

Print version of the Relution documentation

Relution Handbook

For version 26.4.0

Last updated: 2026-10-21 14:01 UTC

Available online at hub.relution.io

Table of Contents

1. Relution Cloud
2. On Premises Installation
    1. Installation
    2. Object Storage
    3. After installation
    4. Knowledge Base
3. Product information
4. Get started
5. General
    1. Dashboard
    2. Relution Apps
    3. App Management
    4. User Management
    5. Device Management
    6. Apple Management
6. Apple iOS
    1. Enroll Devices
    2. Supervision
    3. Actions
    4. Settings
    5. Policies
    6. Knowledge Base
7. Apple tvOS
    1. Enroll devices
    2. Actions
    3. Policies
    4. Knowledge Base

For version 26.4.0

8. Apple macOS
    1. Enroll devices
    2. Actions
    3. Policies
    4. Knowledge Base
9. Apple visionOS
    1. Enroll devices
    2. Actions
    3. Policy
10. Apple watchOS
    1. Enroll devices
    2. Actions
    3. Policy
11. Education
    1. Apple Education
12. Android Enterprise
    1. Enroll devices
    2. Actions
    3. Policies
    4. Knowledge Base
13. Android Classic
    1. Enroll devices
    2. Actions
    3. Policies
    4. Knowledge Base
14. Whiteboards
    1. Android Classic
    2. Android Enterprise
15. Windows
    1. Enroll devices
    2. Actions
    3. Policies
    4. Windows Apps
    5. opsi
    6. Knowledge Base
16. Linux
17. Settings
    1. Licenses
    2. TeamViewer
    3. Conditional Access

For version 26.4.0

Relution Cloud

Relution offers a powerful cloud solution that operates the software as a virtualized cloud server. This hosting takes place in a GDPR-compliant cloud environment, ensuring the security and protection of all processed data. Automatic updates keep the software up to date and secure at all times. Additionally, the infrastructure guarantees a high availability rate of 99.5% for the Relution platform outside of the maintenance window, ensuring reliable usage at any time.

General information

The following general information applies to the operation of the Relution Cloud.

Maintenance Window

Maintenance of the Relution cloud infrastructure is performed from Mondays at 17:00 until Tuesdays at 4:00 CE(S)T. During this period, temporary limitations or service disruptions may occur.

Relution Updates

Relution updates are announced in advance via the newsletter → and are performed on the announced day between 16:00 and 19:00 CE(S)T. No downtime occurs during these updates.

For version 26.4.0

Email notifications

Make sure emails from `no-reply@relution.io` and `no-reply@mail.relution.io` can be received. These addresses are used as senders for emails sent by Relution Cloud servers.

Gateway IP Addresses

The gateway addresses which Relution cloud servers use to send requests are available in two ways:

1. Via DNS: The IP addresses are published as DNS A records under the FQDN `gateway.<cluster-name>.relution.io`, e.g. `gateway.eu.relution.io` for the `eu` cluster. Firewalls that support FQDN-based rules can use this hostname directly in their access rules.
2. As JSON list: The addresses are additionally published at https://repo.relution.io/other/relution-cloud-gateways.json in machine-readable form.

Both sources are updated automatically once addresses are added or removed. If IP-based access control for e.g. LDAP servers is required, the respective source should be queried in regular intervals and the access rules need to be updated. It is recommended to automate this process or to use FQDN-based firewall rules.

Limits und Quotas

See article Limits and Quotas →.

Solution Environments

Relution's cloud offering is available in two environments to flexibly meet different requirements.

Shared Hosting on live.relution.io

The shared hosting model provides an organization on `live.relution.io` within a shared server. This variant offers a cost-effective solution for organizations with less complex demands. An account can be created via the "Prices and demo" overview on the `relution.io` website →.

Dedicated Server

For organizations requiring maximum control and customization, a dedicated server model is available. This exclusive server allows for an independent infrastructure with customization options tailored to specific business needs. Dedicated servers are available at an URL following the pattern `<server name>.<cluster name>.relution.io`, for example `acme.eu.relution.io`.

The `<server name>` must:

- contain at most 20 characters
- contain only lowercase alphanumeric characters or '-'
- start with an alphabetic character
- end with an alphanumeric character

For version 26.4.0

Intial setup

For the intial setup of a dedicated cloud server, the following information is required:

- Desired server name, will result in the domain `<server name>.<cluster name>.relution.io`
- Estimated number of devices to be managed on the server
- Name and email address to be used for the system administrator account

The intial setup is then performed as follows:

1. Relution Sales requests creation of the server with the data listed above
2. The server is created in the corresponding Relution SaaS cluster
3. A notifcation is sent to the customers email address
4. A password reset needs to be triggered by someone with access to the system administrator's email account
5. A login has to be performed, and the End User License Agreement (EULA) has to be accepted
6. The Data Processing Agreement (DPA) under the General Data Protection Regulation (GDPR) has to be digitally signed in Relution
7. It is highly recommended to setup Multi-Factor Authentication (MFA) → for the system administrator account

As an optional step, an account for the Relution support team → can be created.

Custom Domains for Dedicated Server

A custom domain can be used for dedicated servers. In this case, a DNS CNAME record needs to be configured for the custom domain pointing to `<server name>.<cluster name>.relution.io`. The custom domain (e.g. `relution.customer-name.de`) then points to the Relution Cloud instance (e.g. `customer-name.eu.relution.io`).

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

For the dedicated server variant, the Site-to-Site VPN add-on is also available, enabling secure access to customer-specific infrastructures such as intranet services. This add-on offers the following features:

- Integration of intranet services into a Relution UEM cloud server
- Up to 10 GB traffic per month
- Ensured 99.5% availability

As a prerequisite for the setup, the customer-side remote peer (VPN gateway) must support IPSec IKEv2 with EAP-PSK.

These options allow organizations to expand their IT infrastructure individually and align with their specific needs.

Relution Shield in SaaS Mode

As an additional add-on for dedicated servers, Relution offers Relution Shield →, a powerful SaaS-based extension. With Relution Shield, a road-warrior setup for devices can be implemented, providing a secure and flexible solution for accessing internal resources. This add-on includes:

- Certificate-based access control ensuring high security for device connections
- Compliance checks to verify the security parameters of connected devices
- Utilization of the Site-to-Site Tunnel to access internal organization resources

This add-on is ideal for mobile and remote users who need secure access to internal infrastructure.

For version 26.4.0

Limits and Quotas

This chapter describes the standard quotas and limits for the Relution Cloud offering. Unless otherwise agreed, the values apply to all tenants and deployment types.

Category	Shared (`live.relution.io`)	Dedicated Server
Maximum upload size	1 GB per file	1 GB per file
Storage limit	10 GB per tenant	100 GB per server
Actions per device per day	50 actions (7-day average)	50 actions (7-day average)

Upload Size

The maximum upload size defines how large a single file may be when uploaded to the cloud.

- On Shared (`live.relution.io`), the limit is 1 GB.
- On Dedicated Servers, the limit is 1 GB. This limit can be increased upon request.

If a file exceeds this size, the upload will be rejected.

For version 26.4.0

Storage Limit

The storage limit defines the maximum amount of data storage available for organizations or servers.

- On live.relution.io (Shared), each tenant is allocated up to 10 GB of storage.
- On Dedicated Servers, each server is allocated up to 100 GB of storage.

Action Limit per Device per Day

To ensure system stability, the number of actions per device per day is limited.

- A maximum of 50 actions per device per day (7-day average) is covered by the quota.

If this limit is consistently exceeded, the system may apply temporary restrictions or throttling.

On-premises to cloud migration

Relution installations can be easily transferred to the Relution Cloud. Only a few steps and specific configurations are necessary for a successful migration.

Requirements

The following components are required for migration to the Relution Cloud:

- A current dump of the Relution database
- The S3 storage bucket, if used in the existing on-premises installation

Both components are provided in the cloud by the Relution infrastructure team.

> The URL of the Relution instance used previously must continue to point to the new cloud instance after migration – usually by means of a DNS CNAME entry to the new target address (e.g. `customer-name.eu.relution.io`).

For version 26.4.0

Implementation

Relution Support should always be contacted before migration.

If the migration has already been requested, the support team will usually have a corresponding ticket on file, allowing them to provide targeted assistance during the process. First, an SQL dump of the current database is created and provided to Relution Support.

The new cloud instance is then set up and the database imported. The duration depends on the size of the database and can take several hours. During or after the import, the DNS CNAME entry is configured:

The previous URL (e.g. `relution.customername.co.uk`) then points to the new Relution Cloud instance (e.g. `customer-name.eu.relution.io`). Note Hint: The end devices do not need to be re-registered after the migration. Operations continue without interruption – all MDM profiles, apps and certificates are retained.

Summary: Steps for migration

1. Contact Relution Support
2. Schedule an appointment for backup and migration
3. Provide the database (and S3 bucket, if applicable) in coordination with Support
4. Configure the DNS CNAME entry for the new cloud instance

Backups & Recovery

This article describes the backup and recovery measures for Relution-operated ‘Dedicated’ → Cloud instances.

> For self-hosted instances, backup responsibility lies with the respective operator.

Relution employs a multi-layered backup strategy to ensure the availability and integrity of customer data. All measures are reviewed and refined on a regular basis.

Database

The Relution database operates in a high-availability configuration with automatic replication. This means that the failure of a single database instance is not expected to result in data loss. Further technical measures proactively detect and mitigate hardware issues before they can cause data loss.

Beyond the live setup, database changes are continuously backed up off-site and complemented by regular full backups. This enables recovery to any point in time (Point-in-Time Recovery) within the retention period of up to 90 days.

Following the 3-2-1 principle, backups are created using two independent methods, with one copy stored at an independent provider in a geographically separate location. All data is encrypted at rest with customer-specific keys.

For version 26.4.0

Object Store

Data in the object store is versioned and can be restored together with the database.

RPO and RTO

Metric	Value	Description
RPO (Recovery Point Objective)	≤ 5 minutes	Up to 5 minutes of database changes may be lost in a worst-case scenario.
RTO (Recovery Time Objective)	≤ 3 hours (within business hours)	Target time for restoring the service after an outage.

Are backups stored separately?

Yes. Database backups follow the 3-2-1 principle; one copy is stored encrypted at an independent provider in a geographically separate location.

Can I request an individual restore as a customer?

Please contact Relution Support to discuss a restore. On request, recovery to a specific point in time (Point-in-Time Recovery) within the retention period is also possible. A restore by customer request is subject to a fee.

Can the retention period be adjusted?

Yes. The retention period can be customized - at an extra charge - to fit specific requirements. Please contact Relution Support to discuss the details.

What data is covered by the backup?

The backup covers all persistent data of the Relution instance.

For version 26.4.0

System requirements

The following hardware is required to run a Relution server required:

- 2 CPU cores
- 4 GiB RAM
- 1 network card
- 10 GiB HDD/SSD
- Additional storage space for user data, operating system and other applications and programs

External object storage

In general, we recommend using external object storage, especially in these cases:

- Installation and management of native apps on Windows devices
- If a larger number of native apps, or native apps larger than 50 MB, are used
- For servers with more than 5,000 devices

Relution supports configuring a separate S3-compatible object storage system. More information is available at Object Storage →

For Version 26.4.0

Recommended hardware

Depending on the number of managed devices, we recommend the following hardware equipment:

- Up to 150 devices
- 150 to 1,000 devices
- 1,000 to 5,000 devices
- 5,000 to 10,000 devices
- 10,000 to 30,000 devices
- 30,000 to 50,000 devices
- 50,000 to 100,000 devices
- 100,000 to 200,000 devices

Operating System

The following operating systems are supported:

- Alma Linux or Rocky Linux Version 9 or 10
- Red Hat Enterprise Linux (RHEL) version 9 and later
- Ubuntu Server, current LTS version

Docker installation (recommended)

- Current versions of Docker and Docker Compose.

Native Installation

The following software is recommended for running a Relution Server. recommended:

- Java 21
  - AdoptOpenJDK 21 is recommended.
- NGINX 1.8 or newer
- A supported database server.

For version 26.4.0

Supported databases

Relution supports the following database servers:

- PostgreSQL 14.0 or newer
- Deprecated: MariaDB LTS minimum Version 10.11 or newer
  - MariaDB will be supported until the end of 2027, we recommend using PostgreSQL

To use the Relution web portal, please use one of the following browsers in the latest version:

- Chrome
- Firefox
- Safari

Managed devices and platforms

The following operating system versions are officially supported by Relution. Previous versions are not tested, and features and apps might not be available there.

OS versions in end of life (EOL): For security reasons, Relution does not support operating system versions which hav already reached their end of life (EOL), since no security patches will be provided by the manufacturer any more

- Android 10 or later
- iOS 18 or later
- iPadOS 18 or later
- macOS 14 or later
- tvOS 18 or newer
- visionOS 26 or newer
- watchOS 26 or newer
- Windows 10 Professional/Education or newer

Network

- Direct internet connection
- No proxy server between Relution and the Internet
- An SSL certificate from a trusted CA
  - In the Relution default configuration, Traefik obtains a Let's Encrypt certificate via port 80

Internet access

The following ports must be opened on the firewall for incoming and outgoing connections from/to the internet.

For version 26.4.0

Port	Type	Direction	Source	Required	Description
80	TCP	Inbound	All	Yes	Redirect to HTTPS
443	TCP	Inbound	All	Yes	For internet access and client to server communication
7800	TCP	In-/Outbound	Cluster node	Yes	Necessary for the communication between cluster nodes
8099	TCP	Inbound	Local network	No	Necessary for Health Status Monitoring
2197	TCP	In-/Outbound	Associated/Appointed	No[1]	Apple Push Notification Services (APNS)
443	TCP	Outbound	-	Yes	e.g. SMS service, license server, VPP, DEP, …
123	UDP	Outbound	-	Yes	NTP (time server)

[1] Required for communication between iOS devices and Apple Push Notification Services (APNS) up to Relution 4.70. Required as a fallback in later versions.

Apple Network Requirements

Firewall If the firewall supports using hostnames, allowing outbound connections to `*.apple.com` may be sufficient to use most Apple services. If the firewall can only be configured with IP addresses, allow outbound connections to the following IP address ranges owned by Apple, based on the IP version.

```
For IPv4, allow outbound connections to 17.0.0.0/8.
For IPv6, allow outbound connections to these network ranges:
2403:300::/32
2620:149::/32
2a01:b740::/32
```

HTTP Proxy Apple services can be used through a proxy if `disable packet inspection` and authentication are set for traffic to and from the listed hosts. Exceptions to this are noted above. Attempts to perform content inspection on encrypted communications between Apple devices and services will result in a dropped connection to preserve platform security and user privacy. Apple Network Requirements →

Google Network Requirements

Google Network Requirements →

For version 26.4.0

Microsoft Windows WNS Firewall Requirements

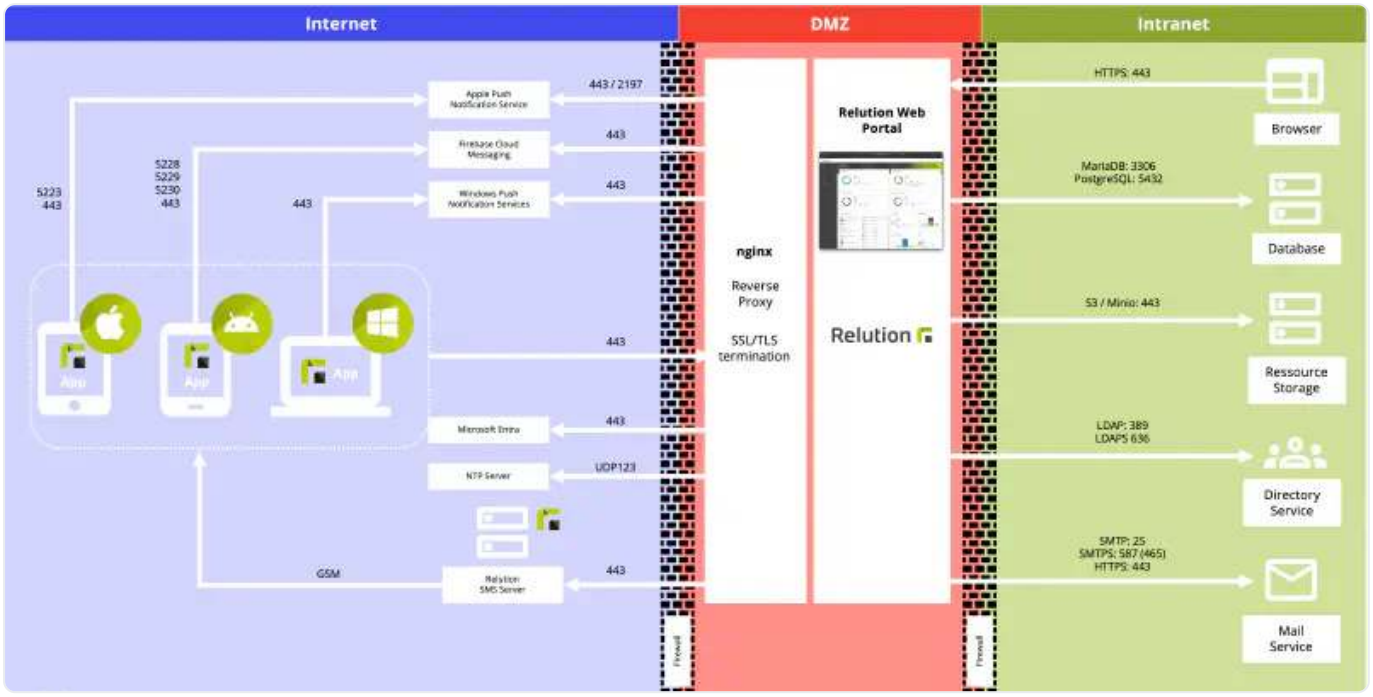
Windows WNS Requirements →

Internal network

The Relution service uses these ports to communicate with external services (database, directory service, mail server). The exact configuration depends on which services are used and whether the services run on separate servers (recommended).

If the servers servers are on the same network, no additional firewall configuration should be required. All ports are TCP.

Port	Description
25	Mail server (SMTP)
389	Directory service (LDAP)
587	Mail server (SMTPS)
636	Directory Service (LDAPS)
3306	MariaDB/MySQL
5432	PostgreSQL



Mobile devices

When mobile devices are connected to internal networks,*additional* inbound and outbound ports have to be opened so that devices can connect to Apple, Microsoft or Google servers in order to receive push to receive push messages. To communicate with Relution, the default HTTPS port 443 is required. Depending on the features to be used on devices, additional ports may be required, which can be found in the manufacturers documentation. When the devices are connected to mobile data, no additional configuration should be required.

Related links:

- Use Apple products on enterprise networks →
- TCP and UDP ports used by Apple software products →
- Apple technotes →
- Apple Classroom →
- Firebase Cloud Messaging →
- Firebase Cloud Messaging ASN of 15169 →

Port	Type	Direction	Description
443	TCP	Outbound	HTTPS, e.g. Relution, Google FCM, Microsoft WNS, Apple Push Notification Service,…
443	UDP	Outbound	QUIC, e.g. iCloud Private Relay, Google services
5223	TCP	Inbound/Outbound	Apple Push Notification Service[1]
5228-5230	TCP	Outbound	Google Firebase Cloud - Firebase Cloud Messaging (FCM)
3283	TCP	Inbound/Outbound	Apple Remote Desktop (e.g. Apple Classroom App)
3283	UDP	Inbound/Outbound	Apple Remote Desktop (e.g. Apple Classroom App)
3284	TCP	Inbound/Outbound	Apple Classroom Document Sharing
3285	TCP	Inbound/Outbound	Apple Classroom App

For v

Before installation

Before starting the installation, go through this checklist to verify that the infrastructure meets our minimum requirements and is configured correctly.

It is possible to host multiple services on the same machine (for security reasons we recommend hosting each service on a separate server).
For example: If Relution and the reverse proxy `nginx` are installed on the same machine, `the server running Relution` and `the server running nginx` refer to the same physical machine. In this case, the server must meet the requirements of both services.

Hardware

The server running Relution has the following minimum requirements →.

Operating System

The server on which Relution is running uses a recommended operating system → and the version of the operating system meets or exceeds the minimum supported version.

For version 26.4.0

Database

The server running Relution has network access to a supported database → server.
This guide contains instructions on how to install MariaDB if a new database server needs to be installed.

Network infrastructure

The server running the reverse proxy `nginx` is set up to host a service available on the Internet. It has a public IP address and a public DNS name or example `mdm.example.com`. When services are hosted on multiple internal servers, they can resolve each other's hostnames.

The public IP address must be static. Dynamic IP addresses are not supported. Exceptions: The server is hosted by a cloud provider, such as Amazon Web Services (AWS) or Microsoft Azure, which provide the necessary DNS infrastructure.

Requirement

- Server has direct access to the Internet
- Server has a static IP address
- Server has a public DNS name
- Internal DNS is properly configured and functioning

Firewall configuration

The firewall is set up to accept incoming HTTP(S) requests from mobile devices and web browsers.

Request

- The reverse proxy is accessible from the Internet via HTTP (80)
- The reverse proxy is reachable from the Internet via HTTPS (443)
- Relution can connect to the Internet (80, 443, 5223, 123 UDP)
- Relution can connect to the SMTP server
- Relution can connect to the database server.
  Optional:
- Relution can connect to LDAP via port 389 or 636.

For version 26.4.0

Certificates

HTTPS requires a valid SSL certificate from a trusted certificate authority (CA).

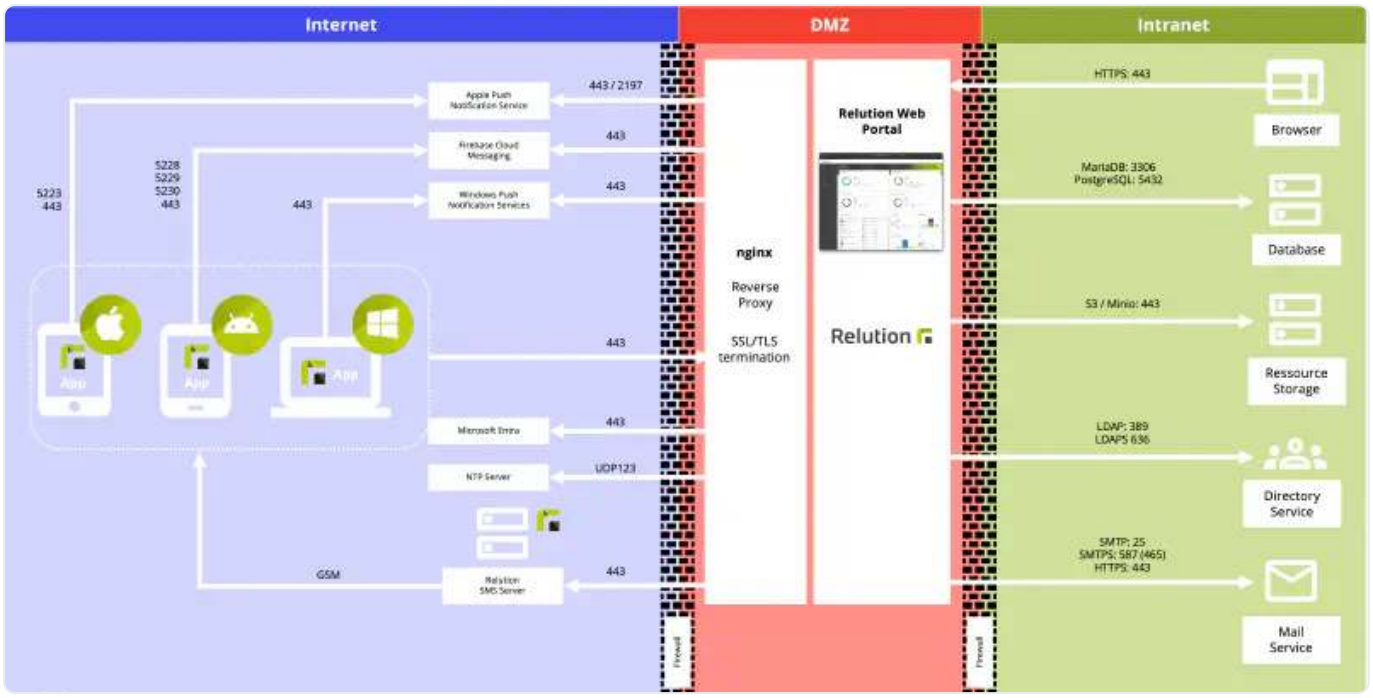
- Self-signed certificates do not work, because mobile devices do not trust them by default
- Certificates from Let's Encrypt → work and are free

W3Techs → provides a list of known certificate authorities based on market share and usage.

