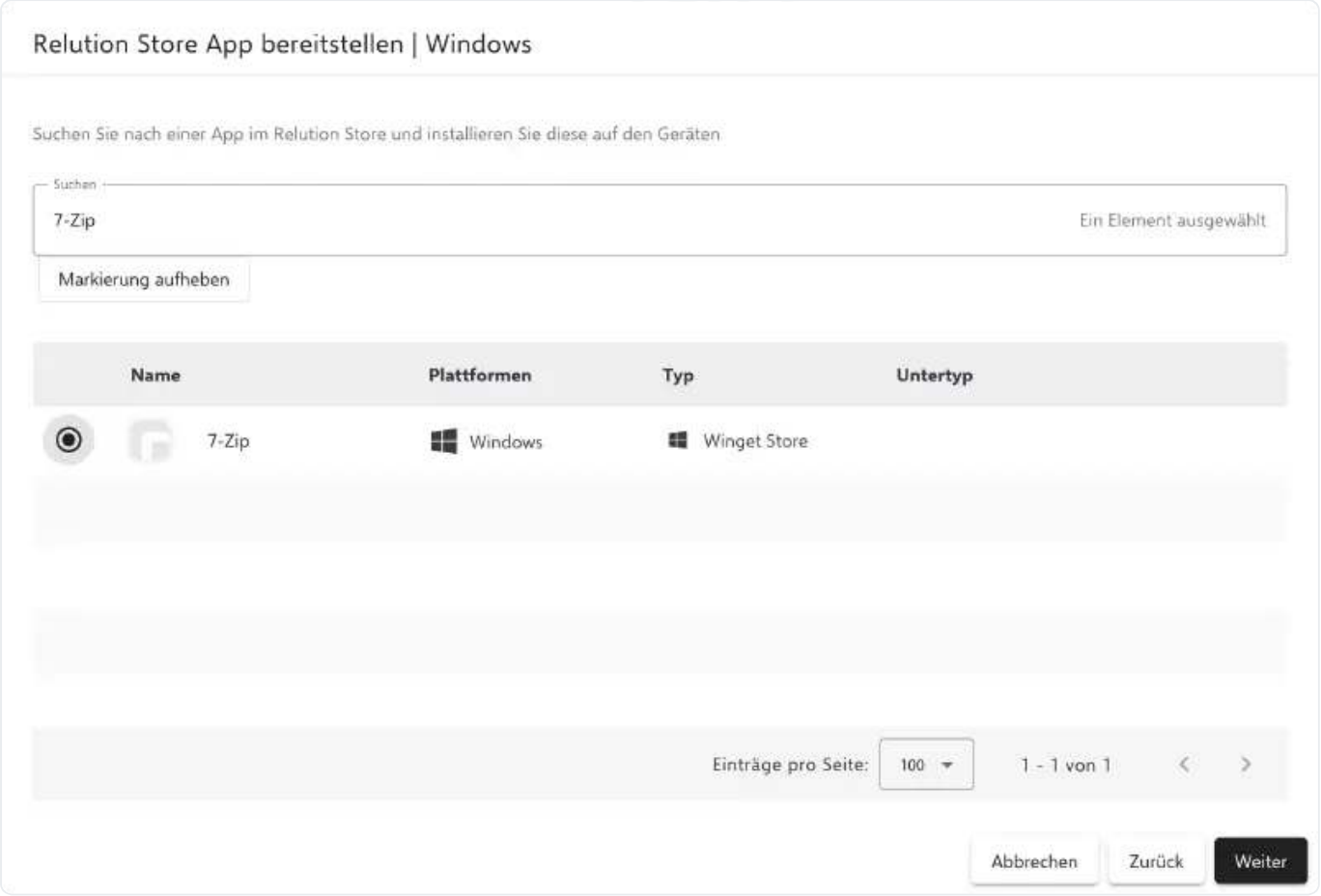
Relution muss alle WinGet Apps vollständig ohne Benutzerinteraktion installieren können, siehe Limitierungen →. Aufgrund dieser Limitierung werden alle Lizenzverträge des Pakets und der Quelle automatisch akzeptiert, wenn eine WinGet App über Relution installiert wird!

Bereitstellen mittels Aktion

Im Aktions-Modal muss Relution Store App bereitstellen ausgewählt werden.



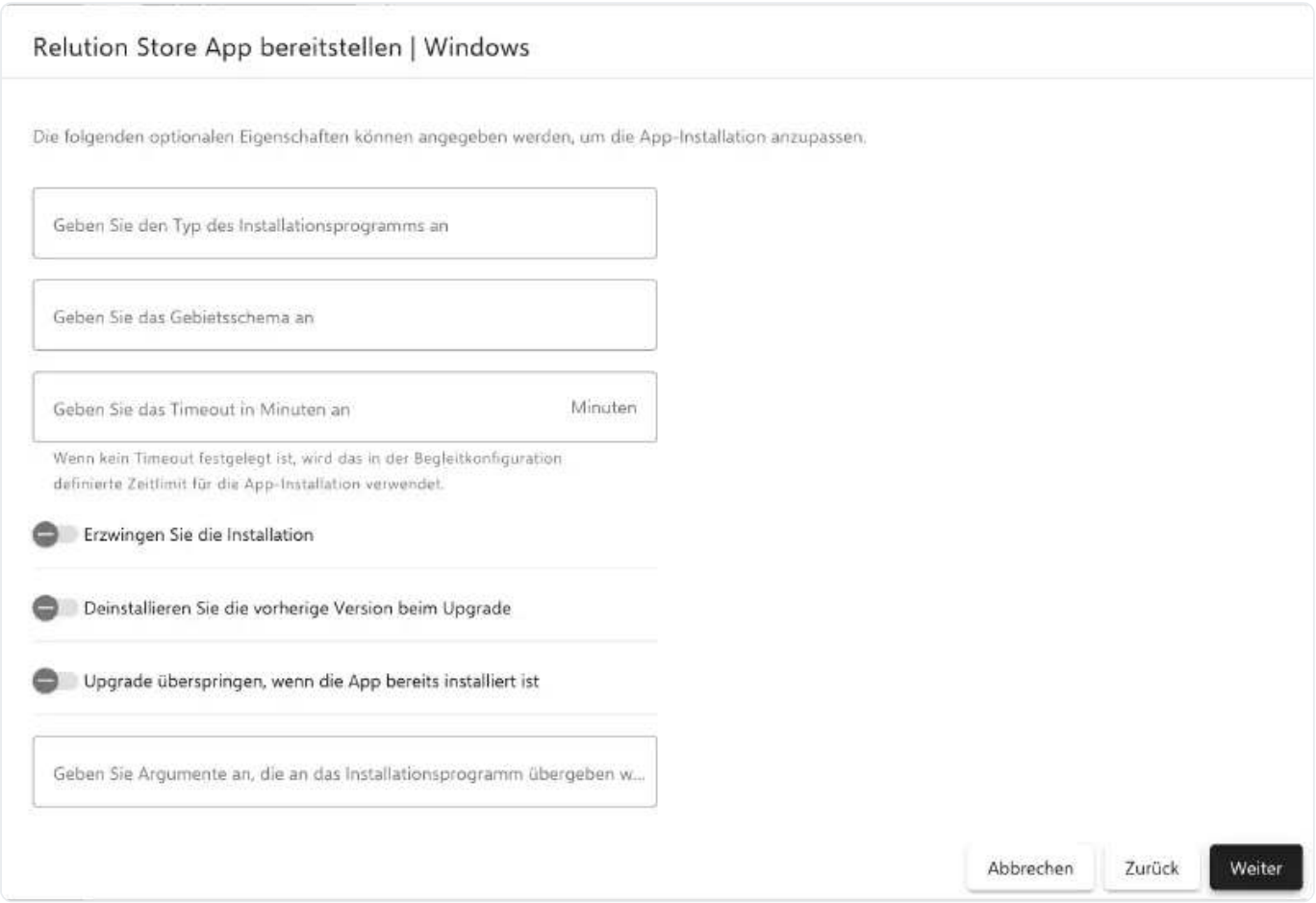
Daraufhin muss die WinGet App gesucht und für die Bereitstellung selektiert werden.



Im nächsten Schritt kann die Bereitstellung optional angepasst werden. Dies ist aktuell nur für die Aktion möglich und nicht bei einer App Konformität oder den Auto-Deployments.

- Typ des Installationsprogramms: Spezifizieren des Installationstyps, der für die Installation verwendet werden soll, siehe unterstützte Formate von Installationsprogrammen →. Die App muss den angegebenen Installationstyp unterstützen oder die Installation wird fehlschlagen.
- Gebietsschema: Spezifizieren des Gebietsschemas, das verwendet werden soll (BCP47 Format, maximal 5 Zeichen, z. B. `de-DE`).
- Timeout in Minuten: Zeit in Minuten (1 bis 150), nach der der Windows Companion die Installation abbricht. Bleibt das Feld leer, gilt die Maximaldauer für App-Installationen aus der Richtlinienkonfiguration Windows Companion →.
- Installation erzwingen: Führt den Befehl direkt aus und fährt mit nicht sicherheitsrelevanten Problemen fort.
- Vorherige Version beim Upgrade deinstallieren: Deinstalliert die vorherige Version des Pakets während des Upgrades.
- Upgrade überspringen: Überspringt das Upgrade, wenn die App bereits installiert ist.
- Argumente für das Installationsprogramm: Übergibt die angegebenen Argumente zusätzlich zu den Standardwerten an das Installationsprogramm.

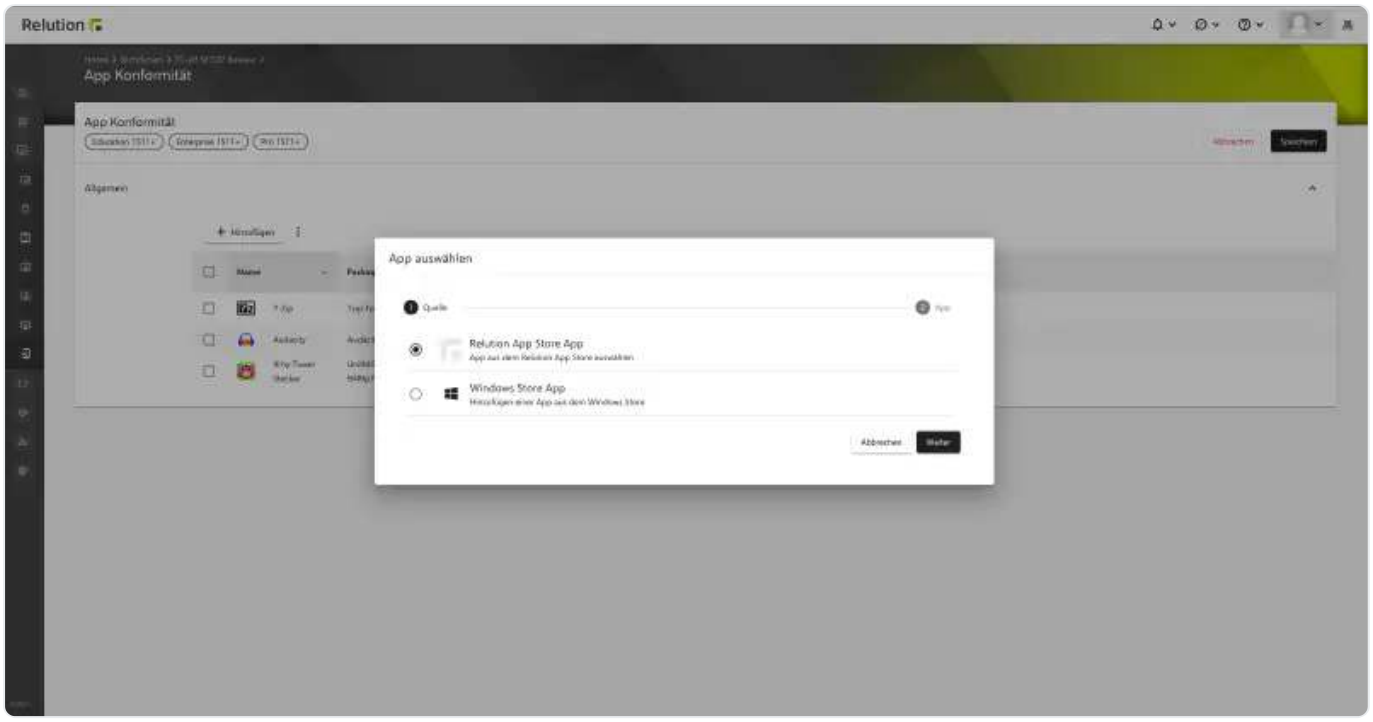
Vorherige Version beim Upgrade deinstallieren und Upgrade überspringen schließen sich gegenseitig aus: Wird eine der beiden Optionen aktiviert, wird die andere deaktiviert.



Nach der Bestätigung im letzten Schritt wird eine Bereitstellungs-Aktion erstellt.

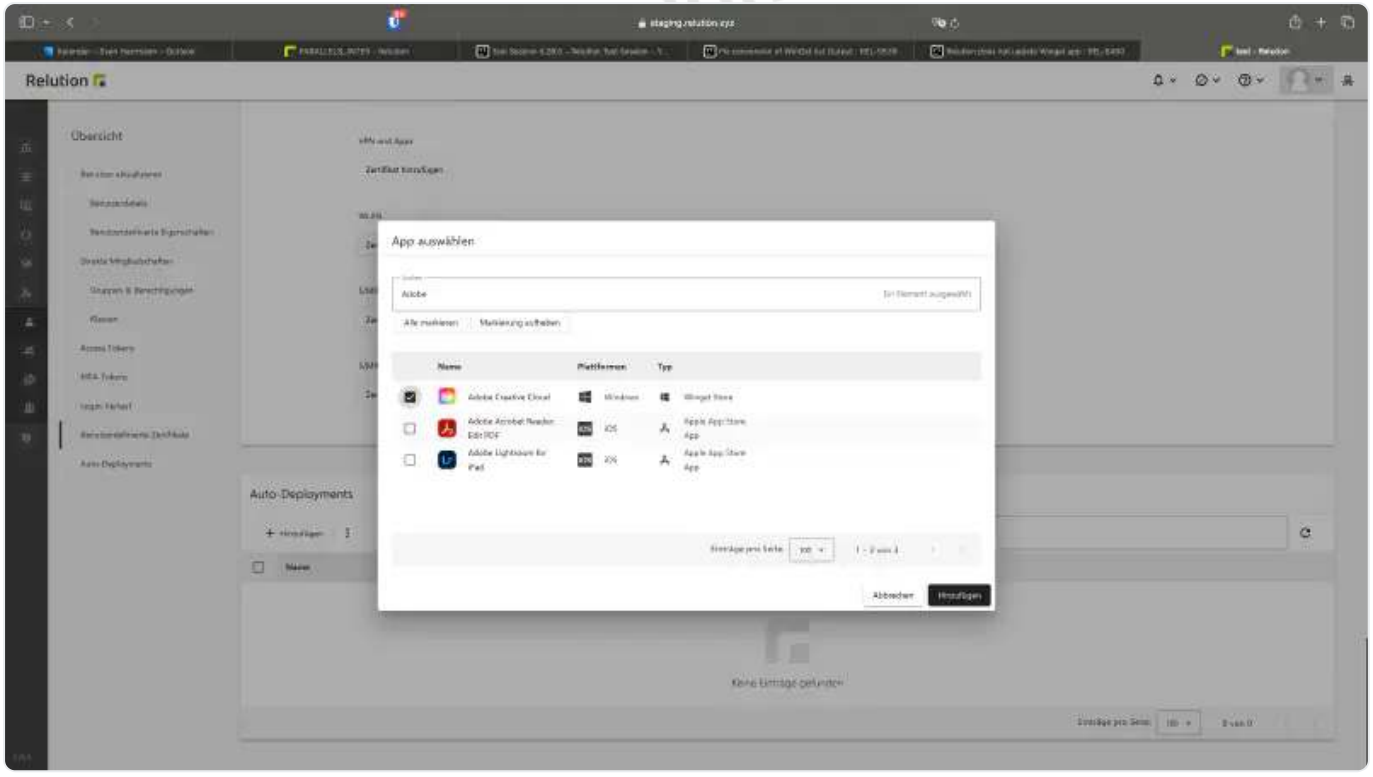
Bereitstellung mittels App Konformität

WinGet Apps können zu der App Konformität einer Windows Richtlinie hinzugefügt werden.



Bereitstellung mittels Auto-Deployments

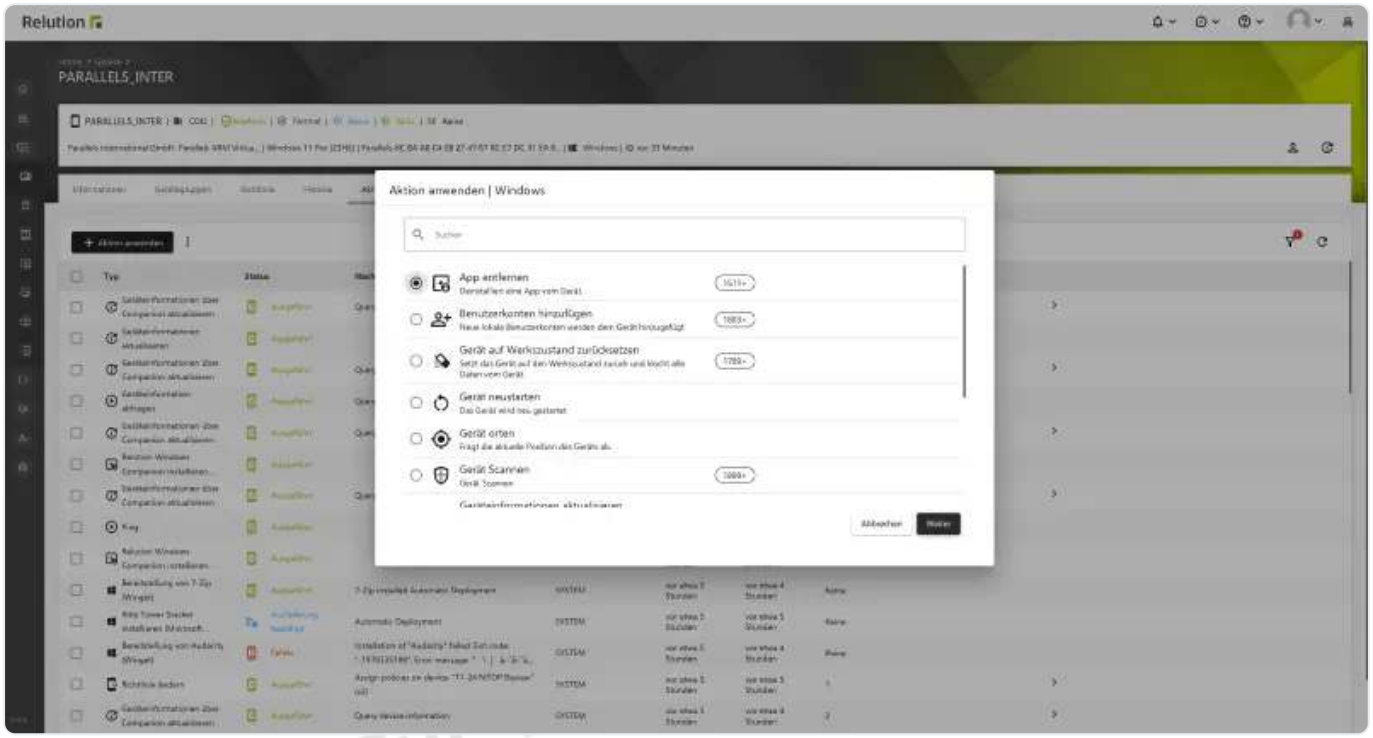
Winget Apps können zu den Auto-Deployments eines Benutzers hinzugefügt werden.



Entfernen von WinGet Apps mittels Aktion

WinGet Apps lassen sich mit der Aktion App entfernen von einem Gerät deinstallieren. Zur Auswahl stehen dabei die WinGet Apps, die im Relution AppStore enthalten sind.

Der Windows Companion wird den winget uninstall Befehl still ausführen, siehe Limitierungen →. Aufgrund dieser Limitierung werden alle Quelllizenz-Verträge automatisch akzeptiert, wenn eine WinGet App über Relution deinstalliert wird!



Automatische Aktualisierungen von WinGet Apps auf den Geräten

Relution wird installierte WinGet Apps automatisch auf den jeweiligen Geräten aktualisieren.

Voraussetzungen:

- Die WinGet App muss im Relution AppStore enthalten sein
- Die WinGet App muss in der installierten App Liste des Geräts enthalten sein

Der Relution AppStore überprüft jeden Tag, ob eine neue Version von enthaltenen WinGet Apps verfügbar ist und aktualisiert die App Informationen automatisch. Wenn der Windows Companion die Geräteinformationen in Relution aktualisiert, werden die Versionen der installierten WinGet Apps mit der Version im Status Produktiv im Relution AppStore verglichen. Berücksichtigt werden dabei nur Einträge der installierten App Liste, die WinGet als Quelle haben. Wird dabei festgestellt, dass eine neuere Version im Relution AppStore vorhanden ist, wird eine Bereitstellungs-Aktion für das Gerät erstellt und so die App darauf aktualisiert. Solange für die App auf dem Gerät noch eine offene Bereitstellungs-Aktion existiert, wird keine weitere erstellt.

Sollte der Vergleich der Versionen fehlschlagen, wird die automatische Aktualisierung nicht stattfinden (siehe Bekannte Probleme →)

Limitierungen

Die folgenden Einschränkungen gelten grundsätzlich für den Einsatz von WinGet Apps in Relution.

Microsoft Visual C++ Redistributable muss installiert sein

Der Windows Companion führt WinGet Befehle im System Kontext aus. Dafür muss die Microsoft Visual C++ Redistributable installiert sein.

Wenn der Windows Companion startet, überprüft dieser ob diese Abhängigkeit auf dem Gerät installiert ist. Sollte diese fehlen, versucht der Companion diese herunterzuladen und zu installieren. Wenn diese nicht installiert werden konnte, schreibt der Windows Companion einen Log Eintrag in die Ereignisanzeige auf dem Gerät.

Wenn dieses Problem auftritt, werden die WinGet Aktionen fehlschlagen. Ein Indikator kann der Fehlercode -1073741515 in der fehlgeschlagenen Aktion sein. In diesem Fall ist es möglich die letzte Version der Microsoft Visual C++ Redistributable → manuell mittels nativer App mit Erkennungsregel zu installieren, siehe Bekannte Probleme →

WinGet Client muss auf dem Gerät installiert sein

Relution installiert den WinGet Client nicht. Ist in der Richtlinienkonfiguration Windows Companion → die Option WinGet und seine Abhängigkeiten verwalten aktiv (Standard), aktualisiert der Windows Companion WinGet und seine Abhängigkeiten wie die Microsoft Visual C++ Redistributable beim Start. Ist die Option deaktiviert, aktualisiert der Windows Companion WinGet nicht; eine fehlende Microsoft Visual C++ Redistributable installiert er trotzdem. Der WinGet Client ist standardmäßig auf allen Windows 11 Versionen und auf Windows 10 ab Version 2004 (Mai 2020 Update) verfügbar. Er ist im AppInstaller paketiert. Dieser kann über den Microsoft Store installiert werden.

Für Version 26.4.0

Ausschließlich stille Installation und Deinstallation sind unterstützt

Die WinGet App Installation oder Deinstallation wird vom Windows Companion durchgeführt. Der Windows Companion ist ein Hintergrund-Prozess, der keine Benutzeroberfläche auf den Geräten anzeigen kann.

Deshalb wird die Installation oder das Entfernen von Apps fehlschlagen, wenn diese nicht vollständig still ausgeführt werden kann.

Der Windows Companion wird deshalb automatisch alle möglichen Befehle angeben, die die Installation bzw. Deinstallation still ausführen.

```
winget install --silent --disable-interactivity --accept-package-agreements --accept-source-agreements
```

```
winget uninstall --silent --disable-interactivity --accept-source-agreements
```

Aber für manche Apps reichen die WinGet Befehle nicht aus, um die App daran zu hindern dabei eine Oberfläche anzuzeigen. Ein Beispiel ist Mozilla Firefox bei der Deinstallation.

Bekannte Probleme

Es wird empfohlen die Installation und Deinstallation für jede WinGet App zu testen, bevor diese produktiv verwendet wird.

Wenn die WinGet-App in einer App Konformität oder in den Auto-Deployments verwendet werden soll, muss sie nach der Installation und Aktualisierung der Gerätedetails in der Liste der installierten Apps auf dem Gerät enthalten sein.

Wenn das automatische Update einer installierten WinGet-App wichtig ist, muss die Liste der installierten Apps die App enthalten und einen korrekten Wert in der Versionsspalte haben.

Einige Apps können nicht daran gehindert werden einen Dialog anzuzeigen

Wenn eine App nicht daran gehindert werden kann, einen Dialog anzuzeigen, schlägt die Installation oder Deinstallation fehl.

Es kann möglich sein, einen anderen Installer in der Bereitstellungsaktion zu verwenden, um dieses Problem zu umgehen.

So lässt sich das herausfinden

- PowerShell als Administrator auf einem Testgerät öffnen
- Den Befehl `winget install --id <id> --silent --disable-interactivity --accept-source-agreements --accept-package-agreements` für die Installation ausführen, wobei `<id>` durch die WinGet-ID der App ersetzt wird
  - Wenn kein Dialog oder keine Eingabeaufforderung angezeigt wird, kann die App still installiert werden
  - Andernfalls kann ein anderer Installer verwendet werden, indem `--installer-type <installer-type>` zum Befehl hinzugefügt wird, wenn die App mehr als einen unterstützt.
- Für die Deinstallation `winget uninstall --id <id> --silent --disable-interactivity --accept-source-agreements` ausführen
- Wenn kein Dialog oder keine Eingabeaufforderung angezeigt wird, kann die App still entfernt werden

Alternative

Wenn die App nicht installiert oder deinstalliert werden kann, wird die Verwendung einer nativen App mit Erkennungsregeln empfohlen.

Einige Apps können nicht im System-Kontext installiert werden

Der WinGet Client bietet aktuell keine vollständige Unterstützung des System-Kontexts. Da jedoch der Windows Companion in diesem Kontext ausgeführt wird, kann die Installation von manchen Apps fehlschlagen.

So lässt sich das herausfinden

- Auf einem Test-Gerät testen, ob die App still installiert werden kann, siehe Bekannte Probleme →.
- Die App wieder von dem Test-Gerät entfernen.
- Dieselbe App auf demselben Gerät mittels Relution installieren.
- Wenn die Installation fehlschlägt, kann diese womöglich nicht im System-Kontext installiert werden

Alternative

Wenn die App nicht installiert oder deinstalliert werden kann, wird die Verwendung einer nativen App mit Erkennungsregeln empfohlen.

Einige Apps werden nicht in der installierten App Liste angezeigt

Einige Apps werden nicht in der installierten App-Liste des Geräts angezeigt, obwohl WinGet diese als installiert erkennt.

Diese Apps sollten nicht in einer App Konformität oder in Auto-Deployments verwendet werden, weil sie aktuell nicht korrekt erkannt werden und dies zu vielen fehlschlagenden Bereitstellungs-Aktionen führen würde.

So lässt sich das herausfinden

- Eine WinGet App auf einem Test-Gerät installieren
- Die Geräteinformationen aktualisieren
- Die App sollte nun in der installierten Apps Liste zu sehen sein

Alternative

Wenn dieses Problem auftritt, wird die Verwendung einer nativen App mit Erkennungsregeln empfohlen.

Einige Apps haben falsche Werte in der installierten App Liste

Für Version 26.4.0

Einige WinGet Apps haben falsche Werte in der installierten App Liste, z. B. für die Version.

Diese Apps können dennoch in einer App Konformität oder in Auto-Deployments verwendet werden.

Enthält jedoch die Version einen falschen Wert, so wird die automatische Aktualisierung nicht ausgeführt.

So lässt sich das herausfinden

- Eine WinGet app auf einem Test-Gerät installieren
- Die Geräteinformationen aktualisieren
- Die App sollte nun in der installierten Apps Liste zu sehen sein
- Die angezeigten Werte überprüfen

Alternative

Wenn die automatische Aktualisierung der App auf den Geräten nicht wichtig ist, kann die App ansonsten vollständig verwendet werden.

Andernfalls wird die Verwendung einer nativen App mit Erkennungsregeln empfohlen.

Doppelte Anzeige in den installierten Apps

Wenn native Apps mit Erkennungsregeln auf einem Gerät bereitgestellt worden sind, kann diese App doppelt in der installierten App Liste angezeigt werden.

Das bedeutet nicht, dass die App doppelt auf dem Gerät installiert ist. Es bedeutet, dass die App von der Erkennungsregel und von WinGet erkannt worden ist.

So lässt sich das herausfinden

- Eine App mit Erkennungsregel auf einem Test-Gerät installieren
- Die Geräteinformationen aktualisieren
- Die App wird doppelt in der installierten App Liste angezeigt. Der Name und andere Informationen können, müssen aber nicht identisch sein.

Alternative

Aktuell gibt es keine Alternative für dieses Verhalten.

Der doppelte Eintrag kann nur verhindert werden, wenn die zugehörige native App mit Erkennungsregeln aus dem Relution AppStore entfernt wird und die passende WinGet App stattdessen verwendet wird.

Aufgrund der Limitierungen → und bekannten Probleme → von WinGet Apps wird nicht empfohlen direkt von Apps mit Erkennungsregeln auf WinGet Apps zu wechseln!

Fehlende Abhängigkeit Microsoft Visual C++ Redistributable

Wie im Abschnitt Limitierungen → beschrieben, wird die Abhängigkeit *Microsoft Visual C++ Redistributable* benötigt damit WinGet Apps in Relution verwendet werden können.

Deshalb versucht der Windows Companion diese auf dem Gerät zu installieren, wenn diese fehlt. Diese Überprüfung wird durchgeführt, wenn der Windows Companion startet, z. B. nach seiner Neu-Installation oder einem Neustart des Geräts.

Es kann vorkommen, dass die automatische Installation der *Microsoft Visual C++ Redistributable* fehlschlägt, wodurch die WinGet Befehle ebenfalls fehlschlagen werden.

Für Version 26.4.0

So lässt sich das herausfinden

- Installieren einer WinGet app über Relution
- Die App ist nicht auf dem Gerät installiert
- Die Aktion ist fehlgeschlagen und enthält eventuell den Fehlercode -1073741515

Alternative

Die neueste Microsoft Visual C++ Redistributable → kann manuell als native App mit Erkennungsregel installiert werden.

1. Herunterladen der .exe Datei für die jeweilige Architektur (x64, arm64, x86) des Geräts

2. Hinzufügen einer nativen App

    - Es wird empfohlen die Architektur in den App Namen hinzuzufügen, um Verwirrung zu vermeiden, z. B. *VC Redist x64*
    - Empfohlene Installationsparameter: `/install /quiet /norestart`
    - Empfohlene Deinstallationsparameter: `/uninstall /quiet`
    - Pfad zum Uninstaller: Dieser muss für jede Version und Architektur individuell bestimmt werden, siehe unten
    - Empfohlene Erkennungsregel:
        - Registry
        - Registrierungsschlüssel: HKLM\SOFTWARE\Microsoft\VisualStudio\14.0\VC\Runtimes\{x64|x86|arm64}, siehe Microsoft-Dokumentation →
        - Name des Registrierungswerts: Version
        - Erkennungsmethode: Ein Wert mit dem angegebenen Name existiert
3. Anwenden der App auf den Geräten mit derselben Architektur

4. Die Aktion sollte erfolgreich angewendet werden

5. Aktualisieren der Geräteinformationen

6. Die App sollte in den installierten Apps enthalten sein

Wie der Pfad zum Uninstaller herausgefunden wird:

- Öffnen des Registrierungsschlüssels: HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\
- Suche nach dem Schlüssel der vc_redist.{x64|x86|arm64}.exe. Der Schlüssel ist ein Produktcode, z. B. *{2d48c97b-0c1e-4160-b3c4-c6dabebde745}*
- Der Pfad zum Uninstaller kann in folgendem Registrierungswert gefunden werden: QuietUninstallString, z. B. *C:\ProgramData\Package Cache\{2d48c97b-0c1e-4160-b3c4-c6dabebde745}\VC_redist.arm64.exe*

Für Version 26.4.0

WinGet Upgrade schlägt aufgrund eines defekten Manifests fehl

Manche Apps lassen sich mit `winget upgrade` nicht aktualisieren, obwohl eine neuere Version bereits im Relution AppStore eingetragen ist. Wenn die Ursache ein defektes Manifest auf WinGet-Seite ist, dann beendet sich der Upgrade-Befehl mit einem der folgenden Fehlercodes -1978335189 (*no applicable upgrade*), -1978335215 (*package not found*), -1978335192 (*no applicable installer found*) oder -1978335216 (Manifest-/Installer-Fehler) und kann mittels Skript gegebenenfalls dennoch installiert werden.

So lässt sich das herausfinden

- Die automatische Aktualisierung oder eine Deploy-Aktion der App schlägt fehl
- Die fehlgeschlagene Aktion enthält einen der oben genannten Fehlercodes

Alternative

Das Upgrade kann per Relution-Skript als erzwungene Installation wiederholt werden, siehe WinGet-Upgrade-Workaround →.

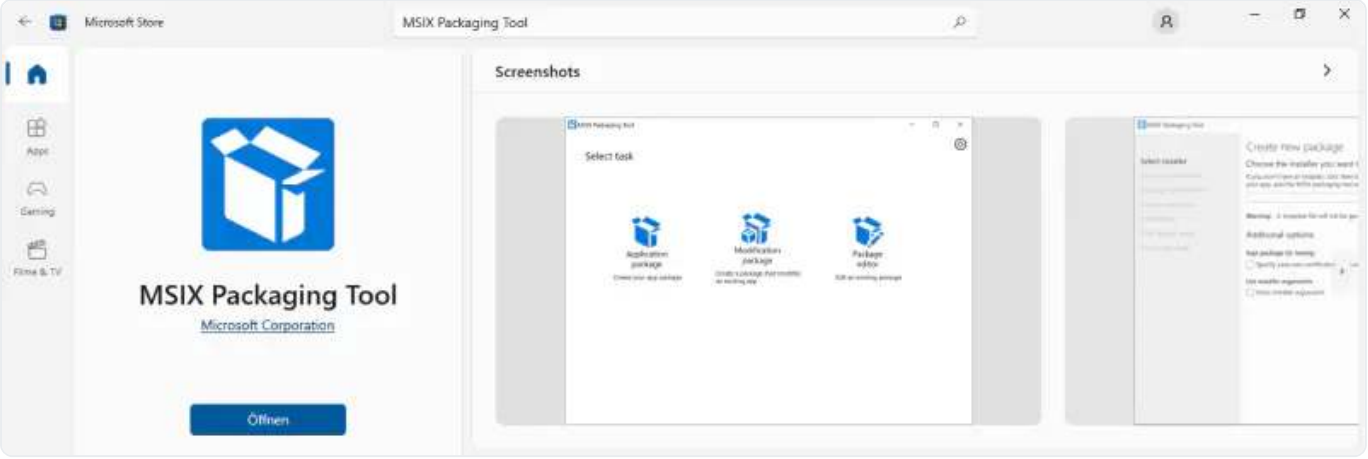
MSIX-Dateien erstellen

Das MSIX-Format ist ein Windows-App-Paketformat, das zum Erstellen und Verteilen von Anwendungen in Windows 10/11 verwendet wird. Diese MSIX-Dateien sind in der Regel nicht über einen einfachen Download zu beziehen, da sie vor der Installation auf Windows-Geräten mit einem Zertifikat versehen und neu “gepackt” werden müssen.

> MSIX-Dateien, APPX sowie Microsoft Store Apps können nicht direkt über Relution von den Geräten deinstalliert werden; deinstallieren lassen sich nur MSI- und EXE-Dateien sowie WinGet-Apps.

MSIX Packaging Tool

Für die Erstellung von MSIX-Dateien wird das MSIX Packaging Tool benötigt, das aus dem Microsoft Store → heruntergeladen und auf einem Windows-Gerät installiert werden kann.

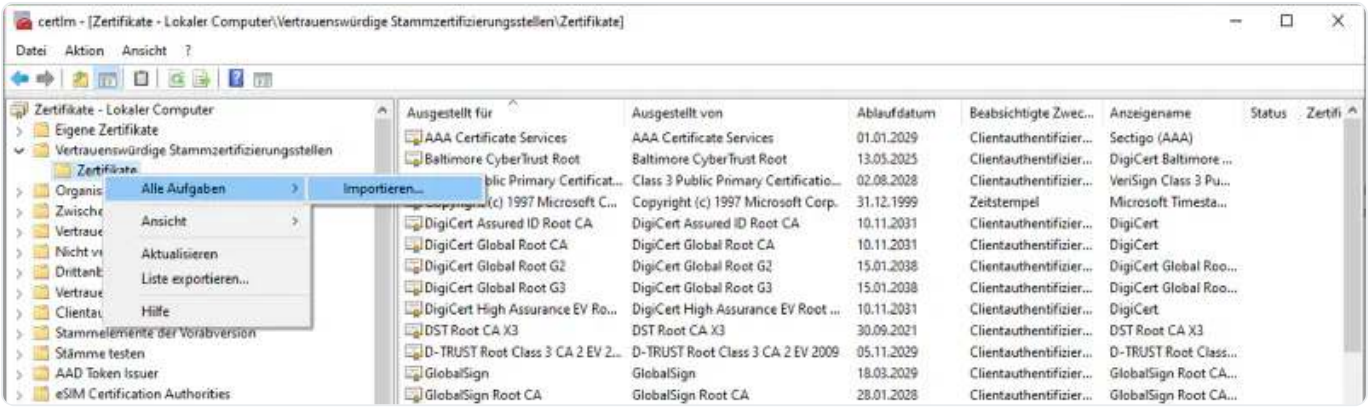


Zertifikatserstellung

Im nächsten Schritt muss ein Zertifikat erstellt werden. Dies kann bequem über die Powershell durchgeführt werden. Hierzu gegebenenfalls den Namen des Zertifikats und/oder das Passwort ändern.

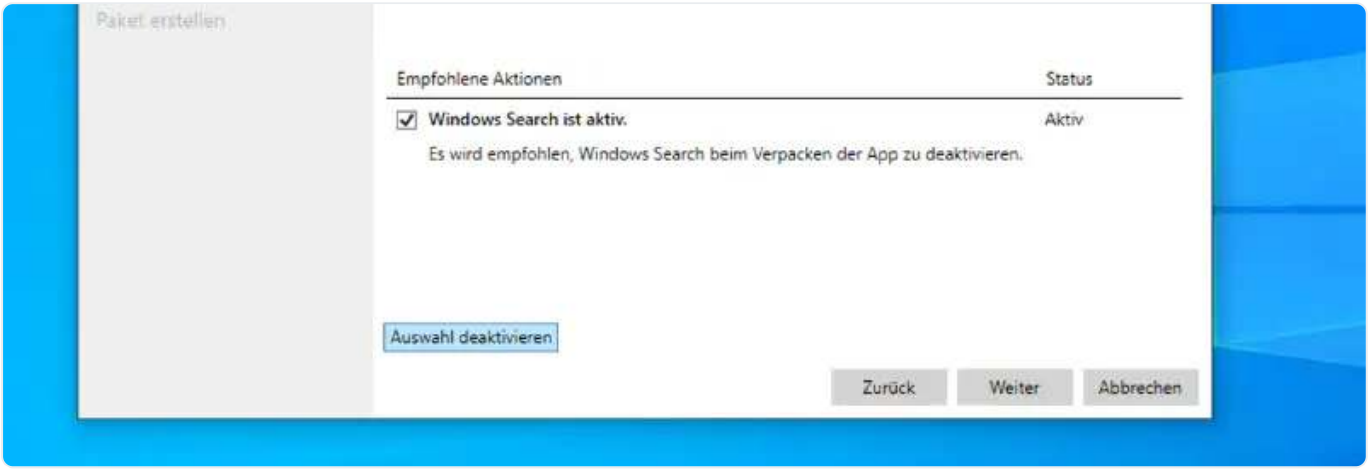
```
# Generiere ein neues selbst signiertes Zertifikat mit dem Betreff 'CN=Relution', dem
Schlüsselalgorithmus RSA,
# der Schlüssellänge 2048, der Schlüsselnutzung DigitalSignature und dem Typ
CodeSigningCert und speichere es
# in dem persönlichen Zertifikatsspeicher des aktuellen Benutzers
$Newcert = New-SelfSignedCertificate -Subject 'CN=Relution' -KeyAlgorithm RSA -
KeyLength 2048 -KeyUsage DigitalSignature -Type CodeSigningCert -CertStoreLocation
Cert:\CurrentUser\My

# Hole den Thumbprint des neu generierten Zertifikats
$thumbprint = $Newcert.Thumbprint

# Hole das Zertifikatsobjekt aus dem Speicher anhand seines Thumbprints
$cert = (Get-ChildItem -Path cert:\CurrentUser\My\$thumbprint)

# Überprüfe, ob das Zertifikat erfolgreich abgerufen wurde
if ($cert -ne $null) {
    # Konvertiere den Klartext-Passwortstring in einen sicheren String
    $Secure_String_Pwd = ConvertTo-SecureString "Passw0rd" -AsPlainText -Force

    # Exportiere das Zertifikat in eine PKCS#12-Datei auf dem Desktop des Benutzers
    Export-PfxCertificate -Cert $cert -FilePath
$env:USERPROFILE\desktop\MSIXZertifikat.pfx -Password $Secure_String_Pwd

    # Entferne das Zertifikat aus dem Speicher
    Remove-Item cert:\CurrentUser\My\$thumbprint
}
```

Das erstellte Zertifikat muss auf allen Windows 10/11-Geräten, auf denen MSIX-Dateien installiert werden sollen, in der Kategorie Vertrauenswürdige Stammzertifizierungsstellen gespeichert werden. Dies kann entweder mit Relution über die Richtlinienkonfiguration Zertifikat oder manuell direkt auf den Geräten durchgeführt werden. Der Passwort String im Beispiel lautet Passw0rd. Um das Zertifikat manuell hinzuzufügen, die Zertifikatsverwaltung Computerzertifikate verwalten als Administrator starten.

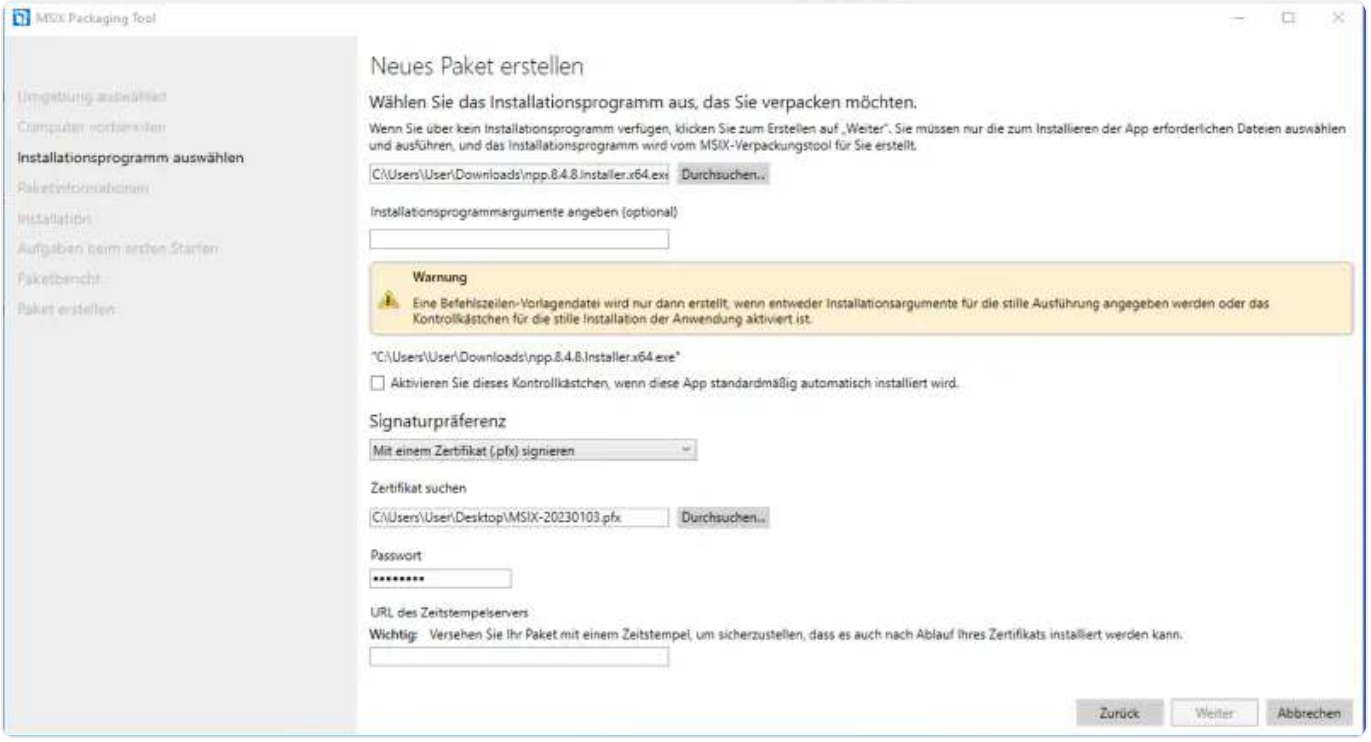


Erstellung von MSIX-Dateien

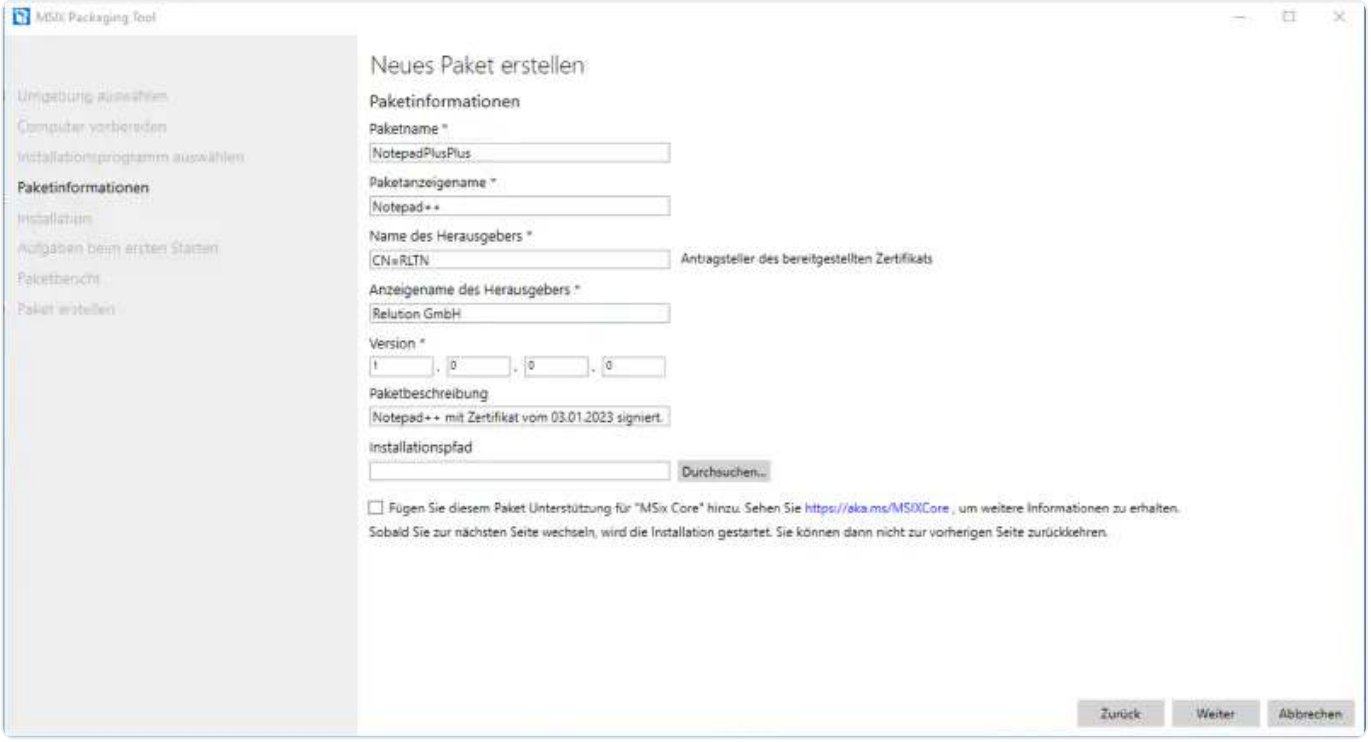
Das MSIX Packaging Tool starten und die Option zur Erstellung eines neuen App-Paketes wählen. Die Auswahl Windows Search ist aktiv im anschließenden Dialog deaktivieren.



Im Beispiel wird eine MSIX-Datei für Notepad++ erstellt. Dazu muss zuerst die Setup-Datei heruntergeladen werden. Im Anschluss im MSIX Packaging Tool die Datei und das Zertifikat auswählen. Die Signaturpräferenz muss auf Mit einem Zertifikat (.pfx) signieren eingestellt sein.

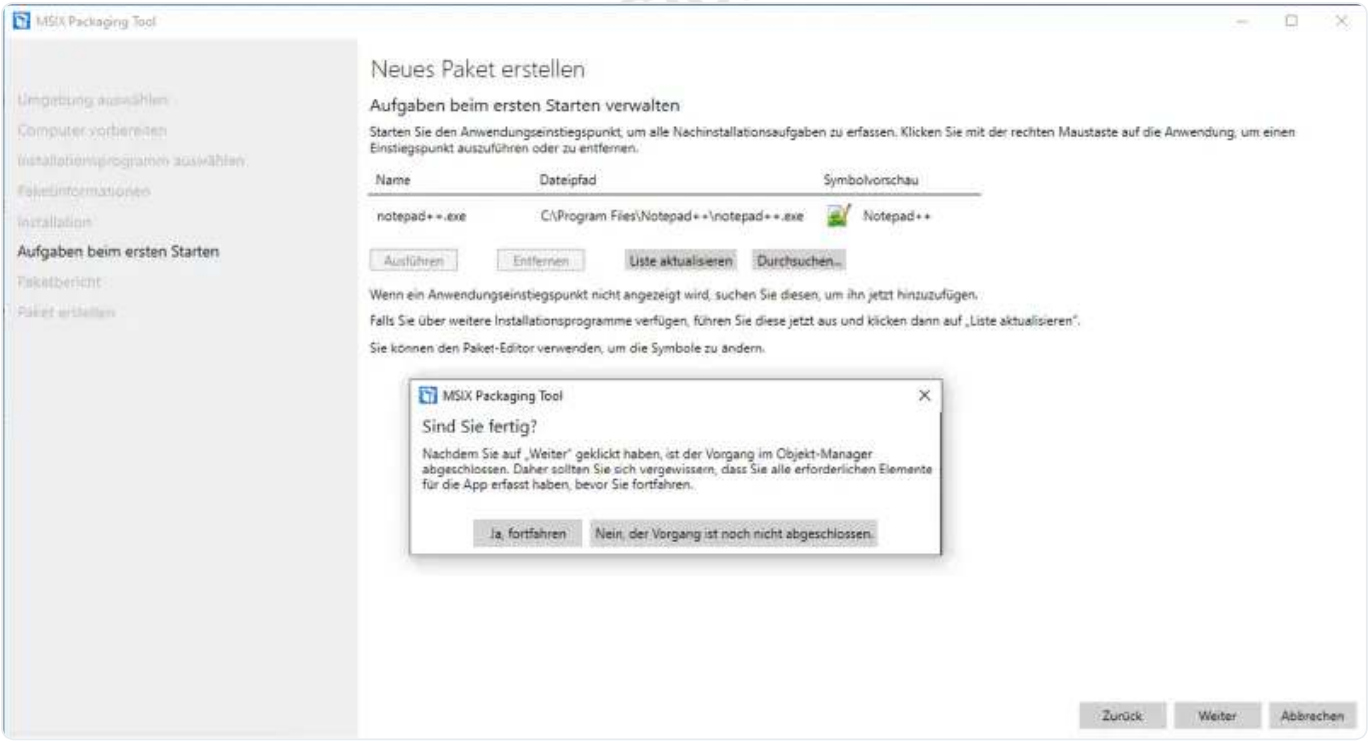


Die entsprechenden Felder ausfüllen.

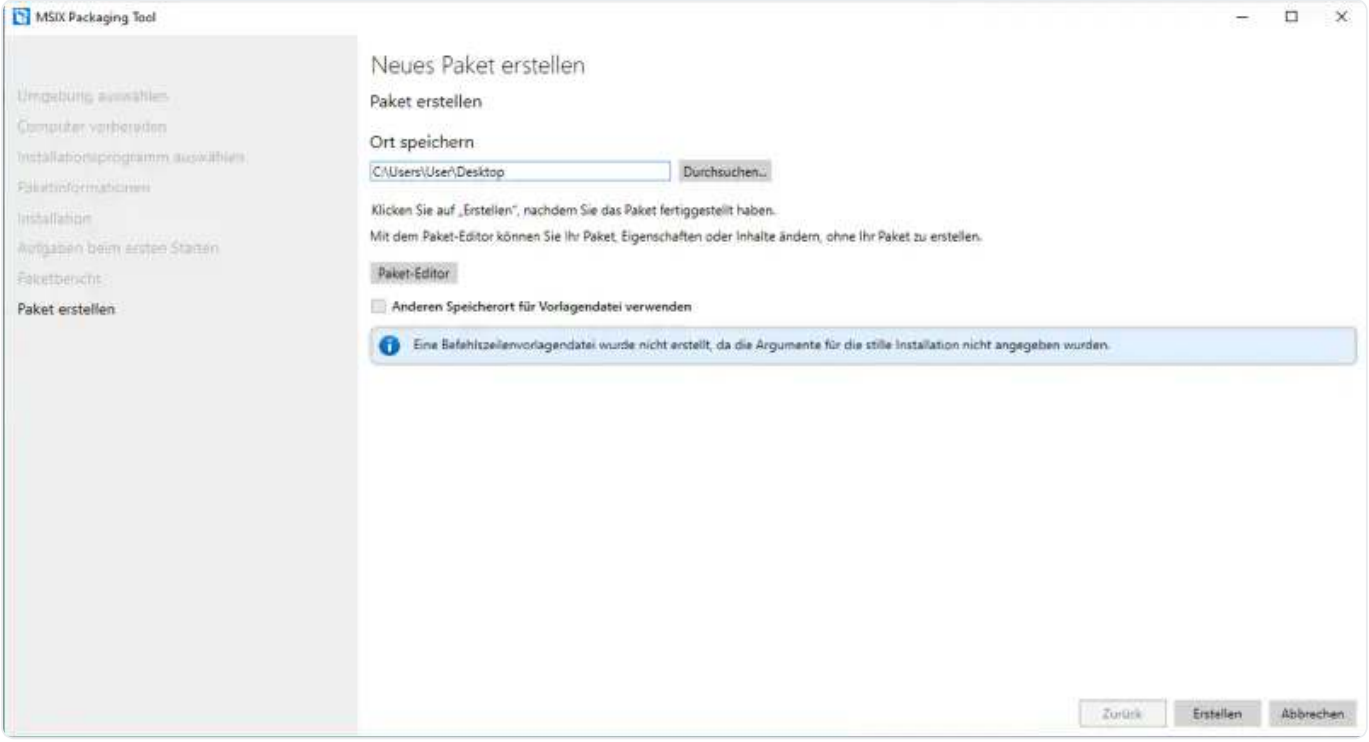


Nun startet der Installer von Notepad++. Diesen wie gewohnt durchführen und die Konfigurationen nach den eigenen Wünschen vornehmen.

Im MSIX Packaging Tool auf Weiter und Ja, fortfahren klicken, wenn die Installation von Notepad++ abgeschlossen ist.



Das Tool wird anzeigen, dass keine Dienste installiert und erkannt wurden. Im letzten Dialogfenster kann der Speicherort des Pakets festgelegt werden. Die Erstellung mit Klick auf Erstellen abschließen.



Zertifikat auf anderen Windows PCs bereitstellen

Für Version 26.4.0

Um das MSIX Paket auf anderen Windows PCs installieren zu können, muss das Zertifikat auf diesen bereitgestellt werden. Hierzu muss das Zertifikat mit OpenSSL aus dem PKCS#12-Container (`.pfx`) als einzelne Zertifikatsdatei (PEM-Format) exportiert werden. Dazu muss OpenSSL auf dem System installiert sein. Dies funktioniert mit diesem Befehl:

```
openssl pkcs12 -in MSIXZertifikat.pfx -clcerts -nokeys -out MSIXZertifikat.der
```

Ab OpenSSL 3.x:

```
openssl pkcs12 -in MSIXZertifikat.pfx -clcerts -nokeys -out MSIXZertifikat.der -passin
pass:Passw0rd #Passphrase entsprechend anpassen
```

Anschließend kann das soeben umgewandelte PKCS1 Zertifikat in Relution unter `Einstellungen` → `Zertifikate` hochgeladen werden. Die Umwandlung ist nötig, weil Relution eine hochgeladene `.pfx`-Datei als Client-Zertifikat installiert und den Zertifikatsspeicher nur bei einzelnen Zertifikaten (PKCS1) auswählen lässt.

Abschließend muss das Zertifikat in einer Richtlinie für Windowsgeräte auf die Geräte ausgeliefert werden. Hierzu wird die Konfiguration Zertifikat genutzt und darin das Zertifikat ausgewählt, siehe Zertifikate installieren →.

Es muss zwingend Vertrauenswürdige Stammzertifikate als Zertifikatsspeicher gewählt werden. Die Voreinstellung Automatisch würde das im Beispiel erstellte Zertifikat in Eigene Zertifikate ablegen, da es kein Zertifizierungsstellen-Zertifikat ist; Windows würde dem MSIX-Paket dann nicht vertrauen.

MSIX-Datei in Relution hochladen

Das fertige Paket wird unter `Apps` → `App Store` über Hinzufügen mit der Quelle Native App hochgeladen. Relution akzeptiert dabei die Formate `.msix`, `.msixbundle`, `.appx` und `.appxbundle`. Anschließend kann die App auf die Windows-Geräte verteilt werden, auf denen das Zertifikat installiert ist.

Für Version 26.4.0

opsi-Server einrichten

Diese Anleitung bietet eine detaillierte Beschreibung des Prozesses zur Einrichtung eines opsi-Servers, um Windows-Installationen effizient bereitzustellen und die Geräteanmeldung in Relution zu automatisieren. Ziel ist es, einen funktionierenden opsi-Server zu konfigurieren, der über Netboot Windows-Betriebssysteme auf Client-Geräten installieren und diese nahtlos in Relution zur zentralisierten Verwaltung integrieren kann.

Die Anleitung umfasst alle wesentlichen Schritte, einschließlich der Installation und Konfiguration des opsi-Servers, der Vorbereitung von Windows- und WinPE-Installationsdateien. Darüber hinaus wird der Prozess der automatisierten Relution-Registrierung unter Verwendung lokaler opsi-Produkte erklärt.

Glossar

Begriff	Erklärung
Administrationskonsole	Bezieht sich auf die Benutzeroberfläche, die im opsi-Server enthalten ist und unter *https://localhost:4447* läuft.
configed	Bezieht sich auf die zusätzliche Java-Anwendung, die auf jedem Gerät ausgeführt werden kann, um sich mit dem opsi-Server zu verbinden.
Client-Debug-Konsole	Bezieht sich auf die Benutzeroberfläche des opsi-Agents, die unter *https://<opsi-client-IP>:4441* läuft.

Einrichtung des opsi-Servers

Dieser Abschnitt führt durch den Prozess der Einrichtung des opsi-Servers und bietet eine detaillierte Anleitung zu den erforderlichen Konfigurationen, Installationsschritten und der Vorbereitung der notwendigen Pakete.

Serverinstallation

Wir empfehlen die Docker-basierte Installation, um den opsi-Server in Linux-Umgebungen einzurichten. Zu beachten ist jedoch, dass die Docker-Installation auf Geräten mit macOS aufgrund von Kompatibilitätsproblemen mit dem integrierten TFTP-Server nicht verwendet werden kann. Für macOS-Systeme sollte die vorkonfigurierte VirtualBox → verwendet werden.

Den Anweisungen der opsi-Dokumentation unten folgen, um den opsi-config-Server einzurichten. Nach der Installation läuft die Administrationskonsole unter *https://localhost:4447*. Zusätzlich die Java-Anwendung → für `configed` herunterladen.

Dokumentation

- Schnellstart →
- Docker-Installation →
- opsi-WebGui →
- Netzwerkkonfiguration →

Installation der benötigten opsi-Pakete

Die Administrationskonsole öffnen und zum Terminal-Tab navigieren. Im Terminal folgenden Befehl verwenden, um die benötigten opsi-Pakete zu installieren:

```
opsi-package-updater -v install <paketname>
```

Eine Übersicht über alle verfügbaren lokalen und Netboot-Produkte ist im opsi-Repository → zu finden.

Die folgenden Pakete installieren:

Paket	Beschreibung
opsi-client-agent	Client, der auf dem Gerät installiert ist, um Befehle auszuführen
opsi-script	Wird vom Client-Agent verwendet, um opsi-Skripte auszuführen
opsi-uefi-netboot	Erforderlich für UEFI-Netboot, um die Bootreihenfolge zu ändern
opsi-winpe	Erstellt ein WinPE auf dem Gerät
hwaudit (optional)	Inventarisierungstool, das Informationen über das Gerät sammelt

Client-Registrierung

Dieser Abschnitt behandelt die Registrierung von Geräten, auf denen bereits ein Windows-Betriebssystem installiert ist, mit dem opsi-Server. Der opsi-Client-Agent wird auf dem Gerät installiert, um die Kommunikation mit dem Server herzustellen und eine zentrale Steuerung und Aktionen zu ermöglichen.

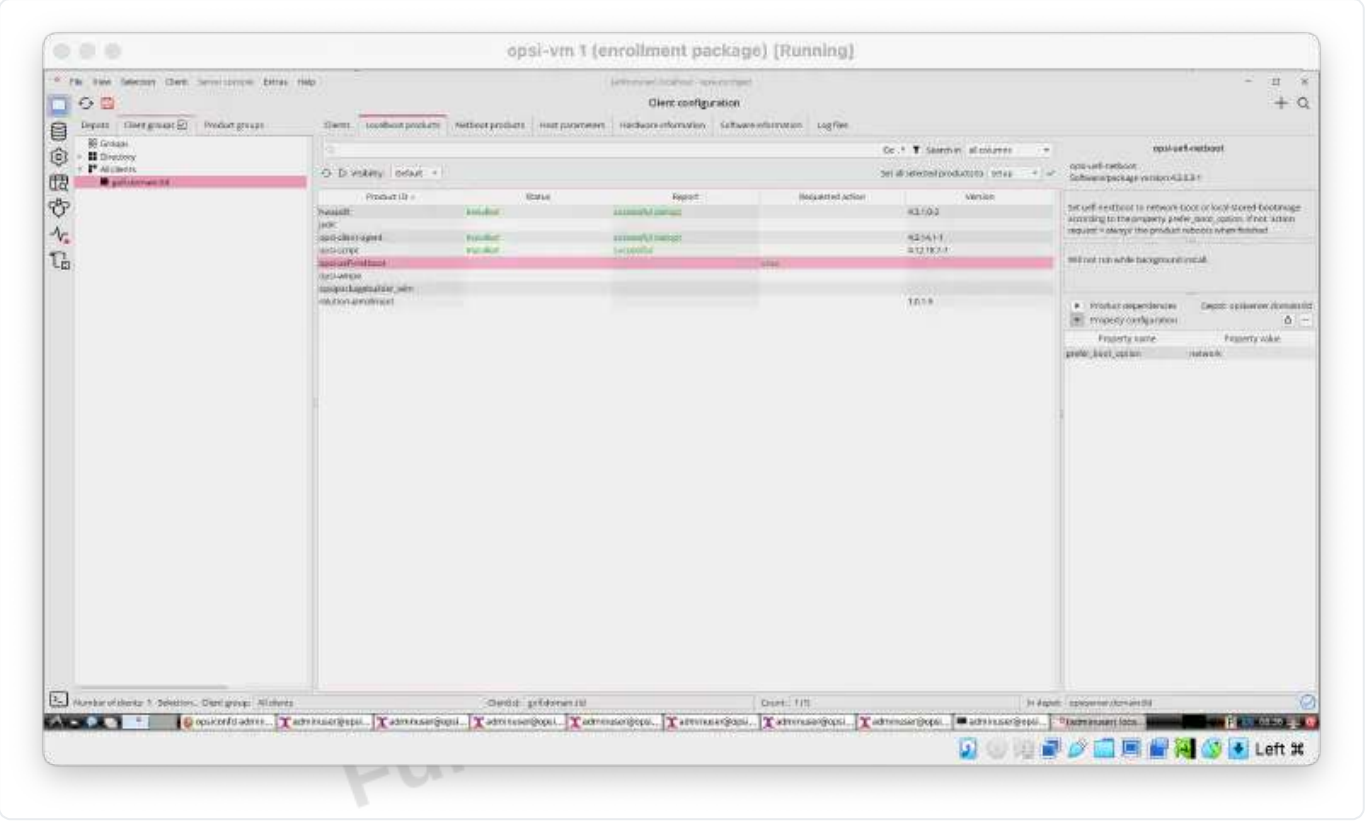
Für Clients ohne installiertes Windows sind zusätzliche Schritte erforderlich, um das Betriebssystem über Netboot zu installieren. In diesem Fall die offiziellen opsi-Dokumentationen für detaillierte Anweisungen zur Client-Initiierung prüfen.

Der opsi-Client-Agent kann unter `https://<opsi-server-ip>:4447/public/opsi-client-agent/` heruntergeladen werden. Nach der Installation auf dem Gerät müssen die Adresse des opsi-Servers und die Anmeldedaten eines Admin-Kontos eingegeben werden.

Nach Abschluss der Registrierung wird der Client im Geräteinventar des `configed` angezeigt. Um die Verbindung zwischen opsi-Server und Client zu überprüfen, kann eine Popup-Nachricht gesendet werden (`Top-Menü` → `Client` → `Popup-Nachricht senden`).

Das UEFI-Netboot-Produkt installieren, indem die Angeforderte Aktion auf `einmal` gesetzt wird.

Der Tab Logdateien enthält detaillierte Informationen zur Fehlerbehebung beim opsi-Client-Agent und dem Linux-Bootimage. Dies ist nützlich, um die Installation von lokalen und Netboot-Produkten zu debuggen.



Dokumentation

- Client-Installation →

Vorbereitung der Windows-Installationsdateien

Dieser Abschnitt enthält Anweisungen zum Erwerb der erforderlichen Windows-ISO-Datei, zum Erstellen einer kompatiblen Windows-Preinstallation-Umgebung (WinPE) und zur Organisation dieser Dateien in der erforderlichen Verzeichnisstruktur für Netboot-Produkte. In diesem Beispiel wurde Windows 11 auf dem Gerät installiert.

Windows-ISO und WinPE

Um den opsi-Server für die Bereitstellung von Windows-Installationen vorzubereiten, sind mehrere Schlüsselkomponenten erforderlich. Zunächst wird die Windows-ISO-Datei für die spezifische Version benötigt, die installiert werden soll, z. B. Windows 11. Die ISO-Datei kann von der offiziellen Microsoft-Website heruntergeladen werden.

Als Nächstes muss ein WinPE erstellt werden. Das WinPE muss mit der Version des bereitgestellten Windows-Images übereinstimmen. Dies kann durch die Nutzung des opsi-winpe-Pakets erreicht werden, welches die Installation von Windows ADK und dem PE-Plugin erfordert. Alternativ kann das WinPE direkt mit Windows ADK erstellt werden, wie in der opsi-Dokumentation beschrieben.

Die Dokumentation zu Netboot-Produkten → beschreibt zwei Möglichkeiten zur Erstellung eines WinPE:

1. Verwendung des Pakets `opsi-winpe` (Windows ADK und das PE-Plugin → müssen installiert sein!)
2. Verwendung des Windows ADK.

Verzeichnisstruktur für Netboot-Produkt einrichten

Das passende Wrapper-Paket für das eigene Windows-Image aus dem opsi-Netboot-Repository → mithilfe des Paketmanagers installieren, z. B. `opsi-local-image-win11-x64_4.3.0.2-13` für Windows 11.

Auf dem opsi-Server wird ein neues Verzeichnis hinzugefügt (z. B. */var/lib/opsi/depot/win11-x64*). Die Windows-Image-Dateien und die WinPE-Dateien müssen in die entsprechenden Verzeichnisse platziert werden (siehe Übersicht der Verzeichnisstruktur →).

Installationsdateien

Der Inhalt der Windows-ISO-Datei muss in das Verzeichnis `installfiles` verschoben werden.

WinPE

Das WinPE muss in das Verzeichnis `winpe` verschoben werden.

Für Version 26.4.0

> Alle Dateien aus den Unterverzeichnissen (fwfiles, media, mount) extrahieren und auf der obersten Ebene platzieren. Es kann zu Problemen bei der Erkennung der setup.exe kommen, daher sollten auch die Verzeichnisse auf der obersten Ebene abgelegt werden.

Am Ende befinden sich alle Dateien und Verzeichnisse des WinPE auf der obersten Ebene des folgenden Verzeichnisses:

> Vollständiges Konfigurationsbeispiel anzeigen

Dokumentation

- Windows-OS-Installation →
- Netboot-Produkte →

DHCP-Server konfigurieren

Um einen DHCP-Server für PXE-Boot einzurichten, müssen spezifische Optionen definiert werden, mit denen PXE-Boot-Clients die benötigten Informationen erhalten, um den TFTP-Server zu finden und die Bootloader-Datei herunterzuladen. Diese Optionen werden üblicherweise als DHCP-Optionen 66 (TFTP-Server) und 67 (Bootloader-Datei) bezeichnet.

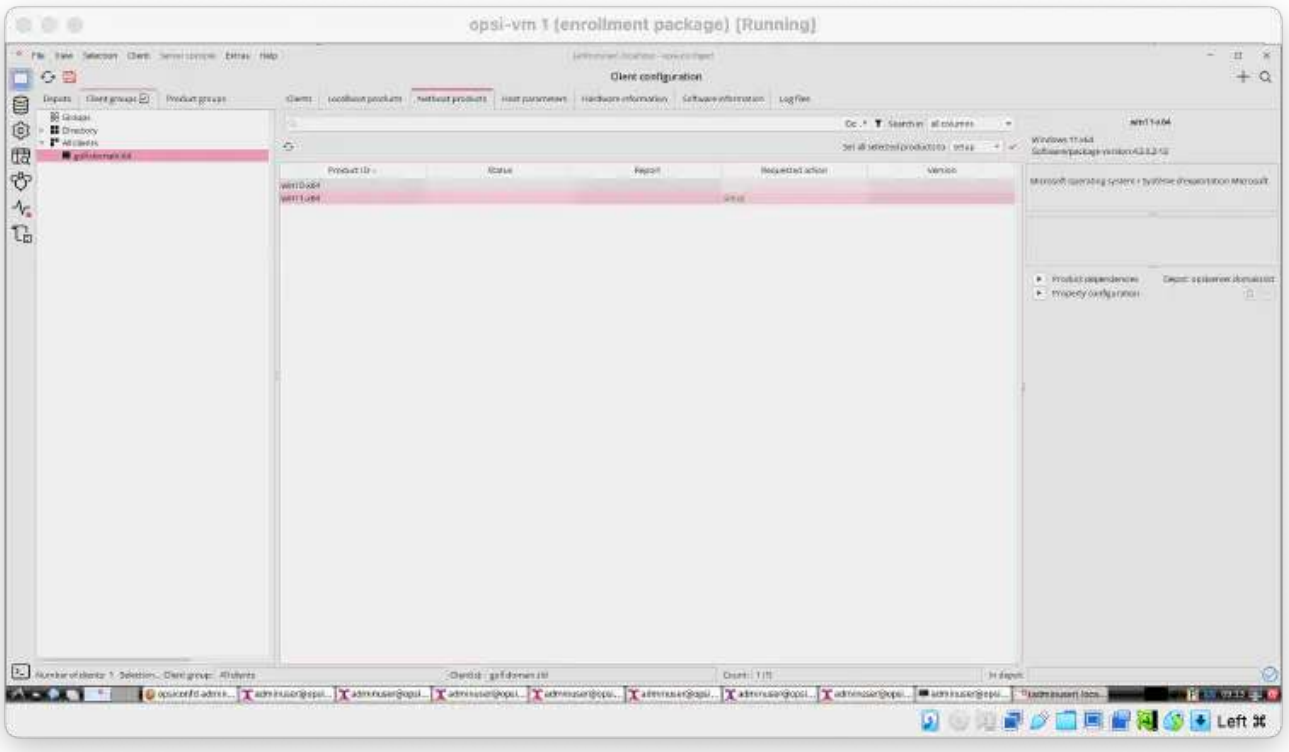
Falls der eigene Router keine Benutzeroberfläche zur Konfiguration dieser Optionen bereitstellt, beispielsweise bei Verwendung eines Linux- oder Windows-DHCP-Servers, müssen die folgenden Optionen zur Datei `dhcpd.conf` hinzugefügt werden:

```
next-server <opsi-server-IP>;
filename "opsi/opsi-linux-bootimage/loader/opsi-netboot.efi";
```

Netboot starten

Um die Installation eines Netboot-Produkts zu starten, zum Tab Netboot-Produkte in der Configed-Oberfläche navigieren. Die Angeforderte Aktion des gewünschten Produkts auf `Setup` setzen und auf das Speichersymbol in der oberen linken Ecke klicken.

Nachdem der Auftrag übermittelt wurde, lässt sich der Prozess überwachen, indem die Logs in den Client-Details von `configed` sowie in der `Client-Debug-Konsole` überprüft werden. Diese Logs zeigen an, ob der opsi-Client den Auftrag erfolgreich erhalten und verarbeitet hat. Nach Abschluss dieser Schritte wird der Windows-Client beim nächsten Neustart nach Netboot-Quellen suchen und den Installationsprozess starten.



Für die Fehlerbehebung können die folgenden Befehle ausgeführt werden, um den TFTP-Verkehr auf dem opsi-Server einzusehen:

```
sudo tcpdump -i lo0 port 69
```

```
journalctl -f
```

Dokumentation

- opsi mit UEFI/GPT →

> Für Windows-11-Installationen muss sichergestellt werden, dass das Gerät TPM 2.0 unterstützt. Im BIOS-Menü prüfen, ob die Option aktiviert ist. Gelegentlich ist es notwendig, TPM aus- und wieder einzuschalten oder es beim nächsten Neustart zurückzusetzen.

Relution-Einschreibung

Dieser Abschnitt beschreibt den Prozess der Einschreibung von Geräten in Relution mithilfe des `relution-enrollment`-Pakets. Dieses Produkt automatisiert die Installation eines Bereitstellungspakets über PowerShell und sorgt so für eine nahtlose Integration der Geräte in Relution.

Bereitstellungspaket vorbereiten

Ein Bereitstellungspaket muss gemäß den Anweisungen zum Windows bulk enrollment → erstellt werden.

Für Version 26.4.0

> Das Paket muss den Namen relution tragen, damit das opsi-Skript die richtige Datei erkennen kann.

opsi-Paket für die Relution-Einschreibung installieren

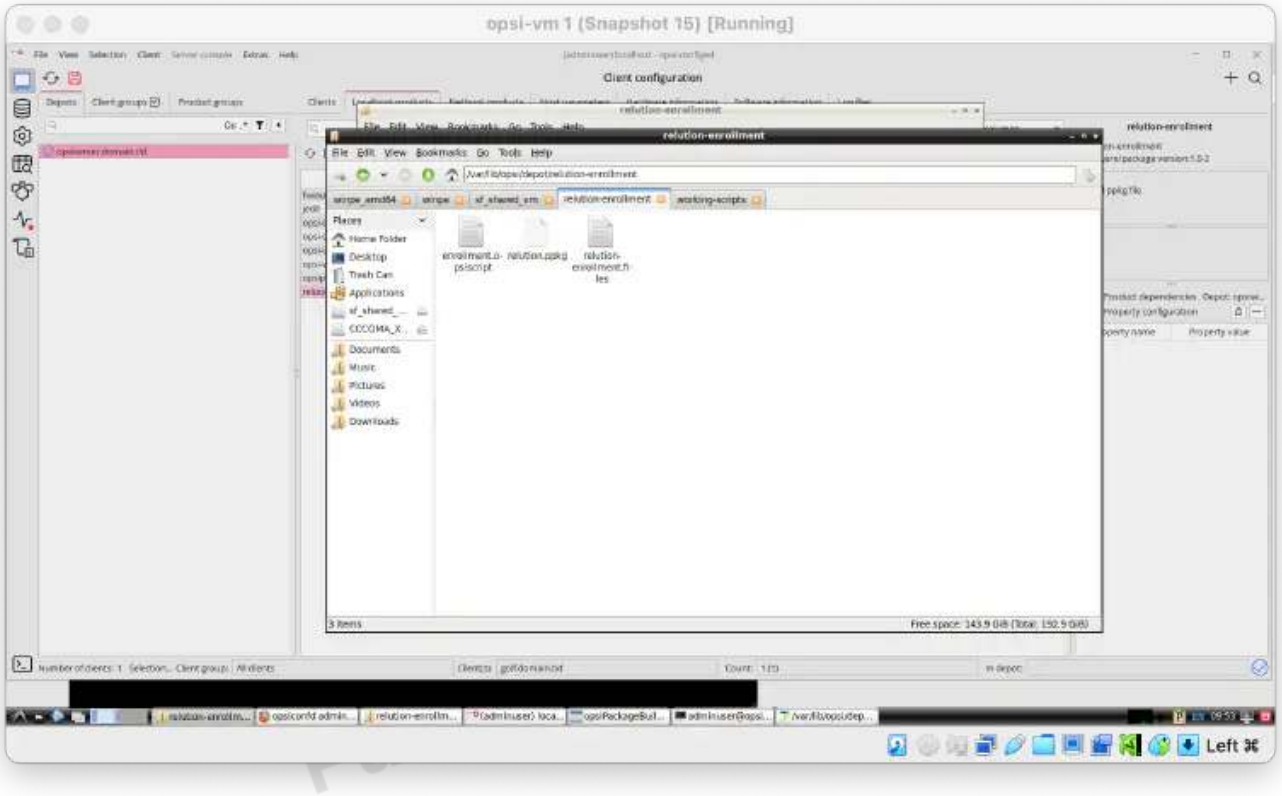
Das Paket `relution-enrollment` ist als *experimentelle* Version im öffentlichen opsi-Repository → verfügbar.

Die `relution-enrollment_<package-version>.opsi`-Datei mit dem Befehl `wget` herunterladen und den folgenden Befehl ausführen, um das opsi-Paket zu installieren, damit es in der `configed`-Oberfläche verfügbar wird:

```
opsi-cli package install relution-enrollment_<package-version>.opsi
```

Nach der Installation ist das Paket im Depot-Ordner (`/var/lib/opsi/depot/relution-enrollment`) vorhanden. Das generierte Bereitstellungspaket in diesem Ordner platzieren und `opsi-set-rights` in diesem Verzeichnis ausführen.

```
/var/lib/opsi/depot/relution-enrollment/
├── enrollment.opsiscript
├── relution.ppkg
├── relution-enrollment.files
```

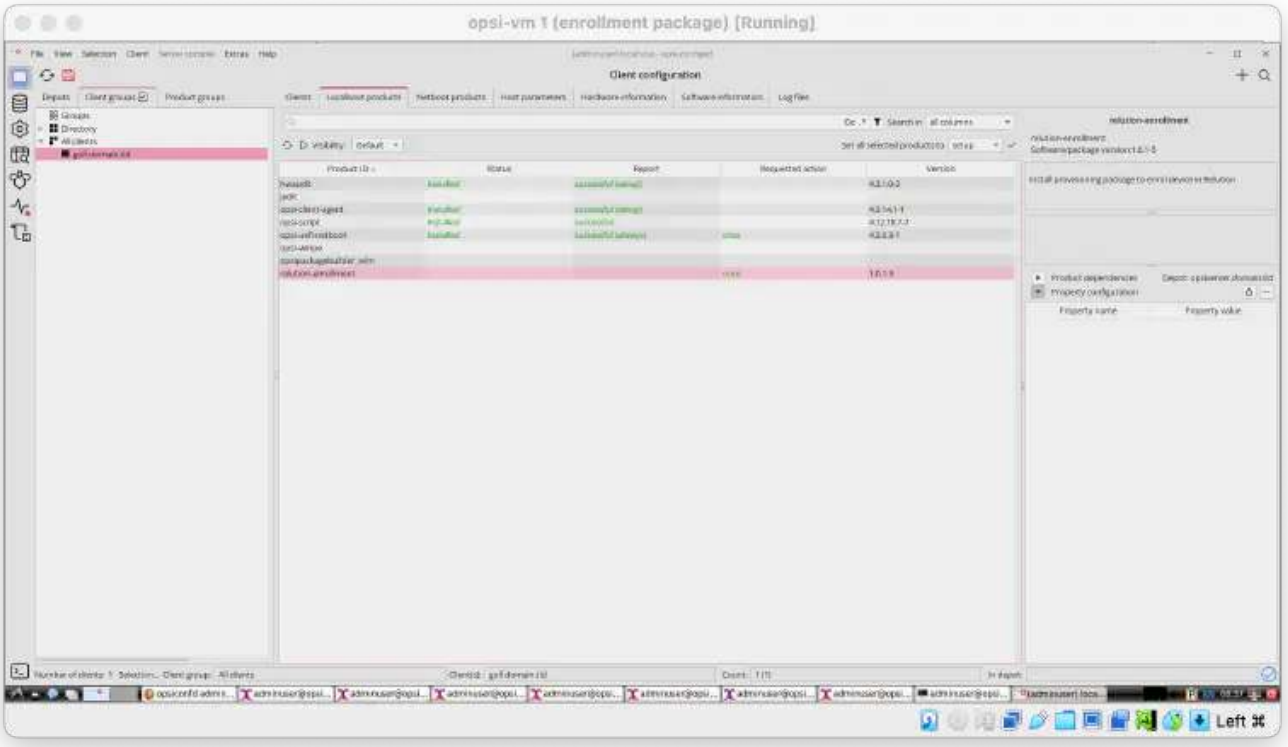


Produkt installieren

Um das Paket zu installieren, den Client auswählen und zum Tab Localboot-Produkte navigieren. Für das Produkt `relution-enrollment` die Angeforderte Aktion auf `einmal` setzen. Den Status speichern und eine `on_demand`-Aktion auslösen (`Menü` → `Client` → `Event opsiclientd auslösen` → `on_demand`).

Da der PowerShell-Befehl zur Installation des Bereitstellungspakets die Aktion immer als erfolgreich markiert, sollten die Logs auf eventuelle Fehler überprüft werden. Der Fehler `Package installation failed, error code -2147024713 (800700B7)` zeigt an, dass ein Paket mit derselben ID bereits installiert ist.

Wenn das Bereitstellungspaket bereits installiert wurde, muss es zuerst entfernt werden.



Für Version 26.4.0

Tipps zur Fehlerbehebung

In diesem Abschnitt werden häufige Probleme beschrieben, die während der Einrichtung des opsi-Servers und der Netboot-Installation auftreten können. Zudem werden Lösungen oder Verweise auf relevante Dokumentationen zur Fehlerbehebung bereitgestellt:

- Fehler: Unable to get geometry for disk '/dev/nvme0n1' →
  - Passwort für den Root-Benutzer setzen, indem der Host-Parameter `netboot.linux-bootimage.cmdline.pwh` eingestellt wird.
  - Wenn der Fehler auftritt, `Strg + Alt + F3/F4/F5` drücken, um auf das aktive Terminal zu wechseln.
  - Die Root-Anmeldedaten und das Passwort eingeben.
  - Den Befehl `sgdisk --zap-all /dev/nvme0` ausführen, um die Partition zu löschen.
  - Zurück zum anderen Terminal wechseln und den Netboot erneut versuchen.
  - Weitere Informationen sind in der Dokumentation über Netboot-Produkte → zu finden.
- opsi winPE ist leer →: Alle Dateien aus den WinPE-Unterverzeichnissen (z. B. media) in die oberste Ebene verschieben
- WinPE-Initialisierung funktioniert nicht →

Identitätszertifikat

In Relution eingeschriebene Apple- und Windows-Geräte erhalten ein Identitätszertifikat. Dieses ist ein Jahr gültig und wird automatisch verlängert, solange eine aktive Kommunikation zum Gerät besteht.

Es kann jedoch vorkommen, dass Geräte eingelagert oder inaktiv sind und das Identitätszertifikat dadurch nicht rechtzeitig verlängert werden kann. Aus Sicherheitsgründen verweigert Relution bei einem abgelaufenen Identitätszertifikat jegliche Kommunikation mit dem betreffenden Gerät.

Identitätszertifikat prüfen und verlängern

Betroffene Geräte können unter `Navigation` → `Geräte` → `Inventar` → `[Gerät]` im Reiter Informationen im Block Sicherheit geprüft werden.

Es folgen drei relevante Felder:

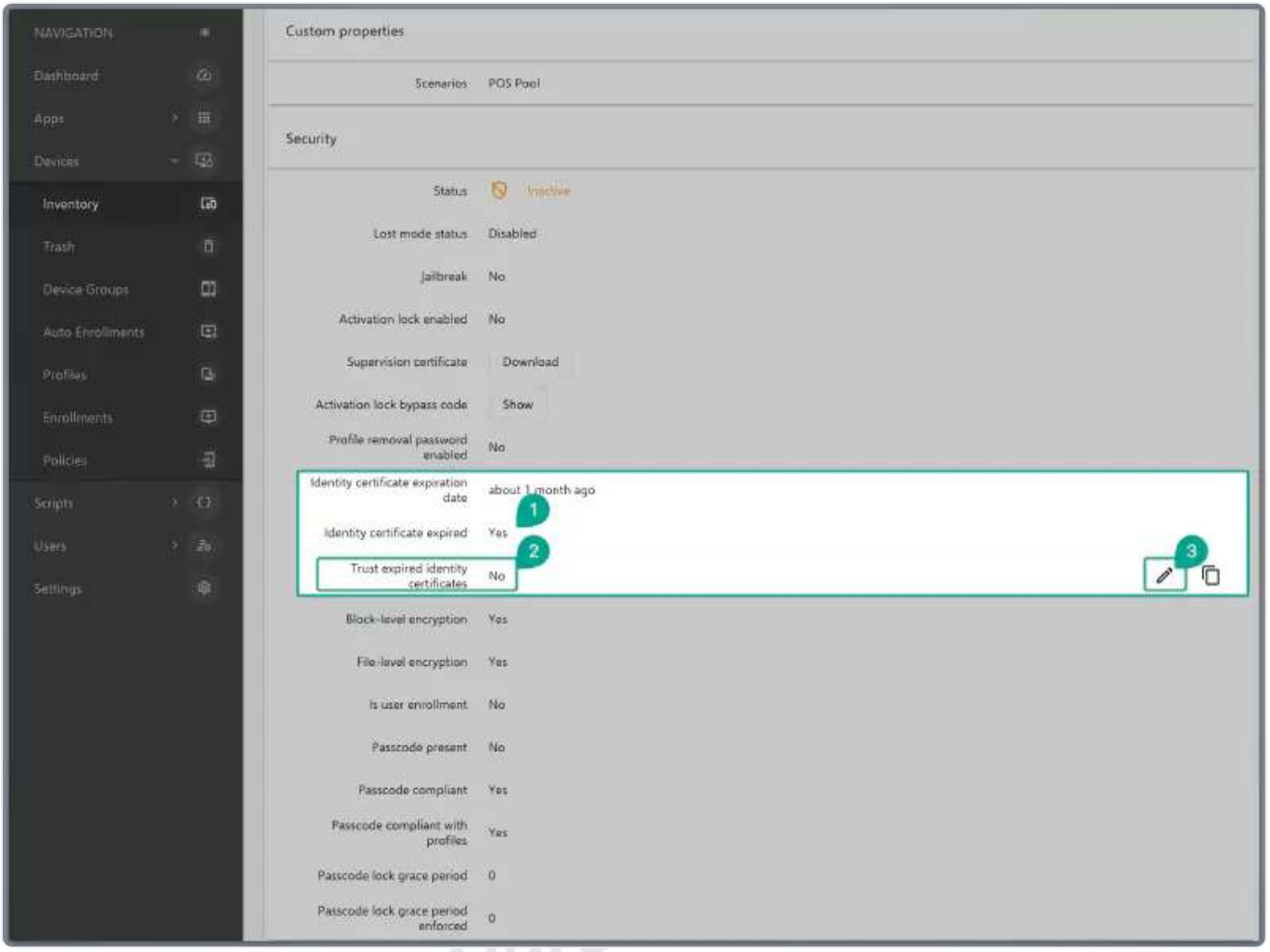
- Ablaufdatum des Identitätszertifikats
- Identitätszertifikat ist abgelaufen
- Abgelaufenen Identitätszertifikaten vertrauen

Ist das Identitätszertifikat abgelaufen und Abgelaufenen Identitätszertifikaten vertrauen noch nicht aktiv, erscheint beim Überfahren dieser Zeile mit der Maus die Schaltfläche Bearbeiten (Stiftsymbol). Ein Klick darauf öffnet einen Bestätigungsdialog. Mit Bestätigen akzeptiert Relution vorübergehend MDM-Nachrichten, die mit dem abgelaufenen Zertifikat signiert sind, und stößt die Erneuerung an: Bei Windows-Geräten wird eine Aktion zur Erneuerung des Client-Zertifikats eingereiht, bei Apple-Geräten das MDM-Profil aktualisiert. Dadurch wird die Kommunikation zum Gerät wieder als vertrauenswürdig eingestuft, und es können MDM-Befehle verarbeitet werden. Sobald das Gerät ein neues Identitätszertifikat erhalten hat, setzt Relution Abgelaufenen Identitätszertifikaten vertrauen automatisch zurück.

Für Version 26.4.0

Die Aktion setzt die Berechtigung zum Bearbeiten von Geräten voraus.

> Abgelaufenen Zertifikaten zu vertrauen stellt ein Sicherheitsrisiko dar, z. B. wenn das Identitätszertifikat Dritten zugänglich gemacht wurde.



Wichtiger Hinweis: Die Aktion steht zur Verfügung, sobald das Identitätszertifikat abgelaufen ist, und kann auch ausgeführt werden, während das Gerät offline ist. Sobald das Gerät wieder online ist, erhält es ein neues, gültiges Identitätszertifikat.

Mehrere betroffene Geräte lassen sich unter `Navigation` → `Geräte` → `Inventar` über die Filter Identitätszertifikat ist abgelaufen und Abgelaufenen Identitätszertifikaten vertrauen gesammelt finden.

Skripte global bereitstellen

Mit Relution `Server Version 5.22` ist es möglich, Windows Skripte zentral zu veröffentlichen und damit allen Organisationen zur Verfügung zu stellen. Dies geschieht in der Global-Organisation (bis Version 5.22: Store-Organisation).

> Ein in der Global-Organisation angelegtes Skript ist zunächst nur dort sichtbar. Erst über Global verfügbar machen steht es allen Organisationen zur Verfügung, auch später angelegten. Dieser Schritt kann nicht rückgängig gemacht werden. Bearbeitet oder gelöscht werden kann das Skript danach nur in der Global-Organisation.

Skript hinzufügen

Nach erfolgreicher Anmeldung in der Global-Organisation lässt sich über die Navigation auf der linken Seite zum Abschnitt Skripte navigieren. Dort besteht die Möglichkeit, neue Skripte zu erstellen, indem der Hinzufügen-Button verwendet wird. Die Erstellung ist in 3 Punkte gegliedert.

Allgemein

- Name - Der globale Anzeigename für das Skript (Pflichtfeld, maximal 255 Zeichen)
- Beschreibung - Eine ergänzende Beschreibung zum Skript (maximal 4000 Zeichen)
- Plattform - Für Windows Skripte wird Windows ausgewählt (Pflichtfeld, voreingestellt). Nur bei Windows werden `*.ps1`-Dateien und das Feld Argumente angeboten. Die Plattform lässt sich nach dem Speichern nicht mehr ändern und ist auch gesperrt, solange eine Skriptdatei geladen ist.

Für Version 26.4.0

> Nachträgliche Änderungen an einem global verfügbaren Skript gelten in allen Organisationen. Auf Geräten, deren Richtlinie das Skript verwendet, wird das Skript automatisch aktualisiert.

Inhalt

- Skript Datei - Über Auswählen (oder per Drag-and-drop) kann eine lokale `*.ps1`-Datei geladen werden. Ihr Inhalt wird in das Feld Inhalt übernommen.
- Inhalt - Alternativ kann das Skript direkt in das Textfeld eingegeben werden. Sobald das Feld Text enthält, wird Skript Datei ausgeblendet.

Ausführung

- Zeitüberschreitung (in Minuten) - Nach Ablauf des angegebenen Zeitraums wird die Skript-Ausführung zwangsweise abgebrochen. Standardwert: 5 Minuten, zulässig sind 1 bis 30 Minuten.
- Argumente - Die Argumente und die zugewiesenen Werte werden am Anfang des Skripts eingefügt, wenn es auf dem Gerät ausgeführt wird (maximal 512 Zeichen). Mehrere Argumente werden durch Semikolon getrennt, nach dem letzten Argument ist kein Semikolon erforderlich. Die Argumente können in dem Skript mittels deren Namen verwendet werden.

Beispiel:

```
# Argumente (Feld „Argumente“)
$arg1=10; $arg2='text'

# Nutzung im Skript
Write-Host $arg1

# Ausführung auf dem Gerät: ./test.ps1
# Ergebnisausgabe: 10
```

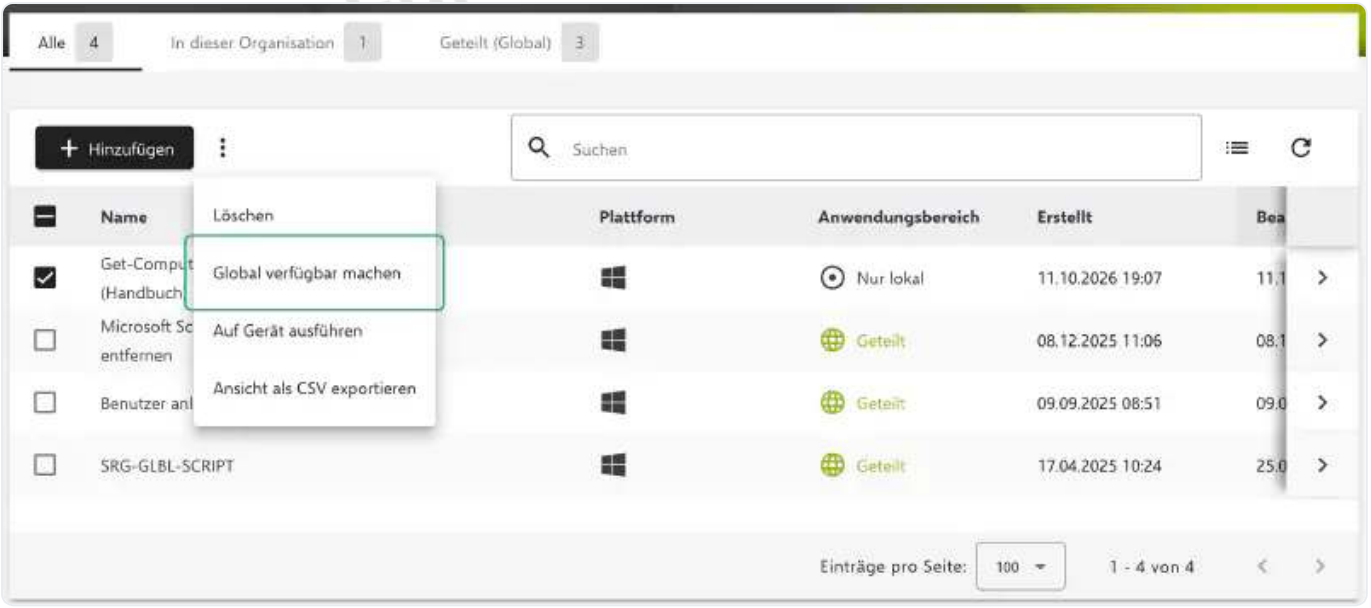
Verfügbare Platzhalter

Die verfügbaren Platzhalter können sowohl direkt im Skriptinhalt (Punkt Inhalt) als auch bei den Argumenten im Punkt Ausführung verwendet werden. Die im Formular verfügbaren Platzhalter werden unterhalb der Eingabefelder angezeigt. Beispiel für ein Argument: `$serial='${device.serialnumber}'`. Weitere Funktionen wie Teilzeichenfolgen oder Standardwerte sind im Artikel Erweiterte Platzhalter → beschrieben.

Skript global verfügbar machen

Für Version 26.4.0

Nach dem Speichern ist das Skript nur in der Global-Organisation sichtbar. Um es allen Organisationen bereitzustellen, wird das Skript unter Skripte in der Liste markiert und im Kontextmenü (Drei-Punkte-Menü der Zeile oder der Aktionsleiste) Global verfügbar machen gewählt. Der folgende Dialog listet die betroffenen Skripte auf; mit Veröffentlichen wird die Änderung übernommen. Die Funktion setzt die Berechtigung zum Bearbeiten von Skripten voraus.



Diese Aktion kann nicht rückgängig gemacht werden.

In den übrigen Organisationen erscheint das Skript anschließend schreibgeschützt im Reiter Von Global der Skriptliste. Es kann dort in einer Richtlinie mit der Windows Skript Konfiguration → oder über die Aktion PowerShell-Skript ausführen verwendet werden. Solange das Skript in einer veröffentlichten Richtlinie einer beliebigen Organisation verwendet wird, lässt es sich auch in der Global-Organisation nicht löschen.

In einer Meta-Organisation steht dieselbe Funktion als Meta-weit verfügbar machen zur Verfügung; das Skript ist dann in den Organisationen dieser Meta-Organisation sichtbar.

Für Version 26.4.0

Office Installation steckt fest

Mit der Relution Server Version 5.21 besteht die Möglichkeit Microsoft Office mit Hilfe einer Konfigurationsdatei (XML) auf verwalteten Windows-Geräten zu installieren. Mit der Version 5.22 ist eine entsprechende Konfiguration und eine Erweiterung der Aktion hinzugekommen. Die Installation ist über die Richtlinienkonfiguration Windows Office → oder über die Aktion Office 365 installieren möglich und wird auf Windows Pro, Enterprise und Education ab Version 1703 unterstützt, nicht auf Windows Home.

Diese Installation kann aus vielen verschiedenen Gründen fehlschlagen.

Grundsätzlich sollte von der Aktion Office 365 installieren kein Gebrauch gemacht werden, wenn dies bereits in der Richtlinie konfiguriert wurde. Während der Installation sollte ein Neustart vermieden werden.

Problemfälle

1. Die Aktion Richtlinie ändern steht im Status Nicht jetzt.
2. Office installiert sich nicht, obwohl in der Liste der Aktionen möglicherweise keine Fehler sichtbar sind.

In beiden Fällen lohnt es sich immer, einen Blick in den Taskmanager des Geräts zu werfen. Häufig laufen Hintergrundaktivitäten, die auf eine laufende Installation hindeuten oder die Netzwerkkarte zeigt Traffic des Downloads an.

Für Version 26.4.0

Fall 1 - Nicht jetzt

Die Aktion Richtlinie ändern für eine Richtlinie mit der Konfiguration Windows Office verbleibt im Status Nicht jetzt. Dieser Status tritt nur bei der Office-Installation über eine Richtlinie auf, wenn auf dem Gerät noch eine Installation läuft oder zuerst eine andere Office-Suite deinstalliert werden muss. Die Aktion Office 365 installieren erhält diesen Status nicht.

1. Eine Aktion Geräteinformationen aktualisieren wird an das Gerät gesendet.
2. Die Installation beinhaltet unter Umständen große Datenmengen die heruntergeladen und verarbeitet werden müssen. Dies kann je nach Anbindung und verwendeter Hardware sehr lange dauern. Hier sollte mindestens eine Stunde gewartet werden, wenn dieser Status auftritt.
3. Nach Ablauf der Stunde wird erneut eine Aktion Geräteinformationen aktualisieren an das Gerät gesendet. Liegt die Zustellung der Aktion Richtlinie ändern mindestens 60 Minuten zurück, setzt Relution die Richtlinienanwendung fort, auch wenn das Gerät noch eine laufende Installation meldet. Ohne diese Aktualisierung geschieht das erst mit der nächsten automatischen Aktualisierung der Geräteinformationen oder wenn das Gerät den Abschluss der Office-Installation meldet.
4. Wenn sich dennoch keine Änderung des Status ergibt, kann die Installation über die Aktion Office 365 installieren mit der Option Office-Installationsdaten löschen zurückgesetzt werden. Optional entfernt der Schalter Deinstallieren Sie die aktuelle Office 365 Suite zusätzlich die installierte Office-Suite. Sind auf dem Gerät keine Installationsdaten vorhanden und ist der Schalter nicht aktiviert, schlägt die Aktion fehl.
5. Nun sollte mindestens fünf Minuten gewartet werden, bevor die Installation erneut ausgeführt wird.