..

Request	Fulfilled
A valid SSL certificate and key is available	

> Relution is shipped with a valid APNS certificate that is used. In this case, the certificate will also be updated with the update of Relution. Automatic updating for own used APNS certificates is not available and has to be organized separately.



For version 26.4.0

Docker (Recommended)

This guide applies to Rocky / Alma Linux 9 and 10 and Ubuntu Server (current LTS version).
(Status Dec. 2025). We recommend using Linux for the host system.

This guide covers the installation and configuration of a basic Relution instance, which runs in Docker containers.

Prerequisites

Before beginning, ensure that the following requirements are met:

- The host machine can connect to the Internet.
- `root` or `sudo` permissions are available.
- Optional: A valid SSL certificate for the URL.

> Self-signed certificates do not work, as mobile devices do not trust them. A root certificate can be installed manually on a device, but this procedure is not recommended due to the high effort. Certificates from Let's Encrypt → have been tested and work.

For version 26.4.0

Preparation

`vim` can optionally be set as the default editor. Skip this section to continue using the standard editor.

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

The installation is divided into the following main steps:

1. Install Docker and Docker Compose.
2. Configure Containers.
3. Configure Traefik or nginx.

Installing Docker and Docker Compose

To run Relution in a Docker container, `Docker` and `docker compose` must first be installed.

Install Docker

Please follow these commands for Alma / Rocky Linux:

```
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
```

For Ubuntu Server, the following commands apply (Docker repository as described in the Docker documentation →):

```
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
```

Make sure to start and enable the Docker service after installation so that it is available after a system reboot.

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

> The minimal and cloud images of RHEL, AlmaLinux and Rocky Linux 10 (EL10) are missing the `kernel-modules-extra` package, which prevents the Docker service from starting. In this case, perform the steps in Docker Fails to Start on EL10 → before starting Docker for the first time. On EL9 this is not required.

Configure Containers

Create a directory for Relution configuration files, e.g., for `docker compose`.

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

Prepare Secrets

Use secure random passwords for the secrets (e.g., with `pwgen -snc 48 1`).

Create the following files:

Placeholder	Description
`/opt/relution/secrets/postgres_password`	The password of the Relution database user
`/opt/relution/secrets/system_admin_password`	The initial password of the system administrator. Change this after the first login.

For version 26.4.0

compose.yaml

Download the file:

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

The Compose file defines three services: `database`, `relution`, and `traefik`.

application.yml

Download the file:

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

Edit the file:

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

Adapt the file to the environment. The following placeholders must be replaced:

Placeholder	Description
`%EXT_HOSTNAME_URL%`	The external address of the Relution server, e.g., `https://mdm.example.com`
`%SYSTEM_ADMIN_EMAIL%`	The email address of the system administrator

> Data Persistence: The default configuration maps the PostgreSQL data directories to the host system. Relution stores all its data in the database, so no additional configuration is required. Ensure that PostgreSQL is included in the backup strategy.

For version 26.4.0

Configuring Traefik (Reverse Proxy)

> Traefik is used as a reverse proxy to enable access to Relution while providing SSL/TLS encryption. Without Traefik or a similar proxy, access to Relution is only possible locally via localhost.

Automatic Certificate Creation (Let's Encrypt)

Download the Traefik configuration file and adapt it to the environment:

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

In the file `/opt/relution/configs/traefik/relution.yaml`, the placeholder `external.url` must be replaced with the actual external URL under which Relution should be made available:

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

```
http:
  routers:
    relution:
      rule: Host(`external.url`) # Replace placeholder
```

The external URL here is specified without a preceding `https://`, unlike in the `application.yml`.

Shutting Down

To shut down and remove the containers (the images remain):

```
cd /opt/relution/
docker compose down
```

Updating Relution

To update the services, use the following commands:

```
cd /opt/relution/
docker compose pull # Downloads the latest image
docker compose up -d # Stops and restarts the containers
```

The Relution service will be unavailable until the container restart is complete.

If startup issues with Relution occur, please send the complete log as a Zip file to support. Support is subject to a fee.

Traefik with static Certificates

Download the configuration file for static certificates:

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

In the file `/opt/relution/configs/traefik/relution.static_cert.yaml`, the placeholder `external.url` must be replaced with the actual external URL under which Relution should be made available:

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

```
http:
  routers:
    relution:
      rule: Host(`external.url`) # Replace placeholder
```

The certificate chain and the corresponding private key must be placed under `server.pem` and `server.key` in the directory `/opt/relution/certs/static`.

Furthermore, the `traefik:` block in the `compose.yml` must be adjusted:

```
...
  traefik:
    ...
    command:
      - --providers.file.directory=/opt/traefik/
      - --entryPoints.web.address=:80
      - --entryPoints.web.http.redirections.entryPoint.to=websecure
      - --entryPoints.web.http.redirections.entryPoint.scheme=https
      - --entryPoints.websecure.address=:443
    ...
    volumes:
      - ./configs/traefik:/opt/traefik
      - ./certs/static:/opt/certs
...
```

Nginx Alternative to Traefik (Reverse Proxy)

> Nginx is used as a reverse proxy to enable access to Relution while providing SSL/TLS encryption. Without Nginx or a similar proxy, access to Relution is only possible locally via localhost.

Download the nginx configuration file:

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

Replace the `traefik:` block in the `compose.yaml` with this `nginx:` block:

```
  nginx:
    image: nginx:stable
    restart: unless-stopped
    container_name: nginx
    depends_on:
      - relution
    environment:
      TZ: "Europe/Berlin"
      NGINX_HOST: "%EXT_HOSTNAME%"
    ports:
      - "80:80"
      - "443:443"
    volumes:
      - "/opt/relution/relution-nginx.conf:/etc/nginx/conf.d/relution-nginx.conf"
      - "/opt/relution/server.pem:/etc/nginx/server.pem"
      - "/opt/relution/server.key:/etc/nginx/server.key"
```

For increased security, the use of better DH parameters is recommended.

1. Generate key:

```
openssl dhparam -out /opt/relution/dhparams.pem 4096
```

2. Adjust `relution-nginx.conf`: Add the line (and activate `ssl_stapling` if necessary):

```
ssl_dhparam /etc/nginx/dhparams.pem;
```

3. Extend `compose.yaml` Volumes: Adjust the `Volumes` of the nginx container to include the DH parameters:

```
volumes:
  - "/opt/relution/relution-nginx.conf:/etc/nginx/conf.d/relution-nginx.conf"
  - "/opt/relution/server.pem:/etc/nginx/server.pem"
  - "/opt/relution/server.key:/etc/nginx/server.key"
  - "/opt/relution/dhparams.pem:/etc/nginx/dhparams.pem" # Added
```

The configuration expects the SSL certificate and key to be in `/opt/relution/server.pem` and `/opt/relution/server.key`. Otherwise, adjust the `Volumes` of the nginx container accordingly.

SSL Certificate Conversion →

> If the Secure Mail Gateway is in use, the `/Microsoft-Server-ActiveSync` location in the nginx configuration must point to the SMG service instead of Relution. See Secure Mail Gateway →.

> If nginx (or another reverse proxy) runs on a different server than Relution, this can result in the message `Access is forbidden` during login from Relution 26.4.0 onwards, since the proxy's request is not classified as trustworthy by default. In addition, the header `proxy_set_header X-Forwarded-Proto $scheme;` must be set correctly in the nginx configuration. For the solution, see Login: Access is forbidden →.

Starting Relution

Navigate to the Relution directory and start the Docker containers:

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

This will download the images and start the services. It may take some time for the services to become available.

To view the log output of a specific container (e.g., Relution):

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

For version 26.4.0

SSL Certificates - Certbot

Certbot is a free solution for issuing SSL/TLS certificates via Let's Encrypt, which enables a secure HTTPS connection for websites. Compared to paid providers, which often involve additional administrative work and recurring costs, Certbot offers an automated, free alternative that simplifies the management of certificates and handles ongoing renewals.

Setup

It is recommended to install Certbot → natively on the host, obtain certificates once via Certbot and integrate it as a volume into the nginx container.

1. Install Certbot

Prerequisites:
→ ALMA / Rocky Linux or Ubuntu Server as host
→ Docker installed according to instructions
→ Relution configured according to instructions

On Alma / Rocky Linux, Certbot is installed with the following command:

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

On Ubuntu Server:

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

2. Stop Nginx

Nginx must be stopped temporarily because Certbot in `--standalone` mode briefly starts its own web server on port 80.

```
docker stop docker_nginx
```

3. Create a certificate

Start Certbot and follow the instructions in the wizard.

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

4. Adjust the certificate path

In `docker-compose.yml`, the path to the created SSL certificates must be adjusted.

```
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'
```

> If Nginx is started with the volumes (path to the certificates) in the docker-compose.yml and the certificates are not present, Docker will create folders instead of files. These folders must be deleted so that the certificates can be created when Docker is started.

5. Start Docker container

If the certificates are successfully created, all containers can be started and checked

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

6. Pre- and post-hooks

For renewal, pre- and post-hooks can be configured in Certbot to stop and then restart the nginx container. The hooks are only executed if Certbot determines when calling Renwal that the certificates actually need to be replaced. Certbot is usually configured to run twice a day and checks whether a replacement is necessary. The certificates are valid for 90 days.

Depending on the host system, Certbot should already automatically set up a renewal (e.g. as a systemd service + timer). The call there can then be extended accordingly by these hooks, e.g.

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

Pre- and post-hooks would then be accordingly:

```
--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”
```

The hooks can also point to script files that contain the actual call, which is usually clearer.

> When trying it out for the first time, always use `--dry-run` so that Let’s Encrypt is not blocked for several days by too many failed attempts. In a productive environment, this must of course be removed, otherwise there will be no certificate.

For version 26.4.0

Docker - 1000 to 5000 Devices

For a device count in the range of 1000 to 5000, it is recommended to operate the application and database servers separately.

The basic setup of the servers and the installation of the necessary software packages are described in detail in the General Docker Installation Guide →.

This guide describes the necessary configuration files with explanatory comments to make customization easier, and supplements the general Docker installation guide.

Hardware Requirements and Setup

1x Application Server

- 2 CPU Cores
- 4 GB RAM
- Approximately 30 GB SSD Storage

1x Database Server

- 4 CPU Cores
- 8 GB RAM
- Approximately 100 GB SSD Storage

For version 26.4.0

App Server

The application server requires the following two files.

compose.yaml

```
services:
  relution:
    image: relution/relution:latest
    restart: unless-stopped
    container_name: relution
    environment:
      TZ: "Europe/Berlin"
    expose:
      - "8080"
      - "8099"
    ports: # Externally exposed application port for testing // deactivate once the
server is reachable under the URL
    volumes:
      - "./application.yml:/opt/relution/application.yml"

networks:
  relution-network:
```

application.yml

```
relution:
  system:
    admin:
      password: $Placeholder # Set initial password here and change it in the portal
after the first login!
      email: $Placeholder # Alternative to username "Admin" and for resetting the
password
  server:
    externalURL: https://$Placeholder # Replace with the URL under which the server
will be reachable. Always starts with https://
  database:
    type: postgresql
    url: jdbc:postgresql://$Placeholder:5432/relution?currentSchema=public # IP, FQDN,
or URL of the database server with port specification. The port will be further
configured on the DB side in the guide.
    username: relution # Database username
    password: $Placeholder # Password of the relution database = POSTGRES_PASSWORD
```

The password from the application.yml will be needed again later for the database configuration in the compose.yaml.

DB Server

A separate compose file is used for the database server.

compose.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" # Password of the relution database =
POSTGRES_PASSWORD
    expose:
      - "5432"
    ports: # externally exposed database port that the application server must be able
to reach
      - "5432:5432" # externally exposed database port that the application server must
be able to reach
    volumes:
      - 'postgresql:/var/lib/postgresql'

volumes:
  postgresql:

networks:
  relution-network:
```

Monitoring with Grafana

Relution provides a variety of metrics that can be visualised using Grafana. Below we have provided a basic configuration for a Docker setup and two dashboards. These configurations can be adapted to individual needs. To monitor a remote server, see the configuration at the bottom of this page.

> Prometheus, Grafana and the individual dashboards are not maintained by Relution Support.

Enabling Prometheus metrics in Relution

As of Relution 26.4, Relution only exposes the health endpoint by default for security reasons; the Prometheus endpoint (`/actuator/prometheus`) is disabled. To make the metrics available, the following section must be added to the `application.yml` configuration file of the Relution server:

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

A restart of the Relution server is required for the change to take effect.

Local service configuration

This configuration implements Prometheus and Grafana in an on-premises Relution setup in a Docker environment.

To monitor a server without direct access, for example, see the configuration below.

Necessary files and directories

As mentioned, the configurations are available, can be downloaded details →.

Files

- docker-compose.yml
  - Contains the configurations of the Docker containers `Prometheus` and `Grafana`.
- prometheus.yml
  - Contains the configuration of `Prometheus`.
- .env
  - Contains the variables `GF_SECURITY_ADMIN_USER` and `GF_SECURITY_ADMIN_PASSWORD`. For productive operation it is recommended to change the password.

Subfolder

- Dashboards Sample dashboards: The configuration files for two sample dashboards are included. These dashboards are automatically imported into the Grafana Docker container.
- Provisioning Base configurations: The configuration files for the Prometheus data source and the two sample dashboards are included. These configurations can be adapted as required.

Integration of the docker-compose.yml

The docker-compose.yml described here can be used in two ways:

- Standalone The file can be used as a standalone file.
- Content The content of the file can be included in an existing `docker-compose.yml`.

In our example, the content of the file is included in the existing `docker-compose.yml`. In this case, it is important that the files and directories of the volumes are in the appropriate place and have the correct permissions. In our `docker-compose.yml` the containers mariadb, relution and nginx are present, so lines two to four have only been inserted for orientation.

For version 26.4.0

> Show full configuration example

In the `docker-compose.yml` the ports for Prometheus and Grafana are set to 9090 and 3000 respectively. This section can be inserted into the existing `docker-compose.yml` for the example.

Adjusting the .env file

For security, it is recommended to adjust the password parameter.

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

Adjusting the prometheus.yml file

```
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"]

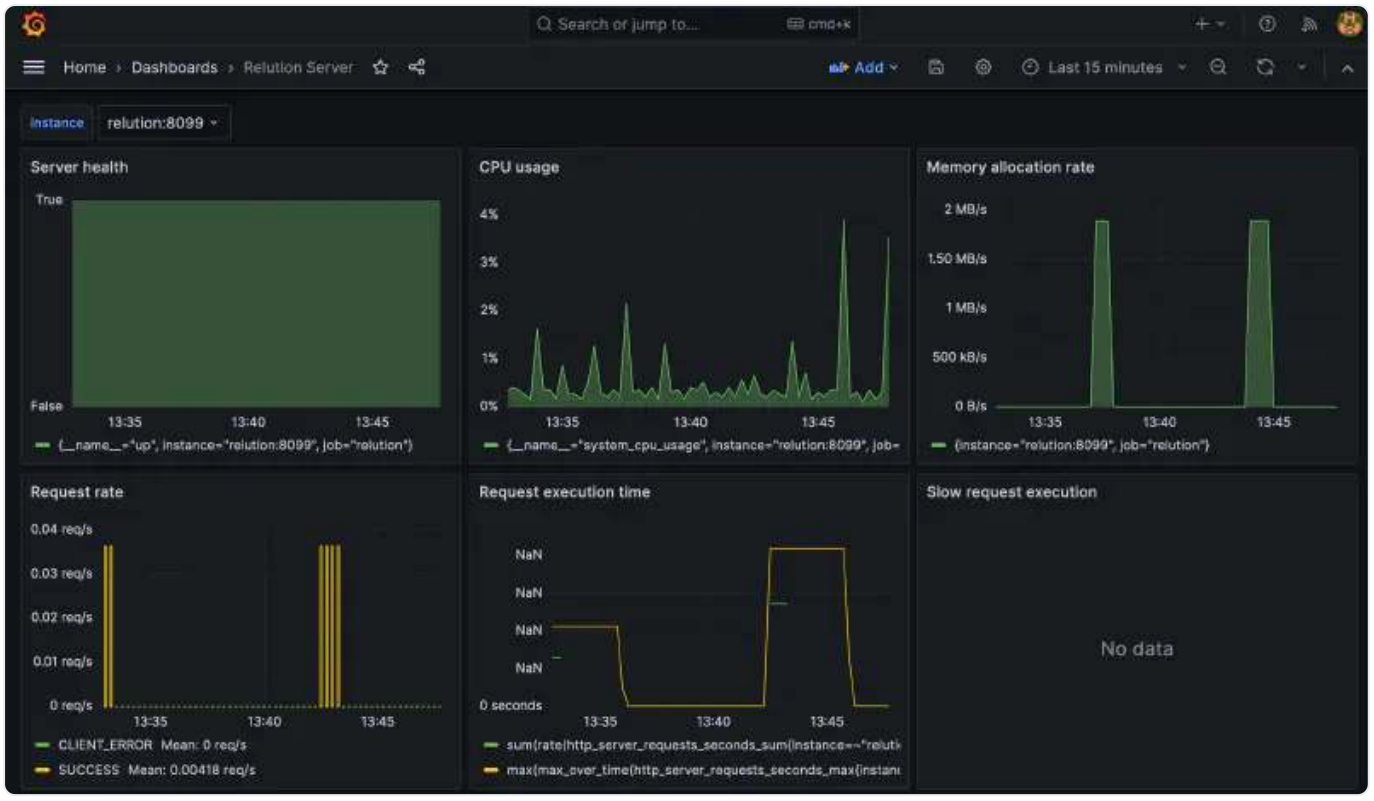
  - job_name: "relution"
 # Job to scrape application metrics
    metrics_path: "/actuator/prometheus"
    scrape_interval: 5s
    static_configs:
 # Call the docker host inside container
      - targets: ["relution:8099"]
```

For version 26.4.0

In our concrete setup, the last line must contain the name of the container and the port 8099, in this case `relution:8099`. With the command `docker ps`, the name and port of the container used can be checked and then adjusted if necessary. When the containers are shut down and started with `docker compose down` and `docker compose up -d`, the Grafana UI is accessible under the IP of the server on port 3000. Two dashboards are now available.

Dashboards

Relution Server Dashboard:



Default Spring Boot Dashboard:



Remote Server Configuration

In this scenario, Grafana is also operated within a Docker container. Specific adjustments are required to correctly read the metrics. The primary difference from the local configuration is that this setup communicates with the Relution instance via HTTPS.

Preparation in Relution

Before starting the containers, a corresponding user must exist in Relution:

- Organization: The user must be created within the Global Organization.
- Permissions: Assign the Health Check (or System State) permission to the user.
- Authentication: Access must be configured via Basic Authentication.
- User accounts using OIDC (Single Sign-On) will not work for this purpose.
- Multi-Factor Authentication (MFA) must be disabled for this specific account.

Download and Extraction

Download the prepared configuration files:
Download Grafana Setup →

Extract the archive into a directory of choice on the target server.

For version 26.4.0

Adjusting Configuration Files

File: compose.yml

Adjust the environment variables for administrative access to the Grafana interface:

- `GF_SECURITY_ADMIN_USER`: The desired administrator username.
- `GF_SECURITY_ADMIN_PASSWORD`: A secure password for the Grafana login.

File: prometheus.yml

This file defines the connection to the Relution interface. Replace the placeholders with the following data:

Parameter	Description
`$SERVER_URL`	The external URL of the Relution server (Important: without the `https://` prefix).
`username`	The username of the Relution user created under Preparation in Relution.
`password`	The corresponding password for that user.

Deployment

Once the configuration is complete, the containers can be started. Run the following command in the directory:

```
docker compose up -d
```

Access Notes:

- Grafana is accessible via port 3000 by default.
- Depending on server hardening, access is possible directly via IP/domain or securely via an SSH tunnel.

To access Grafana securely via an SSH tunnel, port forwarding can be used. This is particularly useful if port 3000 is closed in the server's firewall.

Establish the SSH Tunnel

Run the following command in a local terminal (Windows PowerShell, macOS, or Linux):

```
ssh -L 3000:localhost:3000 username@your-server-ip
```

For ve... 4.0

Parameter Explanation:

- `-L 3000:localhost:3000`: This forwards port 3000 of the local machine to port 3000 of the remote server.
- `username`: The SSH user on the server.
- `your-server-ip`: The IP address or hostname of the remote server.

Accessing the Interface

1. Keep the terminal window with the active SSH connection open.
2. Open a web browser.
3. Enter the following in the address bar: `http://localhost:3000`
4. Log in using the credentials defined in the `compose.yml` file (`GF_SECURITY_ADMIN_USER` and `GF_SECURITY_ADMIN_PASSWORD`).

Relution Files Bridge

The Relution Files app for iOS and Android can access SMB and WebDAV shares. To establish a connection with a DFS (Distributed File System), the Relution SMB Bridge or Relution Files Bridge is necessary. This component can be conveniently operated as a Docker container.

Installation

On the server designated to operate as the Relution Files Bridge, create a `compose.yml` file in the `/opt/rfb` directory and add the following content:

```
services:
  relution-smb-bridge:
 # 1.0.1 - Please check latest version at https://hub.docker.com
    image: relution/relution-smb-bridge:1.0.1
    restart: unless-stopped
    ports:
      - '8080:8080'
    environment:
      - TZ=Europe/Berlin
```

Operation with HTTPS

If the connection should also be established over HTTPS, a reverse proxy can be set up for the Files Bridge. This can be operated within the same `compose.yml` file. In the example, a Traefik proxy is used.

The file should look like this:

> Show full configuration example

Use the same configuration file for Traefik as for Relution and adapt it as needed:

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

Adjust line 4 with the external address and line 15 with the name of the container, `relution-smb-bridge`, accordingly.

Start and Operation

Start the containers with:

```
docker compose up -d
```

Accessing the Share

If the DFS share uses a path such as `smb://mein-fileserver.intra/data`, the configuration in Relution Files should look as follows:

1. Name: Customizable
2. Protocol: WebDAV
3. Path: `https://address-of-relution-files-bridge-server/mein-fileserver.intra/data`
4. Username: Domain\Username
5. Password

The Relution Files Bridge will forward the request, which is received as a WebDAV request, as an SMB/DFS request to the respective server.

For version 26.4.0

HA Cluster (Advanced)

To install Relution in a high availability configuration, a cluster can be set up. In this cluster, multiple Relution instances (application nodes) are started, all connecting to the same database. A load balancer must distribute traffic to these nodes using the round-robin method.

> Configuring a high availability cluster should only be undertaken by experienced administrators.

Prerequisites

To establish a cluster, all Relution instances must reside in the same network. The nodes should be able to communicate with each other via their hostnames and TCP port 7800. For more information, please refer to the network requirements →.

All Relution instances should use the same configuration files (e.g., `application.yml`) or the same environment variables. The only exception is when the hostname cannot be determined, in which case the `EXTERNAL_IP` environment variable can be used to set the IP address for the instance through which other Relution instances can access it.

For version 26.4.0

Functionality

When a Relution instance is started, it connects to the database and writes its hostname into the `JGROUPSPING` table. Subsequently, all entries from the table are loaded, and the instance establishes a connection to other instances through TCP port 7800. The state of the cluster is regularly monitored via the database table. If an instance becomes unreachable, its entries are removed from the database.

Checking Cluster Status

There are various ways to verify the status of the cluster.

1. System Portal

For a clustered environment, we recommend enabling the System Portal. The System Portal provides an overview of registered nodes in the cluster. Full functionality requires communication between the nodes via port `8099`. For details on activating the System Portal and enabling actuator endpoints, see Activation of the system portal →.

2. Metric Endpoint

The `counter_cluster_size_total` metric can be checked by accessing the API endpoint for Prometheus at `https://127.0.0.1:8099/actuator/prometheus`. This metric indicates how many nodes are successfully registered in the cluster. As of Relution 26.4, this endpoint requires exposure in `application.yml` under `management.endpoints.web.exposure.include` (e.g. `prometheus` or `metrics`), see Enabling the actuator endpoints →.

For version 26.4.0

Relution Shield (Add-on)

Relution Shield enables secure access to the organisation's internal intranet from the internet and combines Virtual Private Network (VPN), Public Key Infrastructure (PKI) and UEM - MDM. Further information: Relution Shield →.

Upgrading from Relution Shield 1.x? See Upgrade from 1.x to 2.x →

Relution Server

The existing Relution application server on which Relution Shield is configured and VPN profiles for end devices are managed.

1. Relution Server (version 5.26+)
2. One target organization on the server with Relution Shield license

Relution Shield Server

A separate server on which Relution Shield is installed as the VPN component.

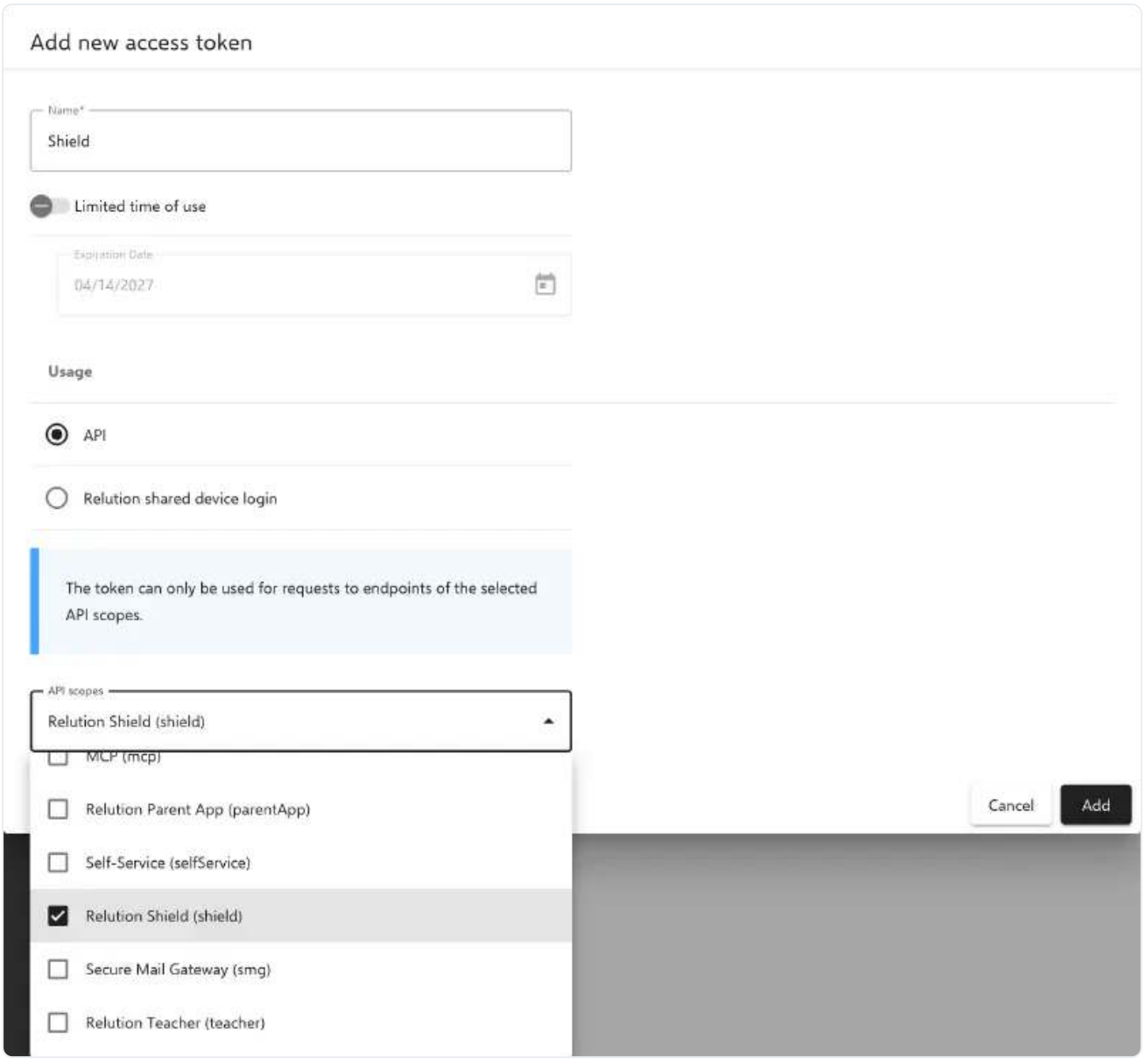
- Ubuntu 22.04+ (check version: `lsb_release -a`)
- UDP ports 500 and 4500 must be available and reachable from the internet (opened during the firewall setup via `ufw allow 500,4500/udp`, check status: `sudo ufw status verbose`)
- Outgoing traffic to all targets which should be protected by Relution Shield
- Outgoing traffic via HTTPS to Relution server
- The Relution Shield server MUST be available from the internet
- Recommended: public DNS entry

For Version 26.4.0

Set up a technical user and create an API access key

New in 26.5

1. Create a new permission role with the Relution Shield Access Check permission
2. Create a new non-password user in the target organisation
3. Assign the role to the user
4. Create an API access key for the user: under Usage, select the API option and, in the API scopes field, enable the Relution Shield (shield) entry



> Configuring the technical user in the Global organisation allows the Relution Shield Server to check access for all organisations of the Relution Server (Requires Relution Shield 2.0 or higher)

As of Relution 26.5, an API access token is only valid for the selected API scopes. Relution Shield requires only the Relution Shield (shield) scope. If it is missing, the Relution server rejects the access check. Relution Shield treats this like an unreachable server: with the default `RELUTION_SERVER_NOT_REACHABLE_ALLOW_DEVICE=true`, devices with a valid certificate are admitted without an access check, and the log shows `Relution: Could not retrieve status, temporarily accepting …`.

API access tokens created before the update to Relution 26.5 automatically receive all API scopes during the update and keep working unchanged.

Required parameters

1. Relution Host: Host name of the Relution server, e.g. `yourserver.eu.relution.io`
2. Relution API key: API access key with the Relution Shield (shield) API scope, see previous step (user creation →)
3. VPN CIDR: The private IP address range from which Relution Shield assigns an internal IP address to connected devices, e.g. `10.1.0.0/16`. This range must not overlap with the existing network.
4. Network interface: Name of the network interface to use for Relution Shield, e.g. `eth0`
5. Relution Shield Host: Host name of Relution Shield, e.g. `vpn.yourserver.eu.relution.io`
6. DNS Servers: The IP addresses of the internal DNS servers in the network, e.g. `10.1.0.1,10.1.0.2`. These are communicated to connected devices so that internal hostnames (e.g. intranet resources) can be resolved. If no internal DNS server is available, public DNS servers (e.g. `8.8.8.8`) can be used — however, internal hostnames will not be resolvable in that case.

Installation

For version 26.4.0

The installation of Relution Shield is demanding and requires attention and time. Also pay attention to variables that need to be set. Check the commands and configurations before saving them.

1. Run `sudo apt update && sudo apt upgrade`
2. Install Docker including docker compose: https://docs.docker.com/engine/install/ubuntu/ (*Do not install via* `snap`)
3. Create install directory and compliance directory

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

4. Create environment file `/opt/relution-shield/.env` – replace `<%Relution Host%>` with the actual hostname, e.g. `RELUTION_HOSTNAME=mdm.mydomain.com`

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

```
RELUTION_HOSTNAME=<%Relution Host%>
RELUTION_REST_API_ACCESS_TOKEN=<access token generated above>
```

If the API access token belongs to Global organisation, enable access check for all organisations of the Relution Server (Requires Relution Shield 2.0 or higher):

```
RELUTION_ACCESS_CHECK_SCOPE=global
```

5. Configure Ubuntu firewall `ufw`

    1. Change default forward policy in `/etc/default/ufw` to `DEFAULT_FORWARD_POLICY="ACCEPT"`

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

    2. Allow SSH and required UDP ports

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

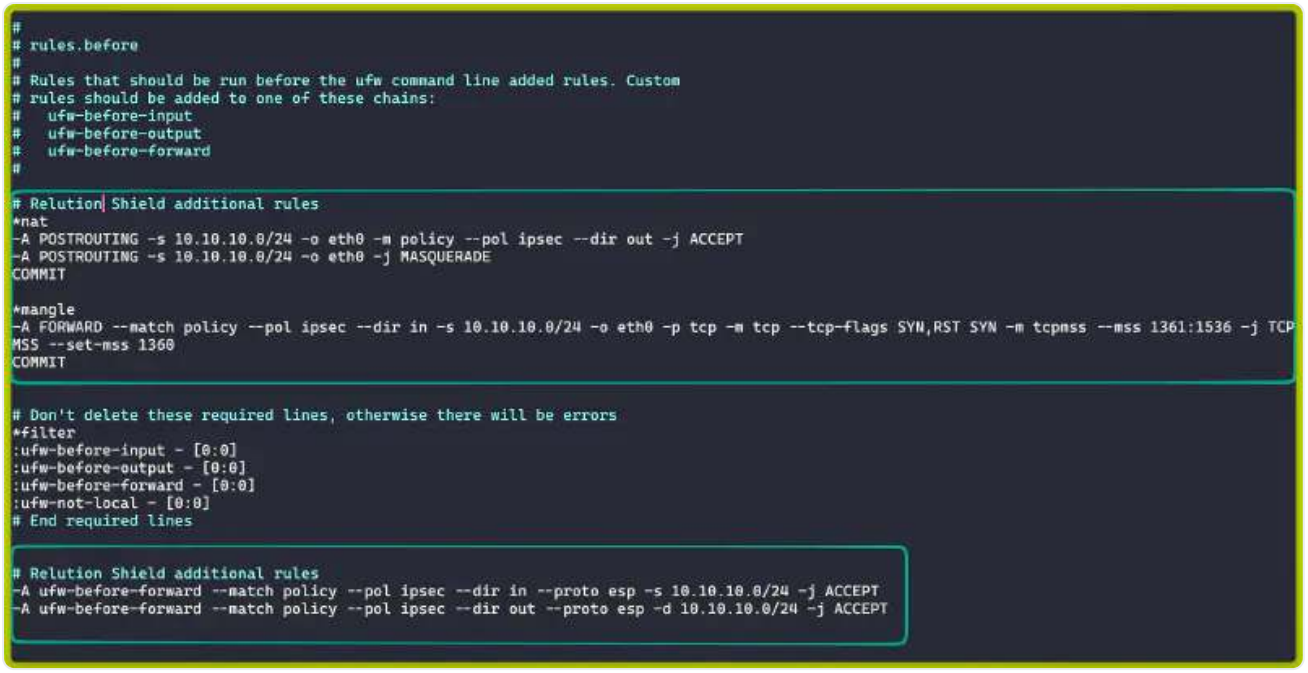
    3. Adjust `/etc/ufw/before.rules`. Add the following lines at the start of the file, before the required lines containing `*filter` (make sure to replace `<%VPN CIDR%>` and `<%Network interface%>` - each value 3 times):

    ```
    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
    ```

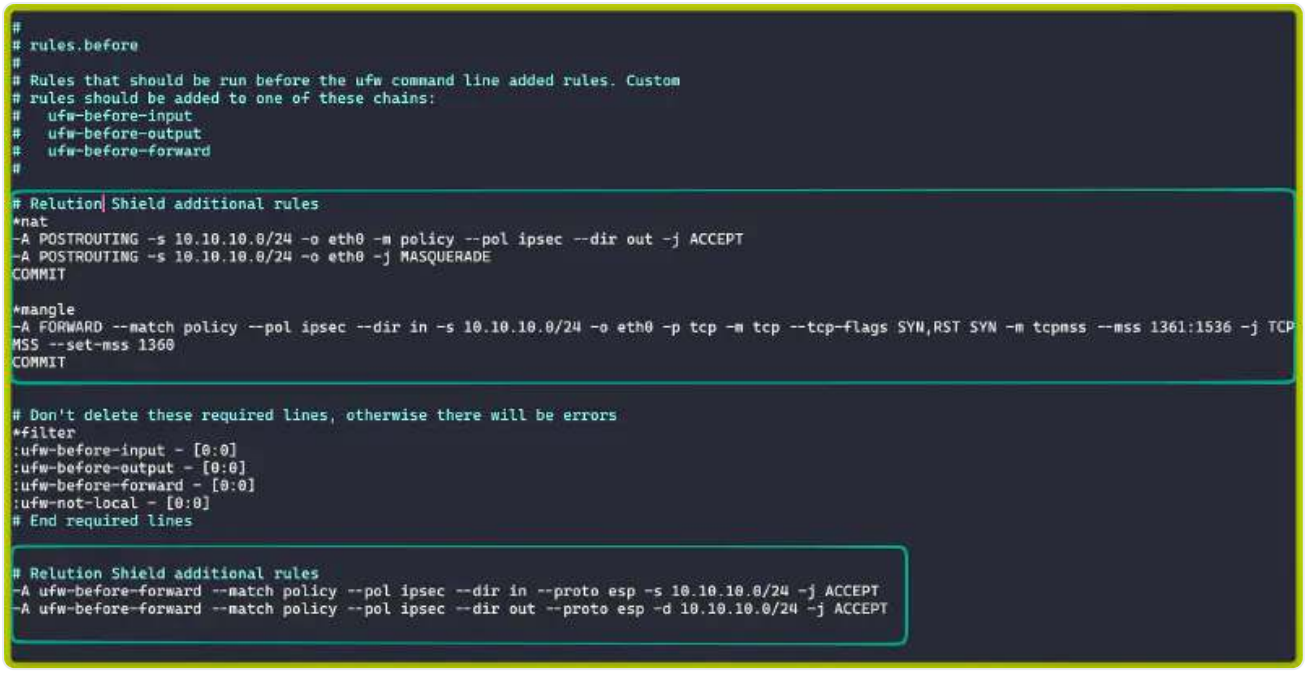
    ```
    # Don't delete these required lines, otherwise there will be errors
    *filter
    ...
    ```



1. Adjust `/etc/ufw/before.rules`. Add the following lines at the start of the file, after the required lines containing `*filter` (make sure to replace `<%VPN CIDR%>`):

```
...
# 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
```



1. Adjust `/etc/ufw/sysctl.conf`, add the following lines at the end:

```
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
```

2. Restart Ubuntu Firewall

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

6. Prepare configuration of Relution Shield

For version 26.4.0

1. Create required certificates and keys (make sure to replace `<%Relution Shield Host%>`)

```
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
```

A line is displayed in the terminal (plugin 'tpm': failed to load…), which indicates a missing TPM plugin. This message can be ignored. This is not an error.

ersion 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
```

```
# 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
```

The Certification Authority (CA) private key needs to be stored securely, as its theft would compromise the VPN Public Key Infrastructure (PKI).

2. Move the certificate files to the appropriate places

```
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. Create configuration file `/opt/relution-shield/etc/strongswan.conf`

Show full configuration example

1. Create configuration file `/opt/relution-shield/etc/swanctl/swanctl.conf` (make sure to replace `<%Relution Shield Host%>`, `<%VPN CIDR%>`, `<%Relution Host%>` and `<%DNS Servers%>`)

Show full configuration example

1. Install Relution Shield via docker

For version 26.4.0

1. Create `/opt/relution-shield/compose.yml`

```
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"
```

If Relution Shield 1.x is used, `RELUTION_REST_API_ACCESS_TOKEN` needs to be replaced by `REST_API_ACCESS_TOKEN`.

2. Start Relution Shield in `/opt/relution-shield` via `docker compose up -d`

3. Automatically restart Relution Shield after network daemon restart (e.g. after auto-updates), create `/etc/systemd/system/relution-shield-networkd-post-restarter.service`

```
[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. Start the service via `systemctl enable relution-shield-networkd-post-restarter --now`

Environment Variables

The following environment variables can be used to configure Relution Shield.

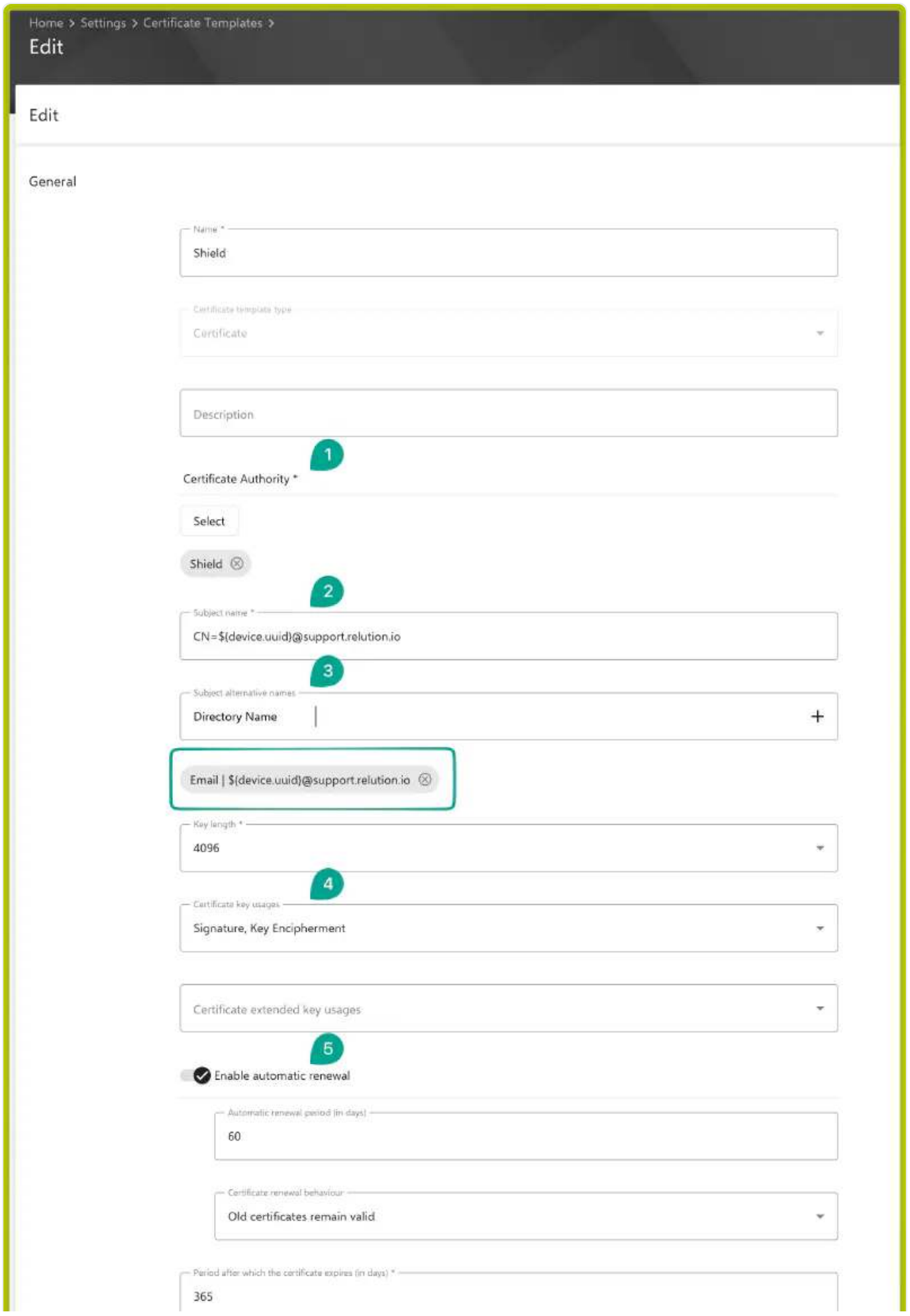
Environment Variable	Description	Values	required	Availability
`RELUTION_HOSTNAME`	Host name of Relution server, e.g. `yourserver.eu.relution.io`		yes	1.0.0
`RELUTION_REST_API_ACCESS_TOKEN`	API token used to access Relution (Relution Shield 1.x.y: `REST_API_ACCESS_TOKEN`)		yes	2.0.0
`RELUTION_ACCESS_CHECK_SCOPE`	Access check scope	`global` / `local`	no (Default: `local`)	2.0.0
`RELUTION_SERVER_NOT_REACHABLE_ALLOW_DEVICE`	Allow connections for valid certificates if Relution cannot be reached to perform compliance checks	`true` / `false`	no (Default: `true`)	26.0.0
`DEVICE_STATE_CACHE_DURATION_MINUTES`	How long the device state is cached before retrieving it from Relution again	Number	no (Default: `1`)	1.0.0