Fall 2 - Office installiert scheinbar ohne Grund nicht

Dieser Fall kann bei Anwendung der Richtlinienkonfiguration auftreten. Hier sollte zuerst immer die Aktion Richtlinien erneut anwenden ausgeführt und das weitere Verhalten beobachtet werden. Ist auch dadurch kein Erfolg erreicht worden, kann die möglicherweise hängende Office-Installation wie in Fall 1, Schritt 4 beschrieben zurückgesetzt werden (Aktion Office 365 installieren mit der Option Office-Installationsdaten löschen). Im Anschluss sollte nochmals Richtlinien erneut anwenden ausgeführt werden.

Meldet das Gerät bei der Installation über die Richtlinie einen Fehler, wechselt die Aktion Richtlinie ändern in den Status Fehler, und es entsteht der Compliance-Verstoß Die Windows Office-Konfiguration ist ungültig. Die Aktion Office 365 installieren meldet dagegen bereits Erfolg, sobald das Gerät den Befehl angenommen hat; ein späteres Fehlschlagen der Installation ist dort nicht sichtbar.

Für Version 26.4.0

Windows Companion

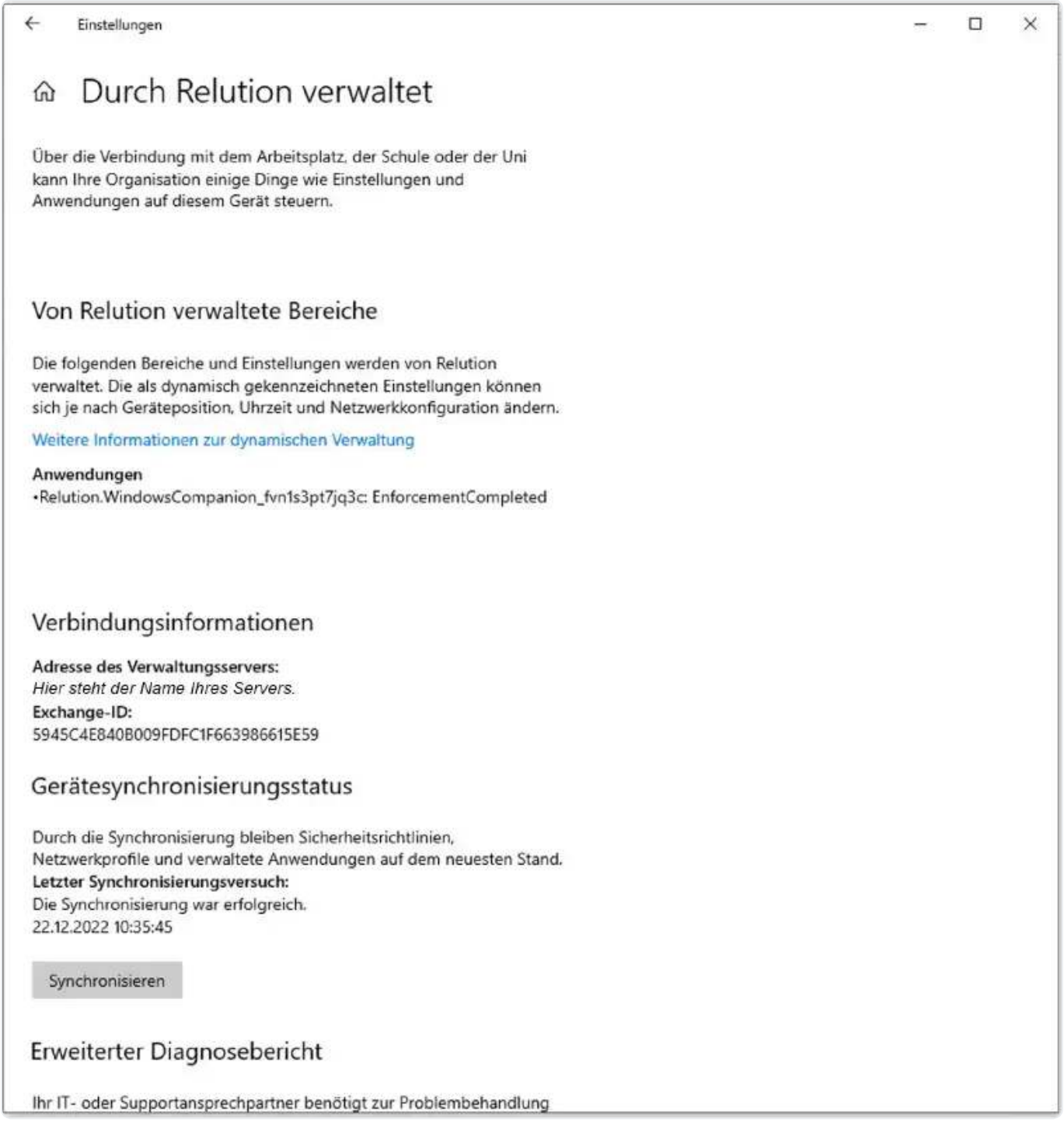
Der Relution Companion für Windows ist ein Windows Service, der auf allen von Relution verwalteten Windows-Geräten installiert wird – ausgenommen sind Geräte mit Windows Home Edition und Geräte, deren Edition nicht erkannt wird. Es handelt sich dabei um keine reguläre App, die im Windows App Store oder im Relution App Store verfügbar ist. Der Relution Companion für Windows besitzt Administrationsrechte, ist lediglich für Administratoren gedacht und wird vollständig im Hintergrund ausgeführt. Interaktionen mit Endanwendern finden nicht statt.

Installation

Mit Relution Server Version 5.15 wird der Relution Companion für Windows automatisch auf allen neu eingeschriebenen Windows-Geräten installiert, sofern es sich nicht um die Windows Home Edition handelt. Ist das Windows-Gerät bereits von Relution verwaltet, wird der Relution Companion für Windows ebenfalls automatisch nachinstalliert. Auf Windows Home stehen der Companion und damit auch PowerShell-Skripte sowie die Installation von MSI- und EXE-Paketen nicht zur Verfügung:
Einschränkungen der Windows Home Edition →

Auf dem Windows-Gerät unter Einstellungen wird die Relution-Einschreibung Mit Relution verbunden angezeigt. Im Untermenü Info ist nachfolgend erkenntlich, dass der Relution Companion für Windows erfolgreich installiert wurde.

Für Version 26.4.0



Bis sich der Companion nach der Installation erstmals beim Server meldet, wird für das Gerät der Compliance-Hinweis „Der Windows-Companion ist nicht installiert!“ angezeigt. Antwortet ein installierter Companion nicht mehr, wird daraus eine Compliance-Verletzung und der Companion wird erneut installiert. Steht auf dem Server eine neuere Companion-Version bereit, wird der Companion auf dem Gerät automatisch aktualisiert.

Wird ein Windows-Gerät nicht mehr über Relution verwaltet, wird der Relution Companion für Windows automatisch vom Gerät entfernt.

Sinn und Zweck des Relution Companion für Windows

Standardmäßig werden bei der Konfiguration von eingeschriebenen Windows-Geräten in Relution die sogenannten Configuration Service Provider (CSP) verwendet, die den Zugriff auf bestimmte Einstellungen im Windows System ermöglichen. Die Konfigurationsmöglichkeiten sind hierbei allerdings beschränkt. Mittels des Relution Companion für Windows werden Konfigurations-Optionen signifikant erweitert.

Zusätzliche Möglichkeiten

Durch den Relution Companion für Windows lassen sich über Relution-Aktionen zusätzlich einmalige, auf Windows basierte PowerShell-Skripte auf eingeschriebenen Windows-Geräten ausführen.

Ein weiterer Vorteil des Relution Companion für Windows ist die Installation und Deinstallation von klassischen Applikationen im Device-Kontext. Dadurch lassen sich `.msi`- und `.exe`-Dateien über den Relution App Store auf eingeschriebenen Windows-Geräten installieren und wieder deinstallieren.

Darüber hinaus laufen folgende Funktionen ausschließlich über den Companion: die Installation von WinGet-Apps, die regelmäßige Skriptausführung per Windows Skript Konfiguration → sowie die Aktionen Passwort zurücksetzen (Windows), Bitlocker aktivieren und Bitlocker deaktivieren. Das Verhalten des Companion selbst wird über die Richtlinie Companion konfigurieren → gesteuert.

Für Version 26.4.0

Anwenden von Powershell-Skripten auf Windows-Geräten

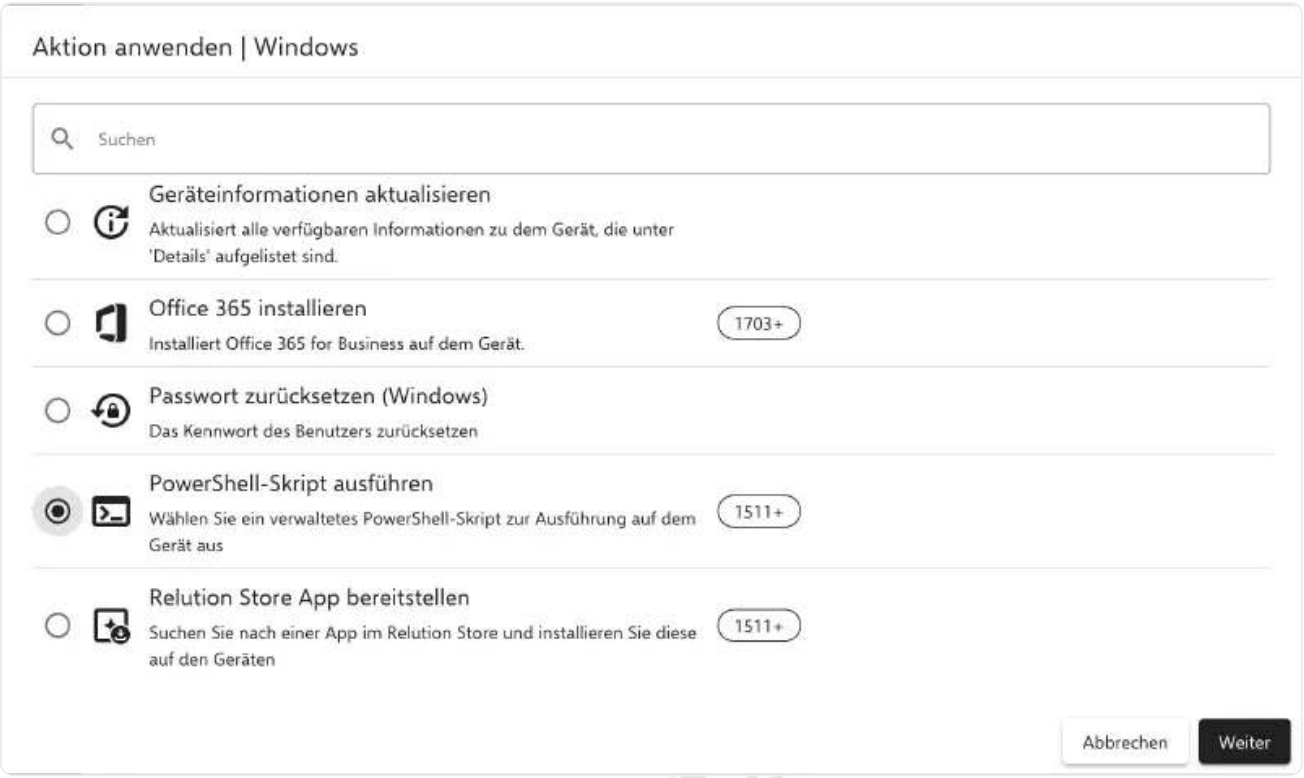
Bei PowerShell-Skripten handelt es sich um Textdateien, die mindestens einen PowerShell-Befehl enthalten, der beim Öffnen der Datei von Windows ausgeführt wird. Abläufe, sowohl auf dem Rechner als auch bei Relution, können dadurch deutlich erleichtert werden. Die Skript-Dateien werden vom Administrator selbst geschrieben und unter der Endung `.ps1` abgespeichert. Dabei lassen sich lediglich PowerShell-Skripte ausführen, die keinerlei Benutzer-Interaktion benötigen, da der Relution Companion für Windows vollständig im Hintergrund läuft. Für das Zurücksetzen vergessener Benutzerpasswörter steht inzwischen die eigene Aktion Passwort zurücksetzen (Windows) zur Verfügung.

Seit Relution 5.16 werden PowerShell-Skripte zentral in Relution verwaltet. Ein Skript wird deshalb nicht mehr in der Aktion hochgeladen, sondern vorab unter `Skripte` → `Skripte` über Hinzufügen angelegt. Dort werden auch die Standardwerte für Zeitüberschreitung (in Minuten) und Argumente hinterlegt. Für die Auswahl in der Aktion ist das Recht zum Lesen von Skripten erforderlich; ohne dieses Recht wird keine Skriptliste angezeigt.

Um ein PowerShell-Skript erfolgreich auf einem Windows-Gerät auszuführen, müssen nachfolgende Schritte durchgeführt werden:

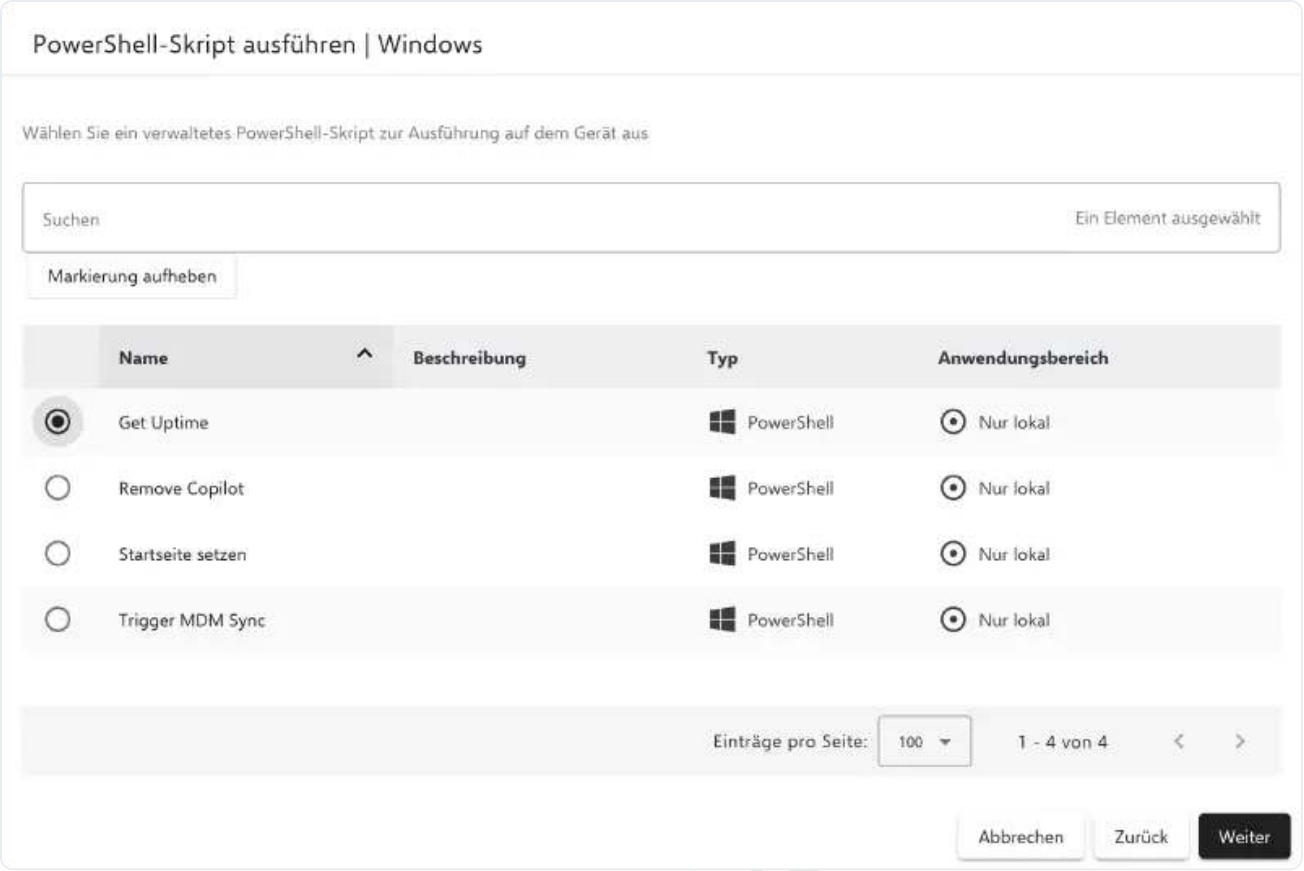
1. Im Geräte-Inventar das gewünschte Windows-Gerät aufrufen und auf der Gerätedetailseite im Tab Aktionen auf die Schaltfläche Aktion anwenden klicken.

2. Anschließend die Aktion PowerShell-Skript ausführen wählen.



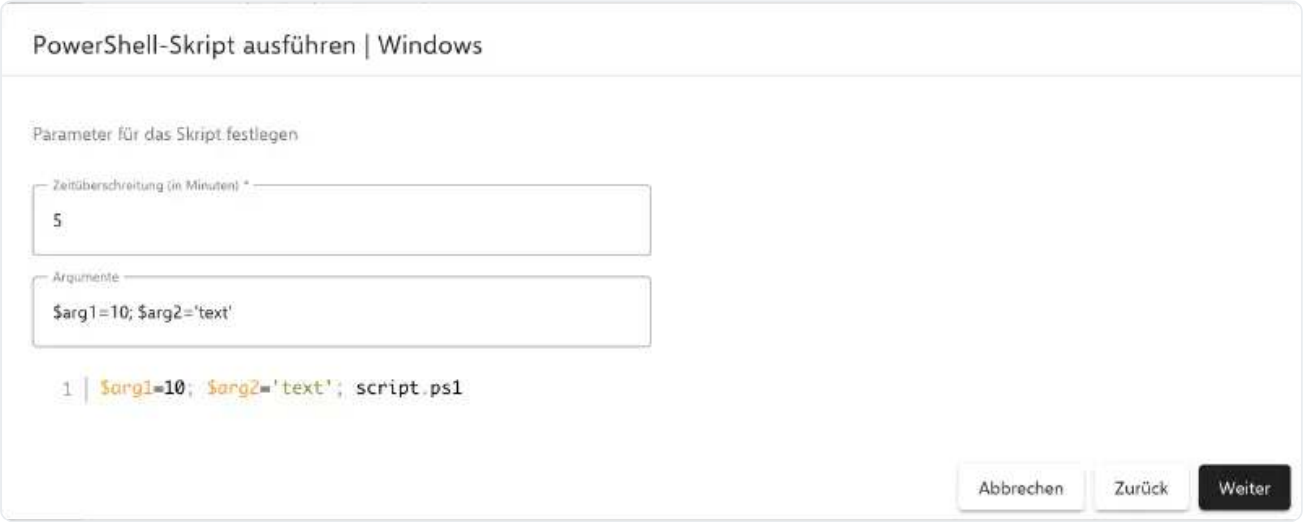
Für Version 2

3. In der Liste der verwalteten Skripte das gewünschte PowerShell-Skript auswählen.



4. Im zweiten Schritt Parameter für das Skript festlegen werden die Werte des gewählten Skripts vorbelegt und lassen sich für diese Ausführung anpassen:

   - Im Pflichtfeld Zeitüberschreitung (in Minuten) (1 bis 30) wird festgelegt, nach welcher Zeit die Skriptausführung zwangsweise abgebrochen wird.
   - Im Feld Argumente lassen sich Variablen im Format `$arg1=10; $arg2='text'` angeben (höchstens 512 Zeichen; jede Zuweisung außer der letzten endet mit einem Semikolon). Sie werden vor der Ausführung an den Anfang des Skripts eingefügt und sind im Skript über ihren Namen nutzbar, z. B. `Write-Host $arg1`.



5. Unter der Gerätedetailseite und dem Tab Aktionen wird das ausgeführte PowerShell-Skript aufgelistet.

Alternativ lässt sich ein Skript direkt unter `Skripte` → `Skripte` über Auf Gerät ausführen starten. Ausführungsstatus sowie Ergebnis- und Fehlerausgabe jeder Ausführung sind in der Historie des jeweiligen Skripts unter `Skripte` → `Skripte` einsehbar (Ergebnisausgabe anzeigen, Fehlerausgabe anzeigen).

Für Version 26.4.0

Einschränkungen der Windows Home Edition

Die Windows Home-Edition ist in Bezug auf Verwaltungsmöglichkeiten gegenüber anderen Editionen eingeschränkt. Funktionen, die nicht zur Verfügung stehen, sind in der Web-Oberfläche häufig daran erkennbar, dass diese mit Badges versehen sind, welche die unterstützten Editionen anzeigen. Hier ist die Home Edition entsprechend nicht enthalten. Nicht alle betroffenen Funktionen tragen jedoch ein solches Badge.

Geräte mit Windows Home lassen sich in der Geräteliste über die Spalte bzw. den Filter OS Edition (Wert Home) finden.

Die Einschränkungen betreffen unter anderem folgende Funktionen:

Installation von Anwendungen

Die Microsoft MDM API (CSP) zur Installation von MSIX und Microsoft Store Apps steht auf Windows Home nicht zur Verfügung. Relution kann somit keine solchen Anwendungen installieren. Als Folge davon stehen davon abhängige Richtlinien (App-Konformität) ebenfalls nicht zur Verfügung.

Diese Einschränkung betrifft auch die automatische Installation des Relution Companion für Windows. Das hat zur Folge, dass auf Windows 10/11 Home die Installation von MSI- und EXE-Paketen ebenfalls nicht zur Verfügung steht, da diese Funktion einen installierten/konfigurierten Companion voraussetzt.

Für Version 26.4.0

Somit stehen auf Windows 10/11 Home folgende Aktionen nicht zur Verfügung:

- Relution Store App bereitstellen (einschließlich der Installation von MSI-, EXE- und WinGet-Apps)
- App entfernen
- Office 365 installieren
- Office 365-Installationsdaten löschen

Des Weiteren steht folgende Richtlinie nicht zur Verfügung:

- App Konformität

Ausführen von PowerShell Skripten

Das Ausführen von PowerShell-Skripten setzt einen installierten Relution Companion für Windows voraus. Aufgrund der Einschränkung bezüglich der App Installation ist es nicht möglich, den Companion zu installieren. Daher ist es auch nicht möglich, PowerShell-Skripte über den Companion auf Geräten mit der Windows Home Edition auszuführen.

Somit steht auf Windows 10/11 Home folgende Aktion nicht zur Verfügung:

- PowerShell-Skript ausführen

Weitere Funktionen des Companion

Der Relution Companion für Windows → wird auf Windows Home grundsätzlich nicht verteilt; dasselbe gilt für Geräte, deren Edition Relution nicht erkennt (OS Edition Andere). Neben PowerShell-Skripten und der App-Installation fehlen damit auch alle übrigen Funktionen, die über den Companion laufen, z. B. die Aktionen Passwort zurücksetzen (Windows), Bitlocker aktivieren und Bitlocker deaktivieren sowie die regelmäßige Skriptausführung per Richtlinie.

Weitere Aktionen und Richtlinien

Auch folgende Aktionen werden auf Windows Home nicht unterstützt:

- Gerät neu starten
- Benutzerkonten hinzufügen

Folgende Richtlinien werden auf Windows Home nicht angewendet:

- Bitlocker
- Windows Update
- Windows Firewall
- Windows Kiosk-Modus
- Shared PC
- Windows Office
- Sicherheitsoptionen für lokales Gerät
- Globale Proxies
- BranchCache
- Hintergrundbild
- App-Kontrolle

Für Version 26.4.0

Bei den Restriktionen werden zahlreiche Einzeleinstellungen auf Windows Home ebenfalls nicht unterstützt.

Verfügbar bleiben auf Windows Home unter anderem die Aktionen Gerät auf Werkszustand zurücksetzen (ab Version 1709) und Gerät Scannen (ab Version 1809) sowie die Richtlinien VPN und Antivirus (teilweise).

Anzeige installierter Anwendungen

Die Microsoft MDM API (CSP) zum Abfragen installierter Modern Apps (Microsoft Store/MSIX) steht auf Windows 10/11 Home nicht zur Verfügung. Somit kann Relution für eingeschriebene Geräte keine installierten Apps ermitteln und dementsprechend auch nicht in den Details eines Geräts unter Installierte Apps anzeigen.

Das Ermitteln von Anwendungen, die über EXE/MSI installiert wurden, setzt einen installierten Relution Companion für Windows voraus. Aufgrund der Einschränkung bezüglich App Installation ist es nicht möglich, den Companion zu installieren. Daher ist es auch nicht möglich, über den Companion installierte Apps auf Geräten mit der Windows Home Edition zu ermitteln.

Somit steht auf Windows 10/11 Home folgende Information nicht zur Verfügung:

- Anzeige installierter Anwendungen.

Upgrade auf eine höhere Edition

Über die Richtlinie Windows Lizenzierung lässt sich ein Gerät mit Windows Home per Produktschlüssel auf eine höhere Edition aktualisieren, siehe Verfügbare Konfigurationen →. Ein so durchgeführtes Upgrade lässt sich durch Entfernen der Richtlinie nicht rückgängig machen.

Microsoft Store URLs

Verwaltete Windows-Geräte, die den Microsoft Store verwenden, um Apps zu erwerben, zu installieren oder zu aktualisieren, benötigen Zugriff auf diese Endpunkte über die TCP-Ports 80 und 443 über die eigene Firewall.

Microsoft Store-API (AppInstallManager):

- `displaycatalog.mp.microsoft.com`
- `purchase.md.mp.microsoft.com`
- `licensing.mp.microsoft.com`
- `storeedgefd.dsx.mp.microsoft.com`

Zum Zeitpunkt der Erstellung dieses Dokuments sind dies die aktuell benötigten Endpunkte. Die vollständige Dokumentation wird hier vom Hersteller aufgeführt: Dokumentation von Microsoft →

Für Version 26.4.0

WinGet-Upgrade-Workaround

Manche WinGet-Apps lassen sich mit `winget upgrade` nicht aktualisieren, obwohl im Relution-AppStore bereits eine neuere Version eingetragen ist. Ursache ist fast immer ein defektes Manifest auf WinGet-Seite — das Upgrade bricht dann mit `no applicable upgrade`, `package not found`, `no applicable installer found` oder einem verwandten Fehler ab.

Microsofts eigener Workaround ist, die App mit dem Schalter `--force` erneut zu installieren. Das folgende Skript automatisiert diese Recovery für eine einzelne WinGet-App und kann mit der Geräteaktion PowerShell-Skript ausführen auf Geräten ausgeführt werden.

> Es handelt sich um einen Workaround. Dieser sollte nur für Apps eingesetzt werden, bei denen ein reguläres Upgrade bekanntermaßen fehlschlägt. Eine erzwungene Installation überschreibt die vorhandenen Paketdateien und kann andere Installationsprobleme verdecken.

Skript

Das Skript wird unter `Skripte` → `Skripte` über Hinzufügen als PowerShell-Skript angelegt und anschließend mit der Geräteaktion PowerShell-Skript ausführen oder in der Skriptliste über Auf Gerät ausführen auf Geräten ausgeführt. Die Ausführung erfolgt über den Windows Companion im Gerätekontext (SYSTEM). Im Skript muss am Anfang die Variable `$AppIdentifier` auf den exakten WinGet-Bezeichner der zu reparierenden App gesetzt werden (z. B. `Nextcloud.NextcloudDesktop`).

Für Version 26.4.0

Alternativ lässt sich der Bezeichner im Feld Argumente übergeben (z. B. `$AppIdentifier='Nextcloud.NextcloudDesktop'`), sodass ein Skript für mehrere Apps genutzt werden kann. In diesem Fall muss die erste Zeile des Skripts entfernt werden, da sie den übergebenen Wert sonst überschreibt.

Für Skripte ist standardmäßig eine Zeitüberschreitung (in Minuten) von 5 Minuten hinterlegt. Da Upgrade und erzwungene Installation großer Apps länger dauern können, sollte der Wert beim Anlegen des Skripts oder in der Aktion entsprechend erhöht werden (höchstens 30 Minuten).

> Vollständiges Skript anzeigen

Funktionsweise

1. Das Skript sucht `winget.exe` unterhalb von `C:\Program Files\WindowsApps\Microsoft.DesktopAppInstaller_*` — das ist die Installation, die der Windows Companion im System-Kontext verwendet.
2. Mit `winget list --id <AppIdentifier> --exact` wird geprüft, ob die App auf dem Gerät installiert ist. Wenn nicht, wird das Skript ohne weitere Aktion beendet.
3. Es wird `winget upgrade --id <AppIdentifier> --exact` mit den von Relution vorgeschriebenen Silent-Parametern → aufgerufen. Die Parameter werden mit `@SilentFlags` gesplattet, damit PowerShell jedes Element als eigenes Argument übergibt — sonst werden sie von WinGet nicht korrekt geparst. Ist das Upgrade erfolgreich, endet das Skript.
4. Wenn das Upgrade mit einem der erkannten Fehlercodes endet, wiederholt das Skript den Aufruf als `winget install --id <AppIdentifier> --exact --force` mit den gleichen Silent-Parametern. Die erkannten Codes sind:
   - `-1978335189` — `no applicable upgrade`
   - `-1978335215` — `package not found`
   - `-1978335192` — `no applicable installer found`
   - `-1978335216` — in der Praxis beobachteter Manifest-/Installer-Fehler
5. Alle übrigen WinGet-Exit-Codes werden unverändert durchgereicht.

Die Erkennung erfolgt ausschließlich über die Exit-Codes von WinGet. Die Textausgabe wäre abhängig von der Sprache des Geräts und würde auf englischen und deutschen Windows-Installationen unterschiedlich ausfallen.

Ausführungsstatus sowie Ergebnis- und Fehlerausgabe des Skripts (z. B. die Meldungen von `Write-Host`) sind in der Historie des Skripts unter `Skripte` → `Skripte` einsehbar (Ergebnisausgabe anzeigen, Fehlerausgabe anzeigen).

Soll die Reparatur regelmäßig laufen, lässt sich das Skript auch über die Richtlinienkonfiguration Windows Skript Konfiguration → zeit- oder ereignisgesteuert ausführen.

Für Version 26.4.0

WinGet Fehlercode

WinGet Fehler -1073741515

Die Installation von WinGet-Apps über Relution schlägt mit dem folgenden Fehlercode fehl: `-1073741515` (`0xC0000135`)

Ursache

Während der Installation von Apps über WinGet kann ein Fehler auftreten, wenn die Microsoft Visual C++ Redistributable auf dem Zielrechner nicht installiert ist.

Lösung

Der Windows Companion installiert eine fehlende Microsoft Visual C++ Redistributable selbst, auch wenn die Option WinGet und seine Abhängigkeiten verwalten in der Richtlinie Companion konfigurieren → deaktiviert ist. Tritt der Fehler dennoch auf, hilft eine manuelle Installation.

Die ausführliche Beschreibung der Ursache sowie die Lösung mittels manueller Installation als native App mit Erkennungsregel, den benötigten Registry-Pfaden und der Ermittlung des Uninstaller-Pfads sind im Artikel WinGet → im Abschnitt Bekannte Probleme beschrieben.

Für Version 26.4.0

WinGet Fehler -1978335230

Die Installation von WinGet-Apps über Relution schlägt mit dem folgenden Fehlercode fehl: `-1978335230` (`0x8A150002`)

Eine der folgenden Fehlermeldungen wird ausgegeben:

```
Argumentname wurde für den aktuellen Befehl nicht erkannt: --disable-interactivity
```

```
Argument name was not recognized for the current command : --disable-interactivity
```

Ursache

Die installierte WinGet Version ist zu alt und unterstützt das erforderliche Argument `--disable-interactivity` noch nicht.

Lösung

WinGet muss mindestens in Version 1.6 installiert sein.

Ist in der Richtlinie Companion konfigurieren → die Option WinGet und seine Abhängigkeiten verwalten aktiviert (Standardwert), aktualisiert der Windows Companion WinGet und seine Abhängigkeiten bei seinem Start.

Ist die Option deaktiviert oder steht sie nicht zur Verfügung, muss WinGet manuell aktualisiert werden. Ein Update ist im Microsoft Store verfügbar (Paket App Installer).

WinGet-Versionen älter als 1.6 können sich noch nicht selbst aktualisieren.

Auf Anfrage

Bei Interesse an der Verwaltung von Linux Endgeräten gerne eine Nachricht an sales@relution.io → schreiben.

Für Version 26.4.0

Built-In CA

Relution unterstützt die Nutzung integrierter Zertifikate. Diese Zertifikate werden in vielen Bereichen genutzt, zum Beispiel bei SSL/TLS-Verschlüsselung, E-Mail-Sicherheit, VPN- und WLAN-Verbindungen und Signierungen.

Die folgende Anleitung beschreibt das Anlegen einer integrierten Zertifizierungsstelle (CA) und einer Zertifikatsvorlage mit Variablen zur Zuweisung. Anschließend wird eine Richtlinie mit der Zertifikat-Konfiguration erstellt und den entsprechenden Geräten zugewiesen. Dadurch wird die Generierung des Zertifikats für die Endgeräte ermöglicht.

Built-In CA anlegen

In Relution wird hierfür unter `Einstellungen` → `Zertifizierungsstellen` → `Hinzufügen` eine Built-In CA erstellt. Im Bereich Allgemein wird ein Name vergeben (optional eine Beschreibung) und im Feld Art der Zertifizierungsstelle die Option Built In ausgewählt. Die Art der Zertifizierungsstelle lässt sich nach dem Speichern nicht mehr ändern.

Im Bereich Zertifikatseinstellungen wird über Generieren am Feld Zertifikat ein neues Root-Zertifikat erstellt. Alternativ lässt sich über Auswählen ein vorhandenes PKCS#12-Zertifikat verwenden, das zuvor unter `Einstellungen` → `Zertifikate` hochgeladen wurde (siehe Zertifikatsverwaltung →). Die Zertifizierungsstelle wird anschließend mit Speichern angelegt.

Die Option Built In steht nur mit der Berechtigung zum Lesen von Zertifikaten zur Verfügung, die Schaltfläche Generieren nur mit der Berechtigung zum Erstellen von Zertifikaten.

Für Version 26.4.0

Built-in Root Zertifikat generieren

Generieren öffnet den Dialog Built-in Root Zertifikat generieren. Mit Bestätigen wird das Root-Zertifikat erstellt und in das Feld Zertifikat übernommen.

Pflichtfelder

- Name: Name des Zertifikats.
- Passwort: Passwort für das Root-Zertifikat.
- Common name: Üblicherweise der Domainname.
- Läuft ab am: Vorbelegt ist eine Laufzeit von 10 Jahren. Das früheste wählbare Datum ist der folgende Tag.

Optionale Felder

- Organisation, Organisationseinheit, Bundesland, Lokalität: Weitere Angaben zum Inhaber, die in den Distinguished Name des Root-Zertifikats übernommen werden.
- Land: Vorbelegt ist Deutschland.

Zertifikatsvorlage

Über die Zertifikatsvorlage `Einstellungen` → `Zertifikatsvorlagen` → `Hinzufügen` werden Parameter für das Zertifikat definiert.

Pflichtfelder

- Name: Name der Vorlage.
- Zertifizierungsstelle: Über Auswählen wird die zuvor erstellte Built-In CA gewählt.
- Name des Inhabers: als Beispiel `CN=MeinAnwendungsfall-${user.email}`. Hier können Variablen wie z. B. `${user.name}`, `${device.serialnumber}` oder `${user.email}` verwendet werden, siehe Erweiterte Platzhalter →. Sonderzeichen werden durch einen vorangestellten Backslash maskiert (z. B. `CN=John\, Doe`).

Der Freitext in `CN=MeinAnwendungsfall` sollte passend zur Verwendung gewählt sein, z. B. VPN oder WLAN.

Weitere Optionen

- Vorlagentyp des Zertifikats: Lässt sich nach dem Speichern nicht mehr ändern.
  - Zertifikat (Standard): Relution erzeugt Schlüssel und Zertifikat und stellt beides über die Richtlinie bereit.
  - SCEP auf dem Gerät: Für iOS, macOS und tvOS wird aus der Vorlage eine SCEP-Konfiguration erzeugt. Das Gerät erzeugt den Schlüssel selbst und fordert das Zertifikat per SCEP bei Relution an. Die zugehörigen Einstellungen (z. B. Wiederholungen, Wiederholungsverzögerung, Zugriff auf den privaten Schlüssel) stehen im Bereich SCEP-Konfiguration.
- Subject Alternative Name: Zusätzliche Namen im Zertifikat, jeweils mit einem der folgenden Typen (bei SCEP auf dem Gerät nur E-Mail, DNS, Benutzerprinzipalname und URI):
  - Verzeichnis-Name
  - DNS
  - E-Mail
  - IP-Adresse
  - Benutzerprinzipalname (UPN)
  - URI
- Schlüsselalgorithmus: RSA (Standard) oder EC. EC steht nur bei einer Built-In CA mit dem Vorlagentyp Zertifikat zur Wahl.
- Länge des Schlüssels: Vorbelegt sind 4096 Bit. Für den Vorlagentyp Zertifikat stehen bei RSA 3072 und 4096 Bit, bei EC 256, 384 und 521 Bit zur Wahl; für SCEP auf dem Gerät 2048 und 4096 Bit. Bereits gespeicherte Vorlagen behalten eine früher gewählte Schlüssellänge, bis sie geändert wird.
- Verwendung von Zertifikatsschlüsseln: Mehrfachauswahl, z. B. Signatur, Schlüsselverschlüsselung, Datenverschlüsselung oder Nichtabstreitbarkeit.
- Erweiterte Schlüsselverwendungen von Zertifikaten: Mehrfachauswahl, z. B. Client-Authentifizierung oder Server-Authentifizierung.
- Automatische Verlängerung aktivieren: Ausgestellte Zertifikate werden automatisch verlängert. Der Schalter ist standardmäßig deaktiviert. Erst wenn er aktiv ist, lassen sich die beiden folgenden Felder bearbeiten:
  - Automatische Verlängerung (In Tagen): Ein Zertifikat wird automatisch verlängert, wenn sein Ablaufdatum in diesem Zeitraum liegt. Vorausgewählt ist 1 Tag. Der Wert muss kleiner sein als der Zeitraum, nach dem das Zertifikat abläuft (in Tagen).
  - Verhalten bei der Zertifikatserneuerung: Alte Zertifikate behalten ihre Gültigkeit (Standard) oder Alte Zertifikate direkt ungültig machen.
- Zeitraum, nach dem das Zertifikat abläuft (in Tagen): Ein Zertifikat ist nach diesem Zeitraum nicht mehr gültig. Vorausgewählt sind 365 Tage.

Für Version 26.4.0

Richtlinie mit Zertifikat-Konfiguration

Damit die Schritte greifen und ein Zertifikat erstellt wird, muss in Relution eine Richtlinie mit einer Zertifikat-Konfiguration erstellt werden. Hier ein Beispiel für iOS:

Unter `Geräte` → `Richtlinien` → `Hinzufügen` wird im Bereich Allgemein die Plattform (hier iOS) gewählt, ein Name für die Richtlinie vergeben und gespeichert.

In der erstellten Richtlinie wird die Konfiguration Zertifikat hinzugefügt. Nach Vergabe eines Namens wird im Feld Zertifikat über Auswählen der Dialog Zertifikat oder Zertifikatsvorlage auswählen geöffnet, im Reiter Zertifikatsvorlagen die zuvor erstellte Zertifikatsvorlage gewählt und mit Bestätigen übernommen.

Ebenso kann die Zertifikatsvorlage für VPN- und WLAN-Konfigurationen verwendet werden.

Validierung

In der Relution Gerätehistorie sollte nach dem Verteilen folgender Eintrag erstellt werden:

`Ein Zertifikat für die Zertifikatsvorlage $Template wurde durch $Benutzer ausgestellt.`

Zusätzlich ist das neue Zertifikat in den Geräteinformationen von Apple- und Linux-Geräten auf der Karte Installierte Zertifikate zu finden (sofern die Geräteinformationen aktuell sind).

Eine Übersicht aller über Zertifikatsvorlagen ausgestellten Zertifikate, einschließlich der Möglichkeit zum Widerruf, bietet `Einstellungen` → `Ausgestellte Zertifikate` (siehe Zertifikatsverwaltung →).

Für Version 26.4.0

Zertifikatsverwaltung

Neben der Built-In CA → für automatisch ausgestellte Zertifikate bietet Relution zwei weitere Ansichten zur Zertifikatsverwaltung: Zertifikate für hochgeladene und von Relution hinterlegte Zertifikate und Ausgestellte Zertifikate für eine Übersicht der Zertifikate, die Geräten über eine Zertifikat-Richtlinie ausgestellt oder zugewiesen wurden.

Zertifikate

Unter `Einstellungen` → `Zertifikate` lassen sich vorhandene Zertifikatsdateien (z. B. `crt`, `cer`, `der`, `pem`, `p12` / `pfx`) hochladen und verwalten.

Pflichtfelder beim Hochladen

- Name: Name des Zertifikats.
- Zertifikats-Datei: Die hochzuladende Zertifikatsdatei.

Optional

- Passwort: Passwort der Zertifikatsdatei, falls diese verschlüsselt ist.

Ein hochgeladenes Zertifikat lässt sich anschließend in vielen Richtlinien-Konfigurationen als generisches Zertifikat auswählen — analog zur Zertifikatsvorlage der Built-In CA, jedoch ohne automatische Ausstellung pro Gerät. Typische Einsatzorte sind z. B. VPN-, WLAN (EAP-TLS)- und Exchange/E-Mail-Konfigurationen sowie die Windows- und Android-Enterprise-Zertifikat-Konfiguration.

Für Version 26.4.0

Neben hochgeladenen Zertifikaten (Verwendungszweck Generisch) zeigt die Liste standardmäßig auch von Relution hinterlegte Zertifikate an, etwa das Built-in PKI-Root-Zertifikat, Built-in Pool-Zertifikate aus einem Zertifikatspool → sowie Push- und Signing-Zertifikate. Über die Filter Verwendungszweck, Typ (`PKCS1` / `PKCS12`) und Status lässt sich die Ansicht eingrenzen. Die Zertifikatsdatei eines Eintrags kann über die Download-Schaltfläche in der Liste heruntergeladen werden.

Ein gelöschtes Zertifikat wird nicht endgültig entfernt, sondern erhält den Status Gelöscht. Da der Filter Status standardmäßig nur Erstellt anzeigt, werden gelöschte Zertifikate erst nach Anpassen des Filters sichtbar; über Zertifikat wiederherstellen lassen sie sich zurückholen.

Ausgestellte Zertifikate (Device Certificates)

Unter `Einstellungen` → `Ausgestellte Zertifikate` findet sich eine Übersicht aller Zertifikate, die automatisch durch eine Zertifikat-Richtlinie für ein Gerät ausgestellt oder zugewiesen wurden (Built-In CA, SCEP/Microsoft ADCS oder Zertifikatspool →) — inklusive Zertifikat, Gerät, verwendeter Zertifikatsvorlage, Zertifizierungsstelle sowie Ausstellungs-, Ablauf- und ggf. Widerrufsdatum. Widerrufene Zertifikate sind standardmäßig ausgeblendet und werden über den Filter Widerrufene Zertifikate eingeblendet; zusätzlich lässt sich die Liste nach Zertifikatsvorlage filtern. Für widerrufene Zertifikate zeigen die Spalten Widerrufen von und Grund des Widerrufs, wer das Zertifikat aus welchem Grund widerrufen hat.

Ein manuelles Ausstellen ist über diese Ansicht nicht möglich — Zertifikate entstehen ausschließlich als Ergebnis eines Enrollment- oder Richtlinien-Vorgangs. Zwei Aktionen stehen zur Verfügung:

- Löschen: Entfernt den Eintrag aus Relution. Fragt ein Gerät das Zertifikat erneut an, wird ein neues Zertifikat ausgestellt. Noch nicht abgelaufene Zertifikate, die einer von Relution verwalteten Sperrliste (CRL) zugeordnet sind, lassen sich nicht löschen, sondern nur widerrufen. Das gilt auch nach einem Widerruf, bis das Zertifikat abgelaufen ist.
- Widerrufen: Widerruft das Zertifikat über die Zertifikat-Sperrliste (CRL) der zugehörigen Zertifizierungsstelle. Dabei muss im Pflichtfeld Grund des Widerrufs ein Grund ausgewählt werden: Nicht spezifiziert, Schlüsselverlust, CA Kompromiss, Zugehörigkeit geändert, ersetzt, Einstellung des Betriebs, Privileg zurückgezogen oder AA-Kompromiss.

Ein Widerruf ist nur für Zertifikate möglich, die über eine Built-In CA ausgestellt wurden, da Relution nur für diese eine Sperrliste führt. Zertifikate einer SCEP- oder Microsoft-ADCS-Zertifizierungsstelle sowie Zertifikate aus einem Zertifikatspool lassen sich in Relution nicht widerrufen, sondern nur löschen; ihr Widerruf erfolgt bei der ausstellenden Zertifizierungsstelle. Bereits widerrufene und abgelaufene Zertifikate lassen sich ebenfalls nicht widerrufen.

Wichtig: Ein Widerruf ist eine echte PKI-Operation: Relution erzeugt daraufhin eine aktualisierte, signierte Sperrliste (CRL). Systeme, die das Zertifikat prüfen (z. B. RADIUS-Server oder VPN-Gateway), rufen sie über den im Zertifikat hinterlegten CRL-Distribution-Point ab oder fragen den Status per OCSP ab. Der Vorgang lässt sich nicht rückgängig machen.

Für Version 26.4.0

Zertifikatspool

Neben der Built-In CA →, die Zertifikate selbst ausstellt, unterstützt Relution Zertifizierungsstellen vom Typ Zertifikatspool. Dabei dient eine bereits vorhandene, externe PKI als Quelle: Die dort ausgestellten Zertifikate werden gesammelt als Archiv nach Relution importiert und als Pool vorgehalten. Wird ein Zertifikat für eine Konfiguration benötigt, erfolgt die Zuweisung aus diesem Pool, anstatt ein neues Zertifikat zu generieren.

Zertifizierungsstelle vom Typ Zertifikatspool anlegen

Die Anlage erfolgt unter `Einstellungen` → `Zertifizierungsstellen` → `Hinzufügen`. Im Drop-down-Menü Art der Zertifizierungsstelle wird der Eintrag Zertifikatspool ausgewählt. Der Typ steht nur in regulären Organisationen zur Verfügung, nicht in der Global-Organisation oder einer Meta-Organisation.

Pflichtfelder

- Name: Bezeichnung der Zertifizierungsstelle in Relution.

Angaben zur Zertifikatsausstellung — etwa ein Passwort für das Root-Zertifikat, ein Common Name oder ein Ablaufdatum — sind nicht erforderlich, da ein Zertifikatspool selbst keine Zertifikate signiert.

Für Version 26.4.0

Zertifikate in den Pool importieren

Der Import erfolgt über die Bearbeitung der zuvor gespeicherten Zertifizierungsstelle; das Feld Zertifikatspool importieren erscheint erst nach dem ersten Speichern. Dort wird ein ZIP-Archiv mit den extern ausgestellten Zertifikatsdateien hochgeladen. Darunter listet Relution die bereits im Pool enthaltenen Zertifikate auf.

Optional lässt sich im Feld Standard-Zertifikatssubtyp ein Subtyp festlegen. Er bestimmt, für welche Funktion die Zertifikate später zur Verfügung stehen. Zur Auswahl stehen dieselben Funktionen wie bei Benutzerzertifikaten: Allgemeines Zertifikat, WLAN, Exchange, VPN und Apps, S/MIME-Verschlüsselung und S/MIME Signierung (siehe Benutzerzertifikate →). Ist ein Subtyp gewählt, gilt er für alle Zertifikate des Archivs; die Spalte `#Zertifikatstyp` der CSV-Datei wird dann ignoriert und darf fehlen. Bei der Voreinstellung Keine gilt der Subtyp aus der Spalte `#Zertifikatstyp`, Zeile für Zeile; Zeilen ohne gültigen Subtyp werden als Fehler gemeldet.

Aufbau des Archivs

Das ZIP-Archiv enthält die extern ausgestellten Zertifikatsdateien sowie genau eine CSV-Datei (UTF-8), die für jedes Zertifikat einen Bezeichner und das Importpasswort angibt. Als Zertifikatsdateien werden PKCS#12-Container (`.p12` oder `.pfx`) sowie PEM-Dateien (`.pem` mit privatem Schlüssel, Zertifikat und Zertifikatskette) akzeptiert. Als Trennzeichen dient das Semikolon, die Kopfzeile lautet:

```
#E-Mail-Adresse;#P12-Passwort;#Zertifikatstyp
```

Spalte	Inhalt
`#E-Mail-Adresse`	Bezeichner des Zertifikats, wird als Zertifikatsname übernommen — muss dem Dateinamen der zugehörigen Zertifikatsdatei im Archiv entsprechen
`#P12-Passwort`	Importpasswort der zugehörigen Zertifikatsdatei
`#Zertifikatstyp`	Funktion des Zertifikats: `GENERAL_CERTIFICATE`, `WIFI`, `EXCHANGE`, `VPN`, `SMIME_ENCRYPTION` oder `SMIME_SIGNING`; wird nur ausgewertet, wenn beim Import kein Standard-Zertifikatssubtyp gewählt ist

Die Spalten werden über die Kopfzeile zugeordnet, ihre Reihenfolge ist daher beliebig. Eine Zeile pro Zertifikat, beispielhaft:

```
#E-Mail-Adresse;#P12-Passwort;#Zertifikatstyp
max.mustermann@example.com;geheimesPasswort;WIFI
```

Für Version 26.4.0

Die Zuordnung zwischen CSV-Zeile und Zertifikatsdatei erfolgt über den Dateinamen: Die Zertifikatsdatei im Archiv trägt den Bezeichner aus der Spalte `#E-Mail-Adresse` als Namen, im Beispiel also `max.mustermann@example.com.p12`. Weicht der Dateiname vom Bezeichner ab, lässt sich das Zertifikat nicht zuordnen. Zertifikatsdateien ohne zugehörige CSV-Zeile werden ignoriert.

> Keine Zuordnung zu Benutzerkonten
>
> Die Spalte `#E-Mail-Adresse` dient nur als Bezeichner; eine Zuordnung zu Benutzerkonten erfolgt nicht. Bei der Verteilung erhält jedes Gerät ein noch nicht vergebenes, gültiges Zertifikat des benötigten Subtyps aus dem Pool, bevorzugt das mit dem frühesten Ablaufdatum. Für Szenarien, in denen das Zertifikat eine bestimmte Benutzeridentität enthalten muss, ist ein Zertifikatspool daher nicht geeignet.