For version 26.4.0

Certificate Setup

1. Import the certificates into the target organisation
    1. Navigate to `Settings` → `Certificates`
    2. Upload the certificate at `/opt/relution-shield/etc/swanctl/x509ca/ca-cert.pem` and give it a name like `<%Relution Shield Host%> CA Certificate`
    3. Upload the certificate at `/opt/relution-shield/etc/swanctl/x509/server-cert.pem` and give it a name like `<%Relution Shield Host%> Server Certificate`
    4. Upload the PKCS12 archive at `/opt/relution-shield/pki/ca.<%Relution Shield Host%>.p12` and give it a name like `<%Relution Shield Host%> CA Key Pair`
    5. Backup the contents of `/opt/relution-shield/pki/` securely, and remove the folder
2. Create certificate authority and certificate template
    1. Navigate to `Settings` → `Certificate Authorities`
    2. Add a new certificate authority with type Built-in and select the `<%Relution Shield Host%> CA Key Pair` certificate uploaded before
    3. Navigate to `Settings` → `Certificate Templates`
    4. Add a new certificate template
        1. Select the certificate authority created before
        2. Set Subject Name to `CN=${device.uuid}@<%Relution Host%>` (Note the `CN=` at the beginning)
        3. In the Certificate Key Usage field, enable Signature and Key encryption
        4. Add a Subject Alternative Name of type Email with `${device.uuid}@<%Relution Host%>` (No `CN=` at the beginning)
           Confirm the entered value by pressing Enter
        5. Enable automatic renewal and set appropriate values, e.g. 60 days and 180 days

For version 26.4.0

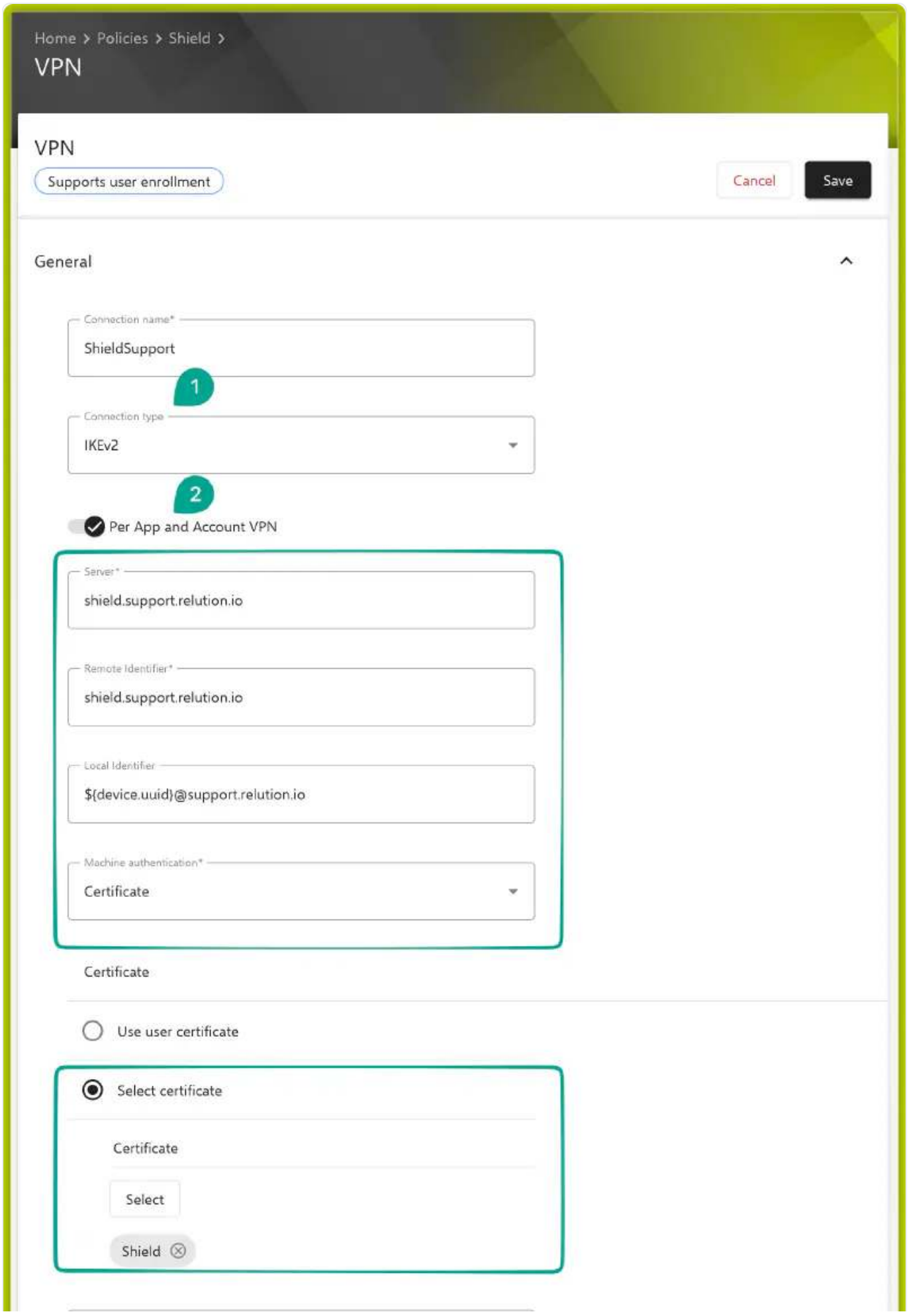

Home > Settings > Certificate Templates >
Edit
Edit
General
Name *
Shield
Certificate template type
Certificate
Description
1
Certificate Authority *
Select
Shield
2
Subject name *
CN=${device.uuid}@support.relution.io
3
Subject alternative names
Directory Name
Email | ${device.uuid}@support.relution.io
Key length *
4096
4
Certificate key usages
Signature, Key Encipherment
Certificate extended key usages
5
Enable automatic renewal
Automatic renewal period (in days)
60
Certificate renewal behaviour
Old certificates remain valid
Period after which the certificate expires (in days) *
365

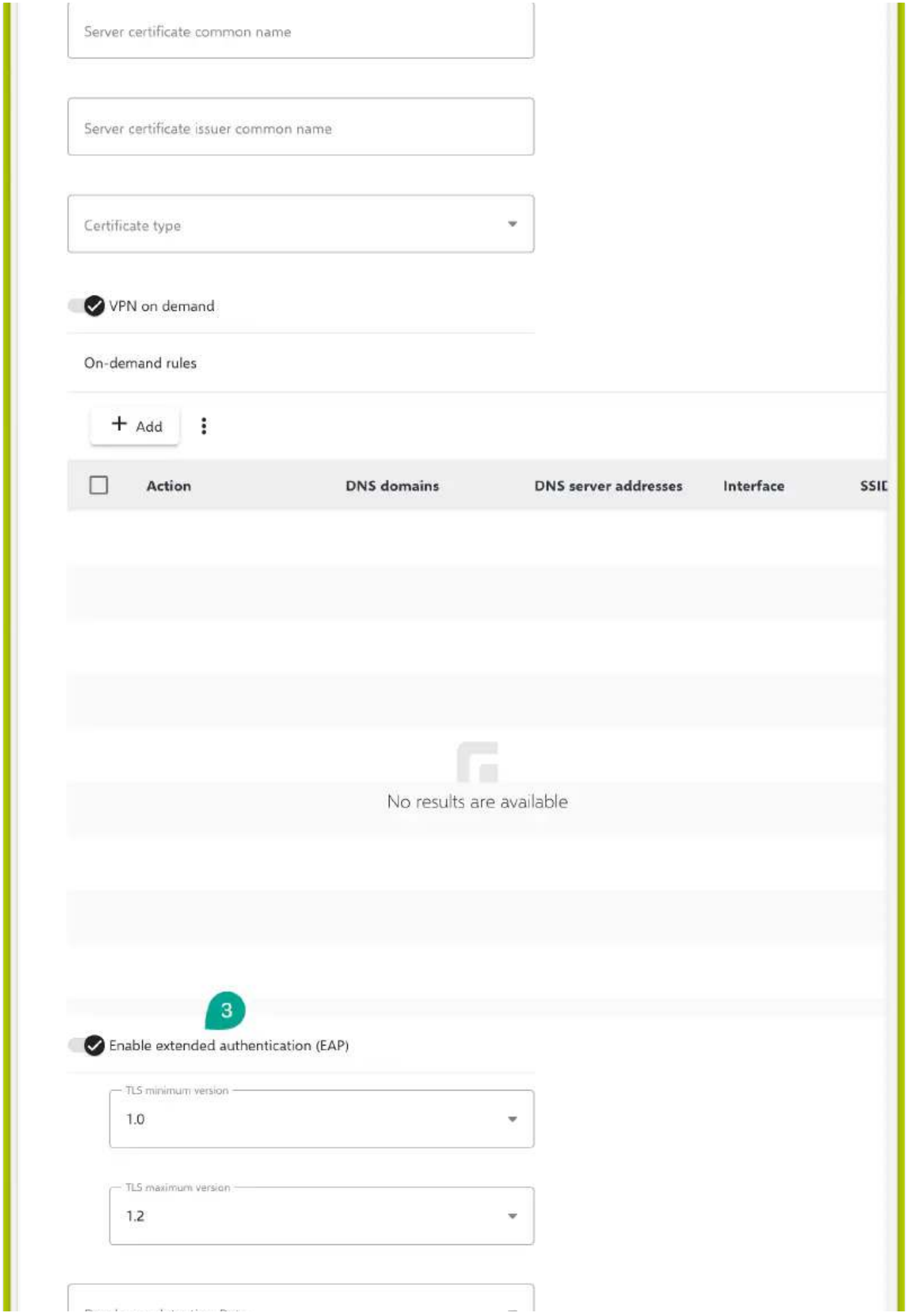
Sample iOS configuration

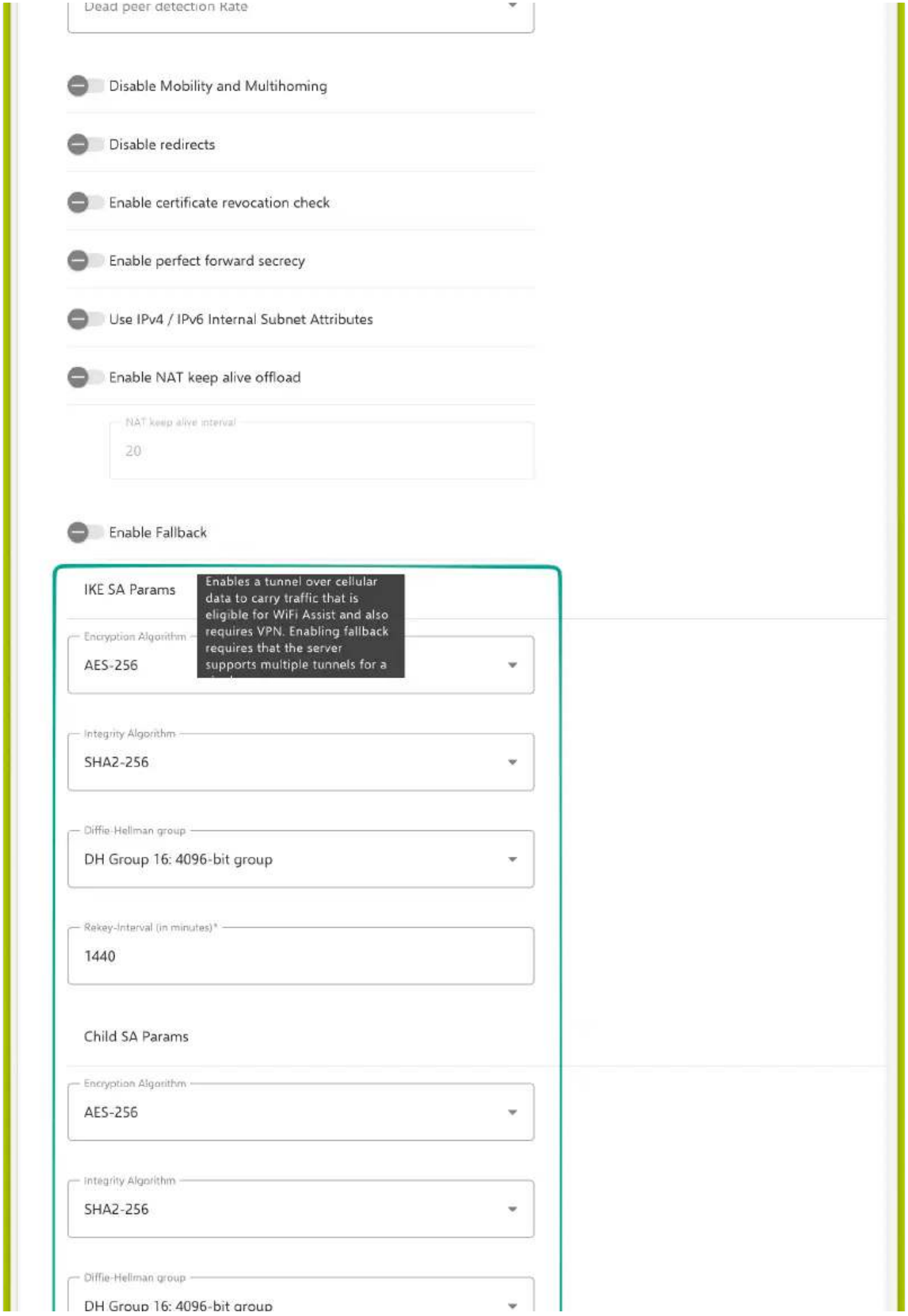
1. Create a new iOS policy or extend an existing one
2. Add a VPN configuration
    1. Select type IKEv2
    2. Enable Per App and Account VPN (see also Relution Hub Docs →)
    3. Set Server and Remote identifier to the value of `<%Relution Shield Host%>`
    4. Set Local identifier to `${device.uuid}@<%Relution Host%>`
    5. Set Machine authentication to Certificate and select the certificate template created before
    6. Activate Enable extended authentication (EAP)
    7. Set both IKE SA params and Child SA params to AES-256, SHA-256, DH group 16: 4096-bit group, 1440 minutes
    8. Optional: Add a test domain to Safari Domains below to automatically activate the VPN when the domain is accessed via Safari
3. Add a Certificate configuration to the policy and select the `<%Relution Shield Host%> CA Certificate` uploaded before
4. Optionally add a App to VPN Mapping configuration and select the VPN configuration created before and another browser app like Firefox or Chrome to test VPN access. It is recommended to also add an app compliance with this app as required to ensure it is installed
5. Publish the policy, and assign it to a device. The VPN can now be manually connected via `Settings` → `General` → `VPN & Device Management` → `VPN`. Relution Shield will also automatically be connected when accessing the Safari domains configured above in Safari or opening the browser app
6. Adjust the configuration according to include the accounts, apps and domains which should only be accessed via Relution Shield



For Version 26.4.0


Home > Policies > Shield >
VPN
VPN
Supports user enrollment
Cancel
Save
General
Connection name*
ShieldSupport
1
Connection type
IKEv2
2
Per App and Account VPN
Server*
shield.support.relution.io
Remote Identifier*
shield.support.relution.io
Local Identifier
${device.uuid}@support.relution.io
Machine authentication*
Certificate
Certificate
Use user certificate
Select certificate
Certificate
Select
Shield

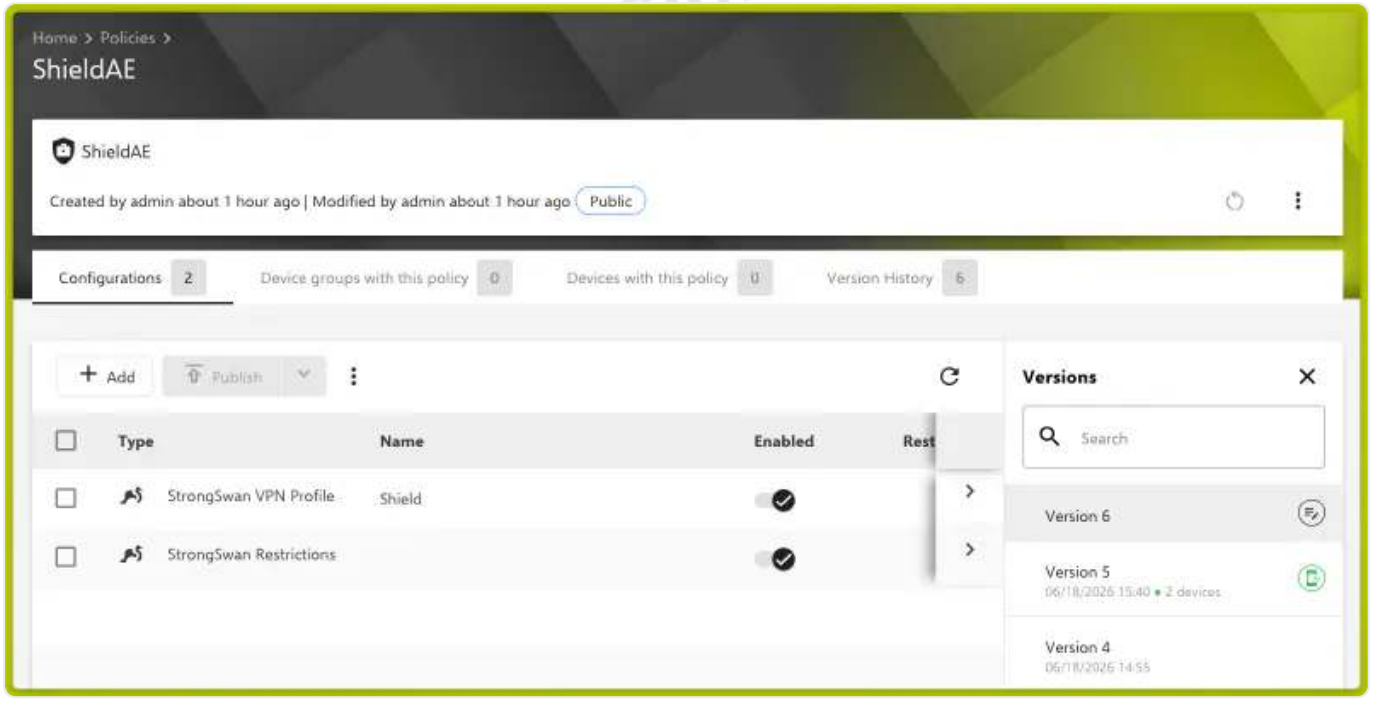

Server certificate common name
Server certificate issuer common name
Certificate type
VPN on demand
On-demand rules
Add
Action
DNS domains
DNS server addresses
Interface
SSID
No results are available
3
Enable extended authentication (EAP)
TLS minimum version
1.0
TLS maximum version
1.2

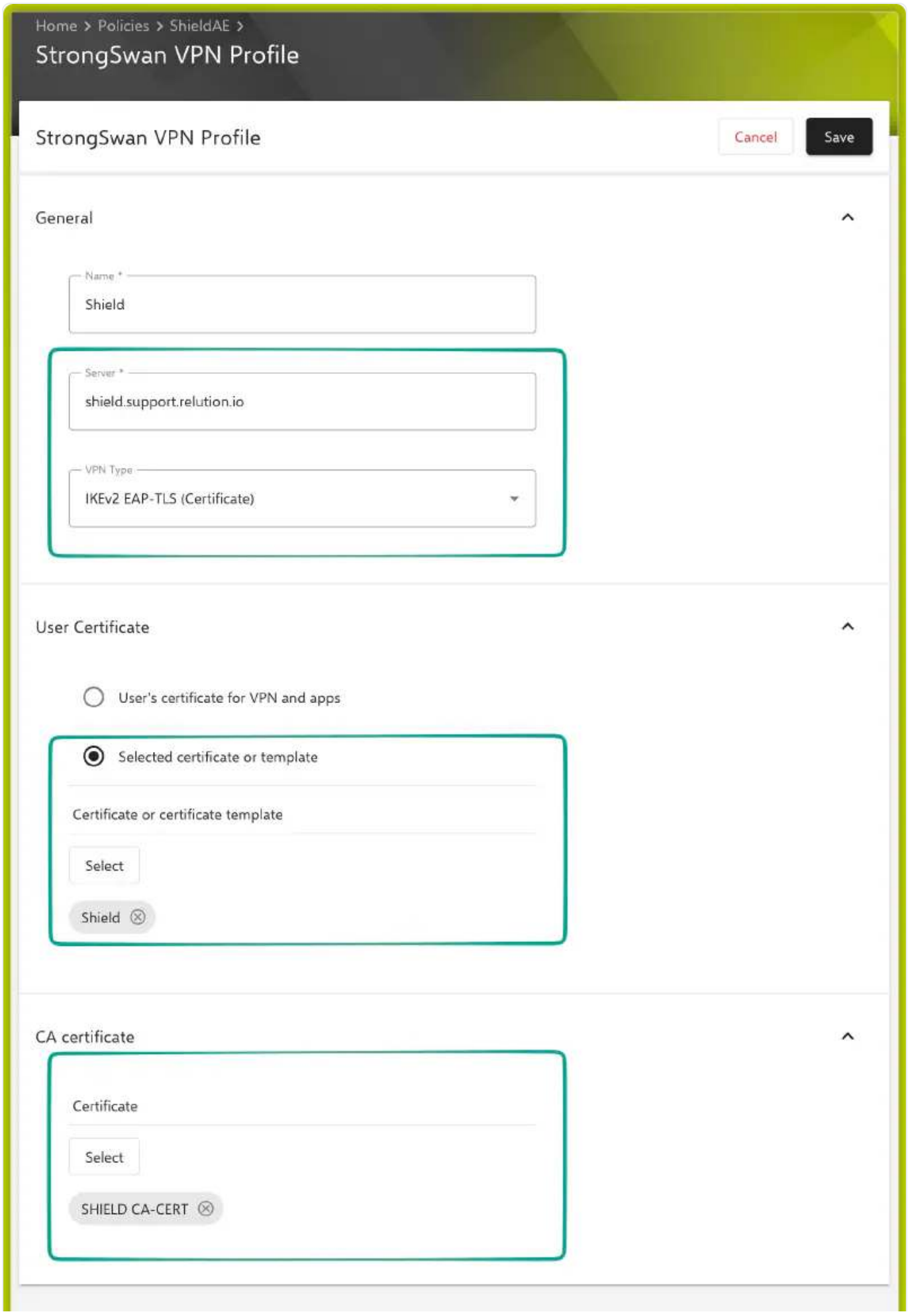

Dead peer detection Rate
Disable Mobility and Multihoming
Disable redirects
Enable certificate revocation check
Enable perfect forward secrecy
Use IPv4 / IPv6 Internal Subnet Attributes
Enable NAT keep alive offload
NAT keep alive interval
20
Enable Fallback
IKE SA Params
Enables a tunnel over cellular data to carry traffic that is eligible for WiFi Assist and also requires VPN. Enabling fallback requires that the server supports multiple tunnels for a
Encryption Algorithm
AES-256
Integrity Algorithm
SHA2-256
Diffie-Hellman group
DH Group 16: 4096-bit group
Rekey-Interval (in minutes)*
1440
Child SA Params
Encryption Algorithm
AES-256
Integrity Algorithm
SHA2-256
Diffie-Hellman group
DH Group 16: 4096-bit group

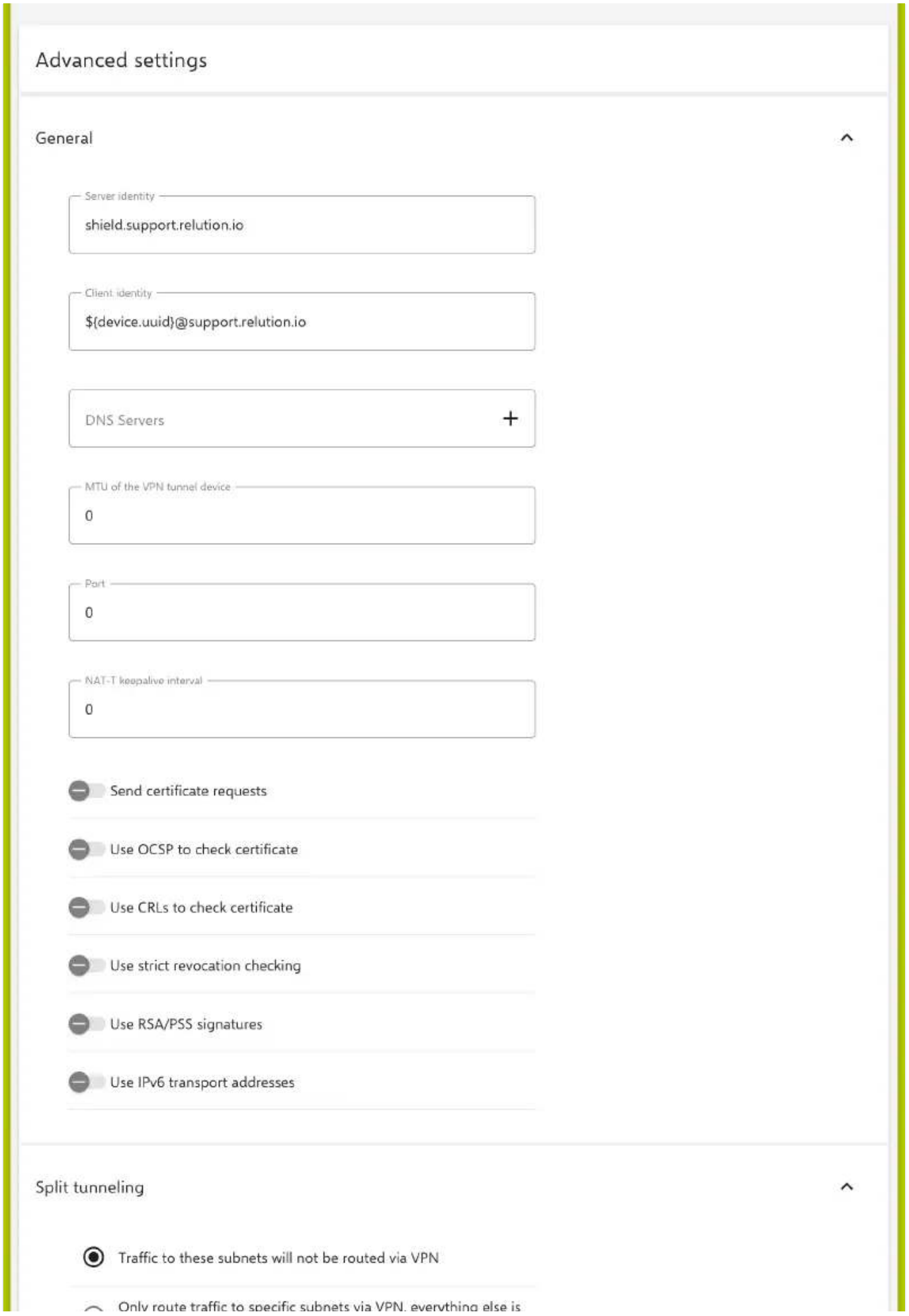


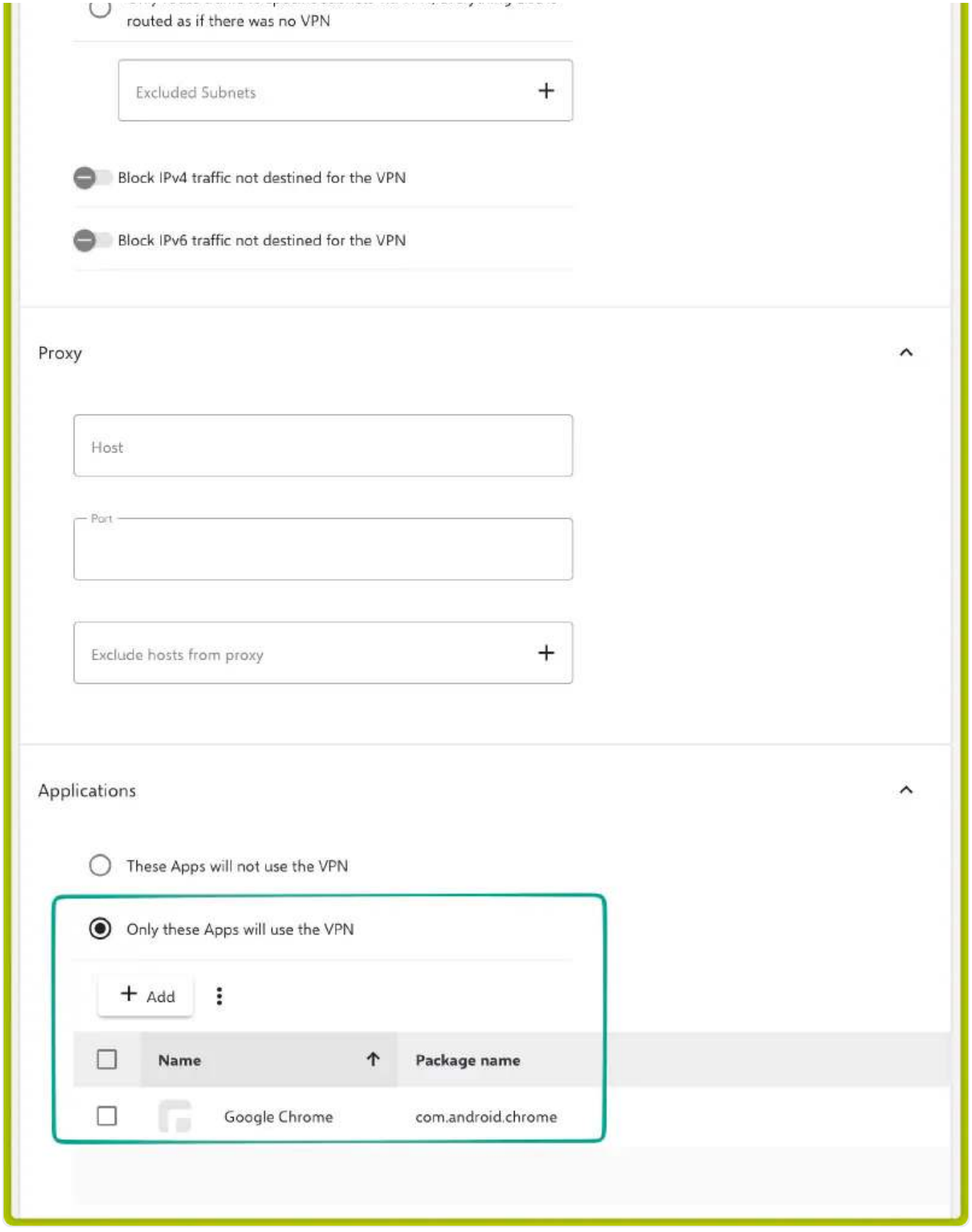
Sample Android Enterprise configuration

1. Create a new Android Enterprise policy or extend an existing one
2. Add a StrongSwan VPN Profile configuration
    1. Select IKEv2 EAP-TLS as VPN Type
    2. Set Server and Server identity to the value of `<%Relution Shield Host%>`
    3. Set User Certificate to the certificate template generated before
    4. Set CA certificate to the `<%Relution Shield Host%> CA Certificate` uploaded before
    5. Set Client identity to `${device.uuid}@<%Relution Host%>`
    6. Set Only these Apps will use the VPN to a browser like Firefox
3. Add a StrongSwan VPN Restrictions configuration and select the VPN profile created before as the default profile
4. Publish the policy, and assign it to a device. The VPN can now be manually connected via the StrongSwan app. Relution Shield will also automatically be connected when opening the browser app configured before
5. Adjust the configuration according to include the apps which should only be accessed via Relution Shield




Home > Policies > ShieldAE >
StrongSwan VPN Profile
StrongSwan VPN Profile
Cancel
Save
General
Name *
Shield
Server *
shield.support.relution.io
VPN Type
IKEv2 EAP-TLS (Certificate)
User Certificate
User's certificate for VPN and apps
Selected certificate or template
Certificate or certificate template
Select
Shield
CA certificate
Certificate
Select
SHIELD CA-CERT


Advanced settings
General
Server identity
shield.support.relution.io
Client identity
${device.uuid}@support.relution.io
DNS Servers
MTU of the VPN tunnel device
0
Port
0
NAT-T keepalive interval
0
Send certificate requests
Use OCSP to check certificate
Use CRLs to check certificate
Use strict revocation checking
Use RSA/PSS signatures
Use IPv6 transport addresses
Split tunneling
Traffic to these subnets will not be routed via VPN
Only route traffic to specific subnets via VPN, everything else is


routed as if there was no VPN
Excluded Subnets
Block IPv4 traffic not destined for the VPN
Block IPv6 traffic not destined for the VPN
Proxy
Host
Port
Exclude hosts from proxy
Applications
These Apps will not use the VPN
Only these Apps will use the VPN
Add
Name
Package name
Google Chrome
com.android.chrome

For version 26.4.0

Upgrade from 1.x to 2.x

Securely store the CA private key `/opt/relution-shield/etc/ipsec.d/private/ca-key.pem` outside the Relution Shield server if not already done.

1. Stop Relution Shield in `/opt/relution-shield` via `docker compose down`
2. Create/adjust the following files as described in the installation instructions:
    1. Create new config folders

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

    2. Create `etc/swanctl/swanctl.conf` → see step 6.4 of the installation
    3. Replace contents of `/opt/relution-shield/compose.yml` → see step 7.1 of the installation
    4. Update `/opt/relution-shield/.env` → see step 4 of the installation
    5. Update `/opt/relution-shield/etc/strongswan.conf` → see step 6.3 of the installation
    6. Move the following files

Previous path	Target path
`/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. Remove the `/opt/relution-shield/etc/ipsec.d` directory
    2. Remove `/opt/relution-shield/etc/ipsec.conf`
    3. Remove `/opt/relution-shield/etc/ipsec.secrets`
    4. Start Relution Shield in `/opt/relution-shield` via `docker compose up -d`

Secure Mail Gateway

If the Secure Mail Gateway is used, the Secure Mail Gateway standalone service is a mandatory component starting with Relution 26.4.0. This article covers the setup for on-premise installations.

For configuring the Secure Mail Gateway in Relution: Secure Mail Gateway →

Technical background

If the Secure Mail Gateway is enabled under `Settings` → `Device Management` → `Secure Mail Gateway`, incoming ActiveSync connections are forwarded to the Exchange server configured there, provided the request originates from a permitted (enrolled) device.

In version 26.3.x and older, ActiveSync requests first reach the Relution service, which forwards them to the Exchange server. The Relution service checks internally whether a request originates from a permitted device and may be forwarded. Requests that are not permitted are rejected.

As of version 26.3.0, the standalone service can optionally be enabled in order to test the switch to the dedicated container in advance. As of version 26.4.0 and newer, the corresponding functionality has been removed from Relution entirely, which means ActiveSync requests always have to be routed through the dedicated Docker container.

The configuration required for this is described below.

For version 26.4.0

Migration — What Needs to Be Done?

Installation	Action required
Relution Cloud – Shared Hosting	No action required. Relution handles the migration of the SMG service.
Relution Cloud – Dedicated Server (existing customers)	Relution will host the SMG service. We will reach out to coordinate the migration.
Relution Cloud – Dedicated Server (new customers)	The SMG service must be operated as a self-hosted on-premise component. Follow the setup guide further down in this article.
On-Premise	The full setup process is described further down in this article.

Feature toggle for on-premise installations (26.3)

New in 26.3

In Relution 26.3, on-premise installations can optionally activate the new mode. To do so, the following preview feature toggle has to be added to the Relution server's `application.yaml`:

`application.yaml`

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

In addition, a further Docker container has to be added to the Docker environment as described below.

> As long as the toggle is active, the new standalone service is used. If it is removed, Relution automatically falls back to the previous behaviour. This makes Relution 26.3 well suited for testing the new service in an on-premise environment before the update to 26.4.0 makes the switch mandatory.

For version 26.4.0

Mandatory component as of 26.4.0

New in 26.4

With Relution 26.4.0 the toggle is dropped. The Secure Mail Gateway must be operated as a separate service. The component has been removed from Relution entirely.

Setup

As an HTTP proxy, the Secure Mail Gateway standalone service forwards ActiveSync requests from mobile devices to the Exchange server and the responses back to the respective mobile device. To do so, it first has to be determined whether a request may be forwarded at all. So that the Secure Mail Gateway can make this decision, it has to communicate internally with the Relution service in order to check whether a request originates from a permitted device.

Relution

For the Secure Mail Gateway to be able to communicate with the Relution service, a technical user with the corresponding permissions has to be created in Relution first.

1. Create a Dynamic Role in Relution

Download the ready-made role template and import it in the Global organisation under `Settings` → `User Management` → `Permissions`:

Download SMG role template →

Alternatively, create the role manually:

1. Navigate to `Settings` → `User Management` → `Permissions` in the Global organisation
2. Add a new Dynamic Role
3. Enable the Secure Mail Gateway (service account) permission
4. Save the role

2. Create a technical user and API access key

1. Create a new user in the Global organisation and assign the Dynamic Role created above
2. Navigate to the user's detail page and create a new API access key
3. Copy the generated key — it is only shown once

Secure Mail Gateway container

The Secure Mail Gateway now has to be added to the environment as a separate Docker container and configured. Afterwards, the reverse proxy has to be adjusted so that requests to the `/Microsoft-Server-ActiveSync` endpoint are no longer sent to the Relution container but to the Secure Mail Gateway container.

For version 26.4.0

1. Deploy the service

Add the following service to the existing `compose.yaml`. This is only needed if the Secure Mail Gateway is used.

> Even if a newer version tag appears on Docker Hub, we strongly recommend keeping `latest`. New builds go through additional quality gates before being promoted to `latest` — pinning a specific version tag may result in running a build that has not yet been validated for production use.

`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` must be on the `reverse-proxy` network like `relution` and `traefik` — otherwise Traefik/nginx cannot route to it.

2. Configure the service

The API access key created in Relution earlier has to be added to the Secure Mail Gateway configuration so that the SMG can communicate with the Relution service.

If both services run in the same `compose.yaml` on one server, they communicate internally via the Docker network.

Create `smg/application.yaml` alongside the `compose.yaml`:

`smg/application.yaml`

```yaml
relution:
  server:
    url: http://relution:8080    # Keep unchanged with a shared compose.yaml
    api-key: your-api-key        # API access key created above
```

URL of the Relution server: If the Secure Mail Gateway and Relution run in the same `compose.yaml` on one server, `url: http://relution:8080` remains unchanged. The service name `relution` is then resolved via the shared Docker network.

The URL only needs to be changed if the SMG does not run in the same network as Relution, e.g. on a different server or in a separate `compose.yaml` with its own Docker network. In that case, the address at which Relution can be reached from the SMG is entered, e.g. `https://relution.example.com`.

For version 26.4.0

Reverse proxy configuration

The SMG service exposes the `/Microsoft-Server-ActiveSync` endpoint on port `8093`. The reverse proxy's configuration must be updated to route incoming requests on this path to the standalone SMG service. The examples below show how to do this for Traefik and nginx.

If a different reverse proxy is used (e.g. Apache, Sophos, ⋯), adjust its configuration accordingly. Please consult the product's documentation how individual paths or locations can be forwarded to separate endpoints.

Note: The examples below use hostnames that can be resolved within the Docker network. This is only possible while Relution, SMG and Traefik/nginx are part of the same Docker network. If reverse proxy or services are on separate networks, hostnames the internal DNS server can resolve must be used instead.

Traefik

Add the following additional `smg` entries below `routers` and `service`. Make sure to keep existing `routers` and `services`, such as `relution`. See also: Traefik configuration →

configs/traefik/relution.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 to Traefik)

Add (or update) the `location ~ /Microsoft-Server-ActiveSync` block into the existing HTTPS `server` block to forward incoming requests to SMG.

For version 26.4.0

relution-nginx.conf

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

    # (NEW) Redirect to Secure Mail Gateway
    location ~ /Microsoft-Server-ActiveSync {
        proxy_read_timeout 2100;
        proxy_pass http://smg:8093;
    }
}
```

The blocks position within the `server` block is not relevant, since nginx evaluates regular expression locations before the `/` prefix location. However, it is recommended to keep individual location blocks next to each other for the sake of readability.

> In a Docker setup, `smg` refers to the Docker service name and is reachable within the Docker network. For a native Linux installation replace `smg:8093` with `127.0.0.1:8093`.

Start or restart the Docker services

For the changes to take effect, the Docker containers have to be restarted afterwards.

```
docker compose up -d
```

> If any `relution.smg.*` properties were previously customised in the Relution server configuration, move them to this file unchanged — the property names are the same.

Advanced configuration

The following settings are only required in specific environments — for internal certificate authorities and for outbound connections that have to go through a corporate proxy.

(Optional) Trusting a custom CA certificate

If the Exchange server presents a server certificate issued by an internal CA (“self-signed”), the root certificate of that CA has to be added as a trusted certificate. To do so, a directory containing the PEM-encoded certificate file can be mounted into the container at `/opt/app/ca-certs`. The folder may contain more than one certificate if required.

For version 26.4.0

`compose.yaml`

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

These certificates are used when communicating with the Exchange and Relution server — there is no configuration property to set. If nothing is mounted, the feature is a no-op and outbound TLS behaves exactly as before. Adding, removing, or changing a certificate requires restarting the container; the directory is only read once, at startup.

(Optional) Proxy for outbound connections

Requests to Exchange honor the JVM’s proxy system properties. These are set via `JAVA_TOOL_OPTIONS` in the `compose.yaml` for the SMG container. In addition, the `honor-proxy-settings` flag has to be set to `true` in the `application.yaml`.

compose.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
```

With `-Dhttp.nonProxyHosts` (a `|`-separated list of host patterns, `*` wildcards supported) specific hosts can be excluded from the proxy — typically Exchange itself, if it is reachable directly without going through the corporate proxy.

By default, calls to the Relution server are not proxied — it is normally reachable directly. If the deployment reaches Relution through the same proxy as Exchange, set `honor-proxy-settings: true` in `smg/application.yaml`:

smg/application.yaml

```
relution:
  server:
    url: https://your-relution-server
    api-key: your-api-key
    honor-proxy-settings: true   # default false; only needed if Relution is also
behind the proxy
```

Troubleshooting

If issues occur with the SMG service — for example connecting to Exchange or starting the container — increasing the log level helps with the analysis. See Set log level → for instructions.

The easiest way is to enable the log level directly in the SMG container via its `application.yaml`, by appending the following section at the end:

smg/application.yaml

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

Changelog

Version currently available via `latest`: 26.0.6 (at 23.09.2026)

Version	Category	Change
26.0.6	Fixes	Incoming HTTP headers are now correctly treated as case-insensitive, avoiding potentially duplicated headers in the forwarded request
26.0.5	Configuration	The default `forward-headers-strategy` is now `native`
		The default `max-http-post-size` is now `1GB`
	Certificates	More useful logs about custom CA certificates in the trust store
		More useful logs when a connection is rejected due to an untrusted certificate
	Logs	A prematurely aborted connection is now logged
		The Exchange server's status code is logged when a message is rejected
		HTTP errors are also visible in the log when HTTP/2 is used
		Successful connections are logged at `INFO`
	Fixes	Prematurely terminated connections are now cleaned up properly
26.0.4	Release process	Adjustment of the internal release process – no functional changes
26.0.3	Feature	Support for self-signed certificates and proxy settings
26.0.2	Fixes	Fix wrongly handled 404 responses
26.0.1	Metrics	Expose health endpoint
26.0.0	Release process	Code migrated out of Relution

Overview

By default, Relution stores certain resources - such as native app binaries - in its database. This can cause the `resource` table to grow very large, especially when managing many native apps.

To optimize performance, Relution supports storing these resources in external S3-compatible object storage buckets.

> MinIO Users: MinIO ceased development in October 2025 and will not receive updates. We recommend migrating to SeaweedFS → using our guide: Object Storage Migration →

When to Use Object Storage

While optional, external object storage is recommended in these cases:

- Installation and management of native apps on Windows devices
- Managing a larger number of native apps, or native apps larger than 50 MB
- Servers with more than 5,000 devices

For version 26.4.0

Available Options

The most widely known object storage is AWS S3, but many S3-compatible solutions exist - both cloud-hosted and self-hosted.

Self-Hosted / On-Premise

Self-hosted solutions avoid cloud costs and provide full control over the data.

Provider	Description
SeaweedFS →	Recommended. Easy to deploy, tested with Relution. Our setup guide →
Garage →	Lightweight, designed for self-hosting.
Ceph →	Enterprise-grade, highly scalable.
RustFS →	Rust-based alternative.
MinIO →	Not Recommended. Has ceased development. Our migration guide →

We have thoroughly tested SeaweedFS with Relution. Other backends can work but have not been tested.

Cloud Providers

Provider	Notes
AWS S3 →	The original S3 implementation, tested with Relution.
Hetzner Object Storage →	German provider, cost-effective, tested with Relution.

For managed Relution hosting with object storage included, please contact our Sales Team → – more info: Relution Cloud →

Next Steps

Choose a path based on the setup:

ion 26.4.0

Situation	Next Steps
New setup with SeaweedFS (recommended)	1. Set up SeaweedFS → 2. Connect object storage →
New setup with a cloud provider	1. Set up at cloud provider 2. Connect object storage →
Migrating from MinIO or another backend	– Migration Guide →

SeaweedFS Setup

SeaweedFS → is an Apache-licensed open-source object storage backend with an S3-compatible API. It offers good performance, scalability, and an easy setup process. It can be deployed via Kubernetes, Docker, or directly on Linux, FreeBSD, macOS, or Windows.

This guide explains how to deploy SeaweedFS alongside Relution using Docker Compose on Linux.

While we have thoroughly tested it, SeaweedFS is third-party software and we cannot make security or reliability guarantees for it. For managed hosting, please contact our Sales Team →. More info: Relution Cloud →

This guide uses SeaweedFS in `mini` mode, which bundles all components with defaults appropriate for single-node deployments of moderate size. For more information: SeaweedFS Wiki →.