Nach dem Upload zeigt das Formular das Ergebnis an: Anzahl der importierten Zertifikate, der übersprungenen Duplikate und der Fehler. Unter Fehlgeschlagene Importe werden die betroffenen Bezeichner aufgeführt. Fehlerhafte Zeilen brechen den Import nicht ab; die übrigen Zertifikate werden trotzdem importiert. Als Duplikat gilt ein Zertifikat, dessen Seriennummer in der Organisation bereits im Pool vorhanden ist.

Importierte Zertifikate in der Zertifikatsverwaltung

Die importierten Zertifikate erscheinen anschließend unter `Einstellungen` → `Zertifikate` mit dem Verwendungszweck Built-in Pool-Zertifikat, jeweils mit dem beim Import gewählten oder in der CSV-Datei angegebenen Subtyp — im beschriebenen Fall WLAN. Über diese Ansicht lassen sich die Zertifikate wie alle übrigen hinterlegten Zertifikate einsehen und verwalten, siehe Zertifikatsverwaltung →.

Zertifikatsvorlage für einen Zertifikatspool

Damit die Zertifikate aus dem Pool in Richtlinien-Konfigurationen verwendet werden können, wird unter `Einstellungen` → `Zertifikatsvorlagen` → `Hinzufügen` eine Vorlage erstellt.

Ist als Zertifizierungsstelle ein Zertifikatspool ausgewählt, entfallen die Felder zur Zertifikatserzeugung (Name des Inhabers, Subject Alternative Name, Schlüsselalgorithmus, Länge des Schlüssels, Verwendung von Zertifikatsschlüsseln, Erweiterte Schlüsselverwendungen von Zertifikaten). Angezeigt werden:

- Name: Name der Vorlage.
- Vorlagentyp des Zertifikats und Beschreibung (optional).
- Zertifizierungsstelle: Die zuvor angelegte Zertifizierungsstelle vom Typ Zertifikatspool.
- Automatische Verlängerung aktivieren mit Automatische Verlängerung (In Tagen): Liegt das Ablaufdatum eines zugewiesenen Zertifikats in diesem Zeitraum, wird es durch ein freies Zertifikat desselben Subtyps aus dem Pool ersetzt. Das bisherige Zertifikat wird als gelöscht markiert und nicht erneut vergeben.
- Verhalten bei der Zertifikatserneuerung und Zeitraum, nach dem das Zertifikat abläuft (in Tagen) (Pflichtfeld, Standardwert 365).

Welcher Subtyp benötigt wird, ergibt sich aus der Konfiguration, in der die Vorlage verwendet wird, z. B. WLAN bei einer WLAN-Konfiguration. Enthält der Pool kein freies Zertifikat dieses Subtyps mehr, kann kein Zertifikat zugewiesen werden, und Relution meldet einen Compliance-Verstoß; der Pool muss dann um weitere Zertifikate ergänzt werden. Steht lediglich eine fällige Verlängerung an, bleibt das bisherige Zertifikat bis zu seinem Ablauf zugewiesen, und Relution erzeugt einen Compliance-Hinweis.

Validierung

Für Version 26.4.0

Die Einrichtung ist vollständig, wenn

- die Zertifizierungsstelle vom Typ Zertifikatspool angelegt ist,
- der Import des ZIP-Archivs (im Beispiel mit dem Subtyp WLAN) ohne Duplikate und ohne Fehler abgeschlossen wurde,
- die importierten Zertifikate unter `Einstellungen` → `Zertifikate` mit dem Subtyp WLAN aufgeführt sind und
- die Zertifikatsvorlage für die Zertifizierungsstelle vom Typ Zertifikatspool ohne Felder zur Zertifikatserzeugung, aber mit den Optionen zu Verlängerung und Ablauf angezeigt wird.

Die weitere Verwendung der Vorlage in einer Richtlinie entspricht dem Vorgehen bei der Built-In CA, siehe Built-In CA →.

Fail2Ban – IP-Sperre

Ab Relution Version 5.19 lässt sich als globale Servereinstellung festlegen, ob eine IP-Adresse bei fehlerhaften Anmeldeversuchen gesperrt wird. Die Einstellungen befinden sich in der Global-Organisation unter `Einstellungen` → `System-Sicherheit`. In der Konfiguration lässt sich definieren, nach wie vielen fehlerhaften Anmeldeversuchen eine IP-Adresse blockiert wird und ob die Sperre nach einer festgelegten Zeit automatisch aufgehoben wird. Zusätzlich hat der Systemadministrator die Möglichkeit, Anmeldungen von einer IP-Adresse oder einem ganzen IP-Bereich dauerhaft zu erlauben oder zu sperren (IP-Zugriffsregeln).

IP-Sperre konfigurieren

Im Abschnitt Allgemein stehen folgende Optionen zur Verfügung:

- Aktiviert: Schaltet die IP-Sperre ein (Standard: aus).
- Maximale Anzahl fehlgeschlagener Anmeldungen (Standard 10): Überschreiten die fehlgeschlagenen Anmeldungen einer IP-Adresse diesen Wert, wird die IP-Adresse blockiert. Eine erfolgreiche Anmeldung von dieser IP-Adresse setzt den Zähler zurück.
- Gesperrte IP-Adressen nach einer bestimmten Zeit löschen mit Freigeben der Blockierung nach (in Minuten) (Standard 60): Hebt die Sperre nach der festgelegten Zeit automatisch auf. Ist diese Option nicht aktiviert (Standard), bleibt die IP-Adresse gesperrt, bis der Eintrag in den IP-Zugriffsregeln manuell entfernt oder die IP-Adresse dort erlaubt wird.

Für Version 26.4.0

IP-Zugriffsregeln

In der Tabelle IP-Zugriffsregeln erscheinen die automatisch erfassten und blockierten IP-Adressen (mit Gesperrt seit). Über IP-Adresse hinzufügen lassen sich zusätzlich einzelne IPv4-Adressen oder ganze Bereiche (IP-Adresse oder CIDR) mit einem Status anlegen: Erlaubt, Blockiert, Dauerhaft erlaubt oder Dauerhaft blockiert. Markierte Einträge lassen sich gesammelt über Auswahl blockieren, Auswahl dauerhaft zulassen oder Auswahl dauerhaft blockieren ändern.

> Die IP-Zugriffsregeln, auch Einträge mit dem Status Dauerhaft blockiert oder Dauerhaft erlaubt, greifen nur, wenn im Abschnitt Allgemein der Schalter Aktiviert eingeschaltet ist.

Die Bedeutung der Statuswerte, CIDR-Beispiele und Empfehlungen gegen ein versehentliches Aussperren sind unter Sicherheitsoptimierungen → beschrieben.

Benutzersperre nach fehlgeschlagenen Anmeldungen

Unabhängig von der IP-Sperre lässt sich je Organisation unter `Einstellungen` → `Verwaltung der Anmeldedaten` im Abschnitt Fehlgeschlagene Anmeldeversuche mit Deaktivierung des Benutzers bei aufeinanderfolgenden fehlgeschlagenen Anmeldeversuchen und Maximale Anzahl fehlgeschlagener Anmeldeversuche (Standard 10) festlegen, ob und nach wie vielen fehlerhaften Anmeldeversuchen ein Benutzer blockiert wird.

Der Benutzer wird deaktiviert, sobald die maximale Anzahl an fehlgeschlagenen Versuchen erreicht wurde. Er kann vom Administrator wieder aktiviert werden. Gezählt werden nur Anmeldeversuche von Benutzern, die sich mit einem in Relution gespeicherten Passwort anmelden; Benutzer, die sich ausschließlich extern authentifizieren (z. B. über LDAP), werden nicht gesperrt. Eine erfolgreiche Anmeldung setzt den Zähler der fehlgeschlagenen Versuche zurück.

Details: Verwaltung der Anmeldedaten →

Für Version 26.4.0

Global-Organisation

Mit der Version `5.23` ist in Relution die Global-Organisation eingeführt worden. Diese fasst die Store-Organisation und die System-Organisation zusammen. Die Store-Organisation musste bis Version 5.22 manuell aktiviert werden. Mit der Version 5.23 geschieht diese Aktivierung automatisch.

Identifizierung der Global-Organisation

Die neue Organisation trägt den Namen Global. Auf sie haben Accounts mit der Berechtigung der System-Administratoren und Accounts mit der Berechtigung der früheren Store-Organisation Zugriff.

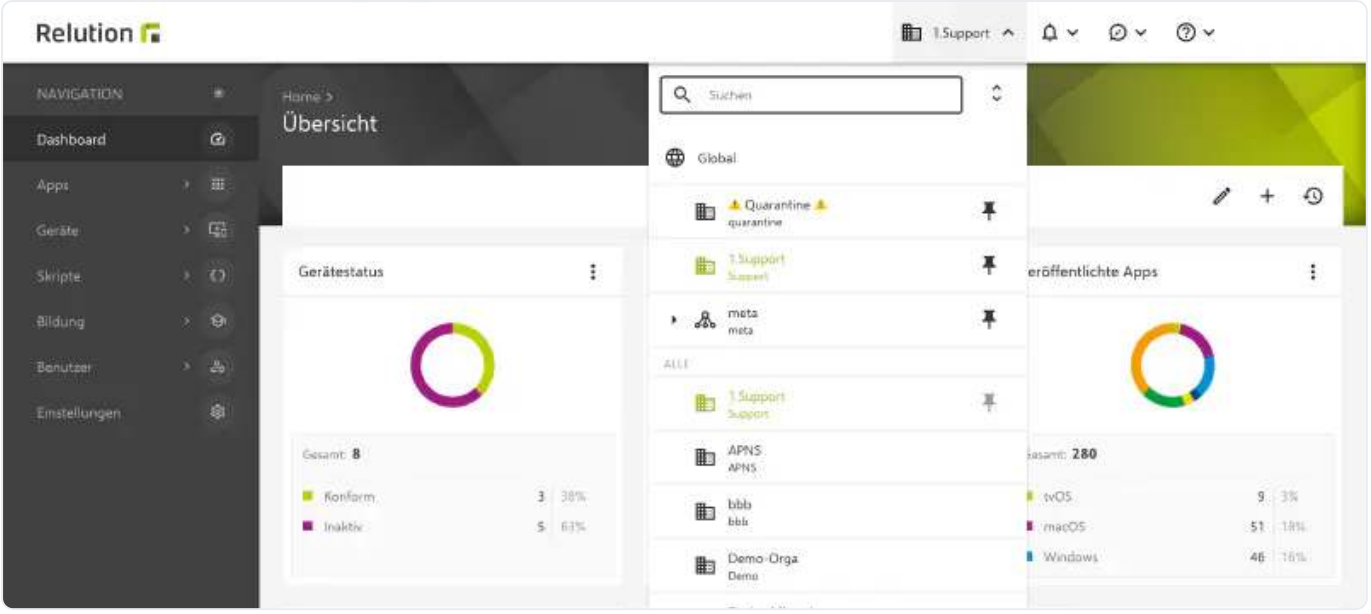
Im Organisationswechsler oben rechts ist die Global-Organisation am Globus-Symbol erkennbar. Meta-Organisationen tragen ein Struktur-Symbol, Unterorganisationen ein eigenes Symbol und eigenständige Organisationen ein Gebäude-Symbol.

Organisationswechsler

Neu in 26.4

Für Version 26.4.0

Über den Organisationsnamen oben rechts in der Kopfzeile lässt sich der Organisationswechsler öffnen. Ab Version 26.4 wird die Global-Organisation dort immer fest oben in der Liste angezeigt. Zusätzlich lassen sich einzelne Organisationen über das Pin-Symbol als Favorit anpinnen, sodass sie oberhalb der vollständigen Organisationsliste erscheinen und schneller erreichbar sind.



Funktionsweise

Benutzern mit System-Administrator-Berechtigungen steht der volle Funktionsumfang zur Verfügung. In dieser Organisation lassen sich auch neue Organisationen anlegen. Dies ist über den neu hinzugefügten Menüpunkt Organisationen möglich.

Benutzer ohne Berechtigung für die Organisationsverwaltung, also Benutzer, die aus einer bestehenden Store-Organisation migriert wurden, haben Zugriff auf die typischen Funktionsumfänge der Store-Organisation.

In der Global-Organisation selbst lassen sich keine Geräte einschreiben. Geräte werden in den untergeordneten Organisationen eingeschrieben und verwaltet.

Apps, Richtlinien und Skripte lassen sich zusätzlich auf Ebene einer Meta-Organisation für deren Unterorganisationen bereitstellen (Meta-Organisationen →).

Globale Benutzer

Auf der globalen Organisation können Benutzer zentral angelegt und anschließend mit spezifischen Rechten oder Rollen verschiedenen Tenants zugewiesen werden.

Diese Struktur ermöglicht eine flexible Identitätsverwaltung: Ein globaler Benutzer kann beispielsweise in Tenant A als Administrator fungieren, während er in Tenant B lediglich die Rolle eines Lehrers innehat.
Weitere Informationen zu Berechtigungen →

Für Version 26.4.0

Systemweite Automatische Geräteregistrierung

Über Apple School Manager bzw. Apple Business Manager können Geräte für die Automatische Geräteregistrierung (ADE, im Portal: DEP) der Global-Organisation zugewiesen werden. Ein DEP-Profil in der Global-Organisation, bei dem unter Benutzerauthentifizierung die Option Benutzername + Passwort gewählt ist, weist die Apple-Geräte der Organisation des angemeldeten Benutzers zu.

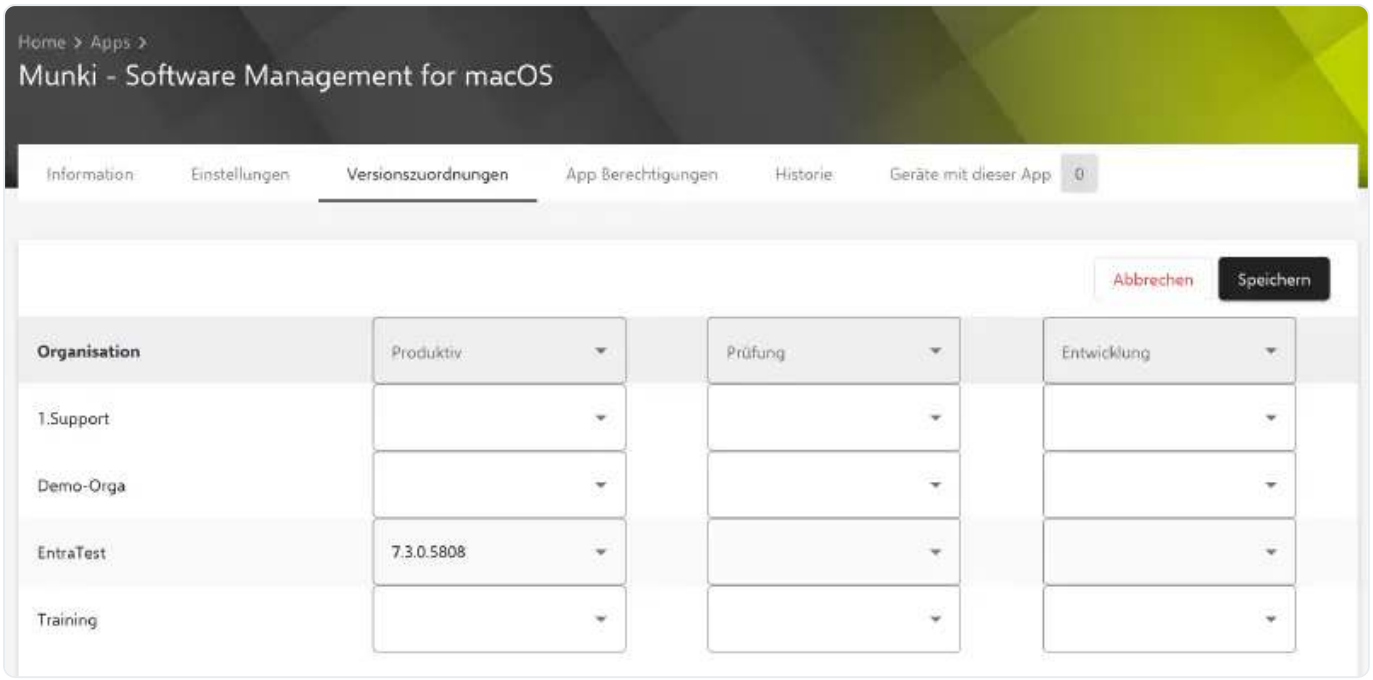
Alternativ lässt sich für eine automatische Einschreibung in der Global-Organisation im Abschnitt Bei der Organisation einschreiben eine Zielorganisation festlegen. Das Gerät wird dann in dieser Organisation eingeschrieben, auch ohne Benutzerauthentifizierung. Ist zusätzlich Benutzername + Passwort gewählt, muss der angemeldete Benutzer zur Zielorganisation gehören. Dasselbe Vorgehen ist über Meta-Organisationen möglich.

DEP →

Es ist weiterhin möglich, DEP-Token in weiteren Organisationen hinzuzufügen.

Native App-Verteilung und Versionierung

Native Apps können über eine Richtlinie mit der Konfiguration App Konformität verteilt werden. Die Zuordnung der Version kann in der Global-Organisation innerhalb der App im Reiter Versionszuordnungen festgelegt werden.



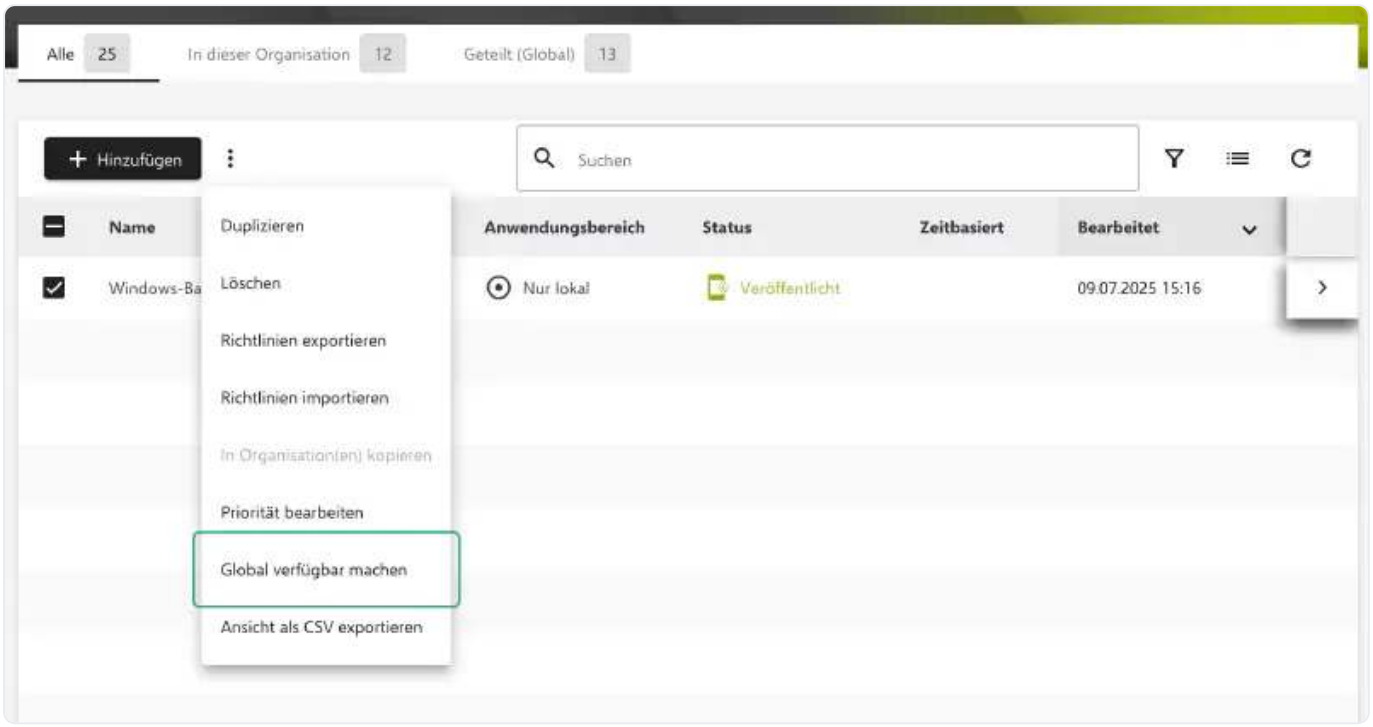
Richtlinien veröffentlichen oder in Organisationen kopieren

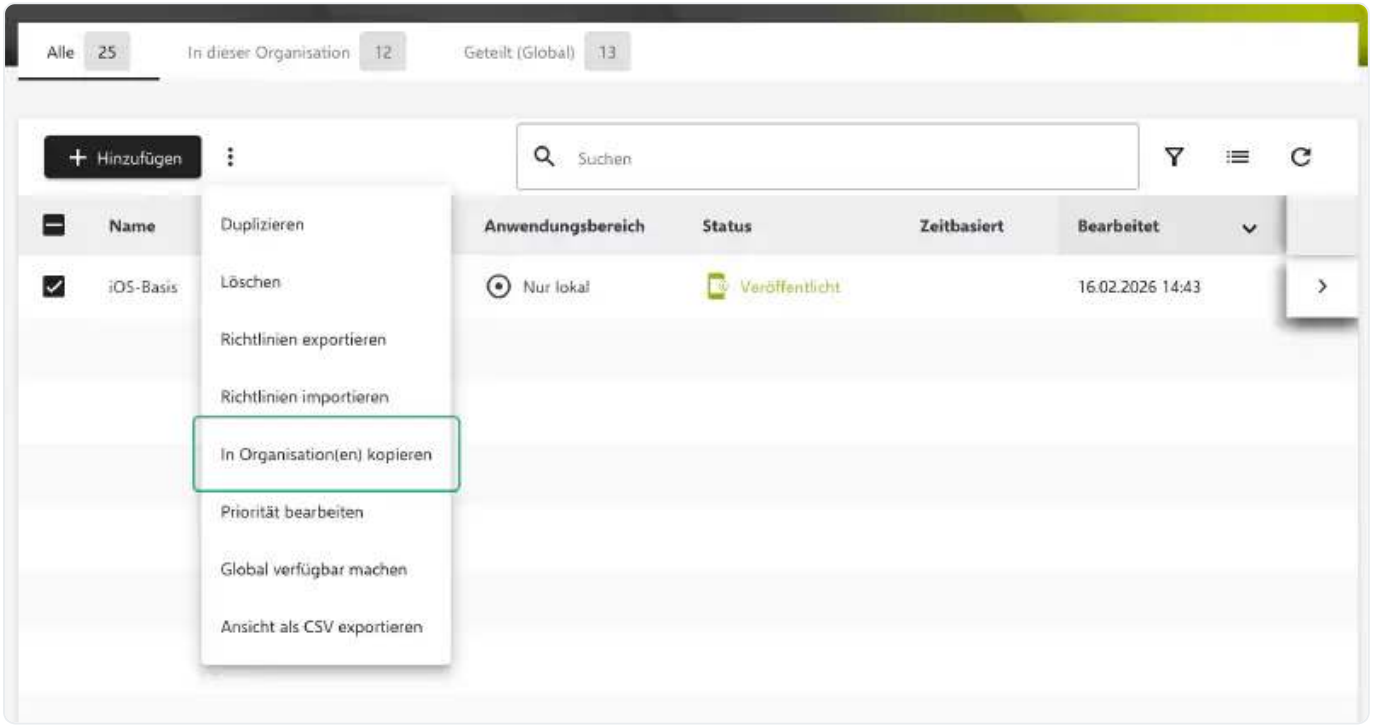
Für Version 26.4.0

In der Global-Organisation erstellte Richtlinien können auf zwei Arten verteilt werden:

- In Organisation(en) kopieren: kopiert die Richtlinie in eine oder mehrere Organisationen. Nur für iOS- und tvOS-Richtlinien verfügbar.
- Global verfügbar machen: stellt die Richtlinie allen Organisationen zur Verfügung. Für veröffentlichte Richtlinien aller Plattformen verfügbar.

Global verfügbar gemachte Richtlinien sind in den untergeordneten Organisationen schreibgeschützt; Änderungen sind nur in der Global-Organisation möglich. Bei der Priorisierung haben globale Richtlinien Vorrang.





Richtlinien Allgemein →

Globale Bereitstellung von Skripten

In der Global-Organisation angelegte Skripte (PowerShell-Skripte für Windows und Shell-Skripte für macOS) können schreibgeschützt in allen untergeordneten Organisationen zur Verfügung gestellt werden. Dies funktioniert ähnlich wie die Veröffentlichung von Richtlinien oder Apps. Hierzu wird beim Eintrag des Skripts in der Tabelle auf das Drei-Punkte-Menü geklickt und die Funktion Global verfügbar machen ausgewählt.

Skripte global bereitstellen →

Systemweite LDAP Konfiguration

Hier kann in den Einstellungen die LDAP → Konfiguration vorgenommen werden und ein organisationsspezifisches Mapping vorgenommen werden. Der Vorteil besteht darin, dass der LDAP Provider nur einmal zentral konfiguriert werden muss.

Im Bereich Objekte zu Organisationen zuordnen kann diese Konfiguration für Benutzerkonten, Gruppen, Klassen, Lehrer- und Schüleraccounts sowie Lehrer- und Schülergruppen eingestellt werden. Die Filter der Zuordnung verteilen nur Objekte, die bereits über die Importfilter der LDAP-Konfiguration erfasst werden.

Die Option Nicht zugeordnete Objekte in diese Organisation synchronisieren legt fest, was mit Objekten geschieht, auf die keine Zuordnung zutrifft: Ist sie aktiviert (Standard), werden sie in die Organisation mit der LDAP-Konfiguration synchronisiert. Ist sie deaktiviert, werden sie nicht importiert und als Synchronisierungsfehler gemeldet.

Für Version 26.4.0

Verschieben von Geräten in andere Organisationen

Über die Schaltfläche Verschieben in der Geräteliste der Global-Organisation können iOS-/iPadOS-, tvOS-, macOS-, Windows- und Android-Legacy-Geräte in andere Organisationen verschoben werden. Für andere Plattformen (u. a. Android Enterprise, ChromeOS, Linux, visionOS, watchOS) ist das nicht möglich.

Beim Verschieben werden benutzer- und organisationsspezifische Daten vom Gerät entfernt, darunter der zugewiesene Benutzer, Gerätegruppen und Zertifikate. Es werden nur Richtlinien auf den Geräten erhalten bleiben, die über die Global-Organisation global verfügbar gemacht wurden.

Gerät in Organisation verschieben →

Globale Anwendungen

Ab Relution `5.29` ist es möglich, native Apps über die Global Organisation an andere Organisationen zu verteilen. Hierbei wird, einfach erklärt, eine Verknüpfung der App in den Child Organisationen erstellt. Dies spart Datenbank-/Speicherressourcen und vereinfacht das Deployment der App erheblich.

Apps, die über ein Konto für Apps und Bücher (im Portal: VPP) der Global-Organisation angelegt werden, ersetzen automatisch bestehende Apps in anderen Organisationen.

Voraussetzungen

1. Um die gewünschte App verteilen zu können, muss der Zugriff auf die Global Organisation möglich sein. Diese ist am Globus-Symbol im Organisationswechsler oben rechts erkennbar, in der Regel auch am Namen Global.
2. Eine hochgeladene native App oder eine noch nicht global verteilte Google-, Apple-, oder Windows-Store App:
   - iOS: .ipa
   - macOS: .pkg, .dmg
   - Android: .apk
   - Windows: .msix, .msixbundle, .appx, .appxbundle, .msi, .exe
3. Die App besitzt mindestens eine Version im Status Produktiv. Andernfalls ist die Funktion Global verfügbar machen deaktiviert (Hinweis Auswahl enthält unveröffentlichte Apps).
4. Die App darf nicht bereits global verfügbar sein.

Ausführung

1. In der Seitennavigation links unter `Apps` → `App Store` mit der Maus auf die gewünschte native App hovern
2. Auf das 3-Punkte-Menü neben dem App-Namen klicken
3. Punkt Global verfügbar machen auswählen
4. Bei bereits (teilweise) zugewiesenen Apps kann ein Dialogfenster mit Konflikten und Hinweisen erscheinen.

   Diese Aktion kann nicht rückgängig gemacht werden. Die folgenden Apps sind bereits in anderen Organisationen vorhanden. Wenn diese global gemacht werden, werden die Apps in den anderen Organisationen ersetzt und gelöscht. Die Apps auswählen, die global verfügbar sein sollen.

   Dieser Vorgang kann einige Zeit in Anspruch nehmen.

Für Version 26.4.0

5. In der Spalte Anwendungsbereich wird die App anschließend als Geteilt angezeigt. In den untergeordneten Organisationen erscheint sie als Von Global.

Verwaltung der Anmeldedaten

Um die Anmeldung in Relution weiter abzusichern, lässt sich unter `Einstellungen` → `Verwaltung der Anmeldedaten` eine Vielzahl an Einstellungen für die jeweilige Organisation setzen. Hier sind die Einstellungen für Passwort-Komplexität, Multi-Faktor-Authentifizierung (MFA) sowie für fehlgeschlagene Anmeldeversuche beschrieben.

Passwort-Richtlinie

- Einfaches Passwort erlauben (Standard: aus): Ein einfaches Passwort kann mit dem Benutzernamen übereinstimmen, z. B. Benutzername test Passwort test. Ist die Option deaktiviert, darf das Passwort weder dem Benutzernamen noch dem Namen der Organisation entsprechen.
- Minimale Passwortlänge: 3 bis 72 Zeichen, Standard 8.
- Maximales Passwortalter in Tagen: Ist das zulässige Alter überschritten, muss bei der nächsten Anmeldung ein neues Passwort vergeben werden. Der Standardwert `0` bedeutet, dass Passwörter nicht ablaufen.
- Minimale Anzahl an Zahlen
- Minimale Anzahl an Kleinbuchstaben
- Minimale Anzahl an Großbuchstaben
- Minimale Anzahl an Sonderzeichen: Als Sonderzeichen gilt jedes Zeichen, das weder Buchstabe noch Ziffer ist.
- Funktion “Passwort vergessen” deaktivieren

Die Mindestanzahlen für Zahlen, Klein- und Großbuchstaben sowie Sonderzeichen stehen standardmäßig auf `0`.

Für Version 26.4.0

Passwort-Zurücksetzen deaktivieren

Die Funktion Passwort vergessen lässt sich unter `Einstellungen` → `Verwaltung der Anmeldedaten` mit der Option Funktion “Passwort vergessen” deaktivieren abschalten. Wenn sie deaktiviert ist, ist ein Zurücksetzen des Passworts ohne Eingriff eines Administrators nicht mehr möglich. Lokale Konten, die ihr Passwort verlieren, erfordern ein direktes Zurücksetzen durch einen Administrator.

Die Wirkung hängt von der Organisationsebene ab:

- In der Global-Organisation gilt die Deaktivierung für alle Organisationen.
- In einer Meta-Organisation überschreibt sie die Einstellung für die Organisationen dieser Meta-Organisation.
- In einer Organisation wirkt sie nur auf dem Anmeldebildschirm dieser Organisation.

Ist die Option in einer übergeordneten Organisation gesetzt, ist der Schalter schreibgeschützt; das Portal zeigt dann den Hinweis, dass der Link von der übergeordneten Organisation deaktiviert wurde.

Vor dem Deaktivieren dieser Option sollte mindestens ein Administratorkonto mit einem bekannten, wiederherstellbaren Passwort vorhanden sein.

Multi-Faktor-Authentifizierung

- E-Mail-Authentifizierung (Standard: an)
- Gültigkeitsdauer des Einmal-Codes: 30 Sekunden bis 1 Stunde, Standard 10 Minuten.
- Authenticator Apps (TOTP) (Standard: an)

Sind beide Faktoren deaktiviert, weist das Portal darauf hin, dass sich alle Benutzer ohne MFA anmelden können.

MFA →

Fehlgeschlagene Anmeldeversuche

- Deaktivierung des Benutzers bei aufeinanderfolgenden fehlgeschlagenen Anmeldeversuchen (Standard: aus)
- Maximale Anzahl fehlgeschlagener Anmeldeversuche (Standard 10, mindestens 1)

Erreicht ein Benutzer die maximale Anzahl, wird er deaktiviert und muss von einem Administrator wieder aktiviert werden. Eine erfolgreiche Anmeldung setzt den Zähler zurück. Die Deaktivierung gilt nur für lokale Relution-Benutzer; Benutzer, die sich ausschließlich extern authentifizieren (z. B. über LDAP), werden nicht gezählt.

Die Sperre von IP-Adressen nach fehlgeschlagenen Anmeldeversuchen ist unter Fail2Ban – IP-Sperre → beschrieben.

Für Version 26.4.0

Multi-Faktor-Authentifizierung

Die Multi-Faktor-Authentifizierung, kurz MFA, ist ein Sicherheitsmechanismus, bei dem Benutzer für den Zugang zu einer Anwendung mindestens zwei unabhängige Verifizierungsfaktoren angeben müssen, um sich eindeutig zu identifizieren.

Unbefugter Zugriff wird durch die zusätzliche Authentifizierungsmethode deutlich erschwert; das Sicherheitsniveau wird somit maßgeblich erhöht.

MFA und Relution

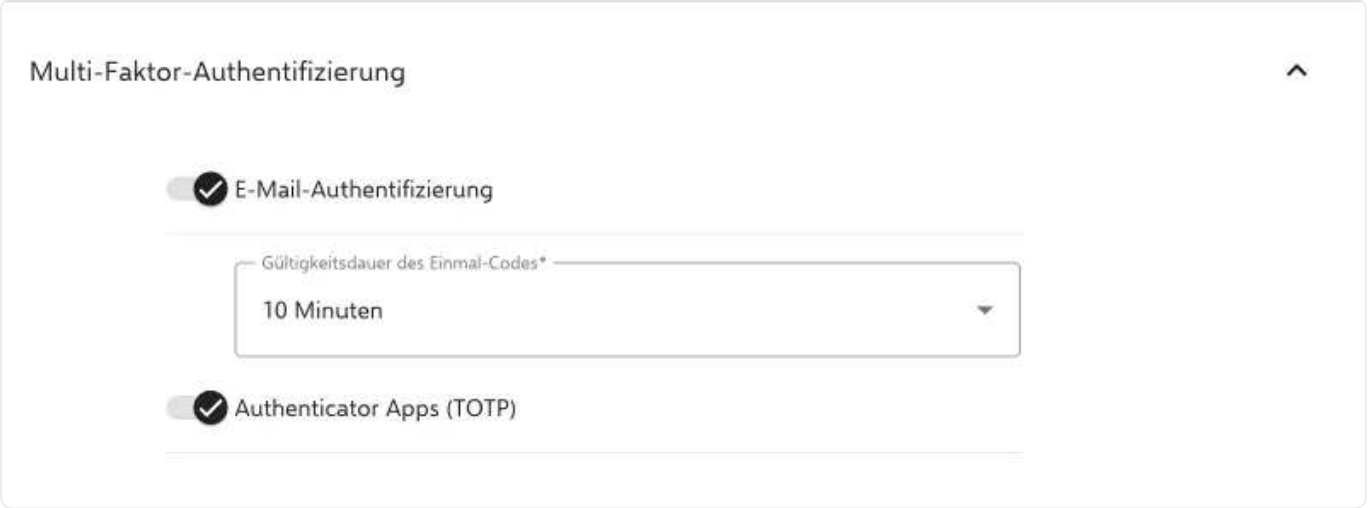
Relution ermöglicht LDAP- und lokalen Benutzern, im Relution Portal zusätzlich zu Benutzername und Kennwort die weiteren Authentifizierungsmethoden E-Mail (Einmal-Code per E-Mail) und Authenticator App zu aktivieren.

Mit dem Release 5.16 wird der Forderung des Bundesamts für Sicherheit in der Informationstechnik (BSI) an MDM-Anbieter Rechnung getragen, die Bereitstellung einer zusätzlichen Sicherheitsstufe umzusetzen.

Wie wird die MFA in Relution konfiguriert?

Für Version 26.4.0

Unter `Einstellungen` → `Verwaltung der Anmeldedaten` legt ein Organisations- oder System-Administrator im Abschnitt Multi-Faktor-Authentifizierung fest, welche MFA-Methoden in der Organisation zur Verfügung stehen. Standardmäßig sind E-Mail-Authentifizierung und Authenticator Apps (TOTP) aktiviert. Maßgeblich ist die Einstellung der Organisation, zu der ein Benutzer gehört.



Für die E-Mail-Authentifizierung wird die Gültigkeitsdauer des Einmal-Codes festgelegt: 30 Sekunden, 1, 2, 5, 10, 15 oder 30 Minuten oder 1 Stunde (Standard: 10 Minuten). Authenticator Apps (TOTP) erlaubt die Anmeldung mit einem zeitbasierten Code aus einer Authenticator-App. Jede der beiden Methoden lässt sich einzeln deaktivieren, beide können auch parallel aktiv sein.

Werden beide Methoden deaktiviert, fragt Relution bei der Anmeldung keinen zweiten Faktor mehr ab – auch nicht für Rollen mit erzwungener MFA und nicht für Benutzer, die bereits MFA-Tokens eingerichtet haben.

MFA-Anmeldung erzwingen

Das Relution Permission-System wurde um die Möglichkeit Multi-Faktor-Authentifizierung erweitert. Dabei kann für eine Rolle definiert werden, ob die MFA-Anmeldung vorausgesetzt wird oder nicht.

Ist die Berechtigung/ Rolle mit aktivierter MFA-Anmeldung einem Benutzer oder einer Gruppe zugeordnet, wird bei einem LogIn eine MFA-Anmeldung zwingend benötigt.

Wurde noch keine MFA-Methode eingerichtet, dann muss der Benutzer dies bei der ersten Anmeldung durchführen.

MFA für eine Gruppe erzwingen

Soll die MFA-Anmeldung für alle Mitglieder einer Gruppe gelten, wird eine Rolle mit aktivierter MFA angelegt und der Gruppe zugewiesen. Berücksichtigt werden auch Rollen aus übergeordneten Gruppen.

1. Unter `Benutzer` → `Berechtigungen` über Hinzufügen eine neue Rolle anlegen oder eine bestehende eigene Rolle öffnen.
2. Im Abschnitt Multi-Faktor-Authentifizierung die Option Multi-Faktor-Authentifizierung wird für die Rolle erzwungen aktivieren und mit Speichern übernehmen.
3. Unter `Benutzer` → `Gruppen` die gewünschte Gruppe öffnen.
4. Über Berechtigungen verwalten die Rolle auswählen und mit Speichern übernehmen.

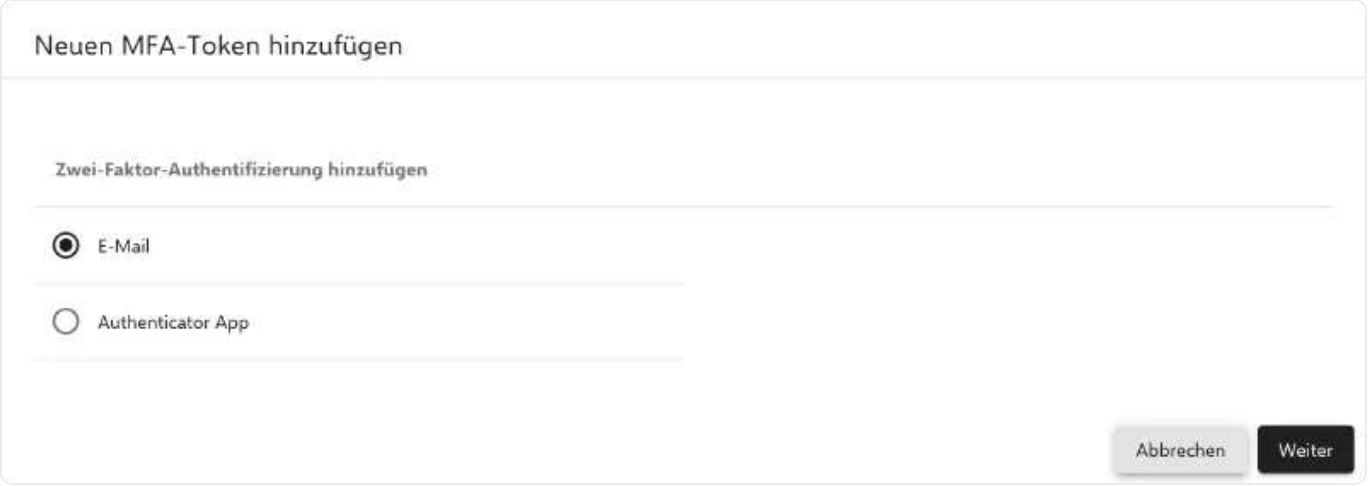
Der Abschnitt Multi-Faktor-Authentifizierung erscheint in der Rolle erst, wenn unter `Einstellungen` → `Verwaltung der Anmeldedaten` mindestens eine MFA-Methode aktiviert ist. Die Standardrollen von Relution lassen sich nicht bearbeiten; für die MFA wird daher eine eigene Rolle benötigt. Die Zuweisung ist auch bei Gruppen möglich, die per LDAP synchronisiert werden. Weitere Informationen zu Rollen enthält der Artikel Berechtigungen →.

Für Version 26.4.0

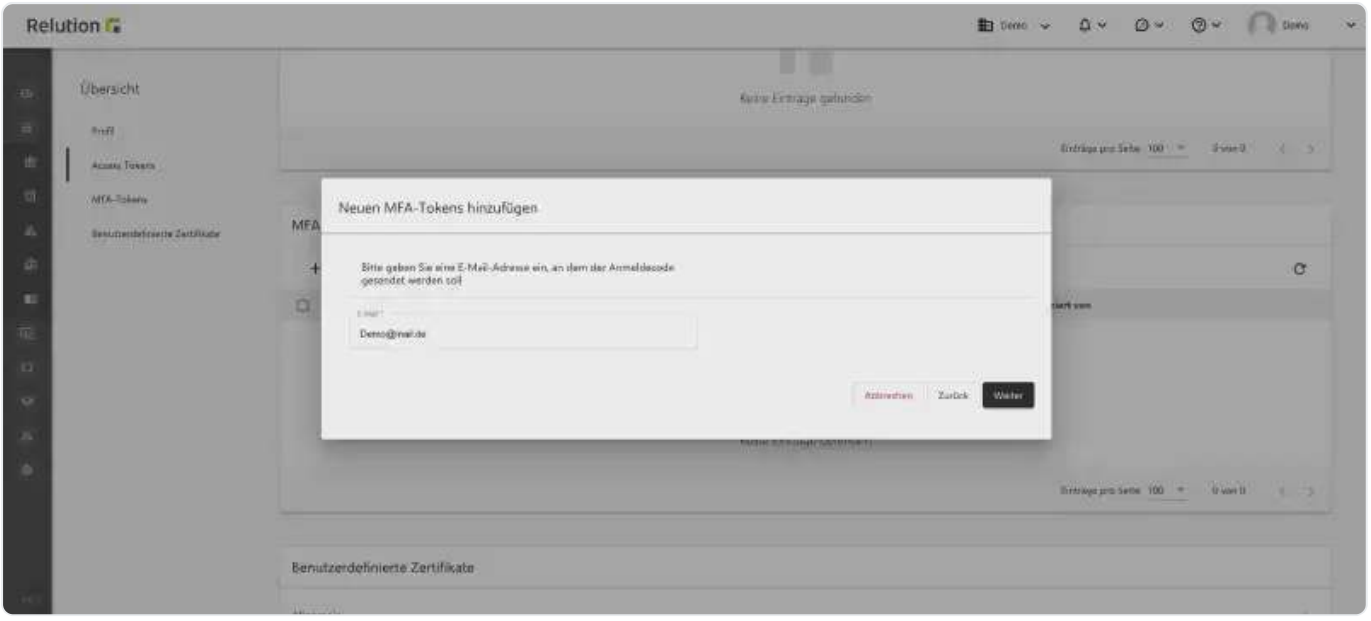
E-Mail-Token

Jeder Benutzer kann die MFA unabhängig von einem Administrator im Relution Portal für sich aktivieren. Ist ein MFA-Token eingerichtet, wird der zweite Faktor bei jeder Anmeldung abgefragt, auch ohne Rolle mit erzwungener MFA.

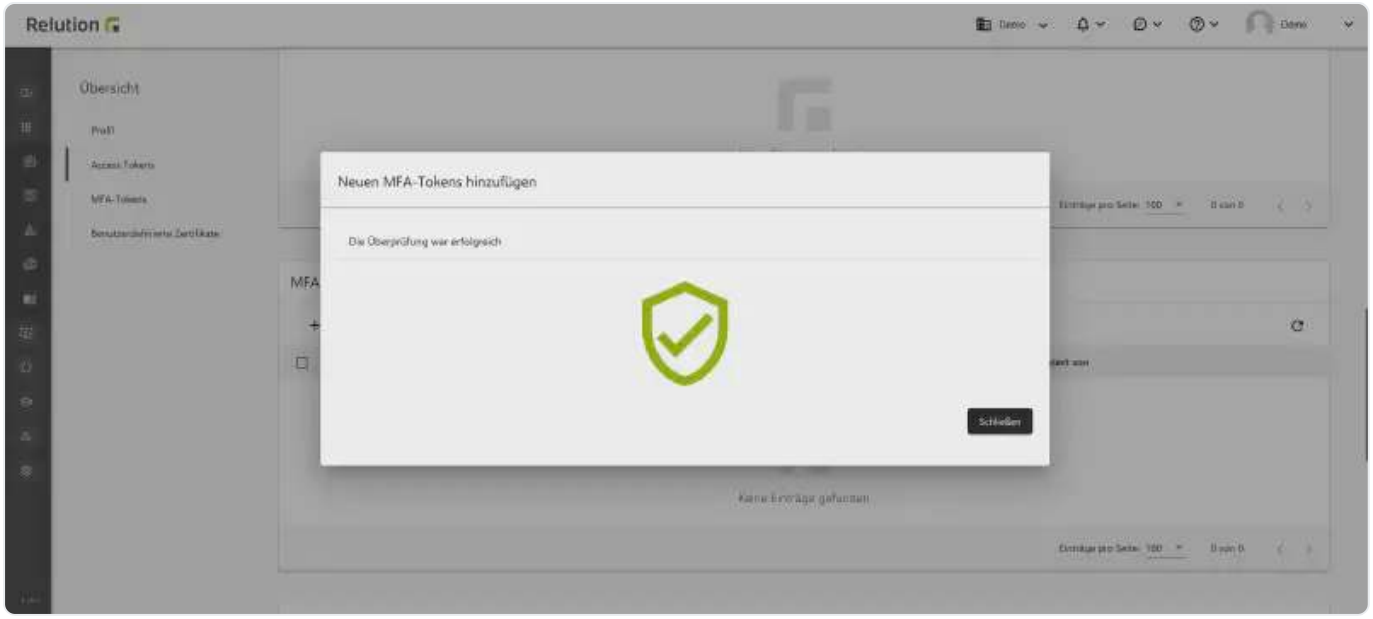
Im Relution Portal öffnet das Benutzermenü oben rechts den Eintrag Profil. Dort öffnet im Reiter MFA-Tokens die Schaltfläche Hinzufügen den Dialog Neuen MFA-Token hinzufügen. Den Reiter gibt es nur, wenn unter `Einstellungen` → `Verwaltung der Anmeldedaten` mindestens eine MFA-Methode aktiviert ist. Nach Auswahl von E-Mail wird im nächsten Schritt die E-Mail-Adresse eingegeben.



Private wie auch vom Benutzer abweichende E-Mail-Adressen lassen sich im System hinterlegen – im Schulkontext sinnvoll.



Nach der Eingabe wird ein Einmal-Code zur Verifizierung an die hinterlegte E-Mail-Adresse versandt. Er bleibt für die vom Administrator festgelegte Dauer gültig. Sobald der sechsstellige Verifizierungscode aus der E-Mail eingegeben ist, ist die Multi-Faktor-Authentifizierung eingerichtet. Wird die Einrichtung vorher abgebrochen, erscheint der Token mit dem Status Unvollendet und gilt nicht als MFA-Faktor.



Im Relution Portal lassen sich beliebig viele MFA-Faktoren hinterlegen. Sind mehrere E-Mail-Tokens eingerichtet, wird der Code bei der Anmeldung an alle hinterlegten Adressen gesendet. Zusätzlich zur E-Mail-Variante wird die Verwendung diverser Authenticator-Apps unterstützt.

Wird im Dialog Neuen MFA-Token hinzufügen die zweite Variante Authenticator App ausgewählt, wird ein QR-Code angezeigt, der mit einer zuvor auf dem Endgerät installierten Authenticator-App gescannt wird.

Es besteht auch die Möglichkeit, auf einen Einrichtungsschlüssel zur Verifizierung zurückzugreifen.

Sind diverse Authenticator-Apps bei mehreren Geräten gleichzeitig in Verwendung, wird für eine korrekte Anmeldung die Gültigkeit von mindestens einer App überprüft.

Bei Verwendung beider Multi-Faktor-Authentifizierungsmethoden wird primär die Authenticator-App abgefragt; die hinterlegte E-Mail-Variante dient als Absicherung. Bei der Anmeldung wechselt die Schaltfläche E-Mail verwenden (unter Kein Zugriff auf die Authenticator App?) zur E-Mail-Variante; E-Mail erneut senden fordert einen neuen Code an.

Ist lediglich die Authenticator-App in Verwendung, gibt es keinen E-Mail-Fallback.

MFA-Tokens manuell löschen

Für Version 26.4.0

MFA-Tokens können vom Benutzer im Profil im Reiter MFA-Tokens manuell gelöscht werden.

Wurden alle MFA-Varianten händisch entfernt, die MFA aber über eine Rolle erzwungen, muss bei der nächsten Anmeldung im Relution Portal erneut eine Multi-Faktor-Authentifizierung hinterlegt werden.

Was passiert im Verlustfall des MFAs?

Hat der Nutzer bei aktivierter MFA keinen Zugriff auf E-Mail und/oder Authenticator-App, ist eine Anmeldung im Relution Portal nicht mehr möglich – der Gang zum Administrator ist Pflicht.

Unter `Benutzer` → `Benutzer` lässt sich der betroffene Benutzer öffnen und im Abschnitt MFA-Tokens der Token löschen. Voraussetzung ist die Berechtigung zum Löschen von Benutzern. Mit der Berechtigung zum Erstellen von Benutzern lassen sich dort auch MFA-Tokens für den Benutzer anlegen.

Die Spalte MFA der Benutzerliste zeigt, ob ein Benutzer MFA eingerichtet hat; der gleichnamige Filter unterscheidet Konfiguriert und Nicht konfiguriert.