Prerequisites

- A working Relution installation with Docker Compose
- Access to edit the `compose.yml` file

For version 26.4.0

Prepare the compose.yml

Generate a 24-character alphanumeric password using a password manager, or from the Linux command line:

```
pwgen -snc 24 1
```

In the Relution `compose.yml` (on older installations: `docker-compose.yml`), add the following service under `services:`:

```
services:
  seaweedfs:
    image: chrislusf/seaweedfs:4.05 # Check for newer versions:
https://github.com/seaweedfs/seaweedfs/releases
    restart: unless-stopped
    ports:
      - 23646:23646
      - 8333:8333
    command: ["mini", "-dir=/data", "-admin.dataDir=/data/admin", "-
admin.password=%YOUR-GENERATED-PASSWORD%"]
    networks:           # Optional: for network segmentation, add `object-storage`
network
      - object-storage  # here and in the `networks` block of the `relution` service
    volumes:
      - seaweedfs-data:/data
```

Add two volumes under the `volumes:` section:

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

> Important: Include the SeaweedFS volumes in the backup routine. Without this data, server operation and device management cannot be ensured.

Start SeaweedFS

Pull the image and start the service:

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

SeaweedFS will be ready within a few seconds.

Create User and Bucket

SeaweedFS provides a web UI for administration.

1. Navigate to `http://localhost:23646/` in a browser
2. Log in with the password generated earlier
3. In the sidebar, go to `Object Store` → `Users`
4. Click Create User (top-right), enter `relution` as the username, and confirm
5. Note down the Access Key and Secret Key shown (they can be retrieved later via the 🔑 icon under *Actions*)
6. In the sidebar, go to `Object Store` → `Buckets`
7. Click Create Bucket, enter `relution` as the name, select `relution` as the bucket owner, and confirm

---

Note the Configuration Values

These values are needed to configure Relution:

Setting	Value
Endpoint	`http://seaweedfs:8333`
Access Key	*(from Step 3)*
Secret Key	*(from Step 3)*
Bucket Name	`relution`

Next Steps

Now configure Relution to use the new object storage:

Connect object storage →

Connect object storage

Once an S3-compatible object storage backend is ready - whether self-hosted or cloud-based - Relution needs to be configured to use it.

Prerequisites

The following information is needed from the object storage provider:

Setting	Description
Endpoint	The S3 API URL
Access Key	Authentication key ID
Secret Key	Authentication secret
Bucket Name	The storage bucket name

For version

In the configuration examples below, we will use example values matching our SeaweedFS guide →. If a different backend or provider is used, adjust them accordingly.

Configuration

Choose one of the two options below. Both achieve the same result.

Option A: Using application.yml

Add the following to the `application.yml`:

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

Option B: Using Environment Variables

Add these environment variables to the `relution` service in the `compose.yml`:

```
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"
```

If the object storage is to be encrypted with a customer-provided key, this must be done before the first start: Server-Side Encryption (SSE-C) →

Starting the Services

1. Pull the latest images:

```
docker compose pull
```

2. Start or restart the containers:

```
docker compose up -d
```

3. Relution will automatically begin migrating content from the `resource` database table to the object storage bucket.

Monitoring Progress

Watch the migration progress in the logs:

```
docker logs -f relution
```

Files being created can also be verified by checking the object storage backend (e.g., via the SeaweedFS web UI or the cloud provider's console).

Important Notes

Irreversible Process: As of Relution 26.0.0, migrating to object storage cannot be reversed.

Backup: Ensure the object storage bucket is included in the backup routine. Without this data, server operation and device management cannot be ensured.

Server-Side Encryption (SSE-C)

Relution can encrypt the objects it stores in an S3-compatible bucket using Server-Side Encryption with a Customer-Provided Key (SSE-C). With SSE-C, Relution sends the encryption key with every request, and the storage backend uses it to encrypt objects on write and decrypt them on read. The backend never stores the key itself - keeping it safe is solely the administrator's responsibility.

> Read before enabling: SSE-C takes effect immediately on startup and Relution does not encrypt objects that already exist in the bucket. Only enable it on a clean instance with an empty bucket, or encrypt all existing objects first. If the key is lost, all encrypted data is permanently lost. See Important Notes below for details.

> SSE-C vs. KMS encryption: SSE-C is not the same as client-side encryption via AWS KMS (added in Relution 26.3.3 →). With KMS, a customer managed key (CMK) is held and managed by AWS KMS. With SSE-C, the key is provided by Relution on each request and stored only by the administrator. These two mechanisms are mutually exclusive - only SSE-C or KMS or neither can be enabled, but never both at the same time.

Prerequisites

- A working S3-compatible object storage setup - see Connect object storage →.
- An object storage backend that supports SSE-C. We have verified support with SeaweedFS and Hetzner Object Storage. Other S3-compatible backends may work but have not been tested.
- A 256-bit encryption key (see below).

For version 26.4.0

Generating the Key

SSE-C requires a 256-bit (32-byte) key, provided as a Base64-encoded string. Generate one with `openssl`:

```
openssl rand -base64 32
```

Store the resulting value securely. If this key is lost, all encrypted objects in the S3 bucket can no longer be decrypted and are permanently lost.

Configuration

SSE-C is activated as soon as a key is configured. The key can either be provided inline via the `relution.storage.s3.serverSideEncryption.key` property (options A and B) or supplied as a file via `relution.storage.s3.serverSideEncryption.keyFile` (option C). If both are set, the key file takes precedence.

Option A: Using application.yml

Add the `serverSideEncryption` block to the `application.yml`:

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

For version 2

Option B: Using Environment Variables

Add the following environment variable to the `relution` service in the `compose.yml`:

```
services:
  relution:
    environment:
      - RELUTION_STORAGE_S3_SERVERSIDEENCRYPTION_KEY=%YOUR-BASE64-KEY%
```

Option C: Key as a file

New in 26.5

Instead of providing the key inline, it can be read from a file. This is particularly useful when the key is mounted into the container as a Docker or Kubernetes secret. The path to the key file is configured via `relution.storage.s3.serverSideEncryption.keyFile`:

```
relution:
  storage:
    s3:
      serverSideEncryption:
        keyFile: /path/to/ssec.key
```

Or via the corresponding environment variable:

```
services:
  relution:
    environment:
      - RELUTION_STORAGE_S3_SERVERSIDEENCRYPTION_KEYFILE=/path/to/ssec.key
```

The file must contain the same Base64-encoded 256-bit key as the inline value (for example, generated with `openssl rand -base64 32`). A trailing newline is harmless because the value is trimmed; binary or hexadecimal keys are rejected.

On startup, Relution logs the read with `Reading SSE-C key from file <path>`. If the file is missing or does not contain a 32-byte key, startup aborts with a corresponding error message.

Important Notes

For version 26.4.0

No migration of existing files: SSE-C takes effect immediately when Relution starts with the key configured. Relution does not encrypt objects that already exist in the bucket. Only use SSE-C on a clean instance with an empty bucket, or encrypt all existing S3 objects before starting Relution with the key. Otherwise, previously stored objects will remain unencrypted and may become inaccessible.

Losing the key means losing all data: The storage backend does not store the key - keeping it safe is solely the administrator's responsibility. If the key is lost, all encrypted objects in the bucket become permanently unrecoverable, and Relution can no longer serve apps or resources from object storage. Keep the key in a secure, backed-up location.

Key rotation requires re-encryption: Rotating the key is the administrator's responsibility. Relution does not re-encrypt objects when the key changes. To rotate the key, all existing objects in the bucket must be re-encrypted with the new key (for example, by copying them with the new key) before starting Relution with the updated configuration. Starting Relution with a new key while objects are still encrypted with the old one will make those objects inaccessible.

Mutually exclusive with KMS: Server-side (SSE-C) and client-side (KMS) encryption cannot be active at the same time. Configure at most one of them.

Migration Guide

This guide explains how to migrate Relution data from one object storage backend to another. Common scenarios include:

- Migrating from MinIO to SeaweedFS (MinIO is no longer maintained)
- Moving from cloud provider to self-hosted (or vice versa)
- Switching cloud providers

The examples below demonstrate a migration from MinIO to SeaweedFS, but the steps can be adapted for any S3-compatible source and destination.

The migration process consists of four steps:

1. Set up the new storage backend
2. Copy data from old to new storage
3. Update Relution configuration
4. Remove the old backend

Prerequisites

- Access to both storage backends simultaneously
- The `rclone` command-line tool (installation guide →)
- Credentials for both storage backends

For version 26.4.0

Set Up the New Backend

If migrating to SeaweedFS, follow our SeaweedFS Setup Guide → first, but do not start Relution yet.

Ensure both old and new storage backends are running:

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

Configure rclone

The `rclone` tool provides a fast and reliable way to copy data between S3-compatible backends.

Install rclone

Follow the instructions at rclone.org/install → for the operating system in use.

Create Remote Configurations

Run the configuration wizard:

```
rclone config
```

Configure the source (MinIO):

1. Type `n` for new remote
2. Name: `source`
3. Storage type: Select `s3`
4. Provider: Select `Minio` (or `Other` for generic S3)
5. Enter the access key and secret key
6. Endpoint: `http://localhost:9000`
7. Accept defaults for remaining options
8. Confirm with `y`

Configure the destination (SeaweedFS):

1. Type `n` for new remote
2. Name: `dest`
3. Storage type: Select `s3`
4. Provider: Select `Other`
5. Enter the new access key and secret key
6. Endpoint: `http://localhost:8333`
7. Accept defaults for remaining options
8. Confirm with `y`

Type `q` to exit the configuration.

Verify Port Access

Ensure the S3 API ports are exposed on the host. Check the `compose.yml`:

For version 26.4.0

```
minio:
  ports:
    - "9000:9000" # S3 API - must be accessible
    - "9001:9001" # Web console
# ...
seaweedfs:
  ports:
    - "8333:8333" # S3 API - must be accessible
    - "23646:23646" # Web console
```

Copy the Data

1. Verify Relution is stopped to prevent data changes during migration:

   ```
   docker compose ps  # Should show storage backends, but NOT relution
   ```

2. Start the transfer:

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

3. Wait for completion. Transfer time depends on the amount of data in the bucket.

4. Verify the transfer:

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

   Expected output: `0 differences found`

Update Relution Configuration

Update the Relution configuration to point to the new backend. The following needs to change:

Setting	Old Value	New Value
Endpoint	`http://minio:9000`	`http://seaweedfs:8333`
Access Key	Old key	New key
Secret Key	Old secret	New secret

See Connect object storage → for detailed instructions on where to make these changes.

Verify and Clean Up

1. Start Relution:

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

2. Verify functionality: Log into Relution and confirm that apps and resources load correctly.
3. Remove the old backend (only after thorough verification):

```
docker compose down minio  # Stop the old service
```

4. Clean up configuration: Remove the old service from the `compose.yml`.
5. Delete old data: Remove the old storage volume or directory (e.g., `./volumes/minio/data`).
6. Clean up rclone: Optionally remove the rclone configuration:

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

Connection Refused / Timeout

Ensure the S3 API ports are exposed and not blocked by a firewall or network segmentation. Test connectivity:

```
curl http://localhost:8333  # Should return an S3 error
```

Access Denied / 401 / 403

Verify that the credentials are correct and the user has access to the bucket.

Missing Files After Migration

Re-run the verification:

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

If differences are found, run `rclone copy` again; it will only transfer missing files.

Deprecated: MinIO

Important: MinIO has discontinued further development without prior notice in October 2025. We therefore discourage the further usage of MinIO.

New information on object storage is available here: Object Storage →
To migrate away from MinIO, we have created a guide: Migration →

Deprecated MinIO Setup Instructions

Checklist

After completing the installation, here is a list of small tasks to go through to confirm the installation works as expected.

Login

For security reasons, logging in is only possible via HTTPS. Attempting to log in via HTTP produces the following error:

```
Access is forbidden
```

System Administrator

The system administrator can be used to create additional organizations.

Logging in to Relution as a System Administrator uses the credentials defined in the `application.yml` or in the environment variables.

application.yml

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

Environment variables

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

> For security reasons it is necessary to change the password after the first login! The sysadmin password is evaluated and set only at the initial creation (usually first server start). It cannot be changed afterwards via the configuration.

For version 26.4.0

Organization administrator

Logging in to Relution as an organization administrator is also possible. If LDAP is used, make sure login works with at least one LDAP user account.

Test
Logging in with a local account is possible
Logging in with an LDAP account is possible

For security reasons, we strongly recommend changing the password after the first login.

Certificates

Make sure a connection to Relution is possible using the external hostname. Mobile devices can be stricter when it comes to verifying SSL certificates. Even if the desktop browser shows a valid HTTPS connection, the devices may reject the connection if some things are not configured properly. We strongly recommend using SSL Labs → to verify that everything is set up correctly.

For version 26.4.0

Common errors.

- Incomplete certificate chain (missing intermediate certificates). Chrome, Firefox, etc. can ignore this, but mobile devices may reject the connection.
- Reverse proxy uses server name indication (SNI). This is not supported by some older Android versions. As a workaround, make sure that the MDM server's certificate is the first one returned.

Mobile devices reject the certificate

Possible Cause.

- The certificate chain may be incomplete. An incomplete chain is ignored by most desktop browsers, but may cause errors on mobile devices.

Solution

- Use SSL Labs → to verify that the SSL certificate is set up correctly. The test takes about 5 minutes to complete. Fix any issues that are reported.

Mobile devices receive a different certificate

Possible Cause.

- The server may be using Server Name Indication (SNI), which is not supported by all mobile devices.

Solution

- Reconfigure the web server so that the first certificate returned is the one required by the mobile devices. The devices are not able to request a specific certificate and always use the first one sent by the server.

Database backups

Make sure a `working` database backup exists. This is important in case the hardware fails or an upgrade goes wrong.

Test
Relution’s database is included in automatic backups
The database can be restored (on another computer)

For versio

---

iOS

We always recommend using the Relution App Family for iOS from the public App Store. These are automatically imported into the Relution App Store.

Android

To use the native version of these applications directly in Relution, they are available here: Until Relution Server 5.10:

- Android →

From Relution Server 5.11:

- Android Companion →
- Android Agent →

Support

For support purposes, allowing remote access to the Relution server can be useful. Consider enabling or installing remote access software such as Remote Desktop, SSH or TeamViewer. For the best possible security we recommend using SSH with key-based authentication.

Consider using a separate user account for support personnel (e.g., for audit purposes). The support staff usually needs read and write access to the installation directory and the ability to restart the Relution service. Relution service to restart.

Note that Relution support is usually chargeable.

For version 26.4.0

Mail dispatch

Starting with Relution Server version 5.22, the SMTP server connection can be configured via web interface. This connection is necessary if Relution is to actively send emails. These can be, for example, emails for a password reset, registration or notification. The connection of an SMTP server is optional. Until version 5.21, the connection to the SMTP server had to be configured on the server via the `application.yml`.

Configuration

For system administrators, the SMTP server configuration is available in the `Global` organization under `Settings` → `Email server configuration`. It comprises the following fields:

- Host and Port
- Connection security: None, STARTTLS, STARTTLS (REQUIRETLS) or SSL/TLS. With STARTTLS, Relution switches to an encrypted connection if the server supports it; with STARTTLS (REQUIRETLS), sending fails if the server does not offer STARTTLS.
- Use Extended Hello (EHLO)
- HELO/EHLO local host name: If the field is left empty, the server's external host name is used.
- Username and Password: If the password field is left empty when editing, the existing password is kept.
- Mail from: Required; this address is used as the sender of outgoing emails.

In the Test email configuration section, Send sends a test email to the email address stored for the system administrator.

For version 26.4.0

Precedence between web interface and application.yml

The configuration saved in the web interface takes precedence. The values from the `application.yml` or from environment variables are only used as long as no configuration is saved in the web interface. An existing configuration is removed in the Email server configuration category, section Clear configuration, via Clear; Relution then falls back to the `application.yml`.

Changes to the `application.yml` only take effect after the Relution server is restarted.

application.yml

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

The settings shown above are the default values if they are not configured. SMTP connectivity is tested as part of the server health check, which are displayed in the System Portal.

The former key `ttls` instead of `starttls` is still evaluated. If both `ssl` and `starttls` are `true`, Relution uses SSL/TLS.

> Relution reads the mail configuration exclusively from `relution.mail` and `relution.smtp`. Entries under `spring.mail` are ignored. If the configuration is placed there, Relution tries to send mail via `localhost` on port `25`.

For version 26.4.0

Alternatively, the values can be set via environment variables, e.g. in a Docker installation:

Environment variable	Key in 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`

A value set explicitly in the `application.yml` takes precedence over the environment variable.

Additional mail session options

Further options can be passed directly to the mail library (Jakarta Mail) via `relution.mail.properties`. The entries are applied unchanged and override the values set by Relution. They only take effect as long as the configuration comes from the `application.yml`, i.e. no configuration is saved in the web interface.

```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
```

For version 26.4

The keys contain dots and are therefore enclosed in square brackets and quotes. Commonly used options:

Option	Effect
`mail.smtp.from`	Sender address. If not set, Relution derives an address from the external server URL (`no-reply+relution@<domain>`).
`mail.smtp.localhost`	Host name announced in the `EHLO` command. If not set, the host name of the external server URL is used.
`mail.smtp.starttls.required`	Aborts sending if the server does not offer STARTTLS.
`mail.smtp.ssl.trust`	Hosts whose certificate is trusted without validation. Helps with mail servers that present an incomplete certificate chain.

`mail.smtp.ssl.trust` should contain the specific host name of the mail server. The value `*` trusts every certificate of every server. The better solution remains to add the certificate of the issuing certificate authority to the truststore.

If sending fails, Relution logs the complete SMTP communication as soon as the log level for `io.relution.setting.system.email.SystemEmailConfigurationService` is set to `DEBUG`. Adjust log level →

Amazon Simple Email Service (SES) SMTP

The recommended settings for connecting to Amazon SES looks like:

```
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
```

Note that the SMTP parameters `username` and `password` are an AWS access key and a secret key of an IAM user with `AmazonSesSendingAccess` permissions, which must be `ses:SendRawEmail` permissions. Make sure the correct region is specified as part of `host`. These settings can be found on the `SMTP Settings` page of the SES service in the AWS console.

For version 26.4.0

Microsoft Office365 SMTP

The recommended settings to be able to send mail via Office 365 are these:

The Mail from address under `Settings` → `Email server configuration` must match the account's username. If the configuration is made via the `application.yml`, the sender address is set via `mail.smtp.from` (see Additional mail session options →). SMTP AUTH must be enabled for the account.

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

Disaster Recovery

This guide describes the backup and security concept for a Relution Server that uses a database (PostgreSQL or MariaDB) and optionally integrates an on-premises S3-compatible storage system (such as MinIO).

The goal is to ensure data integrity, minimize downtime (RTO), and guarantee reliable restorability in an emergency.

> The configuration of backup automation, monitoring, and ensuring the backups are performed is the responsibility of the customer.

System Overview

The Relution infrastructure typically consists of the following components that need to be backed up:

- Application Server: Hosts the Relution application and services.
- Database (On-Premises): MariaDB or PostgreSQL.
- S3 Storage (On-Premises): Object-based storage system (optional) for storing files, backups, and persistent data.

> All applications can also be operated together on a single machine. The use of S3 Storage is optional, but if used, operation of the Relution Server is impossible without the contents of the S3 Bucket.

For version 26.4.0

Backup Goals

- Minimizing data loss (RPO – Recovery Point Objective)
- Fast restoration of services (RTO – Recovery Time Objective)
- Protection against hardware failure, software errors, and human errors
- Protection against data manipulation and ransomware

1. Database Backup

Strategy	Details
Frequency	Daily full dumps (e.g., via `mariadb-dump` or `pg_dump`)
Incremental	Hourly incremental backups (depending on necessity)
Management	Automated rotation and retention rules
Security	Encryption of backup files (AES256 or GPG) depending on necessity
Consistency	During the backup, the Relution service should be temporarily stopped to avoid inconsistencies!

2. S3 Storage Backup (Optional)

Version 26.4.0

Strategy	Details
Method	Replication to a second S3 target or regular syncing (`s3cmd sync`, `rclone sync`)
Scope	Backup of critical buckets at defined intervals
Consistency	During the backup, the Relution service should be temporarily stopped to avoid inconsistencies!

3. Server Configuration Backup

All relevant configuration files must be backed up:

- `/opt/relution` (Directory of the Relution Server)
- `compose.yml` (or comparable startup scripts)
- `application.yml` (Relution configuration)
- NginX configuration file, if applicable
- SSL certificate and key

Backup Storage Locations

Adherence to the 3-2-1 backup principle is recommended:

- 3 copies of the data
- 2 different systems/media
- 1 copy external/offsite

Time Schedule

Interval	Backup
Daily	Full database backup
Hourly	Incremental DB backup (depending on necessity)
Daily	S3 sync of critical buckets
Weekly	Full server configuration backup

For version

Further Aspects

Area	Details
Automation	Cron jobs or systemd timers; Logging all processes; Notifications on errors
Encryption	Encryption of all backups; TLS/HTTPS/SSH for transport
Integrity Check	Monthly test restore

1. Database Recovery

1. Select the correct backup file.
2. Prepare the target system (stop the database service).
3. Perform the data import (e.g., via `psql` or `mysql`).
4. Functional test of the Relution application.

2. S3 Storage Recovery

1. Select the objects/buckets.
2. Restore via `rclone`, `s3cmd`, or API.
3. Integrity check (verify files are available in Relution).

3. Full System Recovery

- Restoration of configurations (from the server configuration backups).
- Restart of all services.
- Functional test of the complete application.

For version 26.4.0

Monitoring & Alerting

- Monitoring of all backup processes (e.g., with tools like Grafana + Prometheus).
- Alerting for:
  - Backup errors
  - Low disk space
  - Integrity errors
  - Test-restore failures

Security

- Access restrictions (Least Privilege principle).
- Secure storage of keys and credentials.
- Regular updates of the software used.

Documentation

- Documentation of all process changes (configuration, schedules).
- Clear responsibilities for backup and restore.
- Log data retention for at least 90 days.

Conclusion

This security concept ensures that both the database and the on-premises S3 storage system are reliably protected and can be quickly restored in an emergency. Through automation and regular checks, operational security is guaranteed long-term.

For version 26.4.0

Update - Relution

Follow these steps to upgrade the Relution installation.

> Before starting, make sure a working backup of the database has been created and, if necessary, the S3 storage! A snapshot of the server is usually also sufficient.

Docker installation

Edit the `docker-compose.yml` file and replace `image: relution/relution:xxx` with `image: relution/relution:latest`.

Updating Relution is then very easy:

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

In newer Docker versions, the spelling has changed to docker compose without a hyphen.

Make sure to compare `docker_relution` with the name of the Relution container `container_name` specified in the `docker-compose.yml` if it is different from the default.

This command will download the latest version of the Docker image and install it. The Relution service will be unavailable for a few minutes while the container is restarting.

The following command can be used to delete old containers and caches, which can free up a lot of memory.

```
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]
```

Verify Image Integrity

Before applying a Docker update, verify the image digest:

1. Obtain the SHA-256 digest for the new release from the Relution release manifest.
2. Pull the new image and verify its digest:

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

3. Compare the digest to the published manifest. Do not proceed if they differ.
4. After verifying, update the image reference in the deployment manifest to pin the verified digest.

For version 26.4.0

Native installation Linux

1. download the latest relution package: Latest Relution Package →
2. stop the Relution service
3. Backup the Relution database
4. backup the installation directory

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

5. extract the zip package to `<INSTALL_DIR>`
6. set the owner of the `<INSTALL_DIR>` directory, for example:

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

7. copy `<INSTALL_DIR>.bak/application.yml` to `<INSTALL_DIR>/application.yml`
8. start the Relution service
9. wait until the Relution service is started

The database will be updated to the latest version. Updating the database may take some time

For version 26

Native Installation Windows

1. download the latest Relution package: Latest Relution Package →
2. stop the Relution service via the Services console (`services.msc`)
3. save the existing installation directory to `relution_bak_`
4. extract the zip package to the old installation directory `<INSTALL_DIR>`
5. copy the configuration file from the backup `relution_bak_/application.yml` to `<INSTALL_DIR>/application.yml`
6. start the Relution service
7. wait until the Relution service has started. in the directory `<INSTALL_DIR>/log/relution.txt` the log can be viewed

   The database is being updated to the latest version. Updating the database may take some time.

Known error messages

Receiving the following message when starting the Relution service can indicate that the Java version used is too low.

```
The service "Relution" on "Local Computer" could not be started
The service did not return an error.
It may be an internal Windows error or an internal service error.
Please contact your system administrator if the problem persists.
```

To fix this, please download and install the latest Java 17 LTS from the following link: Adoptium Java →
During installation, activate the option `Set Home PATH`; otherwise, the Home PATH must be entered manually in the Windows variables afterwards.
After installation, restart the Relution service.

Checklist after the update.

- Do relution apps on mobile devices also need an update?
- Do custom CSS files need an update?
- Are enrolled devices still accessible?
  - Send an `update device information` action to a device
- Is enrollment still working for the different platforms?

Note: Update from Relution 5.3x.x to 26.2.x

When updating from `Relution 5.3x.x` to `Relution 26.2.x`, it is mandatory to first upgrade to the intermediate version `Relution 26.0.3`.

Docker

For Docker installations, the version can be specified directly in the `compose.yml`.

1. First, update to the latest released 5.x version:

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

2. Then, update to the latest released 26.0.x version:

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

3. After a successful update, the version can be set back to `latest` to automatically use the most recent available version:

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

Linux and Windows (native)

For native installations on Linux and Windows, the process is the same as with Docker:

1. Update to `Relution 5.35.4`
2. Update to `Relution 26.0.3`
3. Update to the latest version (`latest`)

Downloads:

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

APNS Push Certificates

To communicate with Apple devices via MDM, Relution requires a signed APNS push certificate → (Apple Push Notification service). This certificate is linked to an Apple ID and must be renewed before it expires.
If a certificate expires, all enrolled Apple devices lose their MDM connection and must be re-enrolled.

> As of Relution 26.3.0, new installations are required to provide their own APNS certificate via the Self-Service Wizard described on this page. Existing installations will continue to function with their current configuration and can migrate to the new method at their own pace.

> Always renew the existing certificate instead of creating a new one. Uploading a certificate with a different push topic causes enrolled devices to continue using the old certificate until it expires — after that, they must be re-enrolled.

Migration from the Previous Process

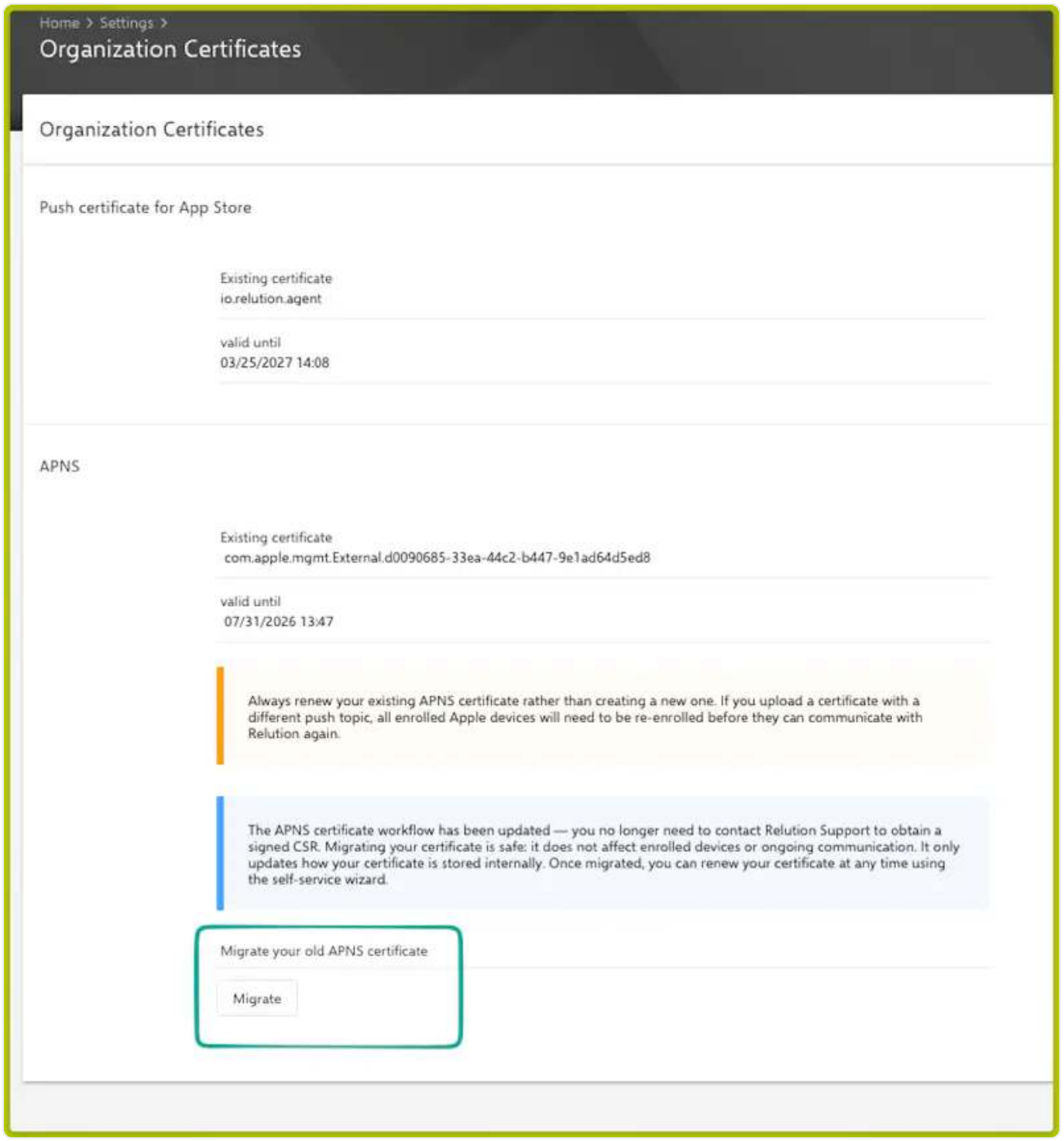
New in 26.3

> This section only applies when a custom APNS certificate was previously provided by submitting a CSR to Relution Support. For a new installation, or when using the Relution default certificate, skip this section.

For version 26.4.0

If the Relution installation was set up prior to version 26.3.0 and a certificate was previously provided by sending a CSR to Relution Support, a one-time migration must be performed before using the Self-Service Wizard.

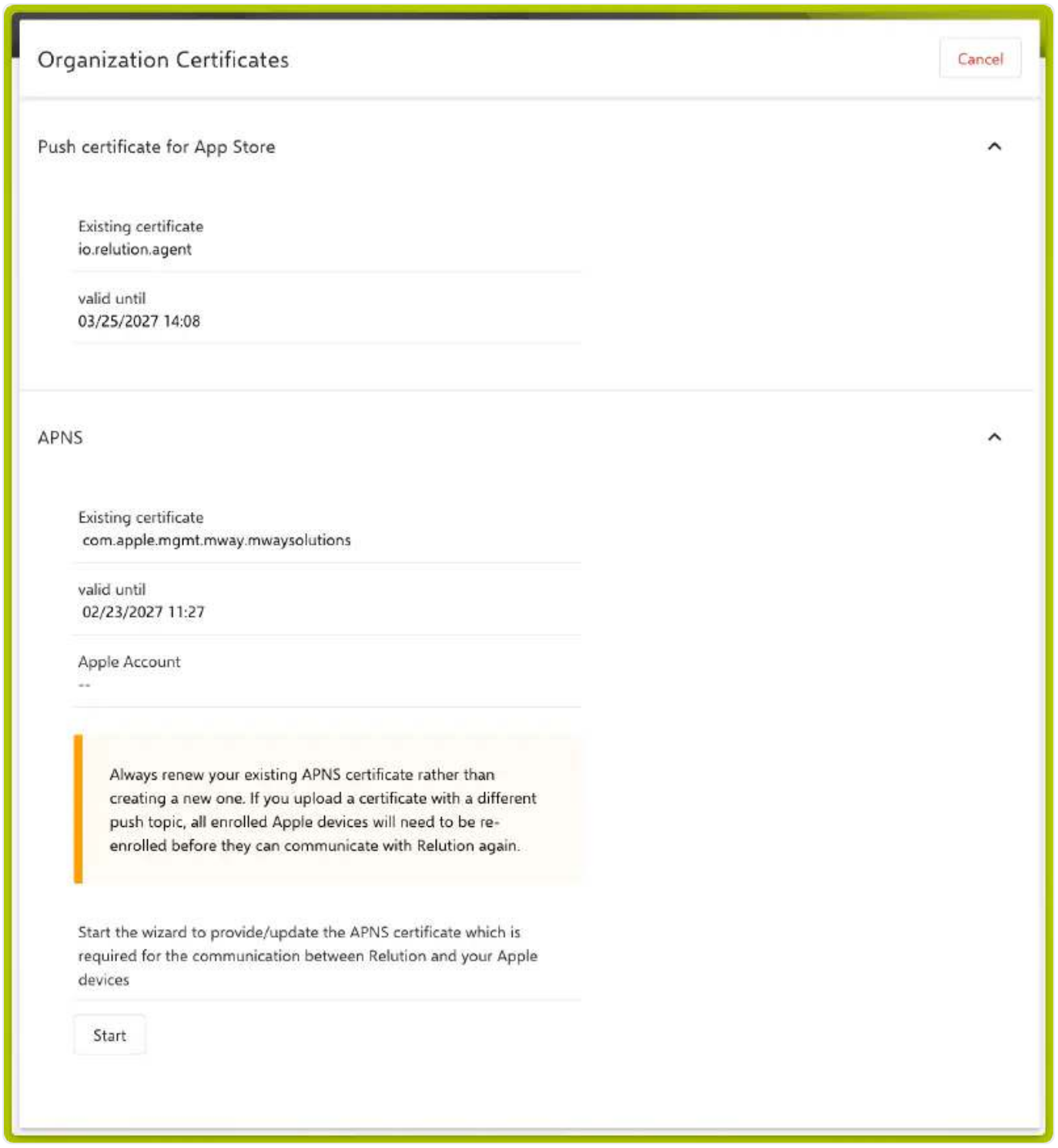
Navigate to `Settings` → `Organization Certificates`. If a migration is available for the organization, an information box with a button labeled Migrate old APNS certificate appears. Click it.



The migration is instantaneous and safe: it has no impact on enrolled devices or ongoing MDM communication. It simply updates how the certificate is stored internally within Relution. After the migration, the Self-Service Wizard can be used for all future certificate renewals.

Setting Up or Renewing a Certificate

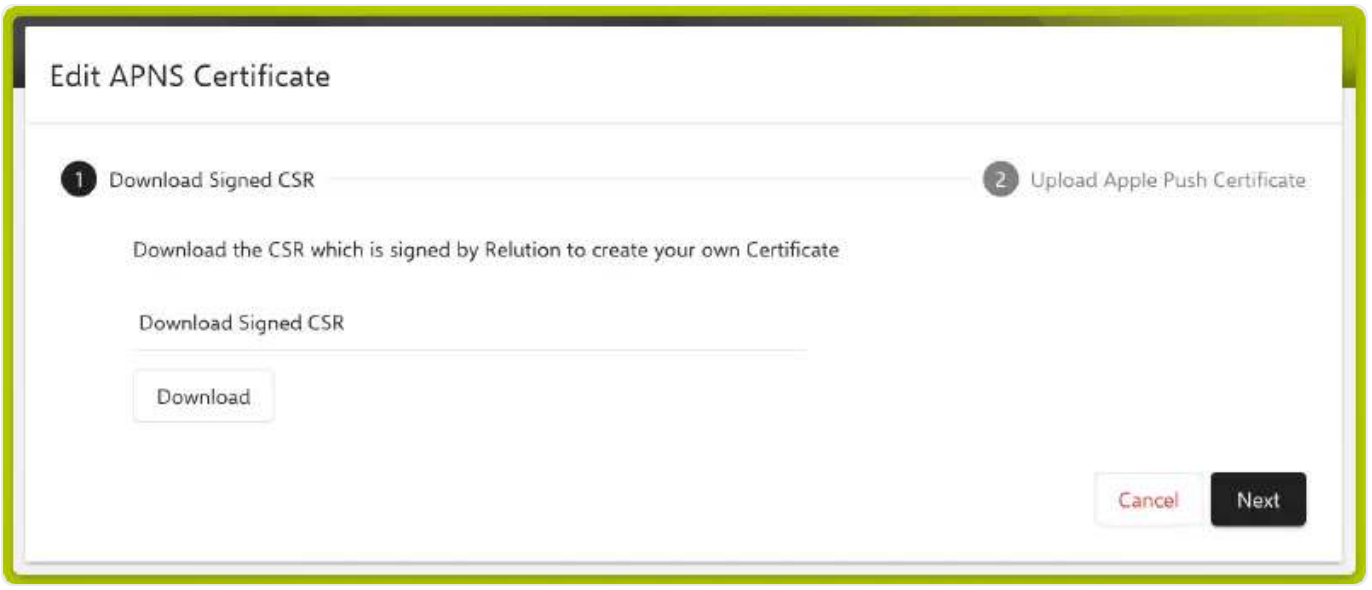
Navigate to `Settings` → `Organization Certificates` and click Start in the APNS section.



This opens the APNS Certificate Wizard.

1. Download Signed CSR

Relution automatically generates and signs a Certificate Signing Request (CSR). Click Download to save it. Wait for the download to complete before clicking Next.



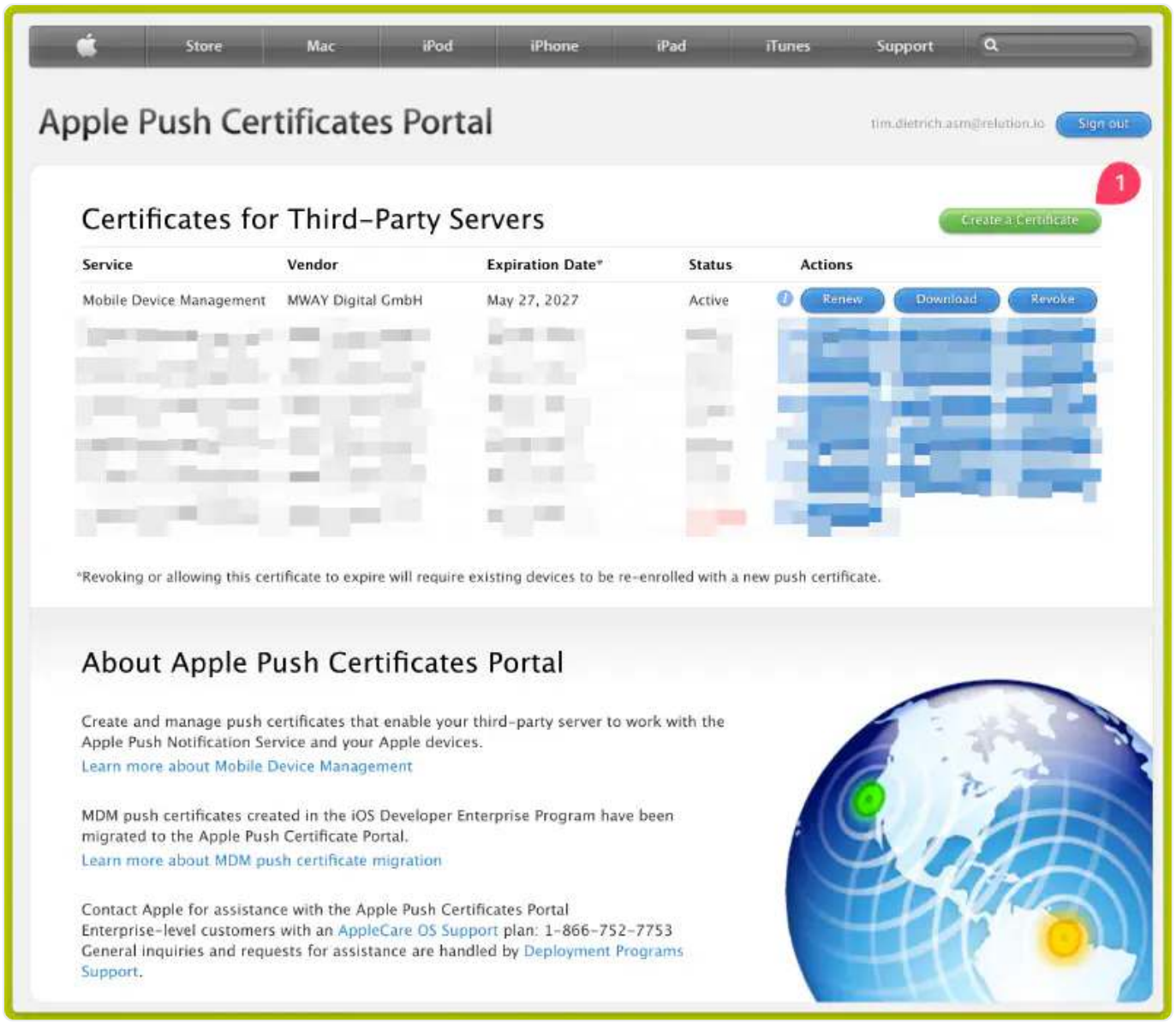
2. Upload Apple Push Certificate

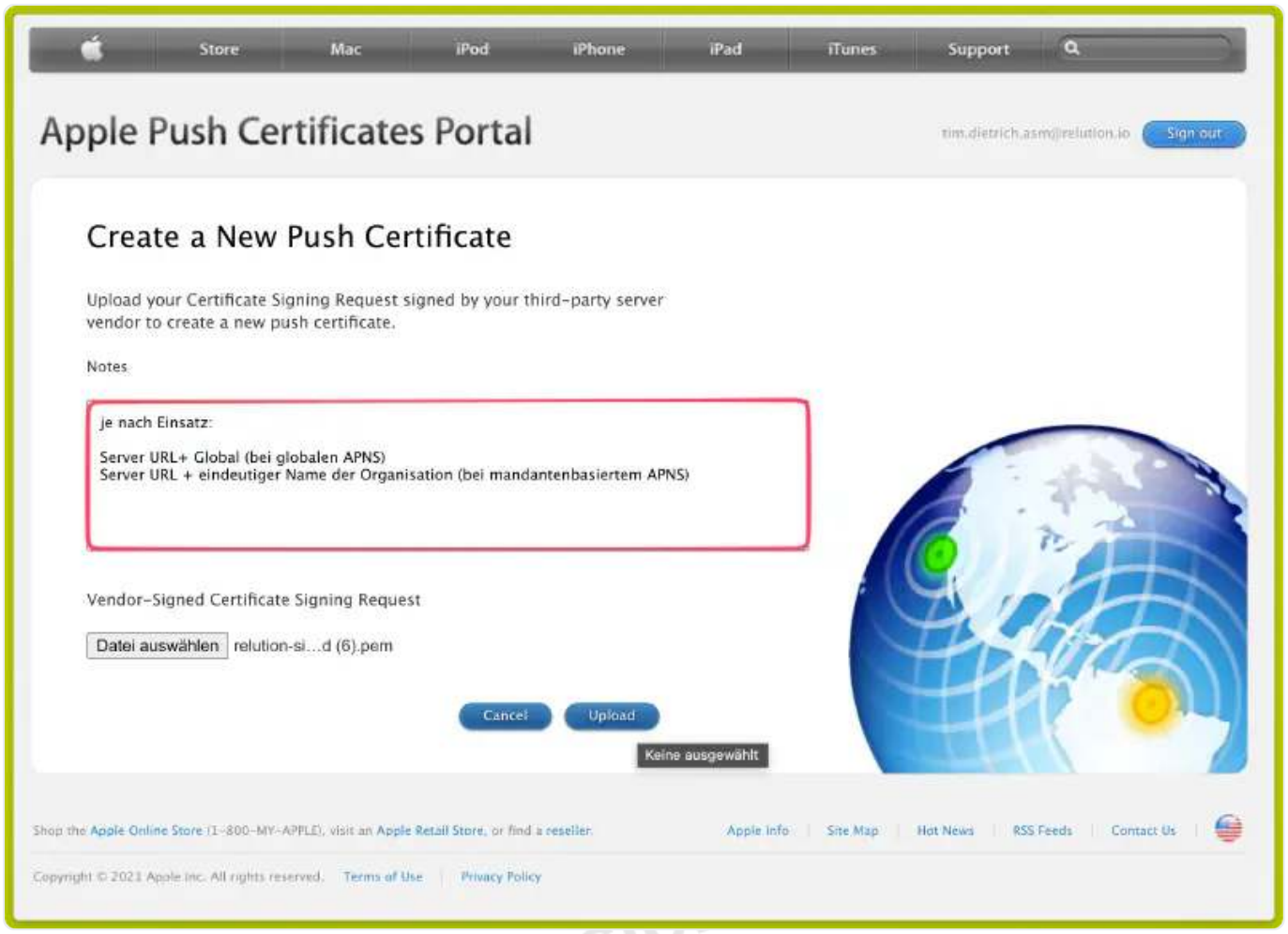
Open the Apple Push Certificates Portal → and sign in with the Apple Account.

- Renewing an existing certificate: Locate the certificate in the list and click Renew. Upload the CSR file from Step 1. This preserves the push topic, so enrolled devices do not need to be re-enrolled.
- New installation: Click Create a Certificate and upload the CSR file.