TLS-Vertrauenskonfiguration

Die TLS-Vertrauenskonfiguration bündelt die serverseitigen Einstellungen für den Aufbau vertrauenswürdiger TLS-Verbindungen. Sie ist unter `Einstellungen` → `TLS-Vertrauenskonfiguration` zu finden und gliedert sich in zwei Bereiche: die vertrauenswürdigen Zertifikate für ausgehende Verbindungen und das Certificate Pinning für das Apple-Enrollment. Die TLS-Vertrauenskonfiguration steht ausschließlich in der Global-Organisation zur Verfügung und gilt serverweit für alle Organisationen. Änderungen in beiden Bereichen werden gemeinsam über Speichern im oberen Bereich der Seite übernommen.

Vertrauenswürdige Zertifikate

Relution akzeptiert die hier hinterlegten CA-Zertifikate zusätzlich zum Standard-Truststore des Systems beim Aufbau ausgehender TLS-Verbindungen. Über Hinzufügen werden CA-Zertifikate ausgewählt, die zuvor unter `Einstellungen` → `Zertifikate` hochgeladen wurden (siehe Zertifikatsverwaltung →). Der Auswahldialog zeigt nur Zertifikate, die als Zertifizierungsstelle (CA) gekennzeichnet sind; Zertifikatscontainer wie `pfx` / `p12` stehen nicht zur Auswahl. Die Übersicht führt je Eintrag Name, Typ und das Ablaufdatum (Läuft ab); über Löschen werden ausgewählte Einträge wieder entfernt.

Zertifikate, die hier als vertrauenswürdiges Zertifikat oder als Anker-Zertifikat verwendet werden, lassen sich in der Zertifikatsverwaltung nicht löschen, solange sie referenziert sind.

Certificate Pinning (Apple-Enrollment)

Für Version 26.4.0

Neu in 26.5

Ist im Bereich Allgemein der Schalter Certificate Pinning aktivieren eingeschaltet, wird die TLS-Verbindung zum MDM-Server gegen ausgewählte Anker-Zertifikate statt gegen den Truststore des Systems validiert. Dadurch werden Man-in-the-Middle-Angriffe und der Einsatz nicht autorisierter Zertifizierungsstellen erschwert. Das Pinning wird bei der Registrierung (Enrollment) von Apple-Geräten in das MDM-Profil übernommen und gilt anschließend für die gesamte Kommunikation des Geräts mit dem MDM-Server, einschließlich des Check-ins. Ist das Pinning deaktiviert, prüft das Gerät die Verbindung gegen den System-Truststore.

Die zu prüfenden Zertifikate werden im Bereich Anker-Zertifikate über Hinzufügen aus den in der Zertifikatsverwaltung hinterlegten CA-Zertifikaten ausgewählt; die Übersicht führt je Eintrag Name, Typ und das Ablaufdatum (Läuft ab). Zum Aktivieren des Pinnings ist mindestens ein Anker-Zertifikat erforderlich. Über den Schalter Zertifikatssperrprüfung erforderlich lässt sich zusätzlich eine Prüfung des Zertifikatswiderrufs erzwingen. Wird Certificate Pinning aktivieren ausgeschaltet, leert Relution die Liste der Anker-Zertifikate und setzt die Sperrprüfung zurück; nach erneutem Einschalten müssen die Anker-Zertifikate neu ausgewählt werden.

Pinning ist im MDM-Profil hinterlegt

Das Pinning wird bei der Registrierung in das MDM-Profil eingebettet. Änderungen an dieser Stelle wirken sich auf neue Registrierungen aus. An bereits registrierte Geräte überträgt Relution die geänderte Konfiguration erst, wenn deren MDM-Profil aktualisiert wird (Aktion MDM Profil aktualisieren oder automatische Erneuerung vor Ablauf des Identitätszertifikats). Eine fehlerhafte Konfiguration kann Geräte von der MDM-Kommunikation ausschließen; ein Gerät, das die Verbindung zum MDM-Server wegen eines falschen Pins nicht mehr aufbauen kann, erreicht auch keine Profilaktualisierung mehr und muss erneut registriert werden. Es sollten ausschließlich langlebige CA-Zertifikate gepinnt werden; beim Rotieren einer CA bleiben sowohl der alte als auch der neue Anker ausgewählt.

Zertifikatssperrprüfung nur mit Sperrinformationen aktivieren

Der Schalter Zertifikatssperrprüfung erforderlich darf nur eingeschaltet werden, wenn das TLS-Zertifikat des Servers Sperrinformationen (OCSP-Responder-URL) bereitstellt. Fehlt diese Information, verweigern Geräte möglicherweise die Verbindung.

Verhalten bei der Registrierung

Bei aktiviertem Pinning wird die Verbindung des Geräts zum MDM-Server während der Registrierung gegen die ausgewählten Anker-Zertifikate geprüft. Lässt sich die TLS-Zertifikatskette des Servers auf eines der Anker-Zertifikate zurückführen, gelingt die Registrierung. Diese Prüfung gilt auch für die spätere MDM-Kommunikation des registrierten Geräts. Bei Abweichung wird die Verbindung abgewiesen und die Registrierung schlägt fehl.

Ist das Pinning eingeschaltet, aber kein Anker-Zertifikat konfiguriert oder ladbar, erzeugt Relution die MDM-Profile ohne Pinning.

Geräte mit einer Betriebssystemversion unterhalb der für das Pinning erforderlichen Mindestversion werden weiterhin ohne Pinning registriert; die Registrierung bleibt dort funktionsfähig.

Für Version 26.4.0

Benachrichtigungen zu Anker-Zertifikaten

Relution überwacht die gepinnten Anker-Zertifikate stündlich sowie nach jedem Speichern und meldet Probleme im Benachrichtigungscenter, damit ein Aussperren von Geräten frühzeitig verhindert werden kann. Die Benachrichtigungen erhalten Benutzer der Global-Organisation, die die TLS-Vertrauenskonfiguration einsehen dürfen. Gemeldet werden unter anderem:

- ein Anker-Zertifikat, das in weniger als 90 Tagen abläuft oder bereits abgelaufen ist,
- ein Anker-Zertifikat, das nicht geladen werden kann oder kein CA-Zertifikat ist,
- ein wirkungsloses Pinning, etwa wenn kein Anker-Zertifikat konfiguriert ist oder keines mit der TLS-Zertifikatskette des Servers übereinstimmt.

LDAP Konfiguration

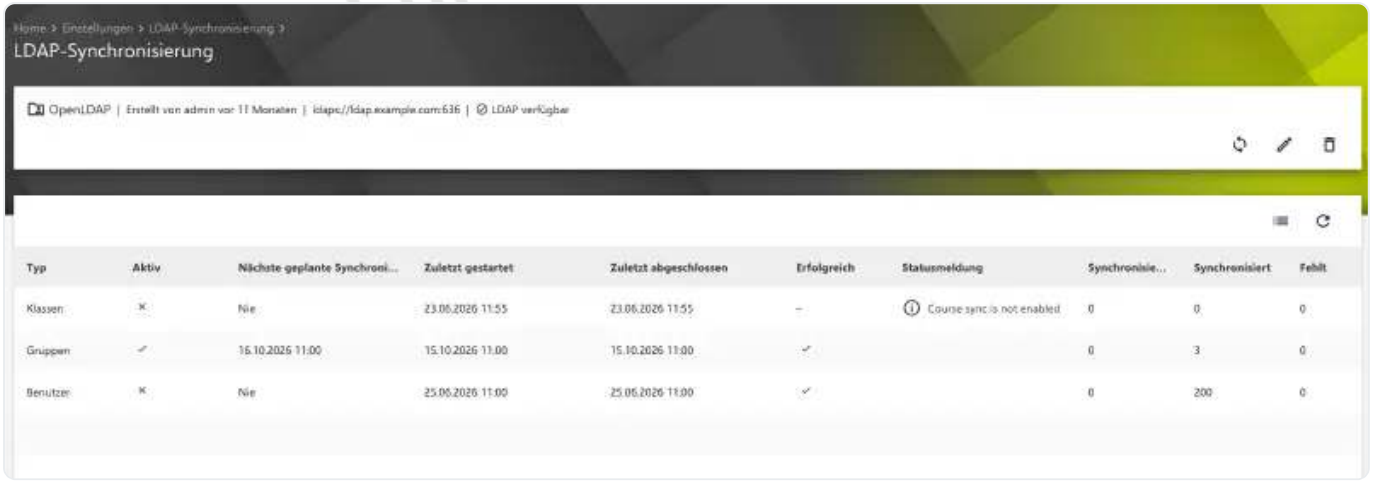
Ab Relution Version `5.18.0` lassen sich LDAP-Provider für den Benutzer-, Gruppen- und Klassenimport direkt über das Relution Portal konfigurieren. Die Maske enthält die üblichen Konfigurationsparameter, die sich über mehrere Funktionstests prüfen lassen. Ein Neustart des Relution-Dienstes ist bei der Konfiguration über das Portal nicht notwendig; Änderungen und Neukonfigurationen unterbrechen den Betrieb daher nicht. Für die Konfiguration der LDAP-Synchronisierung sind Kenntnisse im Thema sowie ein LDAP-Browser empfehlenswert, der Attribute korrekt anzeigen kann. Für Windows hat sich der Softerra LDAP Browser und für Linux oder macOS das Apache Directory Studio bewährt. Beide Tools sind kostenlos.

> Für die Konfiguration von LDAP-Providern über das Relution Portal ist eine kostenpflichtige Lizenz mit dem Feature LDAP Verbindungen erforderlich. Ohne diese Lizenz lässt sich die Konfiguration nicht speichern, und Benutzer, Gruppen und Klassen werden nicht synchronisiert.

Grundlagen

Die LDAP-Konfiguration erfolgt unter `Einstellungen` → `LDAP-Synchronisierung`. Pro Organisation lassen sich mehrere LDAP-Provider einrichten. Die Mailadressen der Benutzer müssen in Relution eindeutig sein. Andernfalls kann es zu Fehlern kommen, sodass einige Benutzerkonten nicht angelegt werden. Ein neuer LDAP-Provider wird über Hinzufügen angelegt.

Eine manuelle Synchronisierung ist jederzeit möglich: in dieser Liste über Synchronisation starten für den markierten Provider sowie in den Listen der Benutzer, Gruppen und Klassen über Einmalige LDAP-Synchronisation. Die Detailseite eines Providers zeigt je Typ (Benutzer, Gruppen, Klassen) das Ergebnis der letzten Synchronisierung.



Basiskonfiguration

Die Maske für die Konfiguration ist in mehrere Ebenen aufgeteilt. Nicht immer sind alle Parameter für den jeweiligen Fall notwendig. In einigen Feldern sind bereits Beispiele hinterlegt, die die Syntax vorschlagen.

LDAP-Synchronisierung

Zunächst wird ein Name für den LDAP-Provider vergeben. Empfehlenswert ist eine kurze und aussagekräftige Bezeichnung.

> Diese Bezeichnung kann im Nachhinein nicht mehr geändert werden.

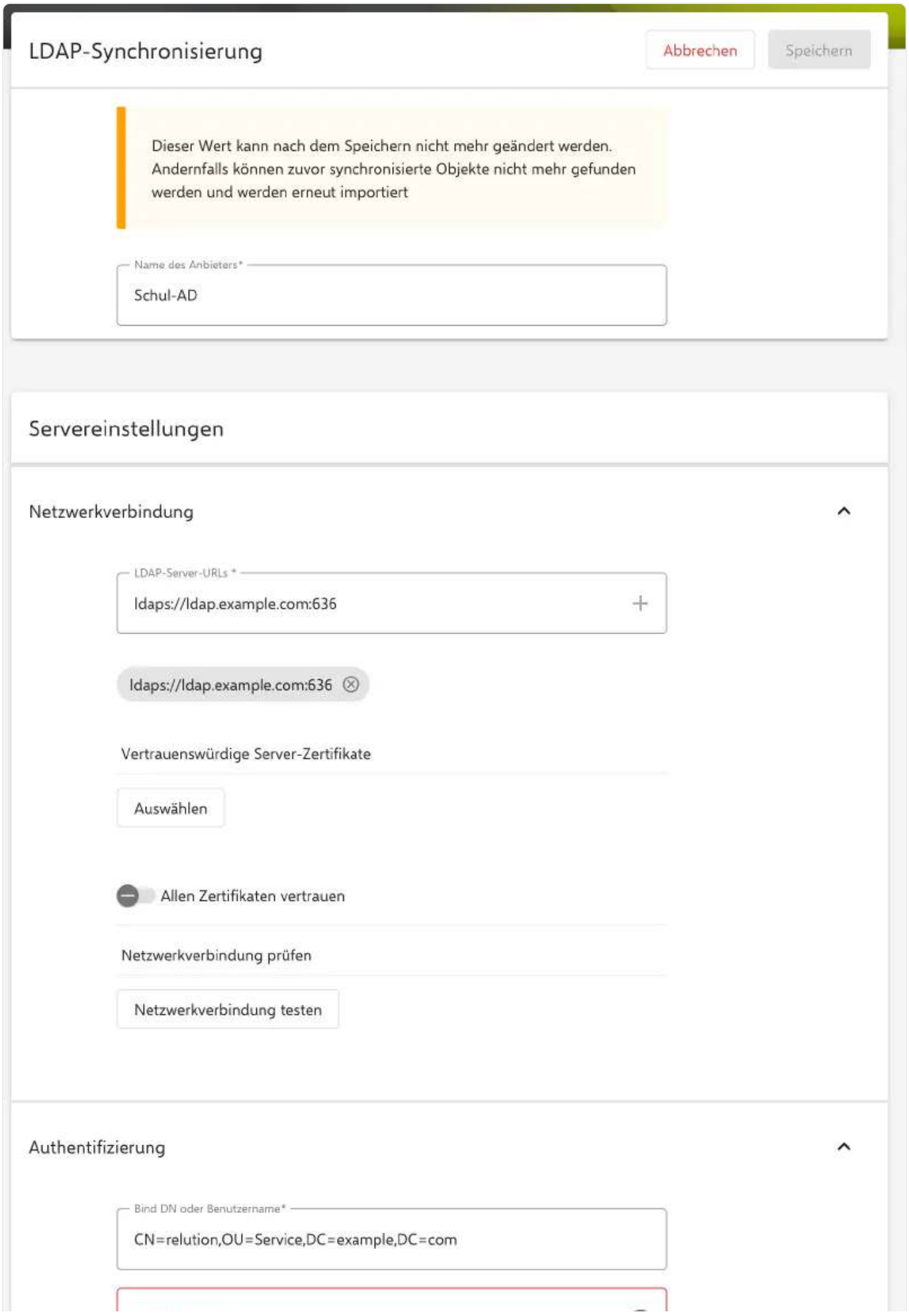
Servereinstellungen

- LDAP-Server-URLs: Die URL des LDAP-Servers wird eingetragen und mit `Enter` bestätigt.

Wird LDAPS verwendet und hat der Server kein vertrauenswürdiges Zertifikat, lässt sich das Zertifikat unter Vertrauenswürdige Server-Zertifikate hinterlegen, damit Relution es als vertrauenswürdig einstuft. Alternativ akzeptiert Relution mit Allen Zertifikaten vertrauen jedes Serverzertifikat. Das Portal weist dabei auf das Sicherheitsrisiko hin; explizit hinterlegte Zertifikate sind vorzuziehen.

Die Verbindung wird mit Netzwerkverbindung testen geprüft. Der Verbindungsversuch sollte erfolgreich sein, bevor die Konfiguration fortgesetzt wird.

Für Version 26.4.0


LDAP-Synchronisierung
Abbrechen
Speichern
Dieser Wert kann nach dem Speichern nicht mehr geändert werden. Andernfalls können zuvor synchronisierte Objekte nicht mehr gefunden werden und werden erneut importiert
Name des Anbieters*
Schul-AD
Servereinstellungen
Netzwerkverbindung
LDAP-Server-URLs *
ldaps://ldap.example.com:636
ldaps://ldap.example.com:636
Vertrauenswürdige Server-Zertifikate
Auswählen
Allen Zertifikaten vertrauen
Netzwerkverbindung prüfen
Netzwerkverbindung testen
Authentifizierung
Bind DN oder Benutzername*
CN=relution,OU=Service,DC=example,DC=com

Authentifizierung

- Bind DN oder Benutzername: Benutzername mit lesenden Berechtigungen im LDAP. Idealerweise wird hier der Distinguished Name (DN) verwendet.
- Bind Passwort: Das zugehörige Passwort.

Die Anmeldedaten werden mit Authentifizierung testen geprüft.

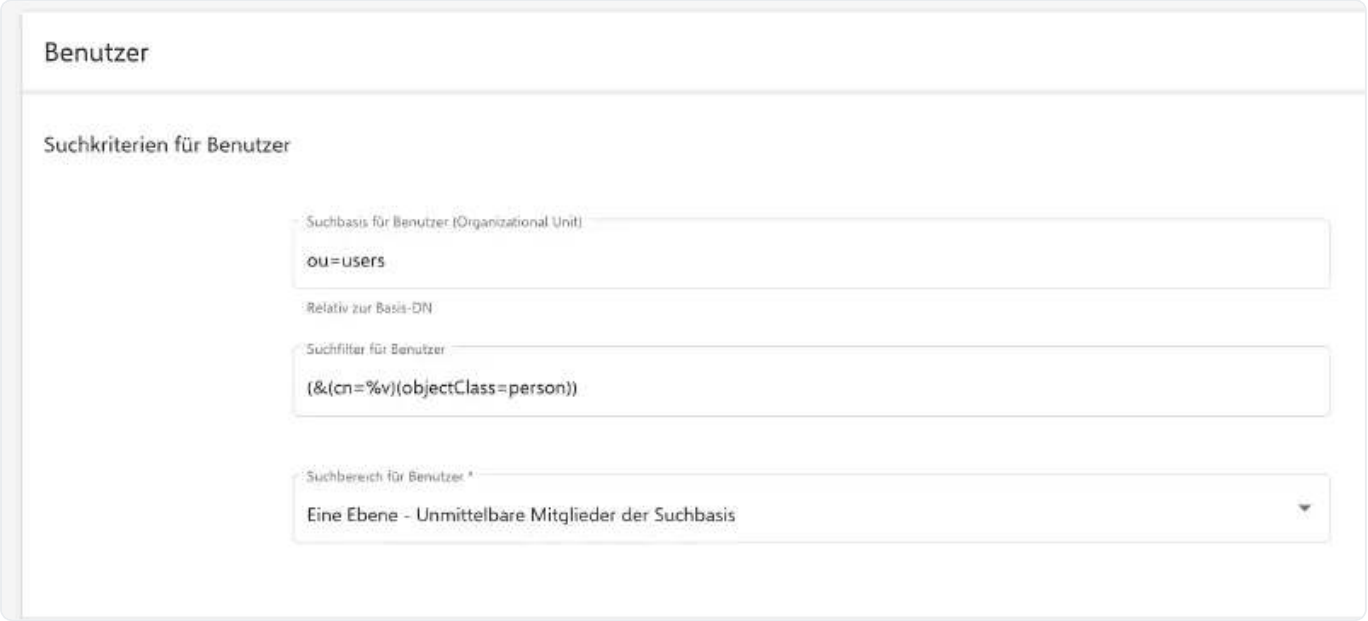
Basis-DN

Nach erfolgreichem Authentifizierung testen werden die vom Server gemeldeten Basis-DNs in der Auswahl Basis-DNs ermitteln angeboten; der erste Eintrag ist vorausgewählt. Mit Ermittelte Basis-DN als Basis-DN verwenden wird der gewählte Eintrag in das Feld Basis-DN übernommen. Eventuell notwendige Änderungen sind jederzeit möglich.

Für Version 26.4.0

Suchkriterien für Benutzer

- Suchbasis für Benutzer (Organizational Unit): Die Suchbasis für die Benutzer, relativ zur Basis-DN, zum Beispiel `OU=users`.
- Suchfilter für Benutzer: Hier kommen konventionelle LDAP-Suchfilter zum Einsatz. Relution verwendet für Benutzereingaben immer den Platzhalter `%v`. Ein einfacher Suchfilter für Benutzer könnte zum Beispiel `(&(cn=%v)(objectClass=person))` sein.
- Suchbereich für Benutzer: Legt fest, wie tief im Pfad nach Benutzerkonten mit dem entsprechenden Suchfilter gesucht wird. Bei der Auswahl von Unterebene kann es zu sehr vielen Treffern kommen.



Manuelles Mapping für Benutzer

Relution prüft nach dem Verbindungsaufbau, um welches LDAP es sich handelt, beispielsweise OpenLDAP oder ein Active Directory. Daraufhin werden die entsprechenden Felder über ein Auto-Mapping vorkonfiguriert. Diese Funktion lässt sich teilweise oder ganz übersteuern, indem Manuelles Mapping von Benutzerattributen aktiviert wird.

Empfehlenswert ist zum Beispiel das Setzen eines Fremdschlüssels. Dies ist sinnvoll, wenn Benutzer ihren Namen ändern: Das Benutzerkonto bleibt so identifizierbar, Name und Mailadresse werden lediglich aktualisiert, ohne dass ein neues Konto in Relution entsteht.

Für Version 26.4.0

Das Feld objectSID eignet sich hier nicht. Es führt zu Fehlern, da es teilweise nicht interpretierbare Zeichen enthält.

Benutzer-Synchronisation

Mit Benutzerimport testen lässt sich prüfen, ob die Benutzer importiert werden können und die Filter die richtigen Ergebnisse liefern.

- Zusätzlich lässt sich der Periodische Benutzerimport aktivieren. Dies ist eine automatische Synchronisierung, die alle 24 Stunden zur gewählten Uhrzeit der Synchronisierung ausgeführt wird. Ist der periodische Import deaktiviert, werden Benutzer, die dem Suchfilter entsprechen, trotzdem bei der Anmeldung oder bei der Zuweisung zu einer Einschreibung importiert.

- Eine manuelle Synchronisierung lässt sich jederzeit starten (siehe Grundlagen →).

- Synthetische Gruppe: Hierbei handelt es sich um eine Gruppe, die durch den LDAP-Sync automatisch angelegt wird. Alle Benutzer, die über den LDAP-Provider importiert werden – bei der geplanten Synchronisation oder bei der ersten Anmeldung –, werden Mitglied dieser Gruppe.

    - Der Gruppenname setzt sich aus dem Eindeutigen Namen der Organisation in Großbuchstaben und dem eingetragenen Wert zusammen. Mit dem Standardwert `LDAP` entsteht so z. B. die Gruppe `MYORG LDAP`.
    - Bleibt das Feld leer, wird keine synthetische Gruppe angelegt.
    - Da sich LDAP-Gruppen Berechtigungen zuweisen lassen, eignet sich die synthetische Gruppe, um allen LDAP-Benutzern gemeinsam eine Rolle zuzuweisen, z. B. für die Multi-Faktor-Authentifizierung →.
- Die Option Wenn ein synchronisierter Benutzer im LDAP entfernt wurde lässt sich nur bei aktivem Periodischer Benutzerimport bearbeiten (Standard: Nichts tun). Sie greift auch, wenn ein Benutzer zwar noch im LDAP vorhanden ist, aber die Suchkriterien nicht mehr erfüllt. Drei Reaktionen stehen zur Verfügung:

    1. Nichts tun: Der Benutzer bleibt in Relution enthalten. Er kann aber nicht mehr zum Login benutzt werden, da der LDAP-Provider die Authentifizierung ablehnt.
    2. Benutzer in Relution deaktivieren: Dies ist die empfohlene Einstellung, da Benutzerkonten mit Geräten verknüpft bleiben und es nicht zu einem Datenverlust kommt, wenn die Konten versehentlich nicht mehr gefunden werden, zum Beispiel nach der Umbenennung einer Gruppe im LDAP, die ein Filter dann nicht mehr findet.
    3. Benutzer aus Relution löschen: Benutzer, die durch den Importer nicht mehr gefunden werden, werden direkt aus der Datenbank entfernt, unabhängig von eventuellen Verknüpfungen zu Geräten, Gruppen oder Klassen.

Vorsicht: Die Löschung ist unwiderruflich — betroffene Benutzer werden sofort aus der Datenbank entfernt, unabhängig von Verknüpfungen zu Geräten, Gruppen oder Klassen.

Für Version 26.4.0

Suchkriterien für Gruppen

- Suchbasis für Gruppen (Organizational Unit): Die Suchbasis für die Gruppen, relativ zur Basis-DN, zum Beispiel `OU=groups`.
- Suchfilter für Gruppen: Hier kommen konventionelle LDAP-Suchfilter zum Einsatz. Relution verwendet für Benutzereingaben immer den Platzhalter `%v`. Ein einfacher Suchfilter für Gruppen könnte zum Beispiel `(&(cn=%v)(objectClass=groupOfNames))` sein.
- Suchbereich für Gruppen: Legt fest, wie tief im Pfad nach Gruppen mit dem entsprechenden Suchfilter gesucht wird. Bei der Auswahl von Unterebene kann es zu sehr vielen Treffern kommen.

Manuelles Mapping für Gruppen

Das manuelle Mapping (Manuelles Mapping von Gruppenattributen) verhält sich bei den Gruppen wie bei den Benutzern. Häufig sind für die Fremdschlüssel (UID) das Feld `entryUUID` und für Mitglied das Feld `member` in Verwendung. Die Attribute lassen sich mit einem der oben empfohlenen LDAP-Tools oder über die Konsole mit `ldapsearch` prüfen.

Für Version 26.4.0

Gruppen-Synchronisation

Mit Gruppenimport testen lässt sich prüfen, ob die Gruppen gefunden werden.

Damit LDAP-Gruppen importiert werden, muss Gruppen von synchronisierten Benutzer importieren aktiviert sein. Relution importiert dann alle Gruppen, in denen synchronisierte Benutzer Mitglied sind und die dem Gruppenfilter entsprechen, einschließlich der Gruppen, denen diese Gruppen wiederum angehören. Ist der Schalter deaktiviert, werden nur synthetische Gruppen angelegt.

Zusätzlich lässt sich Periodischer Gruppenimport aktivieren: Dann werden alle 24 Stunden zur gewählten Uhrzeit der Synchronisierung alle Gruppen importiert, die dem Gruppenfilter entsprechen, auch ohne importierte Mitglieder. Periodischer Gruppenimport und die Uhrzeit lassen sich erst einstellen, wenn Gruppen von synchronisierten Benutzer importieren aktiviert ist.

Der Import geht immer von den Benutzern aus: Gruppen ziehen keine zusätzlichen Benutzer nach. Mitglieder einer Gruppe werden nur importiert, wenn sie selbst den Suchkriterien für Benutzer entsprechen.

> Gruppen, die bei einer erfolgreichen Synchronisierung nicht mehr gefunden werden, etwa nach einer Änderung des Gruppenfilters, werden in Relution gelöscht.

Bildung

Über die LDAP-Synchronisierung lassen sich auch Klassen erstellen, die im Bereich Bildung im Menü angezeigt werden und für die Relution Teacher Console oder in Apple Classroom genutzt werden können. Klassen, die in Relution angelegt werden sollen, sind im LDAP Gruppenobjekte. Sie müssen mindestens eine Lehrkraft oder Lehrkräftegruppe und mindestens einen Schüler oder eine Schülergruppe enthalten.

Suchkriterien für Klassen

Die Konfiguration sieht hier ähnlich aus wie bei Benutzern und Gruppen: Definiert werden eine Suchbasis, in der die Klassen enthalten sind, und ein entsprechender Suchfilter. Der Suchbereich wird wie gewohnt über das Dropdown-Menü konfiguriert.

Die Konfiguration lässt sich mit Klassenimport testen prüfen. Klassen werden später nur angelegt, wenn sie mindestens eine Lehrkraft oder Lehrkräftegruppe und mindestens einen Schüler oder eine Schülergruppe enthalten. Gruppen zählen nur, wenn sie über die Suchkriterien für Lehrkräfte- und Schülergruppen gefunden werden.

Suchkriterien für Lehrkräfte und Schüler

Hier besteht die Konfiguration ebenfalls aus der Suchbasis und einem entsprechenden Filter. Häufig werden die einzelnen Nutzertypen über Gruppenzugehörigkeiten definiert. Suchfilter können beispielsweise so aussehen:

- Lehrer: `(&(memberOf=CN=alle-lehrer,OU=groups,DC=schule,DC=local)(objectClass=person))`
- Schüler: `(&(memberOf=CN=alle-schueler,OU=groups,DC=schule,DC=local)(objectClass=person))`

Die Filter lassen sich mit Lehrkräfte-Import testen und Schüler-Import testen prüfen.

Für Version 26.4.0

Suchkriterien für Lehrkräfte- und Schülergruppen

Ab Relution 5.31 können Gruppen als Mitglieder von Klassen importiert werden. Dazu wird jeweils ein Filter für Lehrkräfte- und Schülergruppen konfiguriert. Diese Filter können ergänzend zu den Filtern für Lehrkräfte und Schüler oder an deren Stelle genutzt werden. Ist der automatische Import der Bildungsdaten aktiviert, muss je Rolle mindestens einer der beiden Filter (Benutzer- oder Gruppenfilter) gesetzt sein. Die Suchfilter können z. B. so aussehen:

- Lehrer: `(&(cn=teacher*)(objectClass=groupOfNames))`
- Schüler: `(&(cn=students*)(objectClass=groupOfNames))`

Die Filter lassen sich mit Lehrergruppen-Import testen und Schülergruppen-Import testen prüfen.

Synchronisierung der Bildungsdaten

Hier wird ebenfalls der automatische Import der Bildungsdaten konfiguriert: Mit Regelmäßiger Bildungsimport werden die Klassen alle 24 Stunden zur gewählten Uhrzeit der Synchronisierung synchronisiert. Klassen, die bei einer erfolgreichen Synchronisierung nicht mehr gefunden werden, werden in Relution gelöscht.

Organisations-Zuordnung (Global und Meta)

In der Global Organisation und in Meta-Organisationen ist es möglich, LDAP-Provider zu konfigurieren und Benutzer, Gruppen und Klassen über Zuordnungen (Objekte zu Organisationen zuordnen) in einzelne Organisationen synchronisieren zu lassen. Je Zielorganisation lassen sich Filter für Benutzer, Gruppen, Klassen, Lehrkräfte, Lehrkräftegruppen, Schüler und Schülergruppen setzen, jeweils als LDAP-Filter oder als DN-Filter. Das Ergebnis lässt sich mit Organisations-Zuordnung testen prüfen.

Die Filter einer Zuordnung verteilen nur Objekte, die bereits über die Importfilter gefunden werden. Standardmäßig werden nur Objekte synchronisiert, die zu einer Zuordnung passen; alle übrigen werden nicht importiert und als Synchronisierungsfehler gemeldet. Ist unter Organisations-Zuordnung konfigurieren die Option Nicht zugeordnete Objekte in diese Organisation synchronisieren aktiviert, landen die übrigen Objekte in der Organisation, in der der Provider angelegt ist. Passt ein Objekt zu den Filtern mehrerer Organisationen, wird es mit einem Fehler übersprungen.

Für Version 26.4.0

Meta-Organisationen

Meta-Organisationen bilden eine Hierarchie unterhalb der globalen Organisation ab. Eine Meta-Organisation bündelt mehrere untergeordnete Organisationen (Untermandanten), die die von der Meta-Organisation freigegebenen Elemente wie Apps, Richtlinien und Skripte erben. Das allgemeine Anlegen von Organisationen ist unter Organisationen anlegen → beschrieben.

Organisationstyp

Beim Anlegen einer Organisation in der globalen Organisation wird der Organisationstyp festgelegt:

- Eigenständig: Eine eigenständige Organisation wird direkt unter der globalen Organisation angelegt. Eine spätere Zuweisung zu einer Meta-Organisation ist möglich.
- Meta: Eine Meta-Organisation wird direkt unter der globalen Organisation angelegt. Andere Organisationen können ihr nach der Erstellung untergeordnet werden und die von ihr freigegebenen Elemente erben.
- Unterorganisation: Eine Unterorganisation wird der gewählten Meta-Organisation untergeordnet und übernimmt die von ihr freigegebenen Elemente. Die Meta-Organisation wird über Meta als übergeordnete Organisation wählen ausgewählt; die Angabe ist Pflicht. Eine Rückverschiebung ist nicht möglich.

Die Auswahl des Organisationstyps steht nur beim Anlegen in der globalen Organisation zur Verfügung. Organisationen, die innerhalb einer Meta-Organisation angelegt werden, werden automatisch zu deren Unterorganisationen. Beim Bearbeiten einer bestehenden Organisation lässt sich der Organisationstyp nicht ändern. Eine eigenständige Organisation kann nur über Einer Meta-Organisation zuweisen nachträglich untergeordnet werden (siehe unten).

Für Version 26.4.0

Für Meta-Organisationen gelten außerdem folgende Einschränkungen:

- Eine Meta-Organisation kann nicht wieder in eine eigenständige Organisation umgewandelt werden.
- Meta-Organisationen lassen sich nicht verschachteln: Eine Meta-Organisation kann keiner anderen Meta-Organisation untergeordnet werden.
- Die globale Organisation kann keine Meta-Organisation sein.
- Eine Meta-Organisation, der Unterorganisationen zugeordnet sind, lässt sich nicht löschen.

Vererbung an Unterorganisationen

Untergeordnete Organisationen übernehmen die Elemente, die die Meta-Organisation für alle Unterorganisationen freigibt, z. B. Apps, Richtlinien, Skripte, Gerätegruppen und Rollen. In der Meta-Organisation sind diese Elemente mit Geteilt gekennzeichnet, in den Unterorganisationen mit Von Meta. In Listen sind sie über den Tab Geteilt (Meta) bzw. Von Meta zu finden. Elemente mit Nur lokal bleiben auf die Meta-Organisation beschränkt. Geerbte Elemente lassen sich ausschließlich in der Meta-Organisation ändern.

Werden Apps meta-weit verfügbar gemacht, die bereits in anderen Organisationen vorhanden sind, weist das Portal auf diesen Konflikt hin. Für die ausgewählten Apps werden die vorhandenen Apps in den anderen Organisationen ersetzt und gelöscht.

Bestehende Organisation zuweisen

Eine eigenständige Organisation kann nachträglich einer Meta-Organisation untergeordnet werden. Diese Aktion steht nur in der globalen Organisation zur Verfügung und setzt die Berechtigung zum Bearbeiten von Organisationen voraus. In einer Meta-Organisation ist sie nicht verfügbar.

Unter `Organisationen` werden eine oder mehrere eigenständige Organisationen markiert und im Kontextmenü Einer Meta-Organisation zuweisen gewählt. Alternativ steht die Aktion in der Detailansicht einer eigenständigen Organisation zur Verfügung. Im Dialog Meta-Organisation zuweisen wird zuerst die Ziel-Meta-Organisation ausgewählt. Nach Weiter zeigt der Dialog die gewählte Meta-Organisation und unter Neue Unterorganisationen die zuzuweisenden Organisationen an; mit Bestätigen wird die Zuweisung ausgeführt.

> Die Zuweisung zu einer Meta-Organisation ist dauerhaft und kann nicht rückgängig gemacht werden. Nur eigenständige Organisationen lassen sich zuweisen.

Für Version 26.4.0

Microsoft Entra ID verknüpfen

Mit der Verknüpfung von `Microsoft Entra ID` und Relution entsteht die Grundlage für Microsoft-basierte Integrationen in der eigenen Organisation. Dazu zählen beispielsweise die Anbindung von Windows-Geräten sowie die Nutzung weiterer Microsoft-Dienste in Verbindung mit Relution.

Somit können Benutzer und Gruppen aus `Microsoft Entra ID` mit Relution synchronisiert werden. Dadurch lassen sich Benutzerkonten zentral in Microsoft verwalten und automatisch in Relution bereitstellen.

Damit sich synchronisierte Benutzer anschließend über Relution anmelden können, muss zusätzlich die OIDC-Authentifizierung → eingerichtet werden. Sollen Zugriffe über Conditional Access → abgesichert werden, sind sowohl die Verknüpfung von `Microsoft Entra ID` als auch die Einrichtung von OIDC → erforderlich.

Die dafür notwendigen Einstellungen werden teilweise in Relution und teilweise im Microsoft-Entra-Admincenter vorgenommen.

Voraussetzungen

Für die Verknüpfung von `Microsoft Entra ID` mit Relution müssen folgende Voraussetzungen erfüllt sein, wenn ausschließlich Benutzer aus `Microsoft Entra ID` mit Relution synchronisiert werden sollen:

- eine bestehende `Microsoft Entra ID`-Umgebung
- ausreichende Berechtigungen in Microsoft Entra, in der Regel die Rolle `Globaler Administrator`
- ein erreichbarer Relution Server
- eine App-Registrierung in Microsoft Entra

Für Version 26.4.0

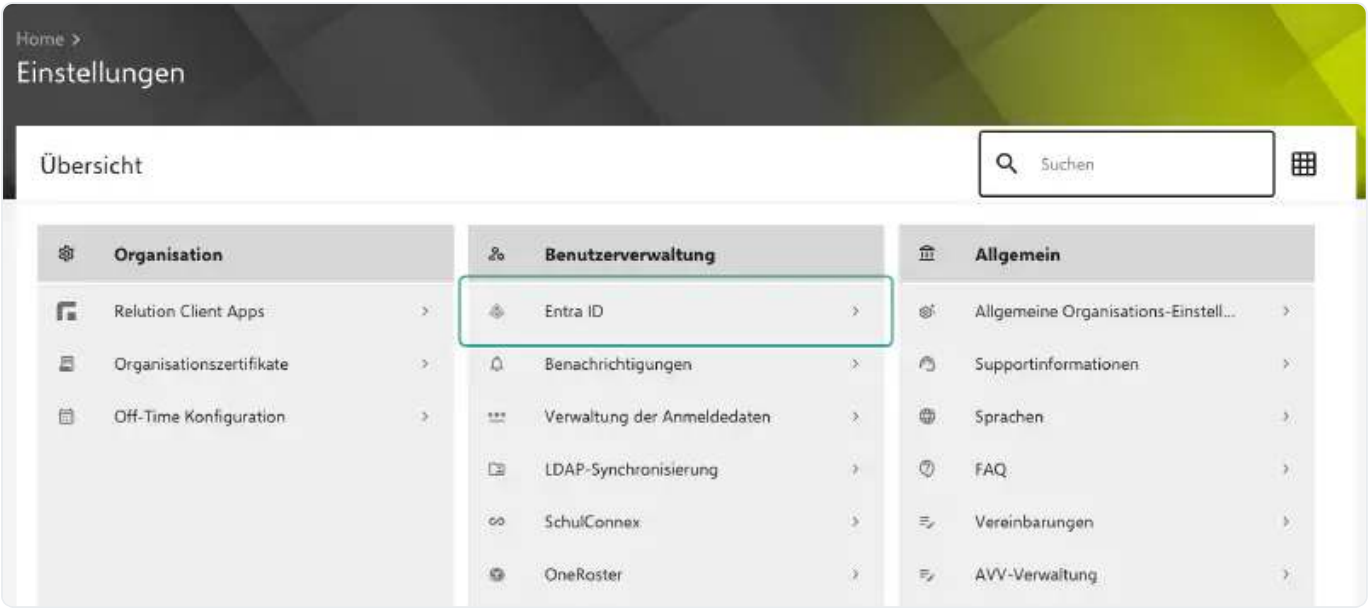
Falls zusätzlich `Windows Autopilot` oder `Entra Join` verwendet werden soll, sind außerdem folgende Voraussetzungen erforderlich:

- die Server-URL des Relution Servers, die später in Microsoft Entra hinterlegt wird
- eine angelegte MDM-Anwendung

Verknüpfung in Relution aufrufen

Im Relution-Portal befindet sich der Bereich für die Einrichtung unter `Einstellungen` → `Benutzerverwaltung` → `Entra ID`.

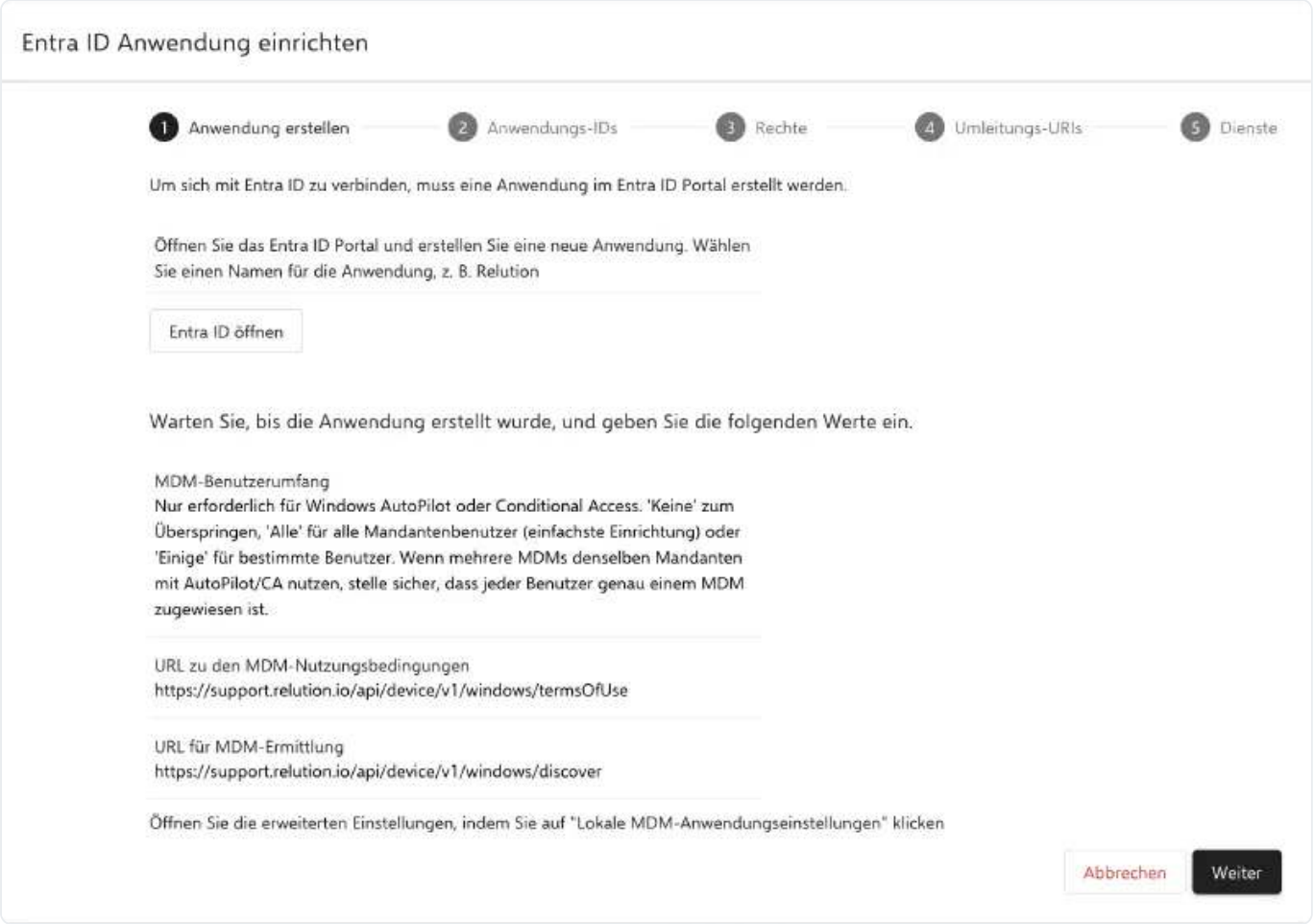
Dort unterstützt eine Anleitung bei der Konfiguration und Verknüpfung mit Microsoft Entra. Sie führt durch die Schritte Anwendung erstellen, Anwendungs-IDs, Rechte, Umleitungs-URIs und Dienste.



Anwendung erstellen

Der erste Schritt Anwendung erstellen weist darauf hin, dass für die Verbindung eine Anwendung im Entra-Portal benötigt wird. Über die Schaltfläche Entra ID öffnen wird in Microsoft Entra der Bereich `Mobilität (MDM und MAM)` geöffnet. Darunter zeigt die Relution-Anleitung die Werte, die in der MDM-Anwendung eingetragen werden:

Für Version 26.4.0



- MDM-Benutzerumfang: nur für Windows Autopilot oder Conditional Access erforderlich. Mit `Keine` wird der Bereich übersprungen, mit `Alle` gilt er für alle Benutzer des Mandanten, mit `Einige` nur für ausgewählte Benutzer. Nutzen mehrere MDM-Lösungen denselben Mandanten mit Autopilot oder Conditional Access, muss jeder Benutzer genau einer MDM-Lösung zugewiesen sein.
- URL zu den MDM-Nutzungsbedingungen: `https://<host>/api/device/v1/windows/termsOfUse`
- URL für MDM-Ermittlung: `https://<host>/api/device/v1/windows/discover`

Die MDM-Anwendung wird für `Windows Autopilot` und `Entra Join` benötigt, laut Hinweis im Portal auch für Conditional Access. Wie sie angelegt und konfiguriert wird (On-Premises-MDM-Anwendung, benutzerdefinierte Domäne, URLs), beschreibt der Artikel Windows Autopilot →.

Sollen ausschließlich Benutzer und Gruppen aus Microsoft Entra mit Relution synchronisiert werden, reicht eine normale App-Registrierung aus, und dieser Schritt wird mit Weiter übersprungen. Die App-Registrierung lässt sich über den folgenden Link erstellen: Neue App-Registrierung in Entra →

Vornehmen der Anwendungseinstellungen

Im Schritt Anwendungs-IDs werden folgende Angaben aus Microsoft Entra in die Relution-Anleitung übertragen. Sie gelten sowohl für die MDM-Anwendung als auch für eine normale App-Registrierung:

1. Anwendungs-ID (Client)
2. Verzeichnis-ID (Mandant)
3. den Wert des Geheimen Clientschlüssels (in Relution im Feld Client-Geheimnis)

Über Überprüfen in der Zeile Konfiguration überprüfen lässt sich direkt testen, ob sich Relution mit diesen Angaben bei Microsoft Entra anmelden kann.

Ist für die Organisation bereits Conditional Access eingerichtet, weist Relution beim Ändern der Verzeichnis-ID (Mandant) darauf hin, dass sich der neue Mandant auch auf die Einstellung für Bedingten Zugriff auswirkt. App-ID und Geheimnis in dieser Einstellung sind danach erneut zu prüfen.

Für Version 26.4.0

Nur bei einer MDM-Anwendung (Windows Autopilot, Entra Join) wird anschließend in den lokalen MDM-Anwendungseinstellungen zum Bearbeiten auf Anwendungs-ID-URI geklickt. Bei einer normalen App-Registrierung entfallen dieser und der folgende Schritt.

In der nachfolgenden Ansicht wird als `Anwendungs-ID-URI` die entsprechende Server-URL eingetragen.

Als Nächstes wird unter Zertifikate & Geheimnisse ein Geheimer Clientschlüssel hinzugefügt:

1. Im Tab Geheime Clientschlüssel auf Neuer geheimer Clientschlüssel klicken.
2. Im Dialogfenster `Geheimen Clientschlüssel hinzufügen` eine Beschreibung und die Gültigkeitsdauer angeben.
3. Auf Hinzufügen klicken.

Für Version 26.4.0

Wenn der Gültigkeitszeitraum abgelaufen ist, besteht keine Verbindung mehr und Relution kann nicht mehr mit Microsoft Entra kommunizieren. In diesem Fall muss ein neuer `Geheimer Clientschlüssel` für die Anwendung in Microsoft Entra erstellt und erneut in Relution hinterlegt werden.

Anschließend wird in der Übersicht im Tab `Geheime Clientschlüssel` der neue Eintrag angezeigt.

Der zugehörige `Wert` wird nur einmalig angezeigt und muss daher direkt kopiert und in Relution übertragen werden.

Für Version 26.4.0

Konfigurieren der API-Berechtigungen

Im nächsten Schritt Rechte werden die API-Berechtigungen konfiguriert. Die Schaltfläche Offene API-Berechtigungen öffnet die API-Berechtigungen der Anwendung direkt in Microsoft Entra:

Für Version 26.4.0

Je nach künftig verwendeten Microsoft-Funktionen kann es erforderlich sein, zu einem späteren Zeitpunkt weitere Berechtigungen hinzuzufügen.

Folgende Einstellungen müssen in Microsoft Entra durchgeführt werden:

1. Unter `API-Berechtigungen` → `Konfigurierte Berechtigungen` auf Berechtigung hinzufügen klicken.

2. Im Dialogfenster API-Berechtigungen anfordern unter Microsoft-APIs den Eintrag Microsoft Graph auswählen.

3. Im nächsten Schritt die Kachel Anwendungsberechtigungen auswählen.

Für Version 26.4.0

4. Für User die Berechtigung `User.Read.All` auswählen.

5. Für Group die Berechtigung `Group.Read.All` auswählen.

Für Version 26.4.0

6. Für Device die Berechtigung `Device.ReadWrite.All` auswählen und die Auswahl mit Berechtigungen hinzufügen bestätigen.

Bei den neu hinzugefügten API-Berechtigungen wird zunächst ein Ausrufezeichen als Status angezeigt. Damit die Anwendung die Berechtigungen erhält, müssen Administratoren sie einmalig über Administratorzustimmung für “” erteilen bestätigen. Anschließend wird der Status mit einem grünen Häkchen als `Gewährt` dargestellt.

Für Version 26.4.0

Über Überprüfen in der Zeile Berechtigungen überprüfen prüft Relution, ob die Berechtigungen gewährt sind. Fehlt die Zustimmung, meldet die Prüfung Berechtigungen nicht erteilt.

Definieren der Umleitungs-URI

Im Schritt Umleitungs-URIs zeigt die Relution-Anleitung die `Umleitungs-URI` an, die anschließend in Microsoft Entra für die Plattform `Web` eingetragen wird. Die Schaltfläche Authentifizierung öffnen öffnet die passende Seite der Anwendung in Microsoft Entra:

Für Version 26.4.0

1. Unter Authentifizierung auf Plattform hinzufügen klicken.
2. Im Dialogfenster Plattform konfigurieren die Kachel Web auswählen.

3. Im Bereich Web unter Umleitungs-URI hinzufügen die Server-URL eintragen.
4. Die Checkbox ID-Tokens deaktivieren.
5. Auf Speichern klicken.

Für Version 26.4.0

Über Überprüfen in der Zeile Überprüfen von Umleitungs-URIs prüft Relution, ob die Server-URL in der Anwendung eingetragen ist. Die eingetragene URI muss exakt mit der angezeigten Server-URL übereinstimmen, andernfalls meldet die Prüfung `Umleitungs-URI … nicht vorhanden`.

Damit ist die Einrichtung in Microsoft Entra abgeschlossen.

Wählen der Relution Serviceoptionen und Abschließen der Einrichtung

Im Schritt Dienste wird festgelegt, welche Dienste Relution nutzen soll. Zur Auswahl stehen die Schalter Autopilot-Registrierung aktivieren, Autopilot Geräte synchronisieren, Entra ID Benutzer synchronisieren und Entra ID Gruppen synchronisieren. Bei einer neuen Verbindung sind alle vier Schalter bereits aktiviert. Sollen nur Benutzer und Gruppen synchronisiert werden (ohne `Windows Autopilot` oder `Entra Join`), werden die Schalter Autopilot-Registrierung aktivieren und Autopilot Geräte synchronisieren deaktiviert.

Für Version 26.4.0

Mit Klick auf Speichern ist die Einrichtung und Verknüpfung von `Microsoft Entra ID` in Relution abgeschlossen.

Verbindung verwalten und synchronisieren

Nach dem Speichern zeigt `Einstellungen` → `Benutzerverwaltung` → `Entra ID` die Übersicht der Entra ID Verbindung mit Anwendungs-ID und Verzeichnis-ID. Dort stehen folgende Funktionen zur Verfügung:

- Verbindung bearbeiten: öffnet die Anleitung erneut, beispielsweise um nach Ablauf des Clientschlüssels einen neuen Wert im Feld Client-Geheimnis einzutragen.
- Verbindung überprüfen: prüft Anmeldung, Berechtigungen und Umleitungs-URI in einem Schritt.
- Verbindung löschen: entfernt die Verknüpfung mit Microsoft Entra.
- Bereich Dienste: Die vier Schalter aus der Einrichtung lassen sich hier nachträglich ändern und mit Speichern übernehmen.

Der Bereich Synchronisierung zeigt je Synchronisierung den Zeitpunkt der Letzten Synchronisierung, die Neuen Einträge, aufgetretene Fehler und die Nächste Synchronisierung. Benutzer und Gruppen werden standardmäßig einmal täglich synchronisiert, Autopilot-Geräte alle 24 Stunden.

Eine Synchronisierung lässt sich auch manuell anstoßen:

- Autopilot Geräte synchronisieren synchronisiert die in Windows Autopilot hinterlegten Geräte.
- Benutzer und Gruppen synchronisieren (im Menü der Aktionsleiste) ist nur verfügbar, wenn sowohl die Benutzer- als auch die Gruppensynchronisation aktiviert ist. Im Dialog wird der Synchronisationsmodus gewählt: Nur Änderungen (empfohlen) ruft nur die seit der letzten Synchronisierung geänderten Benutzer und Gruppen ab. Vollständige Synchronisation importiert alle Benutzer und Gruppen erneut und kann sehr lange dauern. Sie ist nur sinnvoll, wenn die Synchronisierung der Änderungen nicht das erwartete Ergebnis liefert.

In der globalen Organisation gilt die Verknüpfung systemweit, in einer Meta-Organisation metaweit. Die Übersicht zeigt das unter Benutzerbereich als Systemweit bzw. Metaweit an. Über die Organisations-Zuordnung werden dort Entra-ID-Gruppen einzelnen Organisationen zugeordnet. Die Schalter für Benutzer- und Gruppensynchronisation sind in diesem Fall gekoppelt und werden immer gemeinsam ein- oder ausgeschaltet.

Zusammenfassung

Nach Abschluss dieser Schritte ist `Microsoft Entra ID` mit Relution verknüpft. Damit können Benutzer und Gruppen aus Microsoft Entra ID mit Relution synchronisiert sowie weitere Microsoft-bezogene Funktionen genutzt werden.

Für die Anmeldung synchronisierter Benutzer an Relution muss zusätzlich die OIDC-Authentifizierung → eingerichtet werden. Dies gilt ebenfalls für die Nutzung von `Conditional Access`.

Für Version 26.4.0

OIDC mit Entra

OpenID Connect `OIDC` ist ein Identitätsprotokoll, das auf OAuth 2.0 aufbaut und eine sichere Authentifizierung sowie Autorisierung für Web- und Mobile-Anwendungen ermöglicht. Es erlaubt Nutzer, sich sicher bei verschiedenen Diensten anzumelden, während Dienstanbieter gleichzeitig auf verifizierte Identitätsinformationen zugreifen können. In diesem Artikel wird die Konfiguration von OIDC in Relution Schritt für Schritt am Beispiel von Microsoft Azure erklärt.

> Bei der Anmeldung über OIDC werden keine Klassen oder Gruppen synchronisiert. Ein Benutzer wird erst bei seinem ersten erfolgreichen Login in Relution angelegt, und nur wenn Unbekannte Benutzer in Relution anlegen aktiviert ist. Relution fügt neu angelegte Benutzer automatisch der Gruppe `<Name des Anbieters> Users` hinzu und legt diese Gruppe bei Bedarf in der Organisation an. Über diese Gruppe lassen sich Berechtigungen vergeben.

Einstellungen in Relution

OpenID Connect `OIDC` kann im Relution-Portal unter `Einstellungen` → `Benutzerverwaltung` → `OpenID Connect` konfiguriert werden. Die folgenden Screenshots zeigen eine funktionierende Konfiguration mit Microsoft Azure.

Für Version 26.4.0

Für Version 26.4.0

Für Version 26.4.0

Details zur Konfiguration

Name des Anbieters: Pflichtfeld. Wird auf dem Login Button im Relution-Portal angezeigt und kann nach dem Speichern nicht mehr geändert werden. Unbekannte Benutzer in Relution anlegen: Aktiviert die automatische Erstellung neuer, unbekannter Benutzer beim ersten Login in Relution. Standardmäßig ist der Schalter deaktiviert. Dann ist ein Login nur für Benutzer möglich, die bereits in Relution vorhanden sind. Konfiguration prüfen: Prüft vor dem Speichern, ob die Konfiguration gültig ist.

Erfolgt ein Login mit einem unbekannten Benutzer auf der Store Organisation mit aktivierter OIDC-Konfiguration, wird dieser automatisch in der Store Organisation angelegt. Bei mehreren Mandanten mit OIDC Konfiguration muss der Login über die Organisations-URL erfolgen, damit der unbekannte Benutzer in der entsprechenden Organisation angelegt wird. Diese URL wird im Portal bei den OIDC Verbindungen angezeigt.

Client-Details

ClientID Entspricht in Azure der Anwendungs-ID Client Secret Entspricht in Azure dem geheimen Clientschlüssel zur Anwendungs-ID. Beim Bearbeiten einer gespeicherten Konfiguration bleibt das Feld leer. Wird kein neuer Wert eingetragen, bleibt das bisherige Secret unverändert.

Für Version 26.4.0

Server URIs

Discovery-Endpunkt verwenden Wenn vom Provider unterstützt, erfolgt eine automatische Konfiguration der benötigten URIs Manuelle Konfiguration der Endpunkte Notwendig, sobald das automatische Discovery nicht funktioniert.

Bei Verwendung von Microsoft Azure müssen die Endpunkte manuell eingetragen werden.

- Autorisierungs-URI
  `https://login.microsoftonline.com/$-Ihre-Mandanten-ID/oauth2/v2.0/authorize`
- JWK Set URI
  `https://login.microsoftonline.com/common/discovery/keys`
- Token-URI
  `https://login.microsoftonline.com/$-Ihre-Mandanten-ID/oauth2/v2.0/token`
- Endpunkt der Sitzung beenden (optional, für die Abmeldung beim IdP, siehe Logout-Verifizierung)
  `https://login.microsoftonline.com/$-Ihre-Mandanten-ID/oauth2/v2.0/logout`

Erweiterte Konfiguration

Benutzername-Attribut vom OIDC-Provider: Das Attribut des OIDC-Providers, das den eindeutigen Benutzernamen des authentifizierten Nutzers enthält (Standard: `email`).

Benutzernamen-Attribut von Relution: Legt fest, mit welcher Relution-Benutzereigenschaft (Benutzername, E-Mail, UUID oder Fremdschlüssel (UID); Standard: E-Mail) der Wert aus dem Benutzername-Attribut vom OIDC-Provider abgeglichen wird. Bei UUID werden unbekannte Benutzer auch dann nicht angelegt, wenn Unbekannte Benutzer in Relution anlegen aktiv ist.

Autorisierung-Grant Type: Legt fest, über welchen OAuth-Mechanismus die Anwendung Zugriff erhält (Standard: `authorization_code`).

Umfang: Bestimmt als OAuth-Scope, welche Informationen oder Ressourcen von Relution über OIDC angefordert werden dürfen (Standard: `openid`, `email`, `profile`).

Erweiterte Optionen

Benutzer von OIDC abmelden, wenn er sich von Relution abmeldet: Leitet den Browser beim Ausloggen aus Relution zusätzlich zum Logout-Endpunkt des IdP weiter (Standard: deaktiviert). Details dazu stehen unter Logout-Verifizierung.

Für Version 26.4.0

Neue App-Registrierung anlegen

1. Anmeldung im Azure Portal, weiter auf Microsoft Entra ID

2. Neue `App-Registrierung` → `Neue Registrierung` für OIDC anlegen

Für Version 26.4.0

3. Anwendung benennen, Kontotyp Nur Konten in diesem Organisationsverzeichnis wählen und registrieren

Für die reine Anmeldung über OIDC sind keine zusätzlichen API-Berechtigungen und keine Administratorzustimmung nötig. Die Anwendungsberechtigungen für Microsoft Graph (z. B. `User.Read.All`) werden nur für die Verknüpfung mit Microsoft Entra ID → benötigt und dort eingerichtet.

Für Version 26.4.0

Geheimen Clientschlüssel (Client Secret) unter Zertifikate & Geheimnisse hinzufügen

1. Das benötigte Client Secret wird unter Ein Zertifikat oder Geheimnis hinzufügen erstellt

2. Über Neuer geheimer Clientschlüssel kann die Beschreibung und Gültigkeitsdauer Gültig bis festgelegt werden

Für Version 26.4.0

3. Der Client Schlüssel kann direkt kopiert werden

Wichtig: Der Clientschlüssel wird nur einmalig angezeigt! Nach Ablauf der Gültigkeit besteht keine Verbindung mehr und Relution kann nicht mit Azure kommunizieren. In diesem Fall muss ein neuer Geheimer Clientschlüssel für die Anwendung in Azure erzeugt und erneut in Relution übertragen werden.

Für Version 26.4.0

Umleitungs-URI hinzufügen

Neu in 26.4

Die Umleitungs-URI wird im Relution-Portal angezeigt sobald die Verbindung konfiguriert und gespeichert wurde.

Für Version 26.4.0

Migrationshinweis — Scoped Redirect-URIs (ab 26.4.0). Mit 26.4.0 hat sich das Schema der Redirect-URIs geändert: Login-Callbacks sind nun scoped, sodass sie am Reverse-Proxy zukünftig pfadbasiert abgesichert werden können. Welche Redirect-URIs registriert werden müssen, hängt von der jeweiligen OIDC-Konfiguration ab: Ab 26.4 neu angelegte Konfigurationen verwenden immer die scoped Redirect-URIs. Konfigurationen, die vor 26.4 angelegt wurden, verwenden weiterhin die bisherige Redirect-URI (`/login/oauth2/code/`), bis sie auf die scoped Pfade umgestellt werden (siehe Bestehende Konfigurationen umstellen).

Ab 26.5.0 laufen außerdem die Logins während einer Geräte-Einschreibung (`enrollment`), im Relution Agent (`agent`), in Relution Assets (`assets`) und im Self-Service-Portal (`selfService`) über eigene Scopes. Nutzt die Konfiguration die scoped Pfade und werden diese Logins mit OIDC genutzt, müssen die zugehörigen URIs beim Identity Provider eingetragen sein.

Wo sie zu finden sind: Die Redirect-URIs für die jeweilige Instanz werden im Relution-Portal unter `Einstellungen` → `Benutzerverwaltung` → `OpenID Connect` in der Konfiguration im Abschnitt Geltungsbereichsbeschränkte OIDC URLs angezeigt, sobald die Verbindung gespeichert wurde, und lassen sich dort kopieren. Das Portal zeigt allerdings nur die Einträge Redirect-URL (management), Redirect-URL (device) und, mit Education-Lizenz, Redirect-URL (teacher) an. Die URIs für die Geräte-Einschreibung (`/api/enrollment/`), den Relution Agent (`/api/agent/`), Relution Assets (`/api/assets/`), das Self-Service-Portal (`/api/selfService/`) und Relution als Identity Provider → (`/api/idp/`) zeigt es derzeit nicht an. Sie werden nach dem unten aufgeführten Schema manuell ergänzt, soweit die jeweilige Funktion mit OIDC genutzt wird.

Bisherige Pfade (vor 26.4 angelegte Konfigurationen, eine Redirect-URI):

```
https://<host>/login/oauth2/code/<registrationId>
```

Scoped Pfade (ab 26.4 angelegte oder umgestellte Konfigurationen, alle zutreffenden registrieren):

```
https://<host>/api/management/login/oauth2/code/<registrationId>       # Relution-
Portal
https://<host>/api/enrollment/login/oauth2/code/<registrationId>       # Geräte-
Einschreibung (ADE, User Enrollment, Android Enterprise), ab 26.5
https://<host>/api/teacher/login/oauth2/code/<registrationId>          # nur Education-
Lizenz
https://<host>/api/agent/login/oauth2/code/<registrationId>            # Relution
Agent, ab 26.5
https://<host>/api/assets/login/oauth2/code/<registrationId>           # Relution
Assets, ab 26.5
https://<host>/api/selfService/login/oauth2/code/<registrationId>      # Self-Service-
Portal, ab 26.5
https://<host>/api/idp/login/oauth2/code/<registrationId>              # Relution als
Identity Provider (Beta), ab 26.5
https://<host>/api/device/login/oauth2/code/<registrationId>           # nur 26.4.x, ab
26.5 von keinem Login mehr genutzt
```

Die `<registrationId>` ist die OIDC-Konfigurations-UUID, die in Relution angezeigt wird.

Logout-URLs: Zusätzlich zeigt das Portal im selben Abschnitt zwei Logout-URLs an. Sie sind keine Redirect-URIs:

- Logout-URL für Front-Channel: `https://<host>/api/management/v1/logout/connect/front-channel/<registrationId>`
- URL für Back-Channel-Logout: `https://<host>/api/management/logout/connect/back-channel/<registrationId>`

Bestehende Konfigurationen umstellen

Konfigurationen, die vor 26.4 angelegt wurden, verwenden nach dem Update weiterhin die bisherige Redirect-URI. In der Konfiguration erscheint dann zusätzlich der Abschnitt OIDC bisherige URLs mit der aktuell aktiven Redirect-URL und der bisherigen URL für Back-Channel-Logout. Die Umstellung erfolgt in zwei Schritten:

1. Alle zutreffenden scoped URIs werden zur bestehenden Entra App-Registrierung hinzugefügt. Die bisherige URI bleibt vorerst eingetragen.
2. In Relution wird unter `Einstellungen` → `Benutzerverwaltung` → `OpenID Connect` die Konfiguration geöffnet, im Abschnitt OIDC bisherige URLs auf Bereichbeschränkte OIDC-Pfade aktivieren geklickt und der folgende Dialog bestätigt.

> Die Umstellung kann nicht rückgängig gemacht werden. Danach verwendet Relution für diese Konfiguration nur noch die scoped URIs. Fehlt eine davon beim Identity Provider, schlagen die betroffenen Logins fehl.

Bei neu angelegten Konfigurationen erscheint der Abschnitt nicht, da sie die scoped URIs von Anfang an verwenden. Die bisherige URI ist veraltet und kann in einer zukünftigen Version entfernt werden.

Redirect-URI für die Geräte-Einschreibung

Neu in 26.5

Ab Relution 26.5.0 laufen alle Logins während einer Einschreibung über den eigenen Scope `enrollment`. Das betrifft die Automatische Geräteregistrierung (ADE, im Portal: DEP) von Apple, das Apple Account-Driven User Enrollment, die Android Enterprise Einschreibung sowie die Anmeldung im Android Enterprise DPC. Bei Konfigurationen mit scoped Pfaden funktionieren diese Logins nur, wenn die oben aufgeführte `/api/enrollment/`-URI beim Identity Provider registriert ist. Konfigurationen mit den bisherigen Pfaden nutzen auch für Einschreibungen weiterhin die bisherige URI.

Fehlerbild bei fehlender URI: Die Anmeldung am Relution-Portal funktioniert weiterhin, da sie über die `/api/management/`-URI läuft. Erst die Einschreibung eines Geräts schlägt fehl, beispielsweise die ADE-Einschreibung eines Mac mit der Meldung `AADSTS50011: The redirect URI ... does not match`. Tritt dieser Fehler bei einer Konfiguration mit scoped Pfaden während einer Einschreibung auf, fehlt die `/api/enrollment/`-URI in der Entra App-Registrierung.

Für Version 26.4.0

Backchannel Logout

Relution unterstützt den Backchannel Logout ab Server Version 5.32.0

Beispiel-Szenario: Ein Benutzer ist gleichzeitig über SSO bei mehreren Anwendungen angemeldet. Beim Logout vom SSO-Dienst sorgt der Backchannel Logout dafür, dass die Sitzungen in allen anderen Anwendungen ebenfalls beendet werden, auch wenn diese im Hintergrund laufen.

Voraussetzungen für Entra Benutzer für OIDC

Damit die Anmeldung via OIDC mit einem Entra Benutzer funktioniert, muss bei dem Entra Benutzer zwingend eine E-Mail-Adresse hinterlegt sein.

Für Version 26.4.0

Logout-Verifizierung

Vor der Inbetriebnahme werden die Logout-Pfade überprüft:

- Abmeldung beim IdP beim Ausloggen aus Relution: Nach Klick auf Ausloggen in Relution wird die Sitzung widerrufen. Der Browser wird nur dann zusätzlich zum Logout-Endpunkt des IdP weitergeleitet, wenn unter Erweiterte Optionen der Schalter Benutzer von OIDC abmelden, wenn er sich von Relution abmeldet aktiviert ist und ein Endpunkt zum Beenden der Sitzung bekannt ist. Da die Endpunkte für Entra manuell konfiguriert werden, muss dafür das Feld Endpunkt der Sitzung beenden ausgefüllt sein.
- Front-Channel-Logout: Meldet sich der Benutzer beim IdP ab, ruft der IdP die im Portal angezeigte Logout-URL für Front-Channel auf und Relution widerruft die Sitzung. Dafür muss diese URL beim IdP hinterlegt sein.
- Back-Channel-Logout: Der IdP sendet eine Logout-Benachrichtigung an die URL für Back-Channel-Logout — die Sitzung wird ohne Benutzerinteraktion widerrufen.

Durch Tests dieser Pfade wird sichergestellt, dass eine vom IdP initiierte Sitzungsbeendigung (z. B. über die IdP-Administrationskonsole) korrekt an Relution weitergegeben wird.

Relution als Identity Provider

Relution kann ab Version 26.5.0 als OpenID Connect / OAuth2 Identity Provider auftreten: Client-Anwendungen werden direkt in Relution registriert, sodass sich Benutzer mit ihrem bestehenden Relution-Konto bei allen verbundenen Anwendungen anmelden können.

Die Konfiguration erfolgt unter `Einstellungen` → `Identitätsanbieter`. Die Seite ist nur mit der Berechtigung zum Lesen von IdP-Clients sichtbar; für das Registrieren, Bearbeiten und Löschen von Clients sind die jeweiligen Berechtigungen erforderlich.

Das Feature befindet sich aktuell in einer Beta-Phase und kann sich noch ändern. Feedback, Fragen und Anregungen sind willkommen.

Aktuell werden ausschließlich vertrauliche (confidential) OIDC-Clients unterstützt – öffentliche Clients (z. B. Single-Page-Apps oder native Apps ohne Client Secret, wie sie etwa von Zammad verwendet werden) folgen in einer späteren Version.

Funktionsumfang

Für Version 26.4.0

- Standardisierter Login-Ablauf über den Authorization-Code-Flow mit PKCE; Refresh-Token werden unterstützt.
- Je Client konfigurierbare Scopes (`profile`, `email`, `phone`, `relution`) inklusive Zustimmungsbildschirm (Consent Screen) für die Benutzer. Der Scope `relution` liefert Relution-spezifische Daten (z. B. Organisationszugehörigkeit). Der Scope `phone` kann zwar aktiviert werden, liefert derzeit aber keine zusätzlichen Claims (z. B. keine Telefonnummer).
- Übergreifende Abmeldung (Single Sign-Out): Sowohl RP-initiiertes Logout als auch OIDC Back-Channel Logout 1.0 werden unterstützt.
- Signaturschlüssel (JWK): Die Schlüssel, mit denen Tokens signiert werden, werden automatisch von Relution verwaltet und regelmäßig erneuert (ein aktiver Schlüssel wird nach vier Monaten durch einen neuen abgelöst) – hierum muss sich nicht gekümmert werden.

Signaturschlüssel rotieren und widerrufen

Die Signaturschlüssel werden im Bereich Signaturschlüssel der Seite `Einstellungen` → `Identitätsanbieter` verwaltet. Dieser Bereich steht nur in der globalen Organisation zur Verfügung; in Meta- und Unterorganisationen wird er nicht angezeigt.

Die automatische Rotation deckt den normalen Betrieb vollständig ab. Für Ausnahmefälle (z. B. bei einem Sicherheitsvorfall) stehen zwei manuelle Eingriffe zur Verfügung:

- Schlüssel rotieren: Es wird ein neuer aktiver Schlüssel erstellt, der bisherige wird außer Betrieb genommen (Status Wird abgelöst). Bereits ausgestellte Tokens bleiben bis zu ihrem Ablauf gültig. Eine erneute Rotation ist frühestens fünf Minuten nach der letzten möglich.
- Widerrufen: Der ausgewählte Schlüssel wird sofort aus dem veröffentlichten Schlüsselsatz entfernt. Dabei ist zu beachten, dass verbundene Anwendungen (Relying Parties) den zuvor gültigen Schlüssel unter Umständen noch eine Zeit lang zwischengespeichert haben und Tokens damit erst nach Ablauf dieses Caches als ungültig erkannt werden.

Für Version 26.4.0

Endpunkte für die Einbindung

Im Bereich Anbieter oben auf der Seite `Einstellungen` → `Identitätsanbieter` werden die Aussteller-URL (Issuer-URL), das Discovery-Dokument (`.well-known/openid-configuration`) und die JWKS-URI angezeigt und können direkt kopiert werden. Weitere technische Endpunkte (z. B. der Token-Endpunkt) lassen sich bei Bedarf über das Discovery-Dokument ermitteln.

IdP-Verkettung

Relution kann als Identity Provider auch mit einem vorgelagerten Identity Provider verkettet werden (z. B. Microsoft Entra ID → Relution → angebundene Anwendung).

Client registrieren

Für jede angebundene Anwendung wird über Client registrieren ein eigener Client angelegt:

- Client-Name: Frei wählbar, wird Benutzern auf dem Consent Screen angezeigt und dient Administratoren zur Unterscheidung mehrerer Clients.
- ClientID und Client-Geheimnis (Client Secret): Werden automatisch generiert und von der anbindenden Anwendung (Relying Party) benötigt. Die Anwendung authentifiziert sich damit per `client_secret_basic` oder `client_secret_post`. Das Client-Geheimnis wird nur einmal direkt nach dem Anlegen des Clients angezeigt und muss dann kopiert werden; es lässt sich später nicht erneut abrufen. Geht es verloren, kann in der Liste Registrierte Clients über Geheimnis neu generieren ein neues erzeugt werden (ebenfalls nur einmal angezeigt). Dabei wird das bisherige Geheimnis ungültig und alle bestehenden Token des Clients werden widerrufen.
- Aktiviert: Ein deaktivierter Client lehnt neue Anmeldungen und das Erneuern von Tokens per Refresh-Token ab.
- PKCE erforderlich: Standardmäßig aktiviert. Unterstützt die anbindende Anwendung kein PKCE, kann die Option für den jeweiligen Client deaktiviert werden.
- Umleitungs-URIs (Redirect-URIs): Werden von der anbindenden Anwendung vorgegeben und müssen entsprechend hinterlegt werden.
- Abmelde-Rückleitungsadressen (Post-Logout-Redirect-URIs): Adressen, zu denen die Anwendung den Browser nach einem RP-initiierten Logout umleiten darf.
- Back-Channel-Abmelde-URL: Ist sie gesetzt, benachrichtigt Relution die Anwendung im Hintergrund, sobald die Sitzung des Clients endet. Bleibt leer, wenn die Anwendung kein Back-Channel Logout unterstützt.
- Access-Token-TTL und Refresh-Token-TTL: Gültigkeitsdauer der ausgestellten Tokens. Im Formular sind für neue Clients 5 Minuten bzw. 1 Tag vorbelegt; zulässig sind 1 bis 60 Minuten für Access-Tokens und 1 bis 90 Tage für Refresh-Tokens.
- Berechtigungen (Scopes): Je Scope wird Deaktiviert, Optional oder Erforderlich gewählt. Standardmäßig sind `profile` und `email` erforderlich, `phone` und `relution` deaktiviert. `openid` ist immer aktiv (Immer gewährt). Das Aktivieren macht einen Scope nur verfügbar, die anbindende Anwendung muss ihn im Login-Ablauf auch anfragen. Fehlt in der Anfrage `openid` oder ein erforderlicher Scope, wird die Anmeldung mit dem Fehler `invalid_scope` abgelehnt. Optionale Scopes werden nur gewährt, wenn die Anwendung sie anfragt und sie auf dem Consent Screen nicht abgelehnt werden.
- Admin-Zustimmung für alle Benutzer erteilen (Admin Consent): Die Zustimmung zu allen Scopes eines Clients kann bereits durch Administratoren im Voraus erteilt werden (nur als Ganzes, nicht je einzelnem Scope) – Benutzer werden dann beim ersten Login bei der Anwendung nicht mehr über den Consent Screen befragt. Ist die Option aktiviert, lassen sich Scopes nur noch als Deaktiviert oder Erforderlich konfigurieren. Scopes, die zuvor auf Optional standen, werden dabei automatisch auf ihren Standardwert zurückgesetzt (`profile` und `email`: Erforderlich; `phone` und `relution`: Deaktiviert).

Nicht mehr benötigte Clients werden in der Liste Registrierte Clients gelöscht.

Für Version 26.4.0

Für Version 26.4.0

Für Version 26.4.0

Sichtbarkeit je Organisationsebene

Die Organisationsebene, auf der ein Client registriert wird, bestimmt, welche Benutzer sich darüber anmelden können:

- Global: Alle Benutzer im gesamten System können sich anmelden.
- Meta-Organisation: Alle Benutzer der Meta-Organisation sowie ihrer Unterorganisationen können sich anmelden.
- Unterorganisation: Nur Benutzer der jeweiligen Unterorganisation können sich anmelden.

Token-Vorschau

Für die aktuelle Scope-Konfiguration eines Clients kann eine Vorschau der resultierenden Token-Claims eingesehen werden – so lässt sich vorab prüfen, welche Informationen eine verbundene Anwendung im Token erhalten würde.

Die Scopes liefern folgende Claims:

Scope	Claims
`openid`	`sub` (Benutzer-ID), `amr` (Anmeldemethode), bei vorgelagertem Identity Provider zusätzlich `idp`
`profile`	`name`, `given_name`, `family_name`, `preferred_username`, `locale`, `updated_at`
`email`	`email`
`relution`	UUID, Name und eindeutiger Name der Organisation des Benutzers
`phone`	derzeit keine

Erteilte Zustimmungen

Benutzer sehen in ihrem Profil im Reiter Autorisierte Anwendungen, welchen Anwendungen sie welche Berechtigungen erteilt haben, und können den Zugriff dort widerrufen. Administratoren mit der entsprechenden Berechtigung finden denselben Bereich in den Details eines Benutzers. Beim Widerruf werden auch die bestehenden Autorisierungen der Anwendung für diesen Benutzer entfernt, sodass sich die Anwendung keine neuen Tokens mehr per Refresh-Token holen kann; beim nächsten Login wird die Zustimmung erneut abgefragt.

Für Version 26.4.0

Protokollierung

Anmeldungen über den Identity Provider werden sowohl im Audit-Log als auch in der Login-Historie der jeweiligen Benutzer erfasst. In der Login-Historie weist die Spalte IdP-Client aus, über welchen Client die Anmeldung erfolgte.

OIDC mit Workspace

OpenID Connect `OIDC` ist ein Identitätsprotokoll, das auf OAuth 2.0 aufbaut und eine sichere Authentifizierung sowie Autorisierung für Web- und Mobile-Anwendungen ermöglicht.
Es erlaubt Nutzer, sich sicher bei verschiedenen Diensten anzumelden, während Dienstanbieter gleichzeitig auf verifizierte Identitätsinformationen zugreifen können.

In dieser Anleitung wird die Konfiguration von OIDC in Relution am Beispiel von Google Workspace erläutert.

> Bei der Anmeldung über OIDC werden keine Klassen oder Gruppen synchronisiert. Benutzer werden erst beim ersten erfolgreichen Login in Relution angelegt, und nur dann, wenn in der OIDC-Konfiguration der Schalter Unbekannte Benutzer in Relution anlegen aktiviert ist. Ist er deaktiviert (Standard), ist ein Login nur für Benutzer möglich, die bereits in Relution vorhanden sind. Neu angelegte Benutzer fügt Relution automatisch der Gruppe `<Name des Anbieters> Users` hinzu, über die sich Berechtigungen vergeben lassen.

Einrichtung Projekt und Client (Google Cloud Console)

Zunächst muss in der Google Cloud Console eine Anwendung registriert werden, um die erforderlichen Anmeldedaten zu erhalten.

Für Version 26.4.0

1. Unter console.cloud.google.com → anmelden.

2. Ein neues Projekt erstellen oder ein bestehendes auswählen.

Für Version 26.4.0

3. Im Menü zu `APIs & Services` → `OAuth consent screen` navigieren und diesen bei Bedarf konfigurieren.

4. Zu Credentials wechseln, auf Create Credentials klicken und OAuth client ID auswählen.

Für Version 26.4.0

5. Als Application type die Option Web application wählen.

6. Unter Authorized JavaScript origins die eigene Server-URL hinterlegen (z. B. `https://support.relution.io`).
   Hinweis: Das Feld für die Authorized redirect URIs vorerst offen lassen oder vorläufig die URL eintragen; diese wird später mit den Redirect-URIs aus Relution aktualisiert.

Für Version 26.4.0

7. Nach dem Speichern wird die Client ID angezeigt. Diese kopieren.

8. Den neu erstellten Client erneut bearbeiten, um die Details einzusehen.

Für Version 26.4.0

9. Das Client Secret kopieren. ID und Secret für die spätere Verwendung in Relution sicher aufbewahren.

Für Version 26.4.0

Einrichtung SSO (Google Admin Console)

Parallel dazu muss das Single Sign-On (SSO) Profil in der Admin-Konsole hinterlegt werden.

1. Zur Google Admin Console → navigieren.
2. Unter `Security` → `Authentication` → `SSO with third-party IdP` ein neues OIDC-Profil erstellen.

Für Version 26.4.0

3. Die Client ID und das Client Secret aus dem vorherigen Kapitel eingeben.
   - Für die Issuer URL sowie die Change password URL die eigene Relution-Server-URL verwenden (z. B. `https://support.relution.io`).

OIDC Einrichtung in Relution

Nun werden die gesammelten Daten in Relution eingepflegt, um die Brücke zu Google zu schlagen.

Für Version 26.4.0

1. In Relution die OIDC-Einstellungen unter `Einstellungen` → `Benutzerverwaltung` → `OpenID Connect` öffnen.

Für Version 26.4.0

Für Version 26.4.0

Für Version 26.4.0

2. Unter Name des Anbieters eine eindeutige Bezeichnung vergeben (z. B. „Google Workspace“). Der Name erscheint auf dem Login-Button und lässt sich nach dem Speichern nicht mehr ändern.

3. Bei Bedarf Unbekannte Benutzer in Relution anlegen aktivieren, damit neue Benutzer beim ersten Login automatisch angelegt werden.

4. Die Client ID und das Client Secret aus der Google Cloud Console in die Felder ClientID und Client Secret eintragen.

5. Im Abschnitt Server URIs die Option Discovery-Endpunkt verwenden wählen und im Feld Issuer URI die URL `https://accounts.google.com` eintragen.

6. Die Konfiguration kurz speichern und erneut öffnen, um die generierten Felder zu sehen.

7. Im Abschnitt Geltungsbereichsbeschränkte OIDC URLs alle angezeigten Redirect-URL-Einträge kopieren (je ein Eintrag für `management` und `device`, mit Education-Lizenz zusätzlich `teacher`).

8. Zurück zur Google Cloud Console → wechseln.

Für Version 26.4.0

9. Den eigenen OAuth-Client bearbeiten und unter Authorized redirect URIs alle gerade aus Relution kopierten URLs eintragen. Zusätzlich die Redirect-URIs ergänzen, die das Portal nicht anzeigt, mindestens die für die Geräte-Einschreibung (`/api/enrollment/`), siehe Scoped Redirect-URIs.

Für Version 26.4.0

Unter Erweiterte Konfiguration wird festgelegt, wie Relution den angemeldeten Benutzer zuordnet: Das Benutzername-Attribut vom OIDC-Provider (Standard: `email`) wird mit der im Feld Benutzernamen-Attribut von Relution gewählten Benutzereigenschaft abgeglichen (Benutzername, E-Mail, UUID oder Fremdschlüssel (UID); Standard: E-Mail). Bei UUID werden keine unbekannten Benutzer angelegt. Der Umfang ist standardmäßig `openid`, `email`, `profile`. Über Konfiguration prüfen lässt sich die Konfiguration vor dem Speichern validieren.

Scoped Redirect-URIs

Neu in 26.4

Migrationshinweis — Scoped Redirect-URIs (ab 26.4.0). Mit 26.4.0 hat sich das Schema der Redirect-URIs geändert: Login-Callbacks sind nun scoped, sodass sie am Reverse-Proxy zukünftig pfadbasiert abgesichert werden können. Welche Redirect-URIs verwendet werden, hängt davon ab, ob die OIDC-Konfiguration noch die bisherigen Pfade nutzt: Ab 26.4 neu angelegte Konfigurationen verwenden immer die scoped Redirect-URIs. Konfigurationen, die vor 26.4 angelegt wurden, verwenden weiterhin die bisherige Redirect-URI (`/login/oauth2/code/`), bis sie auf die scoped Pfade umgestellt werden (siehe Bestehende Konfigurationen umstellen).

Ab 26.5.0 laufen außerdem die Logins während einer Geräte-Einschreibung (`enrollment`), im Relution Agent (`agent`), in Relution Assets (`assets`) und im Self-Service-Portal (`selfService`) über eigene Scopes. Nutzt die Konfiguration die scoped Pfade und werden diese Logins mit OIDC genutzt, müssen die zugehörigen URIs beim Identity Provider eingetragen sein.

Wo sie zu finden sind: Die Redirect-URIs für die eigene Instanz werden im Relution-Portal unter `Einstellungen` → `Benutzerverwaltung` → `OpenID Connect` in der Konfiguration im Abschnitt Geltungsbereichsbeschränkte OIDC URLs angezeigt, sobald die Verbindung gespeichert wurde, und lassen sich dort kopieren. Das Portal zeigt allerdings nur die Einträge Redirect-URL (management), Redirect-URL (device) und, mit Education-Lizenz, Redirect-URL (teacher) an. Die URIs für die Geräte-Einschreibung (`/api/enrollment/`), den Relution Agent (`/api/agent/`), Relution Assets (`/api/assets/`), das Self-Service-Portal (`/api/selfService/`) und Relution als Identity Provider → (`/api/idp/`) zeigt es derzeit nicht an. Sie werden nach dem unten aufgeführten Schema manuell ergänzt, soweit die jeweilige Funktion mit OIDC genutzt wird.

Bisherige Pfade (vor 26.4 angelegte Konfigurationen, eine Redirect-URI):

```
https://<host>/login/oauth2/code/<registrationId>
```

Scoped Pfade (ab 26.4 angelegte oder umgestellte Konfigurationen, alle zutreffenden registrieren):

```
https://<host>/api/management/login/oauth2/code/<registrationId>       # Relution-
Portal
https://<host>/api/enrollment/login/oauth2/code/<registrationId>       # Geräte-
Einschreibung (ADE, User Enrollment, Android Enterprise), ab 26.5
https://<host>/api/teacher/login/oauth2/code/<registrationId>          # nur Education-
Lizenz
https://<host>/api/agent/login/oauth2/code/<registrationId>            # Relution
Agent, ab 26.5
https://<host>/api/assets/login/oauth2/code/<registrationId>           # Relution
Assets, ab 26.5
https://<host>/api/selfService/login/oauth2/code/<registrationId>      # Self-Service-
Portal, ab 26.5
https://<host>/api/idp/login/oauth2/code/<registrationId>              # Relution als
Identity Provider (Beta), ab 26.5
https://<host>/api/device/login/oauth2/code/<registrationId>           # nur 26.4.x, ab
26.5 von keinem Login mehr genutzt
```

Die `<registrationId>` ist die OIDC-Konfigurations-UUID, die in Relution angezeigt wird.

Logout-URLs: Zusätzlich zeigt das Portal im selben Abschnitt zwei Logout-URLs an. Sie sind keine Redirect-URIs:

- Logout-URL für Front-Channel: `https://<host>/api/management/v1/logout/connect/front-channel/<registrationId>`
- URL für Back-Channel-Logout: `https://<host>/api/management/logout/connect/back-channel/<registrationId>`

Bestehende Konfigurationen umstellen

Konfigurationen, die vor 26.4 angelegt wurden, verwenden nach dem Update weiterhin die bisherige Redirect-URI. In der Konfiguration erscheint dann zusätzlich der Abschnitt OIDC bisherige URLs mit der aktuell aktiven Redirect-URL und der bisherigen URL für Back-Channel-Logout. Die Umstellung erfolgt in zwei Schritten:

1. Alle zutreffenden scoped URIs werden zum bestehenden Google OAuth-Client hinzugefügt. Die bisherige URI bleibt vorerst eingetragen.
2. In Relution wird unter `Einstellungen` → `Benutzerverwaltung` → `OpenID Connect` die Konfiguration geöffnet, im Abschnitt OIDC bisherige URLs auf Bereichbeschränkte OIDC-Pfade aktivieren geklickt und der folgende Dialog bestätigt.

> Die Umstellung kann nicht rückgängig gemacht werden. Danach verwendet Relution für diese Konfiguration nur noch die scoped URIs. Fehlt eine davon beim Identity Provider, schlagen die betroffenen Logins fehl.

Bei neu angelegten Konfigurationen erscheint der Abschnitt nicht, da sie die scoped URIs von Anfang an verwenden. Die bisherige URI ist veraltet und kann in einer zukünftigen Version entfernt werden.

Redirect-URI für die Geräte-Einschreibung

Neu in 26.5

Ab Relution 26.5.0 laufen alle Logins während einer Einschreibung über den eigenen Scope `enrollment`. Das betrifft die Automatische Geräteregistrierung (ADE, im Portal: DEP) von Apple, das Apple Account-Driven User Enrollment, die Android Enterprise Einschreibung sowie die Anmeldung im Android Enterprise DPC. Bei Konfigurationen mit scoped Pfaden funktionieren diese Logins nur, wenn die oben aufgeführte `/api/enrollment/`-URI beim Identity Provider registriert ist. Konfigurationen mit den bisherigen Pfaden nutzen auch für Einschreibungen weiterhin die bisherige URI.

Fehlerbild bei fehlender URI: Die Anmeldung am Relution-Portal funktioniert weiterhin, da sie über die `/api/management/`-URI läuft. Erst die Einschreibung eines Geräts schlägt fehl, und zwar mit einer Meldung zur ungültigen Redirect-URI (`invalid_redirect_uri`, bei Google `Error 400: redirect_uri_mismatch`). Tritt dieser Fehler bei einer Konfiguration mit scoped Pfaden während einer Einschreibung auf, fehlt die `/api/enrollment/`-URI im Google OAuth-Client.

Für Version 26.4.0

Backchannel Logout

Relution unterstützt den Backchannel Logout ab der Server-Version 5.32.0.

Szenario: Ein Benutzer ist über SSO bei mehreren Anwendungen gleichzeitig angemeldet. Sobald die Abmeldung beim zentralen SSO-Dienst erfolgt, sorgt der Backchannel Logout dafür, dass auch die Sitzungen in Relution und anderen angebundenen Anwendungen im Hintergrund sicher beendet werden.

Logout-Verifizierung

Vor der Inbetriebnahme werden die Logout-Pfade überprüft:

- Abmeldung beim IdP beim Ausloggen aus Relution: Nach Klick auf Ausloggen wird die Sitzung in Relution widerrufen. Ist unter Erweiterte Optionen der Schalter Benutzer von OIDC abmelden, wenn er sich von Relution abmeldet aktiv (Standard: aus) und ist ein Endpunkt zum Beenden der Sitzung bekannt (manuell im Feld Endpunkt der Sitzung beenden hinterlegt oder per Discovery vom IdP gemeldet), wird der Browser zusätzlich zum Logout-Endpunkt des IdP weitergeleitet.
- Front-Channel-Logout: Meldet sich der Benutzer beim IdP ab, ruft der IdP die im Portal angezeigte Logout-URL für Front-Channel auf und Relution widerruft die Sitzung. Dafür muss diese URL beim IdP hinterlegt sein.
- Back-Channel-Logout: Der IdP sendet eine Logout-Benachrichtigung an die URL für Back-Channel-Logout — die Sitzung wird ohne Benutzerinteraktion widerrufen.

Durch Tests dieser Pfade wird sichergestellt, dass eine vom IdP initiierte Sitzungsbeendigung (z. B. über die IdP-Administrationskonsole) korrekt an Relution weitergegeben wird.

Für Version 26.4.0

Off-Time Konfiguration

In der Version 5.23 und darüber hinaus ermöglicht die Off-Time-Konfiguration in Relution Benutzern mit den entsprechenden Berechtigungen (standardmäßig den Rollen Administrator und Device Manager einer Organisation) das Einpflegen von Schulferienkalendern für Bundesländer sowie das Hinzufügen eigener Termine, entweder manuell oder durch Hochladen einer bestehenden Kalenderdatei. Richtlinien, in denen die Off-Time aktiviert ist, sind während dieser Zeiträume deaktiviert.

Konfiguration

Die Off-Time-Konfiguration befindet sich innerhalb einer Organisation unter `Einstellungen` → `Off-Time Konfiguration`. In der globalen Organisation steht sie nicht zur Verfügung.

Schulferienkalender synchronisieren

Über den Schalter Schulferienkalender synchronisieren (nur für Deutschland) und die Auswahl des Bundeslands wird die Synchronisation aktiviert und mit Speichern übernommen. Übernommen werden die Ferien des laufenden und des folgenden Jahres; danach aktualisiert der Server die Einträge automatisch. Über die Schaltfläche neben Letzte Off-Time-Synchronisation lässt sich die Synchronisation manuell starten. Wird die Synchronisation deaktiviert, werden alle synchronisierten Einträge gelöscht.

Für Version 26.4.0

Für Version 26.4.0

Schulferienkalender sind nur für Deutschland verfügbar.

Eigene Zeiträume anlegen oder importieren

Über Hinzufügen öffnet sich der Dialog Off-Time Konfigurieren. Im Schritt Art der Ferienzeit wird zwischen Manuell und Importieren gewählt:

- Manuell: Es werden ein Name und der Benutzerdefinierte Off-Time Zeitraum mit Start- und Enddatum angegeben.
- Importieren: Es wird eine Kalenderdatei hochgeladen. Folgende Formate werden unterstützt: `.ical`, `.ics`, `.ifb`, `.icalendar`. Übernommen werden nur ganztägige Termine mit Titel; der Titel wird zum Namen der Off-Time.

Die Liste zeigt für jeden Eintrag Name, Startdatum, Enddatum und Quelle (manuell, importiert mit dem Namen des Kalenders oder Synchronisiert für ein Bundesland). Vergangene Einträge werden ausgegraut dargestellt. Einträge lassen sich bearbeiten und löschen; über das Kontextmenü können die Off-Times als iCalendar-Datei (Off-Times in iCalendar exportieren) oder als CSV exportiert werden. Abgelaufene Off-Times werden standardmäßig zwei Jahre nach ihrem Ende automatisch entfernt.

Für Version 26.4.0

Anwendung in Richtlinien

Beim Erstellen oder Ändern einer Richtlinie lässt sich der Schalter Off-Time Konfiguration aktivieren. Ist er aktiviert, ist die Richtlinie während aller in der Off-Time-Konfiguration hinterlegten Zeiträume (z. B. Schulferien) deaktiviert und wird nicht auf die Geräte angewendet. Das gilt auch, wenn keine zeitbasierte Steuerung eingerichtet ist. Ausgewertet werden die Zeiträume in der Zeitzone der Richtlinie, die bei aktivierter Off-Time auch ohne zeitbasierte Steuerung festgelegt werden kann; ohne eigene Zeitzone gilt die Zeitzone des Servers.

Für Version 26.4.0

Die Off-Time Konfiguration hat eine höhere Priorität als eine zeitbasierte Richtlinie: Während einer Off-Time bleibt die Richtlinie auch innerhalb ihres zeitbasierten Zeitfensters deaktiviert.

Organisationszertifikate

Um mit dem Apple APNS-Dienst zu arbeiten — der für Push-Benachrichtigungen und die Übermittlung von Profilen an eingeschriebene Apple-Geräte verantwortlich ist — benötigt Relution ein signiertes MDM-Push-Zertifikat. Ist kein APNS-Zertifikat konfiguriert, ist die Registrierung von Apple-Geräten deaktiviert, und das Benachrichtigungscenter meldet APNS-Zertifikat fehlt. Vor und nach dem Ablauf des Zertifikats erscheinen die Hinweise APNS-Zertifikat läuft bald ab bzw. APNS-Zertifikat ist abgelaufen.

Für Version 26.4.0

Ein bestehendes APNS-Zertifikat sollte immer erneuert statt neu erstellt werden. Wird ein Zertifikat mit anderem Push-Topic hochgeladen, behalten bereits eingeschriebene Geräte ihr altes Zertifikat; läuft dieses ab, können sie nicht mehr mit Relution kommunizieren und müssen neu eingeschrieben werden. Beim Wechsel vom Relution-Standardzertifikat zu einem eigenen Zertifikat nutzen bestehende Geräte bis zur Neueinschreibung weiterhin das Standardzertifikat.

Angaben auf der Seite

Im Bereich APNS zeigt die Seite unter `Einstellungen` → `Organisationszertifikate` für das hinterlegte Zertifikat das Push-Topic (Existierendes Zertifikat), das Ablaufdatum (gültig bis) und den zugehörigen Apple Account an. Ist kein Zertifikat hinterlegt, erscheint der Hinweis Kein Zertifikat konfiguriert. Über die Schaltfläche Starten öffnet sich der Assistent APNS-Zertifikat bearbeiten.

In regulären Organisationen zeigt der Bereich Push Zertifikat für App Store zusätzlich das Push-Zertifikat für den App Store mit Ablaufdatum an; dieser Bereich dient nur der Anzeige.

Ein in der Global-Organisation oder einer Meta-Organisation hinterlegtes APNS-Zertifikat gilt für alle Unterorganisationen, die kein eigenes APNS-Zertifikat definiert haben. Wird in einer Unterorganisation ein eigenes Zertifikat hinterlegt, überschreibt es das geerbte Zertifikat für diese Organisation. Ein Hinweis auf der Seite zeigt jeweils an, ob das Zertifikat vererbt wird bzw. von der übergeordneten Organisation verwaltet wird.

Für Version 26.4.0

Standardzertifikat (bestehende Installationen)

Bestehende Relution-Installationen können das Relution-Standardzertifikat (`com.apple.mgmt.mway.mwaysolutions`) verwenden. Dieses Zertifikat wird automatisch mit jedem Relution-Update aktualisiert — kein manueller Eingriff erforderlich. Siehe Update →.

Ab Relution 26.3.0 verwenden Neuinstallationen nicht mehr das Relution-Standardzertifikat. Neue Installationen müssen ein eigenes Zertifikat über den Self-Service-Assistenten bereitstellen.

Für bestehende Installationen, die noch das Standardzertifikat verwenden, wird der Wechsel zum Self-Service-Assistenten empfohlen — insbesondere beim Einrichten neuer Organisationen —, da das Relution-Standardzertifikat in einer zukünftigen Version abgekündigt werden soll.

Eigenes Zertifikat einrichten

Der Self-Service-Assistent unter `Einstellungen` → `Organisationszertifikate` führt durch den gesamten Prozess: Relution erstellt automatisch eine signierte CSR, die bei Apple hochgeladen wird; das resultierende Zertifikat wird anschließend zurück zu Relution gebracht — kein Support-Ticket erforderlich.

APNS Push-Zertifikate einrichten oder erneuern →

Migration vom bisherigen Ablauf

Hat die Installation zuvor ein über den Relution Helpdesk bereitgestelltes Zertifikat verwendet, erscheint auf dieser Seite ein Hinweis zur Migration und darunter der Eintrag Altes APNS-Zertifikat migrieren mit der Schaltfläche Migrieren. Die Migration ist ein Einzel-Klick-Vorgang und hat keinen Einfluss auf eingeschriebene Geräte. Solange die Migration aussteht, ist der Assistent (Starten) nicht verfügbar.

Nach der Migration steht der Self-Service-Assistent für alle künftigen Erneuerungen zur Verfügung.

Vollständige Migrations- und Einrichtungsanleitung →

Für Version 26.4.0

Secure Mail Gateway

Relution bietet mit dem Secure Mail Gateway (SMG) die Möglichkeit, die Funktionen eines Exchange Servers zu nutzen, ohne diesen direkt online verfügbar zu machen. Relution arbeitet hier als Proxy und kommuniziert über die Exchange Active Sync (EAS). Die Verwendung des SMG setzt die Verfügbarkeit von Basic-Auth auf dem Exchangeserver voraus. Modern-Auth wird nicht unterstützt.

> Der SMG-Dienst muss für die Geräte über Port 443 erreichbar sein. Dafür leitet der Reverse-Proxy den Pfad `/Microsoft-Server-ActiveSync` an den SMG-Dienst (Port 8093) weiter. Der SMG-Dienst muss den Exchange-Server (Exchange URL) und den Relution-Server erreichen können. Eine Verbindung vom Exchange-Server zum Relution-Server ist nicht erforderlich.

Es ist empfehlenswert, die Möglichkeiten der Restriktionen erst zu konfigurieren, nachdem die Verbindung erfolgreich getestet wurde, um mögliche Fehler auszuschließen. Ist die Verbindung erfolgreich getestet und funktioniert die Arbeit mit den Endgeräten, können die Berechtigungen entsprechend konfiguriert werden.

> Breaking Change mit Relution 26.4.0: Ab Version 26.4.0 erfordert das SMG-Feature einen eigenständigen Standalone-Dienst. Die Einrichtung ist unter Secure Mail Gateway → beschrieben.

Konfiguration des Secure Mail Gateway

Für Version 26.4.0

Neu in 26.4

Die Einstellungen befinden sich unter `Einstellungen` → `Geräteverwaltung` → `Secure Mail Gateway`. Sie gelten je Organisation; in der globalen Organisation steht die Kachel nicht zur Verfügung.

Für Version 26.4.0

Allgemeine Proxy-Einstellungen

- Aktiviert Schaltet das SMG für die Organisation ein. Ist der Schalter deaktiviert, sind die übrigen Felder gesperrt, und in den Exchange-Konfigurationen der Richtlinien lässt sich die Option Secure Mail Gateway verwenden nicht einschalten.
- Exchange URL Die Adresse, unter der der Exchange Server erreichbar ist. Pflichtfeld.
- SMG Service-URL Die öffentlich erreichbare URL des SMG-Dienstes. Dies kann eine dedizierte Subdomain sein (z. B. `https://smg.ihrserver.example.com`) oder dieselbe URL wie der Relution-Server – vorausgesetzt, der Reverse-Proxy leitet `/Microsoft-Server-ActiveSync` korrekt an den SMG-Dienst weiter.

  Das Feld ist ab Relution 26.4.1 verfügbar und ein Pflichtfeld. Wird eine URL eingetragen, die von der Relution-Server-URL abweicht, übernehmen bestehende Exchange-Konfigurationen den neuen Host nicht automatisch. In jeder Richtlinie mit einer Exchange-Konfiguration muss eine neue Version angelegt werden. In der Exchange-Konfiguration muss die Option Secure Mail Gateway verwenden aktiviert werden, damit der Host auf die neue SMG Service-URL gesetzt wird. Danach muss die Richtlinie veröffentlicht werden.
- Exchange Domäne Die entsprechende Domäne des Exchange Servers, auf die zugegriffen werden soll. Optional; ist sie gesetzt, verwendet das SMG bei der Weiterleitung an den Exchange-Server diese Domäne (siehe Generelle technische Funktionsweise →).
- Benutzerdefinierter Exchange-Host-Header Optionaler Wert für den Host-Header bei der Kommunikation mit dem Exchange-Server. Ist ein Wert eingetragen, ersetzt er den Host-Header, der sonst aus der Exchange URL abgeleitet wird.

Berechtigungen für eingeschriebene Geräte

Die Freigaberegeln legen fest, welche in Relution eingeschriebenen Geräte über das SMG mit dem Exchange-Server synchronisieren dürfen. Eine Anfrage wird nur weitergeleitet, wenn das Gerät alle Regeln erfüllt.

Für Version 26.4.0

- Eigentümer Erlaubte Eigentumsverhältnisse: Gerät in Firmenbesitz (COD), Gerät in Mitarbeiterbesitz (BYOD) und Unbekannt. Standardmäßig sind alle ausgewählt.
- Gerätestatus Erlaubte Gerätestatus: Konform, Inaktiv und Nicht konform. Standardmäßig ist nur Konform ausgewählt; inaktive und nicht konforme Geräte werden abgewiesen.
- Betriebsystem Erlaubte Plattformen: Android, iOS und Windows. Standardmäßig sind alle ausgewählt.
- Bestimmte … Versionen ausschließen Für jede ausgewählte Plattform erscheint ein eigenes Feld, z. B. Bestimmte iOS Versionen ausschließen. Geräte mit einer der eingetragenen Betriebssystemversionen werden abgewiesen.

Es sollte zuerst eine Verbindung aufgebaut und die Funktion getestet werden, bevor Einschränkungen konfiguriert werden.

Berechtigungen für unbekannte Geräte

Der Schalter erlaubt unbekannten oder nicht eingeschriebenen Geräten die Synchronisation über das SMG, z. B. Notebooks oder PCs, die nicht in Relution eingeschrieben werden können. Als unbekannt gilt jedes Gerät, das Relution anhand der Anfrage keinem eingeschriebenen Gerät zuordnen kann. Die Option ist standardmäßig aktiviert. Ist sie deaktiviert, können unter Umständen auch eingeschriebene Geräte bei der ersten Einrichtung des Kontos abgewiesen werden, solange Relution sie noch nicht zuordnen kann.

Verwendung in Richtlinien

Damit Geräte das SMG nutzen, wird in der Exchange-Konfiguration einer Richtlinie die Option Secure Mail Gateway verwenden aktiviert, z. B. für iOS → oder Windows →. Exchange Host und Exchange Domäne werden dann automatisch gesetzt. Ist die Plattform oder eine Betriebssystemversion in den SMG-Einstellungen gesperrt, zeigt die Konfiguration eine Warnung.

Für Version 26.4.0

Generelle technische Funktionsweise

Bei Exchange-Konfigurationen, die das SMG verwenden, wird am Gerät als Server-Adresse die SMG Service-URL ohne Protokoll (`https://`) eingetragen. Das Gerät verbindet sich damit mit dem EAS-Endpunkt `<SMG Service-URL>/Microsoft-Server-ActiveSync`. Als Domäne wird der eindeutige Name der Organisation eingetragen. Damit identifiziert Relution die zu verwendenden SMG-Einstellungen.

Sofern in diesen Einstellungen das SMG aktiviert und konfiguriert ist, werden aus der Anfrage die Header `DeviceId` und `DeviceType` extrahiert, und darüber das entsprechende Gerät identifiziert. Je nach SMG-Einstellungen und Vorhandensein, Status bzw. Eigenschaften des identifizierten Geräts (siehe Abschnitt Berechtigungen für eingeschriebene Geräte), wird die Anfrage anschließend abgelehnt oder an den Exchange-Server aus den SMG-Einstellungen weitergeleitet, und die Antwort dann an das Gerät zurückgeliefert. Sofern konfiguriert, wird dabei die Domäne aus den SMG-Einstellungen verwendet.

Passwort

Exchange und SMG verwenden BasicAuth, hier kann es unter Umständen beim Verwenden von Sonderzeichen wie `$ # / * ü ö ä` und `Leerzeichen` zu Accountfehlern am Endgerät kommen. Um das zu prüfen, sollte zum Test ein einfaches Passwort, bestehend aus Buchstaben und Zahlen, verwendet werden.

macOS

MacOS nutzt die Exchange Anbindung über EWS. Das SecureMailGateway kann aber nur ActiveSync weiterleiten. Daher ist es aktuell nicht möglich, macOS Geräte mit SMG zu verwenden.

Für Version 26.4.0

Auftragsverarbeitungsvertrag (AVV)

Um die volle DSGVO-Konformität zu gewährleisten, muss der Verantwortliche mit dem Betreiber der eigenen Relution-Umgebung (dem Auftragsverarbeiter) einen Auftragsverarbeitungsvertrag (AVV) abschließen. Der Bereich Neuen AVV erstellen ermöglicht, diesen Vertrag vollständig digital zu konfigurieren und zu unterzeichnen.

Damit unterstützt Relution einen effizienten, transparenten und rechtskonformen Abschluss von Auftragsverarbeitungsverträgen zwischen der Relution GmbH und dem Kunden.

Solange in einer Organisation die aktuelle AVV-Version nicht unterzeichnet ist, erscheint im Benachrichtigungsbereich (1) die Meldung AVV-Unterzeichnung erforderlich. Sie wird Benutzern mit dem Recht AVV-Verwaltung → Aktualisieren angezeigt. Wird eine neue AVV-Version bereitgestellt, erscheint die Meldung erneut; das Formular ist dann mit den Angaben der zuletzt unterzeichneten Version vorbelegt.

Der AVV kann für jeden Mandanten einzeln abgeschlossen werden. Alternativ lässt er sich in der globalen Organisation oder in einer Meta-Organisation mit der Option Akzeptieren für alle Untermandanten für alle untergeordneten Organisationen abschließen. In diesen Organisationen entfallen dann Meldung und AVV-Einstellungen.

Die AVV-Einstellungen sind über zwei Wege erreichbar:

1. Direkt über die Benachrichtigung (1 + 2) im Benachrichtigungsbereich.
2. Über den Menüpfad (3): `Einstellungen` → `Allgemein` → `AVV-Verwaltung`

Für Version 26.4.0

1. Allgemeine Angaben

Dieser Bereich dient der eindeutigen Identifikation des Unterzeichners und der juristischen Person, die den Vertrag abschließt. Die Person, die diesen Abschnitt ausfüllt, muss zeichnungsberechtigt für die Organisation sein.

Feld	Beschreibung
Vollständiger Name der unterzeichnenden Person	Der Name der Person, die den Vertrag rechtlich bindend unterzeichnet.
E-Mail	Die E-Mail-Adresse der unterzeichnenden Person.
Name des Unternehmens	Der offizielle Name der eigenen Organisation (des Verantwortlichen).
Adresse, Postleitzahl, Stadt, Land	Die offizielle Anschrift der eigenen Organisation.

Name und E-Mail sind mit den Daten des angemeldeten Benutzers vorbelegt, Name des Unternehmens und Anschrift mit den Angaben aus den allgemeinen Organisationseinstellungen. Die Werte lassen sich vor der Unterzeichnung anpassen.

2. Wichtiger Hinweis zu Art. 9 DSGVO

Für Version 26.4.0

Zu beachten ist der hervorgehobene blaue Hinweis:

> Die Verarbeitung von Daten nach Artikel 9 DSGVO ist nicht gestattet und muss durch den Auftraggeber unterbunden werden.

Hintergrund: Artikel 9 DSGVO regelt besondere Kategorien personenbezogener Daten (z. B. Gesundheitsdaten, ethnische Herkunft, politische Meinungen). Da Relution ein MDM-System ist, das primär technische und administrative Daten verarbeitet, ist die Verarbeitung dieser hochsensiblen Datenkategorien im Standardbetrieb nicht zulässig und muss vom Auftraggeber unterbunden werden.

3. Art der Daten

In diesem Bereich wird definiert, welche Kategorien personenbezogener Daten im Rahmen der Nutzung von Relution im eigenen Auftrag verarbeitet werden. Häkchen bei allen zutreffenden Kategorien setzen, deren Daten in der eigenen Relution-Instanz vorkommen:

- Stammdaten (z.B. Vor- und Nachname, Geschlecht, E-Mail-Adresse, Anschrift, Telefonnummer)
- Vertragsstammdaten (Produkte, Kaufvertrag, Kaufpreis, Garantien)
- Protokolldaten (IP-Adresse, Zeitstempel, Ereignisse mit Benutzerkontext)
- Benutzergenerierte Inhalte (z.B. Forenbeiträge, Feature Requests, Supportanfragen)
- Gerätedaten (Gerätetyp, Gerätenummer, IP-Adresse, Betriebssysteminformationen, installierte Apps)
- Positionsdaten (iBeacons, GPS-Position, Funknetz, WiFi-Netzwerke)

Bei Bedarf lassen sich über Andere hinzufügen zusätzliche, hier nicht gelistete Datenkategorien ergänzen.

Mindestens eine Datenkategorie muss ausgewählt oder über Andere hinzufügen ergänzt werden, sonst bleiben Vorschau und AVV unterschreiben deaktiviert.

---

4. Gruppe der Betroffenen

Auswählen, welche Gruppen von Personen von der Datenverarbeitung in der eigenen Relution-Instanz betroffen sind:

- Eltern und Elternvertreter
- Endkunden und Lieferanten
- Mitarbeitende (z.B. Arbeitnehmer, Lehrkräfte, Auszubildende, Verwaltungsangestellte)
- Schülerinnen und Schüler

Auch hier lässt sich die Funktion Andere hinzufügen nutzen, falls weitere Gruppen betroffen sind, die nicht in der Liste aufgeführt sind. Auch hier muss mindestens eine Gruppe ausgewählt oder ergänzt werden.

---

5. Kontakt für Notfälle

Hier die Kontaktdaten der Person in der eigenen Organisation angeben, die im Falle einer Datenpanne oder anderer sicherheitsrelevanter Notfälle sofort kontaktiert werden kann. Name und E-Mail sind Pflichtangaben, die Telefonnummer ist optional.

- Name
- E-Mail
- Telefon

Für Version 26.4.0

---

6. Abschluss und Unterschrift

Vor Vertragsabschluss muss die Zeichnungsberechtigung bestätigt werden:

- Bestätigung der Zeichnungsberechtigung: Die Berechtigung, den Vertrag im Namen der eigenen Organisation abzuschließen, wird bestätigt.

In der globalen Organisation und in Meta-Organisationen steht zusätzlich die optionale Auswahl Akzeptieren für alle Untermandanten zur Verfügung. Sie ist relevant, wenn der Vertrag als übergeordnete Instanz (z.B. Schulträger) auch für untergeordnete, verwaltete Einheiten (z.B. einzelne Schulen) abgeschlossen wird. Ist sie gesetzt, gilt der AVV auch für alle untergeordneten Organisationen; dort wird dann kein eigener AVV mehr angeboten.

Für den Abschluss stehen folgende Optionen zur Verfügung:

- Vorschau: Zeigt den vollständigen Vertragstext vorab. Verfügbar, sobald die allgemeinen Angaben sowie Art der Daten und Gruppe der Betroffenen ausgefüllt sind.
- AVV unterschreiben: Schließt den Vertrag digital ab. Der AVV ist damit rechtsgültig. Die Schaltfläche wird erst aktiv, wenn zusätzlich der Kontakt für Notfälle (Name und E-Mail) angegeben und die Zeichnungsberechtigung bestätigt ist.

Das signierte Dokument im Rahmen der eigenen Dokumentationspflichten (Rechenschaftspflicht nach DSGVO) sorgfältig aufbewahren.

Mit der Unterzeichnung werden die Vertragsangaben automatisch an den Relution Lizenz Server übermittelt. Übertragen werden:

- die Angaben aus dem Formular: unterzeichnende Person und E-Mail, Name des Unternehmens und Anschrift, Art der Daten, Gruppe der Betroffenen, Kontakt für Notfälle sowie die Auswahl Akzeptieren für alle Untermandanten
- der Zeitpunkt der Unterzeichnung, die IP-Adresse und der Relution-Benutzername, mit dem unterzeichnet wurde

Die PDF-Dokumente des AVV werden nicht an den Lizenz Server übertragen. Ohne diese Übermittlung kann der AVV nicht unterzeichnet werden.

Nach der Unterzeichnung wird der AVV als PDF in deutscher und englischer Fassung per E-Mail an die eingetragene E-Mail-Adresse der unterzeichnenden Person gesendet. Schlägt der Versand fehl, bleibt die Unterzeichnung trotzdem gültig.

Unterzeichneter AVV

Nach der Unterzeichnung zeigt die AVV-Verwaltung den Bereich Unterzeichneter Auftragsverarbeitungsvertrag mit AVV-Version, Datum der Unterzeichnung, Signiert von und dem Kontakt für Notfälle. In der globalen Organisation und in Meta-Organisationen wird zusätzlich Für Untermandanten signiert angezeigt.

Für Version 26.4.0

Für Version 26.4.0

- Download: Lädt den unterzeichneten AVV als PDF herunter, bei deutscher Portalsprache in deutscher, sonst in englischer Fassung.
- Widerrufen: Widerruft den unterzeichneten AVV. Zeitpunkt und Benutzer des Widerrufs werden an den Relution Lizenz Server übermittelt. Anschließend wird der AVV erneut zur Unterzeichnung angeboten.

Berechtigungen

Die Rechte für den AVV stehen in den Rollen in der Rechtegruppe AVV-Verwaltung:

- Lesen: Zeigt die Übersicht des unterzeichneten AVV.
- Aktualisieren: Zeigt die Meldung und das Formular zur Unterzeichnung.
- Löschen: Erlaubt den Widerruf eines unterzeichneten AVV.

Die Rolle Administrator enthält alle drei Rechte. Ist noch kein AVV unterzeichnet, erscheint ohne das Recht Aktualisieren statt des Formulars nur der Hinweis Es wurde noch kein AVV unterzeichnet.

Hinweise zur AVV-Unterzeichnung

Besteht keine Berechtigung zur Unterzeichnung des Auftragsverarbeitungsvertrages (AVV), gilt folgendes Vorgehen:

- Account-Erstellung: Für den unterschriftsberechtigten Kollegen einen eigenen Account in der Organisation erstellen, für die der AVV abgeschlossen wird. Der Account benötigt eine Rolle mit dem Recht AVV-Verwaltung → Aktualisieren (z. B. die Rolle Administrator); ohne dieses Recht werden weder die AVV-Benachrichtigung noch das Formular zur Unterzeichnung angezeigt.
- Unterzeichnung: Der Kollege kann sich anschließend im Portal anmelden und den AVV eigenständig unterzeichnen.

Relution 26.0.0

Für Version 26.4.0

Spracheinstellungen

In Relution lassen sich die Sprache der Oberfläche für jeden Benutzer sowie die Sprachen einstellen, in denen Inhalte wie App-Beschreibungen und Benachrichtigungen gepflegt werden.

Sprachen der Organisation und Standardsprache

Unter `Einstellungen` → `Allgemein` → `Sprachen` wird festgelegt, in welchen Sprachen Inhalte in Relution gepflegt werden. Jede hinzugefügte Sprache ergänzt lokalisierte Felder, z. B. Appname und Beschreibung von Apps, Texte für Einschreibungs- und App-Benachrichtigungen sowie Support-Angaben. Diese Sprachen sind unabhängig von der Sprache der Relution-Oberfläche, die jeder Benutzer selbst einstellt (siehe Benutzersprache).

In jeder Organisation sind standardmäßig Deutsch und Englisch angelegt. Als Standardsprache übernimmt eine neue Organisation die Standardsprache der globalen Organisation, ab Werk ist das Englisch.

- Über Hinzufügen lassen sich weitere Sprachen ergänzen. Zur Auswahl stehen zahlreiche Sprachen und regionale Varianten (Gebietsschemata), z. B. Niederländisch, Polnisch oder Deutsch (Österreich), unabhängig von den Oberflächensprachen. Fehlende Inhalte einer neuen Sprache werden aus der Standardsprache übernommen.
- Über das 3-Punkte-Menü → Zum Standard machen wird eine Sprache als Standard festgelegt. Vor dem Wechsel erscheint ein Bestätigungsdialog: Die Übersetzungen für bereits erstellte Apps, Einschreibungs-Benachrichtigungen und App-Benachrichtigungen sollten vorher in der neuen Sprache vorhanden sein, da fehlende Übersetzungen zu Problemen beim Einschreibungsprozess führen können.
- Über Löschen wird eine Sprache entfernt. Die Standardsprache lässt sich nicht löschen.

Für Version 26.4.0

Die Standardsprache gilt für Push-Benachrichtigungen, z. B. App-Benachrichtigungen per Push oder Push-Nachrichten aus einer Gerätegruppenaktion vom Typ Benachrichtigungsaktion, sowie für E-Mails an zusätzlich eingetragene E-Mail-Adressen ohne Relution-Benutzerkonto. Außerdem erhalten neu angelegte Benutzer ohne eigene Sprachangabe die Standardsprache als Benutzersprache, sofern sie eine der unterstützten Oberflächensprachen ist, sonst Englisch.

E-Mails an Relution-Benutzer, z. B. zum Zurücksetzen des Passworts oder zu Apps, werden in der Benutzersprache des Empfängers versendet. Fehlt dafür eine Übersetzung, werden sie auf Englisch versendet.

Benutzersprache

Die Benutzersprache kann von jedem Benutzer individuell eingestellt werden und wirkt sich auf die gesamte Oberfläche in Relution aus. Damit werden etwa das Dashboard, Richtlinien und Tabellen in der gewählten Sprache angezeigt. Auch E-Mails, die Relution an den Benutzer sendet, richten sich nach dieser Sprache.

Die Einstellung befindet sich im Benutzermenü oben rechts unter `Profil`. Im Tab Benutzerinformationen steht in der Karte Einstellungen der Eintrag Sprache. Über das Stift-Symbol (Sprache bearbeiten) wird die Sprache geändert.

Unterstützte Sprachen

Relution unterstützt aktuell folgende Sprachen in der grafischen Oberfläche:

- Deutsch
- Englisch
- Französisch
- Italienisch
- Spanisch
- Türkisch

Für Version 26.4.0

REST API

Die gesamte Funktionalität von Relution steht über eine umfangreiche REST API zur Verfügung. Mit dieser API lässt sich Relution von jeder anderen Anwendung oder per Skript steuern.

API-Dokumentation

Jeder Relution-Server liefert die vollständige API-Spezifikation mit, passend zur installierten Server-Version. Sie dokumentiert alle Endpunkte mit ihren Parametern, Request- und Response-Bodys sowie den zurückgegebenen Statuscodes.

Die Spezifikation wird aus dem Relution-Portal geöffnet: Der Eintrag Web API im Support-Menü (oben rechts) öffnet die interaktive Dokumentation. Alternativ ist sie direkt unter `https://<server>/web-api/index.html` erreichbar.

Anfragen an die REST API unterliegen denselben Berechtigungsprüfungen wie Aktionen im Portal; sicherheitsrelevante Aktionen werden im Audit-Protokoll → aufgezeichnet.

API-Zugriffstoken erstellen

Um Relution von Drittsystemen oder Skripten aus anzusprechen, wird ein API-Zugriffstoken benötigt.

Für Version 26.4.0

Für Version 26.4.0

1. Oben rechts im Relution-Portal auf den eigenen Benutzernamen klicken.
2. Navigieren zu: `Profil` → `Access Tokens` → `Hinzufügen`.
3. Das Token benennen und kopieren.

Beim Anlegen stehen außerdem folgende Optionen zur Verfügung:

- Gültigkeitsdauer: standardmäßig aktiv. Das Ablaufdatum ist mit dem heutigen Datum plus 180 Tage vorbelegt und lässt sich später über Zugangstoken bearbeiten ändern. Ist die Option deaktiviert, läuft das Token nicht ab.
- API-Bereiche: Das Token gilt nur für Anfragen an Endpunkte der ausgewählten Bereiche (Mehrfachauswahl, Vorgabe: Management-Portal). Die Beispiele in diesem Artikel verwenden Endpunkte unter `/api/management/` und benötigen diesen Bereich.

Das Token wird im HTTP-Header `X-User-Access-Token` zur Authentifizierung genutzt.

Administratoren mit der Berechtigung zum Erstellen von API-Zugangstoken können ein Token auch für einen anderen Benutzer anlegen, etwa für ein Dienstkonto. Dazu wird unter `Benutzer` → `Benutzer` genau ein Benutzer ausgewählt und im Kontextmenü die Aktion Access Token hinzufügen aufgerufen.

Das Token wird nur einmalig beim Anlegen angezeigt.

---

1. Benutzer im CSV-Dateiformat

- In die erste Zeile der `.csv`-Datei kommt eine Kopfzeile mit den gewünschten Eigenschaftsnamen.
- Die Reihenfolge der Spalten ist unerheblich.
- Nicht benötigte Eigenschaften können weggelassen werden.
- Pflichtfelder: Die Kopfzeile muss die Spalte `email` enthalten, und jede Zeile benötigt einen Benutzernamen in der Spalte `name`. Die Portal-Vorlage beginnt mit folgenden Spalten:

```
name,email,givenName,surname,password
```

Die Groß-/Kleinschreibung der Spaltennamen spielt keine Rolle. Passwörter müssen der Richtlinie unter `Einstellungen` → `Verwaltung der Anmeldedaten` entsprechen. Telefonnummern müssen im internationalen Format angegeben werden, z. B. `+4912345`.

Es können bis zu 15 eigene Eigenschaften definiert werden: **`custom1`** – **`custom15`**

Die Portal-Vorlage enthält weitere Spalten, etwa `disablePasswordAuthentication`, `locale`, `permissions`, `memberOfGroups`, `teacherOfClasses` und `studentOfClasses`. Ihre Bedeutung beschreibt der Artikel CSV-Import →.

👉 Eine Vorlage kann im Relution-Portal heruntergeladen werden: `Benutzer` → `Benutzer` → `Drei-Punkte-Menü` → `Benutzer per CSV importieren`. Im Dialog steht sie über den Link Vorlage im Beschreibungstext zum Download bereit.

Beispiel-CSV:

Für Version 26.4.0

```
name,email,givenName,surname,password,phone,position,country,managedAppleId,custom1,cus
tom2
user1,user1@company.com,Heinz,Ketchup,p4ssw0rd,+49234346345,user1 position,user1
country,user1.id@company.com,43,Operations
user2,user2@company.com,Heinz,Ketchup,p4ssw0rd,+49234346345,user2 position,user2
country,user2.id@company.com,24,Marketing
user3,user3@company.com,Heinz,Ketchup,p4ssw0rd,+49234346345,user3 position,user3
country,user3.id@company.com,30,HR
user4,user4@company.com,Heinz,Ketchup,p4ssw0rd,+49234346345,user4 position,user4
country,user4.id@company.com,32,Sales
user5,user5@company.com,Heinz,Ketchup,p4ssw0rd,+49234346345,user5 position,user5
country,user5.id@company.com,45,Finance
user6,user6@company.com,Heinz,Ketchup,p4ssw0rd,+49234346345,user6 position,user6
country,user6.id@company.com,30,Purchase
```

2. Benutzer über das Relution-Portal hochladen

1. Aufrufen: `Benutzer` → `Benutzer` → `Drei-Punkte-Menü` → `Benutzer per CSV importieren`
2. CSV-Datei und Trennzeichen auswählen. Die Option Automatisch Gruppen und Klassen erstellen legt in der Datei genannte, noch nicht vorhandene Gruppen und Klassen an.
3. Importierte Benutzer einer oder mehreren Gruppen zuordnen.
4. Die Benutzer erscheinen anschließend in der Übersicht.

3. Benutzer über die Relution API anlegen

Änderung in Relution 5.34:

- Der Benutzerimport läuft nun als Hintergrund-Job mit den Zuständen CREATED, RUNNING, FINISHED und FAILED.
- Jeder Job speichert einen Bericht pro Zeile.
- Der alte Import wurde entfernt.
- Einige Spaltennamen wurden geändert:
  - `first name` → `givenName`
  - `last name` → `surname`
  - `managed apple id` → `managedAppleId`
  - `phone number` → `phone`
  - `userId` → `name`

Für Version 26.4.0

Schritte

1. Eine `users.csv`-Datei erstellen.
2. Das folgende bash-Skript in eine Datei kopieren, z. B. `uploadUserCSV.sh`.
3. Die Datei ausführbar machen:

```
chmod +x ./uploadUserCSV.sh
```

4. Es ausführen:

```
./uploadUserCSV.sh -f 'FILEPATH' -h 'HOST' -a 'YOUR-ACCESS-TOKEN'
```

Argumente

Argument	Bedeutung	Beispiel	Standard	Pflicht
`-f`	Pfad zur `users.csv`	user.csv		✅
`-h`	Relution-Host	https://relution.io		
`-a`	API-Zugriffstoken	xxxxxxxx		
`-r`	Gruppe (Name oder UUID), der die importierten Benutzer zugeordnet werden; Leerzeichen als `%20`	Schule%20Lehrer	`Organame%20Device%20User`	❌
`-s`	Trennzeichen zum Parsen	SEMICOLON	COMMA	
`-w`	Überschreiben vorhandener Benutzer	true	false	❌

- Die Benutzer werden in die Organisation importiert, zu der das Konto des API-Zugriffstokens gehört. Für den Import benötigt dieses Konto die Berechtigungen zum Erstellen und Bearbeiten von Benutzern.
- Ohne `-r` verwendet das Skript die Gruppe `Organame Device User`. „Organame“ ist im Skript durch den Namen der eigenen Organisation zu ersetzen, sonst wird keine Gruppe zugeordnet.
- Mit `-w true` werden vorhandene Benutzer überschrieben; die Zuordnung erfolgt über die Spalte `name`. Benutzer, die aus einem externen Verzeichnis wie LDAP stammen, werden dabei übersprungen.
- Die API kennt zusätzlich den Parameter `createMissingGroupsAndClasses=true`. Er entspricht der Portal-Option Automatisch Gruppen und Klassen erstellen und wird vom Skript nicht gesetzt.

Für Version 26.4.0

Ausgabe-Beispiel

```
============
success: 1, skipped: 1, failed: 1
2: [SUCCESS] User ... successfully stored with version 1.
3: [FAILED] Number of data fields does not match number of headers.
4: [SKIPPED] User Test2 should not be overwritten.
```

4. Benutzer per CSV über Bash-Skript hochladen

Vollständiges Konfigurationsbeispiel anzeigen

5. Neue Organisation erstellen

Das folgende Skript legt eine neue Organisation samt Organisationsadministrator an. Das verwendete Token gehört zu einem Benutzer mit der Berechtigung, Organisationen oder Unterorganisationen anzulegen, zum Beispiel dem Systemadministrator. Pflicht ist der Kurzname `orgaName`; die Angaben zum Administrator (`orgaAdminUser`, `orgaAdminGivenName`, `orgaAdminSurName`, `orgaAdminPwd`) sind erforderlich, solange `skipAdminCreation` nicht auf `true` steht. Das Administratorpasswort muss der Standard-Passwortrichtlinie entsprechen. Bei Erfolg antwortet der Server mit HTTP-Status 202 und gibt die UUID der Organisation, ihren Namen und die UUID des Administrators zurück.

> Vollständiges Konfigurationsbeispiel anzeigen

6. Geräte in einer Organisation abfragen

> Vollständiges Konfigurationsbeispiel anzeigen

Bewährte Praktiken für API-Token

Für Version 26.4.0

- Bei API-Zugriffstoken immer ein Ablaufdatum festlegen. Token ohne Ablaufdatum bleiben unbegrenzt gültig.
- Token sofort widerrufen, wenn sich die Rolle des zugehörigen Kontos ändert, das Konto deaktiviert wird oder der Kontoinhaber die Organisation verlässt.
- Token-Geheimnisse werden nur als Hash gespeichert (SHA-256, bei konfiguriertem HMAC-Schlüssel HMAC-SHA-256) und können nach der Erstellung nicht wiederhergestellt werden. Bei Bedarf einen neuen Token erstellen, anstatt zu versuchen, einen bestehenden abzurufen.

Verwandte Themen

- API-Zugriffstoken in Relution erstellen → — Anleitung zur Token-Generierung.
- LDAP / Active Directory Anbindung → — Benutzer und Gruppen synchronisieren.

Audit-Protokoll

Mit der Version `5.25` ist in Relution ein Audit-Protokoll eingeführt worden. Es ermöglicht das Nachvollziehen von Aktivitäten, ohne dass Logs durchsucht werden müssen.

Audit-Protokoll

Das Audit-Protokoll steht unter `Einstellungen` → `Audit-Protokoll` zur Verfügung. Den Zugriff steuern zwei Berechtigungen:

- Audit-Protokoll: alle Einträge.
- Geräteverwaltungs-Audit-Log: nur Einträge der Kategorie Geräteverwaltung.

Organisationsadministratoren haben beide Berechtigungen standardmäßig. Angezeigt werden die Einträge der eigenen Organisation, in einer Meta-Organisation zusätzlich die ihrer Unterorganisationen. In der Global Organisation umfasst das Audit-Protokoll die Einträge aller Organisationen.

Die Daten werden standardmäßig 180 Tage gespeichert und lassen sich im Relution-Portal durchsuchen und filtern.

Als Informationen stehen folgende Spalten zur Verfügung:

- Datum
- Benutzername
- Authentifiziertes Gerät
- Client
- Imitator
- Methode (POST, GET, PUT, DELETE)
- Beschreibung
- Endpunkt (standardmäßig ausgeblendet, über die Spaltenauswahl einblendbar)
- HTTP-Status
- Organisation (nur in der Global Organisation und in Meta-Organisationen)
- IP
- Kategorie (nur mit der Berechtigung Audit-Protokoll)
- Ergebnis
- Ereignistyp

Für Version 26.4.0

Filter stehen für Methode, HTTP-Status (2xx, 4xx, 5xx), Benutzername, Authentifiziertes Gerät, Client, Organisation, Kategorie, Ergebnis und Ereignistyp zur Verfügung; für Organisation und Kategorie gelten dieselben Einschränkungen wie bei den Spalten.

Damit lassen sich Änderungen am Server nachvollziehen; welche Ereignisse erfasst werden, legt die Serverkonfiguration fest (siehe Umfang der Protokollierung →).

Export

Im Drei-Punkte-Menü öffnet Vollständiges Audit-Log exportieren den Dialog Audit-Log-Export. Über Neuen Export starten wird im Hintergrund eine CSV-Datei erstellt, die anschließend im selben Dialog heruntergeladen werden kann. Es wird immer nur ein Export gespeichert; ein neuer Export ersetzt den vorherigen. Ein laufender Export lässt sich über Abbrechen beenden.

Speicherlimit-Verhalten

Audit-Einträge werden automatisch gelöscht, wenn sie den Aufbewahrungszeitraum überschreiten. Standard sind 180 Tage; in der Serverkonfiguration (`application.yml`) lässt sich der Zeitraum über `relution.cleanup.audit-log.remove-after` in Tagen anpassen (z. B. `365d`, mindestens 1 Tag). Die Bereinigung läuft zwischen 18:00 und 07:00 Uhr etwa alle 17 Minuten und löscht je Lauf höchstens 10.000 Einträge in Stapeln zu je 1.000, um Datenbanksperren zu vermeiden. Jeder Lauf, der Einträge löscht oder fehlschlägt, erscheint selbst als Ereignis Audit-Logs bereinigt im Audit-Protokoll.

Wenn der Speicherplatz vor der Bereinigung erschöpft ist, können neue Audit-Einträge möglicherweise nicht geschrieben werden. Der Systemadministrator muss die Speichernutzung überwachen und sicherstellen, dass für den konfigurierten Aufbewahrungszeitraum ausreichend Speicherplatz verfügbar ist. Es gibt keine automatische Benachrichtigung bei niedrigem Speicherplatz — dies liegt in der Verantwortung des Systemadministrators.

Umfang der Protokollierung

Aktivierung und Umfang des Audit-Protokolls werden über den Block `relution.audit-log` in der `application.yml` gesteuert; das Audit-Protokoll ist standardmäßig aktiv. Im Auslieferungszustand werden einige sehr häufige Geräteereignisse nicht protokolliert: Geräteidentifikation, geänderte Geräteeinstellungen sowie Änderungen an installierten Apps und Zertifikaten. Auch einzelne Endpunkte mit vielen Anfragen sind ausgenommen, etwa Geräteaktionen und Abfragen des aktuellen Geräts. In der Konfiguration für den Betrieb nach Common Criteria (CC-EAL4) ist die vollständige Protokollierung aktiv; diese Werte dürfen dort nicht geändert werden.

Serverstart und -stopp werden ebenfalls als Ereignisse Relution Server gestartet und Relution Server gestoppt protokolliert, jeweils mit Serverversion und Clusterknoten.

Für Version 26.4.0

nginx-Zugriffsprotokolle

Der nginx Reverse Proxy protokolliert die eingehenden HTTP/HTTPS-Anfragen. Diese Protokolle ergänzen das Relution-Audit-Protokoll auf der Ebene des Netzwerkkanals. In der Konfigurationsvorlage für den Betrieb nach Common Criteria (CC-EAL4) werden für HTTPS-Anfragen zusätzlich das ausgehandelte TLS-Protokoll und die Cipher-Suite erfasst. Die Standardvorlage der Docker-Installation → protokolliert diese beiden Felder nicht.

Zugriff auf die Protokolle:

```
docker logs nginx
```

Oder zur Echtzeitverfolgung:

```
docker logs -f nginx
```

In der CC-EAL4-Vorlage `relution-nginx.conf` hat jede Zugriffsprotokollzeile der HTTPS-Ports (443 und 8443) folgendes Format:

```
<remote_addr> - <user> [<time>] "<request>" <status> <bytes> "<referer>" "<user_agent>"
"<x_forwarded_for>" <request_time> <upstream_time> <pipe> <ssl_protocol> <ssl_cipher>
```

Die Felder `$ssl_protocol` und `$ssl_cipher` am Ende jeder Zeile zeichnen die TLS-Version und die Cipher-Suite der jeweiligen Verbindung auf (z. B. `TLSv1.3 TLS_AES_256_GCM_SHA384`). Anfragen auf Port 80, die auf HTTPS weitergeleitet werden, werden im Standardformat des nginx-Images ohne diese Felder protokolliert.

Das Fehlerprotokoll wird auf `stderr` geschrieben und ist ebenfalls über `docker logs nginx` abrufbar.

Audit-Ereignisreferenz

- Geräteverwaltungs-Ereignisse
- Allgemeine Ereignisse

Für Version 26.4.0

Server-Log-Referenzen

Integritätsfehler bei Verschlüsselung/Entschlüsselung:

```
INTEGRITY_FAILURE operation=ENCRYPT entity={} attribute={} outcome=FAILURE subject={}
INTEGRITY_FAILURE operation=DECRYPT entity={} attribute={} outcome=FAILURE subject={}
INTEGRITY_FAILURE operation=DEK_UNWRAP entity=DataEncryptionKeyset
attribute=wrappedDekKeyset outcome=FAILURE kekType={} kekId={} dekVersion={} subject={}
TLS_INTEGRITY_FAILURE host={} outcome=FAILURE reason="{}" error="{}"
```

Kryptographische Schlüsselableitung (die Zeile `TLS_KEY_DERIVATION` wird einmal beim Serverstart geschrieben):

```
CRYPTO_KEY_DERIVATION category={} algorithm={} purpose="{}"
CRYPTO_KEY_DERIVATION category={} algorithm={} iterations={} purpose="{}"
TLS_KEY_DERIVATION outcome=SUCCESS info="Write MAC and write encryption keys derived
via HMAC-SHA-256 (TLS 1.2) and HKDF-SHA-256/SHA-384 (TLS 1.3)"
```

TLS-Kanäle:

```
TLS_CHANNEL_ATTEMPT host={} port={} tls={} cipher={} cert_subject="{}"
cert_fingerprint={}
TLS_CHANNEL_SUCCESS host={} outcome=SUCCESS
TLS_CHANNEL_FAILURE host={} outcome=FAILURE reason="{}"
```

Die Meldungen zu TLS-Verbindungsversuchen und erfolgreichen Verbindungen lassen sich über `logging.level.io.relution.security.audit.tls.channel: WARN` unterdrücken; Fehlermeldungen (`TLS_CHANNEL_FAILURE`) bleiben dabei erhalten.

Für Version 26.4.0

Lizenz-Verwaltung

Für die Konfiguration der Geräte in Relution sind Gerätelizenzen erforderlich. Diese Lizenzen lassen sich entweder direkt vom Sales Team oder von einem der Partner beziehen.
Nach dem Erwerb werden die Lizenzen entweder dem Server oder der Organisation zugewiesen. Bei einem eigenen Server (OnPrem / dedizierter Cloud Server) besteht zudem die Möglichkeit, einzelnen Organisationen (z. B. Standorten oder Schulen) eine Limitierung für die Anzahl der Lizenzen zuzuweisen.

Diese Limitierung bietet die Möglichkeit, die Anzahl der eingebuchten Geräte einer Organisation gemäß der Lizenzanzahl zu beschränken. Die Limitierung wird je Lizenztyp festgelegt, der in der Serverlizenz begrenzt ist, z. B. Geräte, Benutzer oder Native Apps. Für jeden dieser Lizenztypen erscheint in den Lizenzinformationen ein eigener Reiter.
Durch diese Funktion lässt sich sicherstellen, dass Organisationen nicht mehr Lizenzen beanspruchen, als tatsächlich benötigt werden. Standardmäßig haben Organisationen keine Limitierung, es sei denn, die Lizenzen werden explizit über das Sales Team zugewiesen.

Voraussetzungen

- Ein kostenpflichtiges Lizenzmodell; bei der kostenlosen Lizenz wird der Abschnitt Organisations-Limitierungen nicht angezeigt.
- Anmeldung als Systemadministrator in der Global-Organisation. Die Rechte für Lizenzzuweisungen gibt es nur in der Global-Organisation; zum Ändern und Löschen von Limits ist das Bearbeiten-Recht erforderlich.

Für Version 26.4.0

Limitierung anpassen

1. Die Anmeldung am Relution-Portal erfolgt als Systemadministrator in der Global-Organisation.
2. Oben rechts wird das Support-Menü (Fragezeichen-Symbol) geöffnet und Lizenzinformationen gewählt. Die Limitierungen befinden sich im Abschnitt Organisations-Limitierungen.
3. Im Reiter des gewünschten Lizenztyps (z. B. Geräte) wird die Organisation in der Liste gesucht und die Schaltfläche mit den drei Punkten geöffnet.
4. Über Bearbeiten öffnet sich der Dialog Organisationslimit bearbeiten. Die gewünschte Anzahl wird im Feld Limit eingetragen und mit Bestätigen übernommen.

Der Wert darf nicht kleiner sein als die Anzahl der von der Organisation bereits verwendeten Lizenzen (Spalte Verwendet). Die Spalte Zugewiesen zeigt das festgelegte Limit. Die Zeile Global am Tabellenende fasst die verwendeten Lizenzen aller Organisationen zusammen und stellt die Summe der zugewiesenen Limits dem Gesamtlimit der Serverlizenz gegenüber.

> Die Summe der Organisationslimits kann das Gesamtlimit der Serverlizenz übersteigen; der Dialog weist in diesem Fall darauf hin. Ist das Gesamtlimit ausgeschöpft, kann keine Organisation weitere Lizenzen verbrauchen, unabhängig von ihrem eigenen Limit.

Für Version 26.4.0

Limitierung entfernen

Über die Schaltfläche mit den drei Punkten und Löschen wird das Limit einer Organisation aufgehoben, nachdem der Dialog Organisationslimit löschen mit Bestätigen quittiert wurde. Danach kann die Organisation alle verfügbaren Lizenzen nutzen.

Limitierungen exportieren

Über die Schaltfläche CSV Export (Organisationslimits herunterladen) im Abschnitt Organisations-Limitierungen werden die Limits der Organisationen als CSV-Datei heruntergeladen.

Limitierung beim Anlegen einer Organisation

Beim Anlegen einer Organisation lässt sich das Limit direkt mit festlegen: Nach dem Erstellen führt die Schaltfläche Lizenzen zuweisen im Schritt Zusammenfassung zum optionalen Schritt Limitierungen. Der Schritt erscheint nur bei einem kostenpflichtigen Lizenzmodell mit begrenzten Lizenztypen und mit dem Recht zum Bearbeiten von Lizenzzuweisungen. Weitere Informationen unter Organisationen anlegen →.

Für Version 26.4.0

Lifetime Lizenzen

Lifetime-Lizenzen gelten dauerhaft für genau ein Gerät. Dadurch entfallen wiederkehrende jährliche Lizenzkosten.

Eine Lifetime-Lizenz wird fest an die Seriennummer (SN) des Geräts gebunden und kann nicht auf ein anderes Gerät übertragen werden.

Bindung an die Seriennummer

Lifetime-Lizenzen müssen mit einer Seriennummer verknüpft werden, damit sie für ein Gerät wirken. Geräte, deren Seriennummer an eine Lifetime-Lizenz gebunden ist, werden auch dann eingeschrieben, wenn das Gerätekontingent der übrigen Lizenzen erschöpft ist.

Geräte und Auto-Einschreibungen ohne Seriennummer können nicht zugewiesen werden. Die Anzahl der Bindungen ist durch das Gerätelimit der Lifetime-Lizenz begrenzt; ist es erreicht, werden weitere Zuweisungen abgelehnt.

> Wichtig: Wenn Lifetime-Lizenzen nicht an Seriennummern gebunden wurden, kann es in einem Mischbetrieb mit Lifetime und Perpetual-/Subscription-Lizenzen zu Einschränkungen bei der Einschreibung kommen.

Für Version 26.4.0

Voraussetzung für die Nutzung

Damit die Funktionalität von Lifetime-Lizenzen gegeben ist, muss entweder auf der Global Organisation oder auf dem jeweiligen Tenant mindestens eine Lifetime-Lizenz zugewiesen sein.

> Die Zuweisung kann nur auf Global oder auf einem Tenant erfolgen — nicht gleichzeitig auf beiden Ebenen.

Welche Ebene gilt, zeigt das Feld Art der Zuweisung in den Lizenzinformationen: Bei Global basiert liegen die Lifetime-Lizenzen und ihre Zuweisungen in der Global-Organisation, bei Organisations basiert im jeweiligen Tenant.

Für alle Wege der Zuweisung ist das Recht zum Bearbeiten der Lizenzinformationen erforderlich. Ohne Lifetime-Lizenz sind die Schaltflächen gesperrt (Hinweis Die Organisation hat keine Lifetime-Lizenz).

Unterstützte Plattformen

Aktuell sind Lifetime-Lizenzen nur für folgende Plattformen verfügbar:

- iOS / iPadOS
- Android Enterprise

Nicht unterstützte Plattformen werden weiterhin über andere Lizenztypen lizenziert, z. B.:

- Perpetual – läuft bis zur Kündigung
- Subscription – läuft bis zum definierten End-of-Life (EoL)

Keine Rücknahme möglich

Ein Entziehen bereits übermittelter Lifetime-Lizenzen ist nicht möglich.

Möglichkeiten zur Zuweisung von Lifetime-Lizenzen

Es gibt aktuell 4 Möglichkeiten, Lifetime-Lizenzen zuzuweisen:

1. Über Auto-Einschreibungen

Lifetime-Lizenzen können auf Globaler oder Tenant-Ebene über Auto-Einschreibungen zugewiesen werden. Dazu werden in `Geräte` → `Auto-Einschreibungen` die gewünschten Einträge markiert. Anschließend wird die Aktion Seriennummer der Lifetime-Lizenz zuweisen gewählt und der Dialog mit Seriennummern der Lifetime-Lizenz zuweisen bestätigt. Die Zuweisung kann nicht rückgängig gemacht werden.

Die Aktion ist nur verfügbar, wenn eine Lifetime-Lizenz vorhanden ist und alle markierten Einträge eine Seriennummer haben und zur selben Organisation gehören.

Für Version 26.4.0

2. Direkt im Inventar beim Gerät

Die Zuweisung kann direkt im Inventar am Gerät erfolgen. Dazu werden in `Geräte` → `Inventar` die gewünschten Geräte markiert, die Aktion Seriennummer der Lifetime-Lizenz zuweisen gewählt und der Dialog mit Seriennummern der Lifetime-Lizenz zuweisen bestätigt.

Voraussetzungen:

- die Zuweisung erfolgt auf dem Tenant
- das Gerät verfügt über eine Seriennummer
- alle markierten Geräte gehören zur selben Organisation

Für Version 26.4.0

3. Bei einer manuellen Einschreibung auf einem Tenant

Lifetime-Lizenzen können im Rahmen einer manuellen Einschreibung auf einem Tenant zugewiesen werden. Beim Anlegen einer Einschreibung unter `Geräte` → `Einschreibungen` für iOS / iPadOS oder Android Enterprise steht im Bereich Konfiguration der Schalter Eine Lifetime-Lizenz, nach erfolgreicher Einschreibung für die Seriennummer des Geräts, beanspruchen.

Der Schalter wird nur angezeigt, wenn der Organisation eine Lifetime-Lizenz zur Verfügung steht. Er lässt sich nur beim Anlegen der Einschreibung setzen, nicht beim späteren Bearbeiten. Relution bindet die Seriennummer erst nach erfolgreicher Einschreibung an die Lifetime-Lizenz. Diese Bindung lässt sich nicht rückgängig machen.

> Bei iOS / iPadOS prüft Relution die Gerätelizenz bereits vor der Einschreibung. Sind im Mischbetrieb keine Perpetual- oder Subscription-Lizenzen mehr frei, schlägt die Einschreibung fehl. In diesem Fall wird die Seriennummer vorher über Auto-Einschreibungen oder einen CSV-Upload (Wege 1 oder 4) zugewiesen.

4. Über CSV-Upload

Für Version 26.4.0

Die Zuweisung ist außerdem über einen CSV-Upload möglich. Dazu wird oben rechts das Support-Menü (Fragezeichen-Symbol) geöffnet und Lizenzinformationen gewählt. Im Bereich Lizenzzuweisungen öffnet die Schaltfläche Über CSV hochladen den Import. Die CSV-Datei enthält eine Spalte `serialNumber` mit einer Seriennummer pro Zeile.

Den Bereich Lizenzzuweisungen gibt es nur, wenn eine Lifetime-Lizenz vorhanden ist. Wo er erscheint, hängt von der Art der Zuweisung ab: Bei Global basiert nur in der Global-Organisation, bei Organisations basiert nur auf dem Tenant, auf dem die Lifetime-Lizenzen liegen.

Bereits zugewiesene Seriennummern werden beim Import übersprungen. Ist das Gerätelimit der Lifetime-Lizenz erreicht, werden die übrigen Zeilen als fehlgeschlagen gemeldet.

Für Version 26.4.0

Übersicht der Zuweisungen

Der Bereich Lizenzzuweisungen in den Lizenzinformationen listet alle an die Lifetime-Lizenz gebundenen Seriennummern auf, unabhängig vom Weg der Zuweisung. Zu jedem Eintrag werden unter anderem Datum der Zuweisung, Zugewiesen durch, Gerätename und Organisation angezeigt.

Zusammenfassung

- Lifetime-Lizenzen gelten lebenslang pro Gerät
- sie sind fest an die Seriennummer gebunden
- eine Übertragung auf andere Geräte ist nicht möglich
- bereits übermittelte Lifetime-Lizenzen können nicht entzogen werden
- aktuell werden nur iOS / iPadOS und Android Enterprise unterstützt
- nicht unterstützte Plattformen benötigen weiterhin andere Lizenztypen (z. B. Perpetual oder Subscription)

Lizenzverwaltung durch Partner

Die Verwaltung der eigenen Lizenzen lässt sich an einen Partner oder Dienstleister übergeben. Dazu wird der in Relution angezeigte Verbindungsschlüssel (Connection Key) an den Partner übermittelt. Relution erhält diesen Schlüssel bei der Lizenzprüfung vom Lizenzserver. Mit diesem Schlüssel verbindet sich der Partner über den Lizenzserver mit der Organisation und kann anschließend die Lizenzen verwalten.

Diese Verbindung lässt sich nicht nur für die Global-Organisation, sondern auch für einzelne Tenants herstellen, die durch den Partner verwaltet werden.

> Der Verbindungsschlüssel gewährt Zugriff auf die Lizenzverwaltung der eigenen Organisation. Er sollte ausschließlich über einen vertrauenswürdigen, sicheren Weg übermittelt werden.

Verbindungsschlüssel kopieren (Kunde)

1. In Relution anmelden und in die Global-Organisation bzw. in den Tenant wechseln, dessen Lizenzen verwaltet werden sollen.
2. Oben rechts das Support-Menü (Fragezeichen-Symbol) öffnen und Lizenzinformationen wählen. Der Eintrag erscheint nur mit dem Leserecht für Lizenzinformationen.
3. Im Bereich Allgemein den Wert des Feldes Verbindungsschlüssel kopieren, z. B. über die Kopier-Schaltfläche neben dem Wert.

Der Verbindungsschlüssel wird erst nach einer erfolgreichen Lizenzprüfung angezeigt. Ist das Feld leer, etwa weil keine Verbindung zum Lizenzserver bestand, lässt sich die Lizenzprüfung im selben Bereich über die Schaltfläche bei Zuletzt durchgeführte Lizenzprüfung erneut anstoßen.

Für Version 26.4.0

Für Version 26.4.0

Verbindungsschlüssel übermitteln

Der kopierte Verbindungsschlüssel wird an den Partner oder Dienstleister übermittelt, der die Lizenzverwaltung übernehmen soll.

Organisation verbinden (Partner)

1. Der Partner meldet sich am Lizenzserver an: https://license.relution.io →
2. In der Seitennavigation Tenants öffnen und auf Connect klicken.
3. Den Verbindungsschlüssel (Connection Key) in das Eingabefeld einfügen und mit Connect bestätigen.

Für Version 26.4.0

Ergebnis

Die Organisation ist nun mit dem Partner verbunden und erscheint in dessen Tenants-Liste. Der Partner kann ab sofort die Lizenzen der verbundenen Organisation verwalten.

Zusammenfassung

- Die Lizenzverwaltung kann an einen Partner oder Dienstleister delegiert werden.
- Grundlage ist der Verbindungsschlüssel, der sich in den Lizenzinformationen findet.
- Die Verbindung ist sowohl für die Global-Organisation als auch für einzelne Tenants möglich.
- Der Verbindungsschlüssel sollte nur über einen sicheren Weg übermittelt werden.

Für Version 26.4.0

TeamViewer konfigurieren

Mit dem Relution Lizenz-Add-On für die TeamViewer-Fernwartung ist die TeamViewer-Lizenz in der Relution-Lizenz enthalten. In diesem Fall lässt sich auch ein bereits angelegtes TeamViewer-Konto ohne eigene TeamViewer-Lizenz direkt mit Relution verknüpfen.

Mit Relution lässt sich die TeamViewer-App direkt auf den verwalteten Geräten verteilen; Fernwartungssitzungen lassen sich über das Relution-Portal starten.

Voraussetzungen

Für die TeamViewer-Integration im Lizenzmodus Lizenz enthalten ist eine zusätzliche Lizenz für dieses Add-On erforderlich. Der Erwerb erfolgt über das Relution-Vertriebsteam.

Unterstützte Plattformen

Nach erfolgreicher Verknüpfung können Fernwartungssitzungen über Relution auf den folgenden Plattformen initiiert werden:

- Android Enterprise
- macOS
- Windows

Für Version 26.4.0

Weitere Informationen zur Registrierung des Geräts stehen unter Fernwartungssitzungen → zur Verfügung.

Konto einrichten

Die Verknüpfung erfolgt im Relution-Portal unter `Einstellungen` → `Fernwartung`: Neben Teamviewer-Konto verbinden wird auf Verbinden geklickt. Anschließend erfolgt die Anmeldung mit den Zugangsdaten des TeamViewer-Kontos, womit die Einrichtung abgeschlossen ist. Die Schaltflächen auf dieser Seite stehen nur mit der Berechtigung zum Ändern der Fernwartungseinstellungen zur Verfügung.

Nach der Verknüpfung wird das TeamViewer-Konto als Tenant-Konto unter dem Relution-Anbieter-Konto mit der eigenen Organisation verknüpft. Unter Kontoinformationen zeigt die Seite anschließend Account (E-Mail-Adresse), Name und Beschreibung des TeamViewer-Kontos an. Die Verbindung lässt sich jederzeit über Verbindung prüfen testen. Sollten dabei Probleme auftreten, kann das Konto über die Schaltfläche Verbinden neben Teamviewer Account neu verbinden erneut verknüpft werden, um die Integration mit TeamViewer wiederherzustellen.

Voraussetzung für die Einrichtung ist das Add-On für die enthaltene TeamViewer-Lizenz (in den Lizenzinformationen: Teamviewer Fernunterstützung). Unter Lizenzmodus muss Lizenz enthalten angezeigt werden. Relution legt den Modus anhand der Lizenz automatisch fest; er ist nicht wählbar. Wird ein falscher Modus angezeigt, aktualisiert eine Lizenzprüfung die verfügbaren Funktionen. Sie wird in den Lizenzinformationen (über das Support-Menü (Fragezeichen-Symbol) oben rechts) mit der Schaltfläche bei Zuletzt durchgeführte Lizenzprüfung ausgelöst. Fehlt das Add-On, während Lizenz enthalten aktiv ist (z. B. nach Ablauf der Lizenz), zeigt die Seite einen Warnhinweis an.

Ein TeamViewer-Konto lässt sich nur mit einer Organisation verknüpfen. Ist es bereits mit einer anderen Organisation verknüpft, wird die Verknüpfung mit einer entsprechenden Fehlermeldung abgelehnt.

Mehrere Organisationen

Die Verbindung wird entweder in einer übergeordneten Organisation (global oder Meta-Organisation) oder in einzelnen Unterorganisationen eingerichtet, nicht in beiden. Ist sie bereits in einer übergeordneten Organisation eingerichtet, gilt sie auch für deren Unterorganisationen; dort weist ein Hinweis darauf hin, und die Schaltflächen werden nicht angezeigt. Ist sie in einer Unterorganisation eingerichtet, lässt sie sich in der übergeordneten Organisation erst konfigurieren, nachdem sie in allen Unterorganisationen entfernt wurde.

Für Version 26.4.0

Konto entfernen

Im Abschnitt Konto entfernen trennt die Schaltfläche Trennen neben Trennen des Teamviewer-Kontos die Verbindung. Dabei wird der TeamViewer-Tenant deaktiviert, und die TeamViewer-Anmeldedaten der Geräte der Organisation werden aus Relution entfernt. Ein Wechsel zurück in den Lizenzmodus Eigene Lizenz ist erst nach dem Trennen möglich.

Fernwartungssitzungen

Die Integration von TeamViewer mit Relution ermöglicht es, über das Relution-Portal effiziente Fernwartung für verwaltete Geräte bereitzustellen. Nachdem das TeamViewer-Konto in den Fernwartungs-Einstellungen konfiguriert und die TeamViewer Host-App auf dem Gerät installiert wurde, können sowohl beaufsichtigte als auch unbeaufsichtigte Fernwartungssitzungen gestartet werden.

Dieser Artikel erklärt die Einrichtung und Verteilung der TeamViewer Host-App auf Geräten mit Android Enterprise, macOS und Windows sowie die Registrierung des Geräts für die Fernwartung und das Starten von Fernwartungssitzungen über Relution.

Geräteregistrierung

Um ein Gerät zu registrieren, ist die Installation der TeamViewer Host-App erforderlich. Die Aktion Für Fernwartung registrieren ruft anschließend die für Fernwartungssitzungen erforderlichen TeamViewer-Anmeldedaten ab. Ausgeführt wird sie von der Relution Companion-App der jeweiligen Plattform (Android Enterprise: Relution-App, macOS: macOS Companion, Windows: Windows Companion). Ist die Companion-App nicht aktiv, wird das Gerät nicht registriert.

- Android Enterprise: Die Aktion wird automatisch ausgelöst, sobald das Gerät die TeamViewer Host-App als installiert meldet.
- macOS: Die Aktion wird nach der Installation automatisch ausgelöst, sofern der macOS Companion aktiviert ist (`Einstellungen` → `Relution Client Apps`, Schalter macOS Companion aktivieren). Benutzerseitig eingeschriebene Macs (User Enrollment) werden nicht unterstützt.
- Windows sowie alle Fälle ohne automatische Registrierung: Die Aktion lässt sich manuell über den Fernwartungsdialog senden (siehe Fernwartungssitzungen starten →).

Wird die TeamViewer Host-App vom Gerät deinstalliert, entfernt Relution die Registrierung des Geräts automatisch.

Im Folgenden wird erläutert, wie die TeamViewer-Apps über Relution verteilt und auf den Geräten je nach Plattform installiert werden.

Für Version 26.4.0

Android Enterprise

Eine Apps verwalten →-Konfiguration im Relution-Portal erstellen und die TeamViewer Host-App → sowie das herstellerspezifische TeamViewer-Add-On oder das TeamViewer Universal-Add-On aus dem Managed Google Play Store hinzufügen. Eine weitere Konfiguration ist hier nicht erforderlich.

> Nach der Installation der TeamViewer Host-App muss diese gestartet werden, um die angezeigten Schritte auszuführen und alle erforderlichen Berechtigungen freizugeben.
>
> Schlägt die Für Fernwartung registrieren-Aktion mit dem Fehler verify failed fehl, wurden vermutlich nicht alle erforderlichen Berechtigungen in der TeamViewer Host-App bestätigt.

macOS

Die TeamViewer Host App von der TeamViewer-Webseite herunterladen und die .dmg-Datei als native App im Relution App Store hinzufügen. Eine Erkennungsregel definieren, indem der Bundle-Identifier des TeamViewer Hosts (`com.teamviewer.TeamViewerHost`) angegeben wird.

Die App mithilfe einer App Konformitäts-Konfiguration oder einer Relution Store App bereitstellen-Aktion auf den Geräten verteilen.

Die installierte App auf dem macOS-Gerät öffnen und den eingeblendeten Schritten folgen, um die Installation abzuschließen.

Windows

Die TeamViewer Host-App aus dem WinGet → Store auf den Geräten verteilen. Die WinGet-Paket-ID lautet `TeamViewer.TeamViewer.Host`.

Fernwartungssitzungen starten

Eine Fernwartungssitzung wird aus der Detailansicht des Geräts im Relution-Portal gestartet, und zwar über das Symbol Fernwartungssitzung starten in der Kopfzeile. Alternativ steht in der Geräteliste die Schaltfläche Fernwartungssitzung starten zur Verfügung, sobald genau ein Gerät ausgewählt ist. Beides erfordert die Berechtigung zum Anfordern von Fernwartungssitzungen.

Für Version 26.4.0

Ein Dialog wird geöffnet, in dem zwischen Beaufsichtigter Modus und Unbeaufsichtigter Modus gewählt werden kann; voreingestellt ist Unbeaufsichtigter Modus. Der Hauptunterschied zwischen den Sitzungsarten liegt im Bedarf an Benutzerinteraktion:

- Beaufsichtigter Modus: Ein Benutzer am Gerät muss die Verbindung genehmigen.
- Unbeaufsichtigter Modus: Es ist keine Benutzerinteraktion erforderlich, um die Verbindung zu starten.

Es werden Links für die TeamViewer-Web-App und die TeamViewer-Desktop-Anwendung generiert. Administratoren können einen der beiden Links verwenden, um eine Fernwartungssitzung zu starten.

Um den Desktop-Link zu öffnen, ist eine TeamViewer-Desktop-App, wie beispielsweise der TeamViewer Full Client, erforderlich.

Im beaufsichtigten Modus ist der Link 24 Stunden gültig, im unbeaufsichtigten Modus 5 Minuten. Danach ist eine neue Anfrage erforderlich. Ist das Gerät offline oder über TeamViewer nicht erreichbar, zeigt der Dialog eine entsprechende Fehlermeldung an.

Für Version 26.4.0

Falls die TeamViewer-Anmeldedaten des Geräts noch nicht an Relution übertragen wurden, zeigt der Dialog einen entsprechenden Hinweis an. Unter Gerät registrieren sendet die Schaltfläche Aktion senden die Aktion Für Fernwartung registrieren an das Gerät, danach schließt sich der Dialog. Sobald die Aktion erfolgreich abgeschlossen wurde, lässt sich die Fernwartungssitzung erneut starten.

Nach erfolgreicher Durchführung aller Schritte für die Fernwartungssitzung ist ggf. eine Freigabe auf dem gewünschten Endgerät erforderlich.

Für Version 26.4.0

TeamViewer konfigurieren

Mit Relution lässt sich der eigene TeamViewer-Account mit eigener Lizenz verknüpfen, um eine nahtlose Integration in Relution zu ermöglichen. Darüber hinaus lässt sich der TeamViewer Host effizient auf die verwalteten Geräte verteilen und konfigurieren, was eine unkomplizierte Fernwartung direkt über das Relution-Portal erlaubt.

Voraussetzung

Für die Nutzung der Integration ist eine TeamViewer (Classic) Corporate- oder Tensor-Lizenz erforderlich. Zudem sollte das verwendete Benutzerkonto Zugriff auf das TeamViewer-Portal besitzen, um die notwendigen Einstellungen vornehmen zu können.

Unterstützte Plattformen

Auf den folgenden Plattformen kann die TeamViewer App über Relution verteilt und konfiguriert werden:

- Android Enterprise →
- iOS →
- macOS →
- Windows →

Für Version 26.4.0

Anlegen der Rollout-Konfiguration

Für die Konfiguration der Geräte wird eine *Zuweisungs-ID* benötigt. Dafür die Schritte befolgen, um eine Rollout-Konfiguration → im TeamViewer Portal → zu erstellen.

Um Fernwartungssitzungen mit unbeaufsichtigtem Zugriff auf die Geräte zu ermöglichen, den Benutzern in der Sektion Verwaltung der Zugriffsrechte die Berechtigung für Einfachen Zugriff geben.

Für Version 26.4.0

TeamViewer Konto in Relution verknüpfen

Die Verknüpfung erfolgt im Relution-Portal unter `Einstellungen` → `Fernwartung`. Im Abschnitt Kontoinformationen führt die Schaltfläche Verbinden neben Teamviewer-Konto verbinden zur Anmeldeseite von TeamViewer. Mit der Anmeldung über das TeamViewer-Konto wird die Integration abgeschlossen; anschließend zeigt Relution die Daten des verknüpften Kontos an.

Der Lizenzmodus ergibt sich automatisch aus der Relution-Lizenz: Ohne Add-on für die enthaltene TeamViewer-Lizenz lautet er Eigene Lizenz.

Für Version 26.4.0

Nach erfolgreicher Authentifizierung lässt sich die Verbindung unter Test der Fernwartungsverbindung mit Verbindung prüfen überprüfen. Bei Verbindungsproblemen wird das Konto über Verbinden neben Teamviewer Account neu verbinden erneut autorisiert, um die Integration mit TeamViewer wiederherzustellen. Im Abschnitt Konto entfernen hebt die Schaltfläche Trennen die Verknüpfung wieder auf.

Einschränkungen

Für die Verknüpfung gelten folgende Einschränkungen:

- Ein TeamViewer-Konto lässt sich nur mit einer Organisation verknüpfen. Ist das Konto bereits mit einer anderen Organisation verbunden, lehnt Relution die Verknüpfung ab.
- Ist die Verbindung in einer übergeordneten Organisation (global oder Meta-Organisation) eingerichtet, gilt sie auch für die untergeordneten Organisationen und lässt sich dort nicht ändern. Ist sie bereits in einer Unterorganisation eingerichtet, kann sie global erst konfiguriert werden, nachdem die Einrichtung in allen Unterorganisationen entfernt wurde.

Für Version 26.4.0

Android Enterprise

Dieser Artikel beschreibt die Konfiguration der TeamViewer Host App in Relution, um eine automatische Gerätezuweisung im TeamViewer-Portal zu ermöglichen.

Konfiguration der TeamViewer Host App

Im Relution-Portal eine Apps verwalten →-Konfiguration erstellen und die folgenden zwei Apps aus dem Managed Google Play Store hinzufügen:

1. TeamViewer Host
2. TeamViewer Universal

Anschließend die App-Konfiguration anpassen und die folgenden relevanten Einstellungen definieren:

Name	Beschreibung
Zuweisungs-ID	Zur automatischen Gerätezuweisung als verwaltetes Gerät in TeamViewer.
Partnerliste Gerätename	Anzeigename in der TeamViewer-Weboberfläche.

Für ve

Details zu den Einstellungen

- Zuweisungs-ID Die Zuweisungs-ID aus dem TeamViewer-Portal eintragen, die im Rahmen des Einrichtungsschritts → erhalten wurde.
- Partnerliste Gerätename Den Namen bestehend aus Gerätenamen und Seriennummer mithilfe der Platzhalter konfigurieren, die im Konfigurationsdialog unter Verfügbare Platzhalter aufgeführt sind:

```
${device.name}_${device.serialnumber}
```

Um eine eindeutige Zuordnung der Geräte zwischen Relution und TeamViewer herstellen zu können, muss die Seriennummer im Gerätenamen enthalten sein. Dies wird durch den Platzhalter `${device.serialnumber}` gewährleistet.

Abschluss

Neu hinzugefügte Apps erhalten standardmäßig den Installationstyp Installation erzwungen und werden damit automatisch installiert. Die Konfiguration auf die Android-Enterprise-Geräte anwenden. Sobald die Installation abgeschlossen ist, wird die Zuweisung automatisch durchgeführt und die Geräte erscheinen ordnungsgemäß im TeamViewer-Portal.

Hinweise

> Anmeldung abgebrochen oder Authentifizierung abgelehnt

Wichtige Informationen zur Benutzerinteraktion

Je nach Android-Version unterscheidet sich das Verhalten beim Fernzugriff:

- Android 13 und älter: Bei vielen Geräten (insbesondere mit herstellerspezifischen TeamViewer-Add-ons) funktioniert der Zugriff oft komplett ohne Benutzerinteraktion im Hintergrund.
- Android 14 und neuer: Aufgrund verschärfter Sicherheitsrichtlinien von Google (Media Projection API) erscheint beim Start eines Remote-Zugriffs zwingend ein System-Pop-up. Der Benutzer muss die Freigabe des Bildschirms manuell bestätigen. Dies lässt sich bei Standard-Android-Enterprise-Geräten derzeit nicht umgehen.

Für Version 26.4.0

iOS

Dieser Artikel beschreibt, wie die TeamViewer QuickSupport App auf iOS-Geräten mithilfe von Relution bereitgestellt und konfiguriert werden kann.

Bereitstellung der TeamViewer QuickSupport App

Eine Richtlinie mit einer App Konformität →-Konfiguration erstellen. Die TeamViewer QuickSupport App (Bundle-Identifier: `com.teamviewer.teamviewerQS`) aus dem App Store zur Liste der erforderlichen Apps hinzufügen.

Für Version 26.4.0

App für die Gerätezuordnung konfigurieren

Eine Managed App →-Konfiguration hinzufügen und die TeamViewer QuickSupport App aus dem App Store auswählen. Im Feld Payload die folgenden Schlüssel innerhalb des vorbelegten `<dict>`-Elements (zwischen `<dict>` und `</dict>`) einfügen; außerhalb davon gilt das XML als ungültig und die Konfiguration lässt sich nicht speichern:

```
<key>mdv2AssignmentID</key>
<string>YOUR_ASSIGNMENT_ID</string>
<key>partnerListDeviceName</key>
<string>${device.name}_${device.serialnumber}</string>
```

Für Version 26.4.0

- mdv2AssignmentID: Wird für die automatische Gerätezuordnung als verwaltetes Gerät in TeamViewer verwendet. Die Assignment ID aus dem TeamViewer-Portal eingeben, die während des Einrichtungsprozesses → erhalten wurde.
- partnerListDeviceName: Anzeigename des Geräts in der TeamViewer-Weboberfläche. Den Gerätenamen konfigurieren, indem der Gerätename sowie die Seriennummer wie folgt und mithilfe der vorhandenen Platzhalter angegeben werden: `${device.name}_${device.serialnumber}`

Um eine Verknüpfung zwischen Geräten in Relution und TeamViewer herzustellen, muss die Seriennummer Teil des Gerätenamens sein. Dies wird durch die Verwendung des Platzhalters `${device.serialnumber}` sichergestellt. Der Name lässt sich anders zusammensetzen, solange die Seriennummer darin enthalten bleibt; beim Start einer Sitzung sucht Relution in TeamViewer nach einem Gerät, dessen Name die Seriennummer enthält.

Die Konfigurationen auf die iOS-Geräte anwenden. Nach Abschluss der Installation wird die Gerätezuordnung automatisch durchgeführt, und die Geräte erscheinen im TeamViewer-Portal.

Fernwartungssitzungen auf iOS-Geräten

Fernwartungssitzungen für iOS-Geräte, auch bei iOS Benutzereinschreibung, stehen in Relution nur mit eigener Lizenz zur Verfügung. Der Start erfolgt wie unter Fernwartungssitzungen → beschrieben. Auf dem iOS-Gerät muss die Sitzung in der TeamViewer QuickSupport App durch den Benutzer bestätigt werden.

Für Version 26.4.0

macOS

In diesem Artikel wird beschrieben, wie der TeamViewer Host auf macOS-Geräten über Relution bereitgestellt und konfiguriert werden kann.

Herunterladen des TeamViewer Clients

In das TeamViewer-Portal einloggen und zu `Admin-Einstellungen` → `Rollout-Konfiguration` wechseln, um den macOS-Installer herunterzuladen. Das Paket enthält sowohl den *TeamViewer Full Client* als auch den *TeamViewer Host*, wobei für die Integration mit Relution ausschließlich der *TeamViewer Host* benötigt wird.

Verteilen des TeamViewer Clients

Im Relution-Portal anmelden und zu `Apps` → `App Store` navigieren. Eine neue native App mit der zuvor heruntergeladenen PKG-Datei erstellen. Eine Erkennungsregel vom Typ Package Name anlegen (für macOS-Apps der einzige verfügbare Regeltyp) und darin den Bundle-Identifier des TeamViewer Hosts (`com.teamviewer.TeamViewerHost`) eintragen.

Die App kann entweder über eine Konfiguration vom Typ App Konformität oder durch die Aktion Relution Store App bereitstellen auf die macOS-Geräte verteilt werden.

Für Version 26.4.0

Zuweisung via Skript durchführen

Im Relution-Portal ein Skript für die Plattform macOS erstellen und den folgenden Befehl einfügen:

Skript für den TeamViewer Host:

```
sudo /Applications/TeamViewerHost.app/Contents/Helpers/TeamViewer_Assignment -
assignment_id 'YOUR_ASSIGNMENT_ID' -device_alias
"${device.name}_${device.serialnumber}"
```

`YOUR_ASSIGNMENT_ID` durch die eigene Zuweisungs-ID aus dem TeamViewer-Portal ersetzen, die im Rahmen des Einrichtungsschritts → erhalten wurde.

Um eine Zuordnung der Geräte aus Relution und TeamViewer herstellen zu können, muss die Seriennummer im Gerätenamen enthalten sein. Dies wird durch die Verwendung des Platzhalters `${device.serialnumber}` im Skript gewährleistet. Dieser zusammengesetzte Name wird nach erfolgreicher Registrierung im TeamViewer Portal angezeigt.

Für Version 26.4.0

Voraussetzung für die Ausführung ist der aktivierte macOS Companion (`Einstellungen` → `Relution Client Apps`, Schalter macOS Companion aktivieren). Der macOS Companion wird nur auf Macs ab macOS 12 und nicht auf benutzerseitig eingeschriebenen Macs bereitgestellt; dort lassen sich keine Skripte ausführen. Anders als unter Windows lässt sich das Skript nicht an die App anhängen. Es wird deshalb erst nach der Installation des TeamViewer Hosts ausgeführt, und zwar auf einem dieser Wege:

- einmalig über die Aktion Shell-Skript ausführen (siehe macOS-Aktionen →) oder auf der Seite `Skripte` → `Skripte` über Auf Gerät ausführen,
- zeitgesteuert über eine Konfiguration vom Typ Script in einer macOS-Richtlinie; diese erfasst auch später hinzukommende Macs.

Sobald die Zuweisung abgeschlossen ist, sollten die Geräte im TeamViewer-Portal sichtbar sein.

Windows

Die folgende Anleitung beschreibt die Schritte zur Einrichtung von TeamViewer Host für Windows über Relution, einschließlich der Verteilung des TeamViewer Hosts als Relution Store App und der Erstellung eines Skripts zur Konfiguration der Applikation.

Herunterladen des MSI-Pakets

Zunächst das für die jeweilige Architektur passende MSI-Paket von TeamViewer herunterladen. Dazu im TeamViewer-Portal anmelden. Anschließend zu `Admin-Einstellungen` → `Rollout-Konfiguration` navigieren und das MSI-Paket herunterladen. Der heruntergeladene Installer enthält sowohl den *TeamViewer Full Client* als auch den *TeamViewer Host*, wobei für die Integration mit Relution ausschließlich der *TeamViewer Host* benötigt wird. Weitere Informationen zum Download des MSI-Pakets stehen in der TeamViewer Dokumentation → zur Verfügung.

Anlegen der Relution Store App

Nach dem Herunterladen des MSI-Pakets von TeamViewer im Relution-Portal anmelden. Unter `Apps` → `App Store` eine neue native App mit der zuvor heruntergeladenen MSI-Datei anlegen. Für die App ist mindestens eine Erkennungsregel erforderlich, sonst lässt sie sich nicht speichern. Installation und Skriptausführung übernimmt auf den Geräten der Relution Companion, der deshalb auf den Zielgeräten installiert sein muss: Windows Companion →. Weitere Informationen stehen unter Windows App Installation → zur Verfügung.

Für Version 26.4.0

Anlegen des Zuweisungsskripts

Um den TeamViewer Host auf den Geräten zu konfigurieren, im Relution-Portal unter `Skripte` → `Skripte` ein neues Skript für die Plattform Windows anlegen. Je nach Architektur des Zielgeräts eines der folgenden Skripte verwenden:

Skript für Geräte mit 64-Bit-Betriebssystem:

```
& "C:\Program Files\TeamViewer\TeamViewer.exe" assignment --id $assignmentId --device-alias=${device.name}_${device.serialnumber}
```

Skript für Geräte mit 32-Bit-Betriebssystem:

```
& "C:\Program Files (x86)\TeamViewer\TeamViewer.exe" assignment --id $assignmentId --device-alias=${device.name}_${device.serialnumber}
```

In der Sektion Ausführung im Feld Argumente der Variable `$assignmentId` die Zuweisungs-ID aus dem TeamViewer-Portal zuweisen, die im Rahmen des Einrichtungsschritts → erhalten wurde: `$assignmentId='YOUR_ASSIGNMENT_ID'`. Der Inhalt dieses Felds wird bei der Ausführung an den Anfang des Skripts gesetzt.

Um eine Zuordnung der Geräte aus Relution und TeamViewer herstellen zu können, muss die Seriennummer im Gerätenamen enthalten sein. Dies wird durch die Verwendung des Platzhalters `${device.serialnumber}` im Skript gewährleistet. Dieser zusammengesetzte Name wird nach erfolgreicher Registrierung im TeamViewer Portal angezeigt.

Für Version 26.4.0

Ausführung des Skripts nach der Installation

Die im Abschnitt „Anlegen der Relution Store App“ angelegte TeamViewer Host MSI App öffnen. Im Reiter Skripte das zuvor erstellte Konfigurationsskript unter Skripte nach der Installation hinzufügen. Mehrere Skripte lassen sich dort per Drag & Drop in ihrer Ausführungsreihenfolge anordnen. Der Reiter erscheint nur bei klassischen Windows-Apps der eigenen Organisation und nur mit Leserechten für Skripte.

Die Anwendung auf den gewünschten Windows-Geräten über eine Konfiguration App Konformität oder die Aktion Relution Store App bereitstellen installieren.

Nach der Installation des TeamViewer Hosts wird das Skript automatisch ausgeführt. Sobald die Konfiguration abgeschlossen ist, sollten die Geräte im TeamViewer-Portal sichtbar sein.

Für Version 26.4.0

Fernwartungssitzungen

Sobald das TeamViewer-Konto mit einer gültigen Lizenz in den Relution-Einstellungen konfiguriert ist und das Gerät erfolgreich im TeamViewer-Portal registriert wurde, lassen sich unbeaufsichtigte Fernwartungssitzungen durchführen. Dies gilt für Android Enterprise (vollständig verwaltete Geräte und Arbeitsprofile), macOS und Windows. Mit eigener Lizenz werden zusätzlich iOS-Geräte unterstützt, auch bei iOS Benutzereinschreibung. Für iOS sind mit der TeamViewer QuickSupport App nur beaufsichtigte Sitzungen möglich, die eine aktive Benutzerinteraktion erfordern.

Auf dem Endgerät muss der passende TeamViewer-Client installiert und im TeamViewer-Portal registriert sein (siehe Android Enterprise →, iOS →, macOS → und Windows →). Zum Öffnen der Sitzung über den Link für Administratoren wird auf dem Rechner des Administrators eine TeamViewer-Desktop-Anwendung benötigt, z. B. der TeamViewer Full Client.

Relution ordnet das Gerät über die Seriennummer zu: In TeamViewer wird nach einem Gerät gesucht, dessen Name die Seriennummer aus Relution enthält. Der in den Rollout-Artikeln konfigurierte Gerätename muss deshalb den Platzhalter `${device.serialnumber}` enthalten.

Fernwartungssitzung starten

Eine Fernwartungssitzung wird in der Detailansicht des Geräts über das Symbol Fernwartungssitzung starten in der Kopfzeile gestartet. Das Symbol erscheint nur, wenn ein TeamViewer-Konto verknüpft ist, die Registrierungsart des Geräts unterstützt wird und der angemeldete Benutzer berechtigt ist, Fernwartung anzufordern.

Für Version 26.4.0

Mit eigener Lizenz entfällt die Auswahl des Sitzungstyps; Relution erzeugt sofort einen Link für eine unbeaufsichtigte Fernwartungssitzung. Der Dialog Fernwartung beginnen zeigt ihn unter Link für Administratoren: als Link Desktop an; über das Symbol daneben lässt er sich in die Zwischenablage kopieren. Der generierte Link kann ausschließlich mit einer installierten TeamViewer-Desktop-Anwendung geöffnet werden.

Nach erfolgreicher Durchführung aller Schritte für die Fernwartungssitzung ist ggf. eine Freigabe auf dem gewünschten Endgerät erforderlich.

Meldungen im Dialog

Kann keine Sitzung erzeugt werden, zeigt der Dialog statt des Links eine der folgenden Meldungen:

- „Das Gerät konnte in TeamViewer nicht gefunden werden.“ In TeamViewer gibt es kein Gerät, dessen Name die Seriennummer des Geräts enthält. Die Zuweisung und den Gerätenamen gemäß dem jeweiligen Rollout-Artikel prüfen.
- „Das Gerät ist derzeit offline oder nicht über Teamviewer erreichbar“ Das Gerät ist nicht erreichbar oder die Anfrage an TeamViewer ist fehlgeschlagen. Der Versuch kann später wiederholt werden.

Für Version 26.4.0

Microsoft bedingter Zugriff

Microsoft bedingter Zugriff (Conditional Access) → oder Bedingter Zugriff ist die Zero-Trust-Richtlinien-Engine von Microsoft. In dieser Dokumentation wird zur besseren Lesbarkeit die Abkürzung `MSCA` verwendet. Sind die Relution-Benutzer über `Entra ID` synchronisiert, lässt sich zusätzlich der bedingte Zugriff aktivieren. Sobald ein von Relution verwaltetes Gerät seinen Status auf „konform“ oder „nicht konform“ ändert, werden diese Informationen automatisch an Microsoft übermittelt. Basierend auf den Bedingter Zugriff-Richtlinien → ist es dann möglich, beispielsweise Benutzern den Zugriff auf bestimmte Anwendungen zu verweigern, wenn ihr Gerät als nicht konform gilt.

Unterstützte Plattformen

- Android Enterprise
- iOS
- macOS
- Windows
  - Das Gerät muss über `Microsoft Entra Join` oder `Windows Autopilot` registriert worden sein.

Voraussetzungen

Für Version 26.4.0

Um den Bedingten Zugriff mit Relution nutzen zu können, müssen folgende Bedingungen erfüllt sein:

- Relution in Version 5.33.1 oder höher erforderlich.
- Eine aktive Microsoft Entra ID P1-Lizenz. Weitere Informationen sind hier → zu finden.
- Eine konfigurierte Benutzersynchronisierung mit `Entra ID`, siehe Verknüpfen von Entra ID und Relution →
- Damit Entra Benutzer sich in Relution anmelden können, muss zusätzlich OIDC → konfiguriert werden.

Für Android Enterprise, iOS und macOS gilt zusätzlich:

- Relution ist in Intune für die jeweilige Plattform als Compliance-Partner hinzugefügt, siehe Plattformen einrichten →.
- Die betroffenen Benutzer verfügen über eine Intune-Lizenz. Fehlt sie, wird das Gerät auf der Einstellungsseite Bedingter Zugriff mit dem Status Intune-Lizenz fehlt aufgeführt.
- Die Konfiguration `Bedingter Zugriff` muss über eine entsprechende Richtlinie auf die betroffenen Geräte angewendet werden (unter iOS und macOS nur bei Geräteregistrierung). Optional kennzeichnet die Konfiguration ein Gerät als nicht konform, solange der Nutzer es noch nicht registriert hat, und fordert den Nutzer per Push-Benachrichtigung zur Registrierung auf, siehe Bedingter Zugriff (Richtlinie) →.
- Das Gerät wird über den Relution Agent → mit `Entra ID` verknüpft.
- Eine `Broker-App` für die Authentifizierung:
  - Android Enterprise & iOS: `Microsoft Authenticator` (wird automatisch installiert, sobald Relution in Intune als Compliance-Partner für die Plattform hinzugefügt ist und dem Gerät die Konfiguration `Bedingter Zugriff` per Richtlinie zugewiesen wurde)
  - macOS: `Company Portal App` - muss auf dem Gerät installiert sein. Kann hier → heruntergeladen werden.

Für Windows gibt es weder die Konfiguration `Bedingter Zugriff` noch eine Broker-App oder einen Compliance-Partner in Intune. Der bedingte Zugriff für Windows wird auf der Einstellungsseite Bedingter Zugriff über Aktivieren bei Conditional Access für Windows aktivieren eingeschaltet, siehe Plattformen einrichten →.

Einschränkungen

- `Bedingter Zugriff` kann derzeit nicht innerhalb der globalen Organisation konfiguriert werden.
- Die Benutzer müssen über den Entra Sync importiert worden sein; zuvor z. B. per LDAP synchronisierte Benutzer können nicht verwendet werden.
- Die per Entra Sync importierten Benutzer müssen in derselben Organisation vorhanden sein wie die zugehörigen Geräte.
- Unter iOS und macOS wird die Benutzerregistrierung (User Enrollment/BYOD) nicht unterstützt; die Konfiguration `Bedingter Zugriff` steht nur für die Geräteregistrierung zur Verfügung.
- `Geteiltes iPad` hat verschiedene Einschränkungen bei CA-Konfigurationen, z. B. wird die Anforderung, dass das Gerät als konform markiert sein muss, nicht unterstützt. Dadurch erscheint in Relution auf der Karte Microsoft Entra ID des Geräts der Hinweis Microsoft Bedingter Zugriff ist nicht eingerichtet. Weitere Informationen hierzu sind in der Microsoft-Dokumentation hier → zu finden.

Für Version 26.4.0

Plattformen einrichten

Diese Einrichtungsanleitung zeigt Schritt für Schritt, wie sich `Relution` erfolgreich mit `Microsoft Entra/Intune` verbinden lässt, um bedingten Zugriff für die verwalteten Geräte einzurichten. Vor Beginn sollte sichergestellt werden, dass die Anforderungen → erfüllt sind.

Einrichtung vom bedingten Zugriff mit Relution und Entra ID

Während der folgenden Einrichtungsschritte wird Relution mit Microsoft Entra ID und Microsoft Intune verbunden, um den Bedingten Zugriff zu aktivieren:

1. Zuerst `eine Entra ID-Anwendung erstellen`, die den Zugriff des Servers über den Relution Microservice validiert.
2. `Der Multi-Tenant-App Relution die Zustimmung erteilen`, die Relution benötigt, um den Konformitäts-Status der Geräte an die `Entra ID` zu melden.
3. Hinzufügen von `Relution` als Compliance-Partner in `Intune`.
4. Überprüfen, ob die Einrichtung korrekt ist.

Jeder Schritt ist für den nächsten entscheidend. Alle Schritte sorgfältig nacheinander ausführen und bei Aufforderungen zur Überprüfung sicherstellen, dass die Meldung Überprüfung erfolgreich (beim Synchronisieren Synchronisierung erfolgreich) angezeigt wird.

Für Version 26.4.0

Navigieren zu “Bedingter Zugriff”

Sobald Entra ID → korrekt konfiguriert und die Benutzer erfolgreich synchronisiert wurden, lässt sich in den Einstellungen zu `Bedingter Zugriff` navigieren.

Plattformen aktivieren: Android Enterprise, iOS und macOS

Für Version 26.4.0

Der Assistent zum Aktivieren der gewünschten Plattformen wird im Abschnitt Allgemein über Hinzufügen bei Verbindung hinzufügen gestartet.

Assistent (1): Entra ID-Anwendung erstellen

Dieser Schritt lässt sich auch überspringen, indem die Anwendung wiederverwendet wird, die bei der Entra ID-Einrichtung verwendet wurde. Relution empfiehlt die Nutzung zweier separater Anwendungen, um Berechtigungen und Einsatzzwecke zu trennen.

Eine neue `Entra ID-Anwendung` erstellen, damit der Relution Microservice den Zugriff auf den Mandanten verifizieren kann. Eine einfache App-Registrierung ist ausreichend – eine vollständige MDM-App ist nicht erforderlich. Die Anwendung muss sich im selben Mandanten befinden wie die konfigurierte Entra ID. Über Entra ID öffnen im Assistenten geht es zu den Entra ID-App-Registrierungen →. Nach der Erstellung der App wird mit Weiter zum nächsten Schritt gewechselt; dort wird die Anwendungs-ID eingetragen.

Assistent (2): Anwendungs-IDs und Clientschlüssel hinterlegen

Die App benötigt außerdem einen geheimen Client-Schlüssel. Einen solchen Schlüssel erstellen und die Anwendungs-ID (Client) sowie das Client-Geheimnis in die Eingabefelder eintragen. Nach erfolgreicher Überprüfung über Überprüfen mit dem nächsten Schritt fortfahren.

Assistent (3): API verfügbar machen

Aufgrund technischer Einschränkungen bei der Validierung von Tokens durch Microsoft muss eine API freigegeben und ein benutzerdefinierter Bereich hinzugefügt werden. Über Expose-API öffnen im Assistenten wird die entsprechende Einstellungsseite der Entra-App direkt geöffnet. Auf der Einstellungsseite API freigeben der Entra-App folgende Schritte ausführen:

1. Auf Bereich hinzufügen klicken.
2. Die erforderlichen Informationen eintragen:
   - Name des Bereichs: `Relution.Auth`
   - Sichtbarkeit: Die Option Nur Administratoren aktivieren
   - Anzeigename und Beschreibung: beliebige Angaben möglich, empfohlen wird beispielsweise: `Von Relution zur Identifizierung der Mandanteneigentümerschaft verwendet`.
3. Auf Bereich hinzufügen klicken.
4. Der Bereich sollte nun unter Von dieser API definierte Bereiche angezeigt werden.

Oben in der Ansicht API freigeben in Entra wird eine Anwendungs-ID-URI angezeigt. Der passende Wert wird im Assistenten unter Art des Geltungsbereichs ausgewählt: `api://<Anwendungs-ID>` für eine neu erstellte App (Schritt 1) oder die Relution-Server-URL (`https://<Relution-Host>`), falls die App aus der Entra ID-Einrichtung wiederverwendet wird. Weicht die Anwendungs-ID-URI davon ab, wird die dritte Option gewählt (im Portal derzeit als Vordefiniert beschriftet) und die Anwendungs-ID-URI im Feld Benutzerdefiniert Geltungsbereich eingetragen.

Für Version 26.4.0

Dieser Schritt sollte sich nun im Assistenten über Überprüfen erfolgreich überprüfen lassen.

Assistent (4): Relution als Compliance-Partner in Intune hinzufügen

In der Einstellung Intune-Partner-Compliance-Verwaltung → muss `Relution` als Partner für jede Plattform hinzugefügt werden, die synchronisiert werden soll. Die Seite lässt sich über Partnereinstellungen öffnen im Assistenten direkt aufrufen.

Für Version 26.4.0

Für Version 26.4.0

1. Auf Compliance-Partner hinzufügen klicken.
2. Die Plattform auswählen, die synchronisiert werden soll (diese Schritte lassen sich für alle Plattformen wiederholen): Android, iOS oder macOS. Windows wird nicht über den Compliance-Partner aktiviert, sondern im Abschnitt Windows-Plattform unterstützen →.
3. Eine Gruppe von Benutzern zuweisen, die synchronisiert werden sollen. Auch Alle Benutzer hinzufügen lässt sich auswählen – dabei jedoch darauf achten, sich später nicht selbst auszusperren.
    - Hinweis: Die Option Gruppen ausschließen hat derzeit keine Wirkung.
4. Nachdem überprüft wurde, dass alles korrekt ausgewählt wurde, auf Erstellen klicken.
5. `Relution` sollte für diese Plattform nun mit dem Status `🔄 Aktivierung ausstehend` angezeigt werden. Der Status kann abweichen, wenn dies nicht die erste Einrichtung ist.

Für Version 26.4.0

Für Android Enterprise und iOS verteilt Relution die Broker-App `Microsoft Authenticator` selbst. Für macOS muss die `Company Portal App` selbst auf die Geräte verteilt werden, z. B. über den Relution Store und eine Richtlinie, siehe Voraussetzungen →.

Assistent (5): Administrator-Zustimmung erteilen

Dieser Schritt schlägt fehl, wenn im vorherigen Schritt keine Plattform verknüpft wurde.

Der `Multi-Tenant-App Relution` die erforderliche `Admin-Zustimmung` erteilen. Dies erlaubt `Relution`, den Compliance-Status der `Entra ID-Geräte` zu verwalten. Ein Klick auf Einwilligung öffnen speichert die bisherigen Angaben des Assistenten und öffnet die Zustimmungsseite in einem neuen Tab (möglicherweise wird dieser vom Browser als Pop-up blockiert). Nach erfolgreicher Zustimmung erscheint eine Bestätigungsseite mit der Meldung `Success! You can now close this tab`. Anschließend lässt sich dieser zusätzliche Tab schließen. Im Assistenten lässt sich die Zustimmung über Überprüfen kontrollieren, bevor es weitergeht. Ist die Zustimmung bereits erteilt, ist Einwilligung öffnen deaktiviert.

Für Version 26.4.0

Assistent (6): Entra ID-Gruppen synchronisieren

Als letzter Schritt müssen die `Entra ID-Gruppen` synchronisiert werden. Im Assistentenschritt Synchronisieren wird zunächst über Überprüfen die Konfiguration geprüft. Erst nach erfolgreicher Prüfung lässt sich Entra ID Gruppen synchronisieren anklicken; bis dahin ist die Schaltfläche gesperrt und ein Hinweis weist auf die fehlende Prüfung hin. Bei der Synchronisation stellt `Relution` eine korrekte Einrichtung sicher und synchronisiert die Gruppen, die im Assistenten in Schritt 4 in Intune zugewiesen wurden. Abschließend wird der Assistent über Speichern beendet.

In den Einstellungen für Intune Partner Compliance Management → sollte `Relution` nun als `✅ Aktiv` angezeigt werden.

Werden in den Compliance-Partner-Einstellungen in Intune Einstellungen angepasst, z. B. Gruppen oder Plattformen hinzugefügt/entfernt, muss die Synchronisation erneut manuell gestartet werden.

Windows-Plattform unterstützen

Für Windows-Geräte ist weder der Assistent noch ein Compliance-Partner in Intune erforderlich. Auf der Einstellungsseite Bedingter Zugriff wird im Abschnitt Windows bei Conditional Access für Windows aktivieren auf Aktivieren geklickt. Die Änderung wird sofort übernommen.

Für Version 26.4.0

Windows-Geräte sollten nun ihren Status erfolgreich synchronisieren.

Verbindung verwalten

Nach der Einrichtung zeigt die Einstellungsseite Bedingter Zugriff folgende Bereiche:

- Allgemein: Verbindung bearbeiten öffnet den Assistenten erneut, Verbindung löschen entfernt die Verbindung. Über Conditional Access deaktivieren werden keine Konformitätsänderungen mehr an Microsoft gesendet, Conditional Access aktivieren schaltet die Übertragung wieder ein. Über Überprüfen lässt sich die Konfiguration jederzeit prüfen.
- Angaben zum Partner: Entra ID Gruppen synchronisieren startet die Synchronisation manuell, z. B. nach Änderungen an Gruppen oder Plattformen in Intune. Zusätzlich werden Letzter Kontakt, Letzte Synchronisierung und die Plattformen (Android, iOS, macOS) angezeigt, deren Gruppen synchronisiert wurden.
- Geräte, bei denen während der letzten Synchronisierung Probleme aufgetreten sind: Liste der betroffenen Geräte mit Benutzer, Status (z. B. Intune-Lizenz fehlt) und Letzte Fehlermeldung. Nach Behebung der Ursache, z. B. Zuweisung einer Intune-Lizenz, wird die Übertragung über Synchronisieren erneut angestoßen.

Ist die Verbindung fehlerhaft, z. B. wegen fehlender Admin-Zustimmung, ungültiger Anmeldeinformationen (abgelaufenes Client-Geheimnis), fehlendem Bereich `Relution.Auth` oder ohne in Intune verknüpfte Plattform, zeigt die Seite einen Warnhinweis. Nach Behebung des Problems müssen die Partnerdetails über Entra ID Gruppen synchronisieren erneut synchronisiert werden.

Verwandte Themen

- Bedingter Zugriff Übersicht → — Anforderungen und Grundlagen zum bedingten Zugriff.
- Microsoft Entra ID verknüpfen → — Verknüpfung von Entra ID und Synchronisierung der Benutzer, Voraussetzung für den bedingten Zugriff.
- OIDC mit Entra → — Anmeldung der Entra-Benutzer an Relution über OpenID Connect.

Für Version 26.4.0

Einrichten von Intune

Diese Kurzanleitung zeigt, wie sich `Richtlinien für Bedingten Zugriff` in `Microsoft Intune` einrichten und testen lassen. Mit diesen Richtlinien wird festgelegt, welche Maßnahmen bei nicht konformen Geräten greifen sollen – etwa Zugriffsbeschränkungen auf Anwendungen. Weitere Informationen sind in der offiziellen Dokumentation → zu finden.

Eine fehlerhafte Konfiguration der bedingten Zugriffsrichtlinien kann dazu führen, dass sich Benutzer nicht mehr anmelden können. Relution übernimmt keine Haftung für Schäden durch inkorrekte Einstellungen.

Werden in den Zielressourcen strenge Richtlinien für Alle Cloud-Apps festgelegt, können Benutzer ihre Geräte ebenfalls nicht registrieren.

Empfehlungen für die Einführung

`Relution` empfiehlt, bei der Einführung von Bedingtem Zugriff vorsichtig vorzugehen:

- Zunächst entweder beginnen
  - mit der Verwendung von Richtlinien im Modus Nur Bericht, anstatt sie direkt anzuwenden
  - ODER mit zunächst nur ausgewählten Benutzern, um sicherzustellen, dass alles wie erwartet funktioniert.
- Die Auswahl von Alle Cloud-Apps in den Zielressourcen vermeiden. Werden Alle Cloud-Apps mit strengen Richtlinien ausgewählt, können Benutzer ihre Geräte nicht registrieren. Derzeit kann die `Microsoft Broker-App` nicht im Filter Ausschließen ausgewählt werden, der immer aktiviert sein muss.
  - Die Auswahl von Office 365 → ist empfehlenswert.

Für Version 26.4.0

Beispielkonfiguration in Intune

Richtlinien können unter Intune > Endpunktsicherheit > Bedingter Zugriff > Richtlinien → konfiguriert werden.

Siehe den folgenden Screenshot als Beispiel:

Für Version 26.4.0

1. Unter Benutzer werden die Benutzer ausgewählt, auf die die Richtlinie angewendet wird.
2. Unter Zielressourcen wird festgelegt, dass die Richtlinie für ausgewählte Ressourcen gilt.
3. Als Ressource wird in diesem Beispiel Microsoft Teams ausgewählt.
4. Unter Gewähren wird die Zugriffsanforderung definiert, z. B. nur konforme Geräte zulassen.
   -
5. Die Richtlinie wird auf Nur Bericht gesetzt, um sie ohne Auswirkungen zu testen.

Die Anforderung, dass das Gerät als konform markiert sein muss, wirkt bei Android Enterprise, iOS und macOS nur für Geräte, denen in Relution die Konfiguration `Bedingter Zugriff` per Richtlinie zugewiesen ist und deren Benutzer in Intune über den Compliance-Partner Relution synchronisiert werden. Die betroffenen Benutzer benötigen außerdem eine Intune-Lizenz; fehlt sie, wird das Gerät auf der Einstellungsseite Bedingter Zugriff mit dem Status Intune-Lizenz fehlt aufgeführt. Nach Zuweisung der Lizenz wird die Übertragung dort über Synchronisieren erneut angestoßen. Weitere Informationen: Voraussetzungen → und Plattformen einrichten →.

Für Version 26.4.0

Sicherheitsstandards deaktivieren

Manchmal wird beim Einrichten von Richtlinien eine Fehlermeldung angezeigt, dass die Sicherheitsstandards deaktiviert werden müssen, bevor sich Richtlinien für bedingten Zugriff aktivieren lassen. In der offiziellen Microsoft-Dokumentation → gibt es weitere Informationen darüber, ob ein Wechsel zu bedingtem Zugriff sinnvoll ist.

So werden die Standards deaktiviert:

1. Sicherheitsstandards deaktivieren wird gewählt.
2. Deaktiviert wird ausgewählt.
3. Die Auswahl wird mit Meine Organisation plant die Verwendung von bedingtem Zugriff bestätigt.

Für Version 26.4.0

Fehlerbehebung und Debugging

In der Ansicht Anmeldelogs in `Entra/Intune` lässt sich nachvollziehen, ob und welche Richtlinie für den bedingten Zugriff angewendet wurde:

Darüber hinaus bietet `Microsoft` ein nützliches Werkzeug zur Fehleranalyse und Richtlinien-Simulation: What If tool →. Damit lassen sich Richtlinienwirkungen vor der tatsächlichen Aktivierung simulieren und analysieren.

Problembehandlung

- Wo kann ich bei Microsoft sehen, ob ein Gerät konform oder nicht konform ist?
- Das Gerät ist bei Microsoft als N/A gekennzeichnet
- Das Gerät ist bei Microsoft als nicht konform markiert, aber der Benutzer kann weiterhin auf blockierte Apps zugreifen
- Der Benutzer kann sein Gerät nicht registrieren, da es von MSCA blockiert wird
- Das Gerät ist als nicht konform gesperrt
- Das Gerät ist nicht registriert
- Der Benutzer/das Gerät kann nicht registriert werden

Für Version 26.4.0