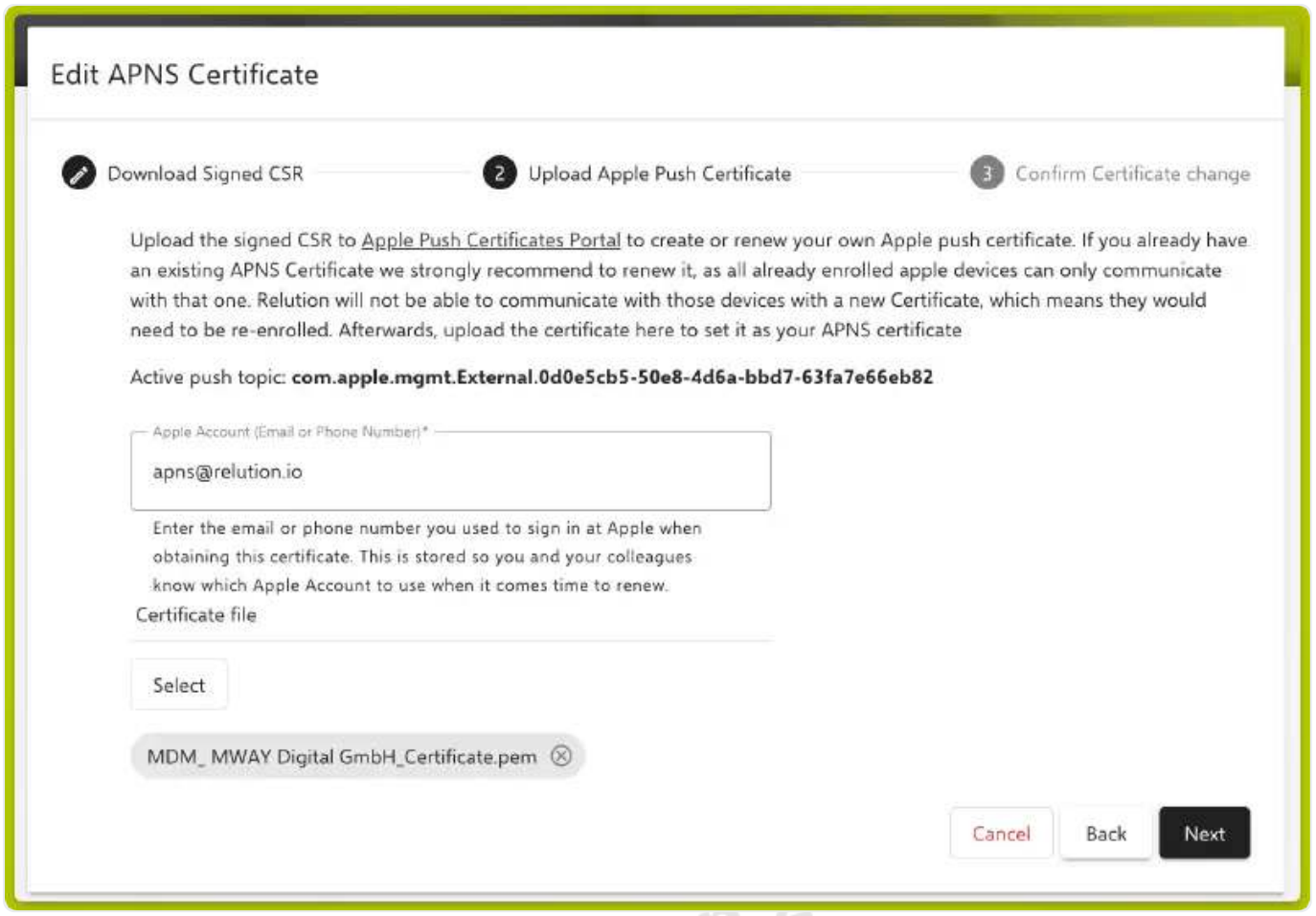
Download the `.pem` certificate file from the Apple portal.

For version 26.4.0


Store
Mac
iPod
iPhone
iPad
iTunes
Support
Apple Push Certificates Portal
tim.dietrich.asm@relution.io
Sign out
1
Certificates for Third-Party Servers
Create a Certificate
Service
Vendor
Expiration Date*
Status
Actions
Mobile Device Management
MWAY Digital GmbH
May 27, 2027
Active
Renew
Download
Revoke
*Revoking or allowing this certificate to expire will require existing devices to be re-enrolled with a new push certificate.
About Apple Push Certificates Portal
Create and manage push certificates that enable your third-party server to work with the Apple Push Notification Service and your Apple devices.
Learn more about Mobile Device Management
MDM push certificates created in the iOS Developer Enterprise Program have been migrated to the Apple Push Certificate Portal.
Learn more about MDM push certificate migration
Contact Apple for assistance with the Apple Push Certificates Portal
Enterprise-level customers with an AppleCare OS Support plan: 1-866-752-7753
General inquiries and requests for assistance are handled by Deployment Programs Support.


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



Enter the Apple Account that generated the certificate into the free-text field.

Upload the certificate into Relution using the file uploader in this step.

The active push topic is displayed above the file uploader. Confirm that the correct certificate is being renewed — the push topic of the uploaded certificate should match the one displayed.

- If the push topic matches, click Save — the wizard is complete.
- If the push topic has changed, the wizard proceeds to Step 3.

3. Confirm Certificate Change (Only in Case of Push Topic Conflict)

This step only appears if the uploaded certificate has a different push topic than the current one. This can happen if a new certificate was created instead of renewing the existing one, or if a different Apple ID was used.

When using the wizard for the first time in an organization that previously used the Relution default certificate, a push topic conflict is expected — the new certificate has a different push topic. A certificate configured on the global organization applies to all organizations; one on a meta-organization applies to all its sub-organizations. Individual organizations can override it with their own certificate. Before confirming, check which organizations inherit this setting and whether any Apple devices are enrolled in that scope.

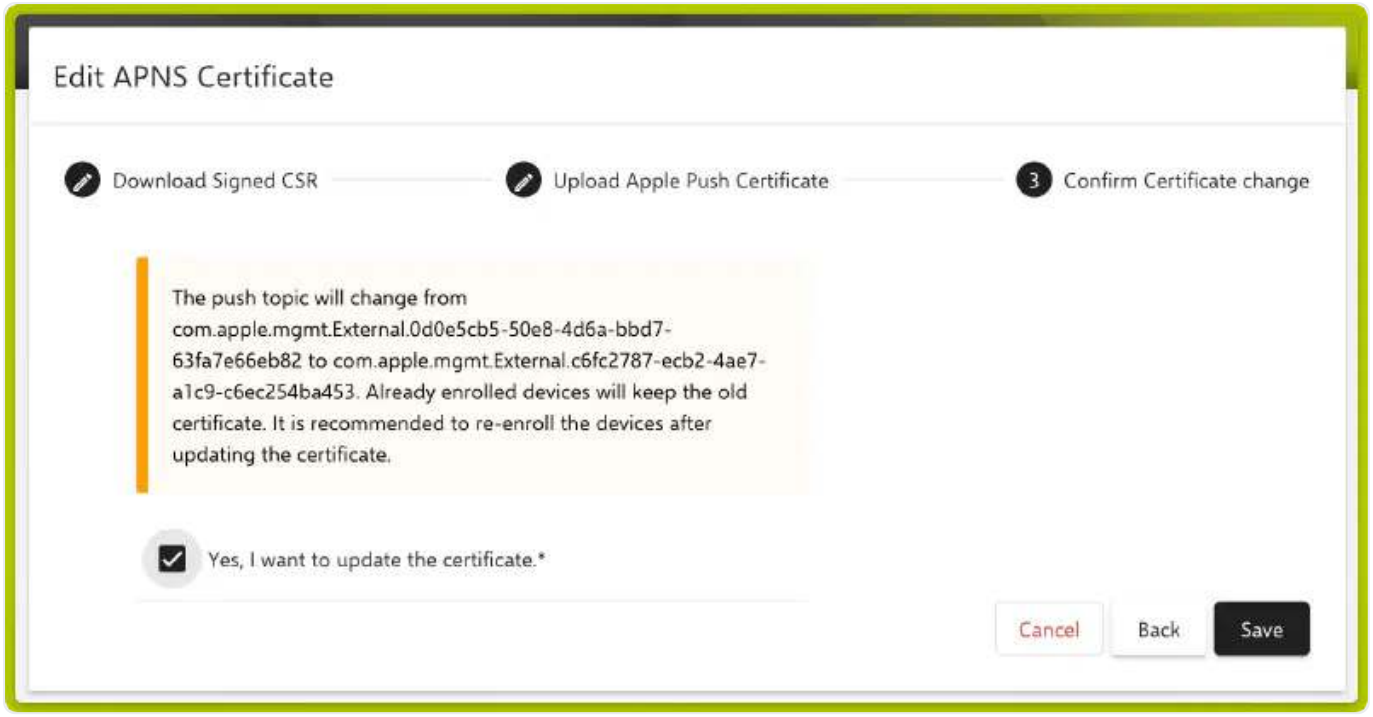
Changing the push topic affects enrolled Apple devices in the affected organization:

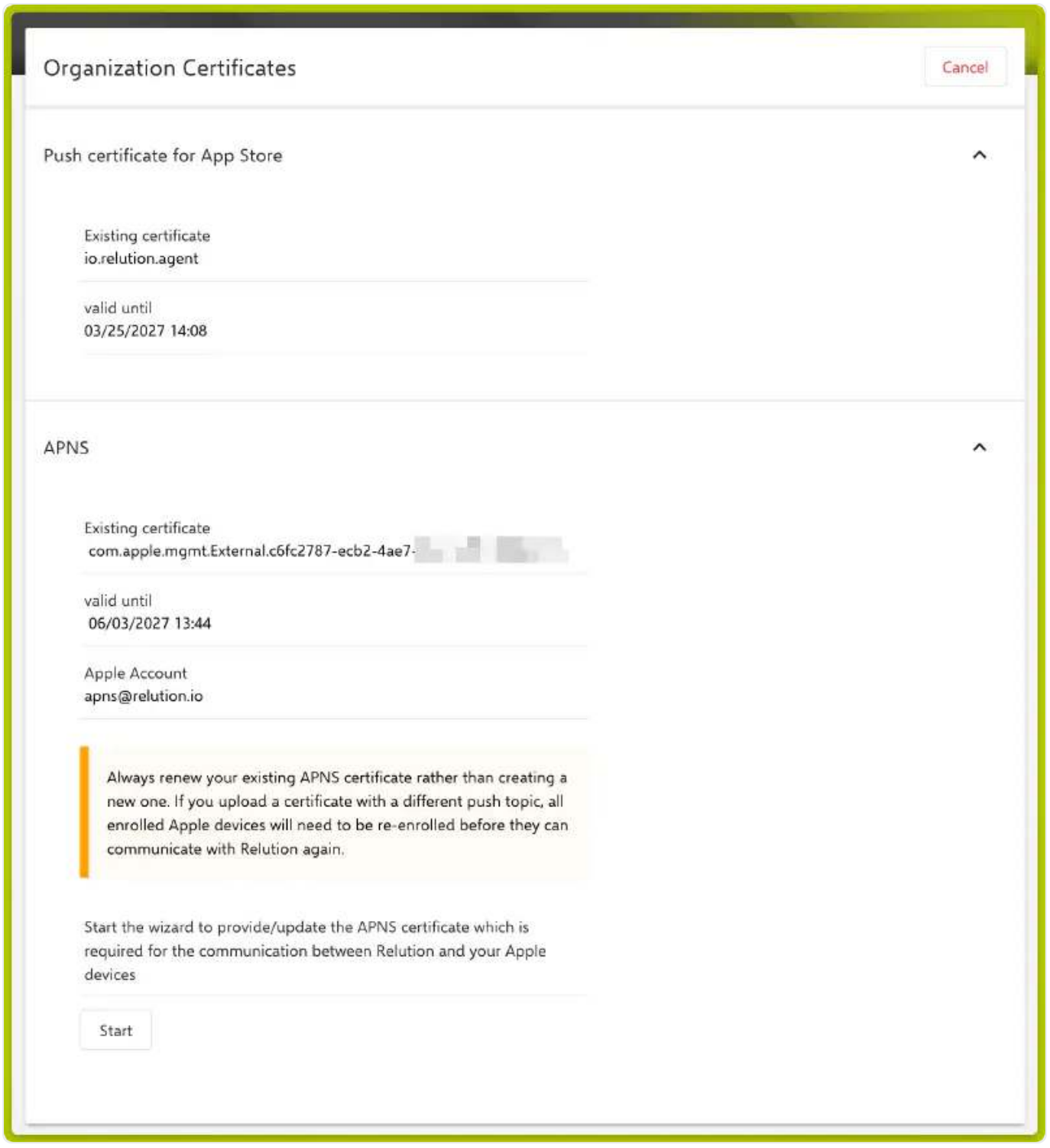
- When transitioning from the Relution-provided certificate to a custom one: Existing devices will keep using the Relution-provided certificate — no immediate re-enrollment is required. Relution plans to retire the shared certificate in the future, but will ensure adequate migration time.
- When replacing the existing certificate with a different one: Enrolled devices will continue using the old certificate until it expires. Once it expires, they will lose MDM communication and must be re-enrolled.

The wizard displays the old and new push topics. To confirm the change:

1. Check the Yes, I want to update the certificate checkbox to confirm.

Click Save to apply the change.





Certificate Expiration and Renewal

The Organization Certificates page displays the expiration date of the active certificate. Relution issues a warning as the expiration date approaches.

Renew the certificate before it expires. If the deadline is missed:

- All enrolled Apple devices instantly lose their MDM connection.
- Devices must be re-enrolled after the renewed certificate is uploaded.

Notes

- Always use the same Apple ID when renewing a certificate. Using a different Apple ID creates a new push topic and requires a full re-enrollment of all devices.
- Always renew the existing certificate instead of creating a new one. Uploading a certificate with a different push topic causes enrolled devices to continue using the old certificate until it expires — after that, they must be re-enrolled.
- If a certificate expires, all enrolled Apple devices lose their MDM connection and must be re-enrolled.

For version 26.4.0

Configure iOS signing certificate

> If a custom signing certificate is not required, Relution provides a valid signing certificate starting from version 5.31.0. The following steps are therefore only necessary if the on-premise server version is below 5.31.0, or when using a custom certificate for this purpose.

When enrolling Apple devices, Relution delivers a signing certificate in the basic configuration that is not trusted and has expired. This is not a functional problem, but can be fixed by changing the configuration. To be found on the end device under `Settings` → `General` → `VPN & Device Management` → `MDM Profile` → `Signing Certificate`

```
SIGNING CERTIFICATE
scep-WIN2008SCEP-CA
Issued by: scep-WIN2008SCEP-CA
Expires: October 28, 2015
```

Adjust configuration

For version 26.4.0

The certificate can be changed. In this case, the following section must be added to the `application.yml`:

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

Relution always expects the files in `/opt/relution`. When specifying the two paths, only the filename of the certificate needs to be given, provided it is stored in `/opt/relution`.

In this example, both the certificate and the corresponding key must be stored under the appropriate path.

Docker environment

If Relution is operated in Docker, the certificates must still be mounted in the corresponding container:

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

The volume application.yml only needs to be added if there is no such file already.

For version 26.4.0

Convert SSL Certificate

PFX certificates are used to store digital identities and encryption in a file format. Their conversion is necessary to ensure compatibility between different systems. Conversion to other formats such as PEM allows the certificates to be used in a wider range of applications.

Conversion to separate PEM files

Extract private key from a PFX file to a PEM file

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

Remove the password from the extracted private key

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

Export the certificate

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

> The intermediate must be included in server.pem, this can be easily checked and corrected on the following page WhatsMyChainCert →

SMG

When using SMG, the complete certificate chain must be exported as `server.pem`.

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

For version 26.4.0

Renew SSL Certificate

An expired SSL certificate of the server affects the management of enrolled devices. Therefore, it is important to update the SSL certificate regularly to ensure smooth operation and control over the devices.

The certificate must be renewed. The procedure differs depending on the operating system and installation.

Docker

For a Docker installation, do the following:

1. check the `docker-compose.yml` to see where the certificate or `key` is stored. Usually these files are named `server.pem` and `server.key`. They are usually located in the same directory
2. look for the following section in the `docker-compose.yml`

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

3. in this example, the files are in the same directory as `docker-compose.yml`
4. replace the `server.pem` file with the new certificate. Alternatively, open the file and replace the contents
5. restart the Docker container. To do this, use the commands `docker compose down` to stop the container first and then `docker compose up -d` to start it again

Native installation Windows with nginx

For a Windows installation, do the following:

1. if the `server.pem` file is not in the `%ProgramFiles%\nginx\conf\` directory, check the `nginx.conf` file to see where the certificate was placed. This file can usually be found at `%ProgramFiles%\nginx\conf\nginx.conf`
2. within this file, look for this section:

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

Replace the `server.pem` file with that of the new certificate, or open the file in an editor (run as administrator) and replace the contents with those of the new certificate. Restart the `nginx` service afterwards.

Native installation CentOS Linux with nginx

For a native Linux installation, proceed as follows

1. check if there is the expired certificate at `/etc/pki/tls/certs/server.pem`
2. if it does, make a copy, open the file, remove the contents, and copy the contents of the new certificate into the `server.pem` file
3. alternatively, rename the existing file and place the new certificate under the name `server.pem` in that path

```
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. after that the service `nginx` has to be restarted. To do this, type `systemctl stop nginx` followed by `systemctl start nginx`

For version 26.4.0

Certbot

It may happen that Certbot has not requested a new certificate for various reasons. This can be done manually by typing `certbot renew` in the console to request a new certificate.

CA certificate in Docker

To connect services using a self-signed or internal TLS certificate, the corresponding root or intermediate CA must be added to the trust store of the Relution container so the connection is treated as trusted. Depending on the Relution version, different methods apply.

Adding certificates via the user interface

New in 26.4

Starting with version 26.4, the Relution Docker image is based on Ubuntu instead of AlmaLinux. As a result, the path `/etc/pki/ca-trust/source/anchors/` no longer exists inside the container, so a copy script relying on that path fails. From Relution 26.4 onward, CA certificates are therefore added through the user interface instead — which also allows the configuration to be adjusted while the system is running.

The required steps are:

- Any existing prerun script (the `RELUTION_PRERUN_SCRIPT` environment variable in `docker-compose.yml`) is removed from the configuration, after which the Relution container is restarted.
- Sign in to the global organization.
- Under `Settings` → `Certificates`, the desired CA certificates are uploaded (see Certificate management →).
- Under `Settings` → `TLS Trust configuration` → `Trusted certificates`, the uploaded CA certificates are selected from the certificate library via Add certificate.

For version 26.4.0

Script-based approach (before Relution 26.4)

Show instructions

CA certificate in Java keystore

It may be necessary to load a certificate into the Java keystore and make it trustworthy. This may be necessary if, for example, a self-signed certificate from an Exchange server is to be used with the Relution Secure Mail Gateway.

Instructions

1. Open the Windows command line with administrative authorization
2. Change to the directory `%JAVA_HOME%\lib\security`
   The path may vary depending on the Java version and provider.
3. Execute this command in the CMD (in the example, the certificate is located under C:\temp\mdeCert.cer):

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

4. If prompted for a password, enter `changeit`. This is the default password of the keystore.
5. If prompted to trust the certificate, enter `yes`. The certificate will be imported and a message with the content: “Certificate has been added to the keystore” should appear.

For version 26.4.0

DB Conversion to UTF8MB4

UTF8MB4 is an extension of the UTF-8 character encoding format. The original UTF-8 format uses a variable number of bytes to represent Unicode characters. However, it only supports the characters of the original Unicode standard, which had a maximum of 65,536 characters.

Converting the DB

Make sure that:

- The `my.cnf` / `my.ini` matches the one specified in the Relution installation guide for the operating system.
- A database exists.
- The database has the correct permissions.

To update:

1. stop the Relution service.
2. run this query on the database.

For 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;
```

This will generate an SQL script that can be used to migrate the database.
3. copy the result of the query and execute it as a new SQL query 4. make sure that the tables have the following modified specifications: - Row Format = Compressed - File Format = Barracuda - Table collation = utf8mb4_general_ci.

Illegal mix of collations

On installations using MariaDB, individual operations fail with database error `1267`. This is often first noticed with Automated Device Enrollment (ADE, DEP in the portal): the device synchronization fails for all organizations, while all other operations continue to work normally. With every synchronization, a message like the following appears in the Relution log:

```
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`
```

The collations shown may differ depending on the installation, e.g. `utf8mb4_uca1400_ai_ci` instead of `utf8mb4_unicode_ci`. The characteristic sign is a table with the prefix `TL_` in the query. The location of the log files is described under Relution Logs →.

Cause

Relution expects the collation `utf8mb4_general_ci` for all text columns. The database tables are created accordingly, and the Relution database connection uses this collation as well.

For bulk operations, such as deleting multiple device enrollments during the ADE synchronization, Relution briefly creates temporary helper tables with the prefix `TL_`. No collation is specified for these tables, so they inherit the default collation of the database. If this default collation differs from `utf8mb4_general_ci`, MariaDB cannot compare the columns of the helper table with the columns of the actual tables and aborts the query. The stored data is not affected.

A differing default collation typically occurs in the following cases:

- The database was created on a MariaDB server whose `collation-server` is not set to `utf8mb4_general_ci`. Newer MariaDB versions use a different default collation unless explicitly configured.
- The database was transferred to a new server or container via a dump. The dump restores the tables with their original collation, but the newly created database itself receives the default of the new server.

Solution

The default collation of the database is aligned with the collation of the Relution tables. This only changes the default for newly created tables; existing tables and data remain unchanged.

> A complete backup of the database is recommended before modifying the database.

For version 26.4.0

Required steps:

1. The Relution service is stopped.
2. A backup of the database is created.
3. The script below is saved as `repair_temp_table_collation_mariadb.sql` and executed against the Relution database.
4. The output of the script is checked (see below).
5. The Relution service is started.

The restart is mandatory. The temporary helper tables exist for the lifetime of a database connection. Otherwise, connections that are already open continue to use the helper table created with the wrong collation.

Script

The script determines the collation of the Relution tables, lists deviating columns and sets the default collation of the database. It can safely be executed multiple times.

repair_temp_table_collation_mariadb.sql

In the following commands, the placeholders in angle brackets are replaced with the values from the `application.yml` or `docker-compose.yml`. The name of the Relution database (`<database>`) is found in the `application.yml` at the end of the database URL, e.g. `relution` in `jdbc:mariadb://localhost/relution?useServerPrepStmts=true`.

Docker

The commands are executed in the `/opt/relution/` directory, where the script is also stored.

For version 26.4.0

```
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
```

The password is specified directly after `-p` here, because the script is passed via standard input and an interactive password prompt is not possible in that case.

> To prevent the password from being stored in plain text in the shell history, the command can be prefixed with a space, or the history can be cleaned up afterwards.

Native

On 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
```

Alternatively, the script can also be executed against the Relution database using a management tool such as `HeidiSQL` or `DBeaver`.

Check the output

The last output of the script shows the new default collation of the database. It then matches the collation of the Relution tables, usually `utf8mb4_general_ci`.

If the message `ERROR: mdm_auto_enrllmnt.uuid not found - wrong schema?` is displayed instead, the script was not executed against the Relution database, usually because the database name is missing from the call. In this case, nothing was changed.

Section 2 of the script lists all text columns whose collation deviates from the reference. Normally, this list is empty. If it contains entries, tables with the wrong collation have been created since the database was set up, for example by database updates as part of Relution updates. These tables can trigger the same error in other operations. They are fully converted to `utf8mb4_general_ci` following the guide under DB Conversion to UTF8MB4 →.

For version 26.4.0

Prevention

To ensure that newly created databases receive the correct collation right away, the MariaDB server is operated with the following settings in the `[mysqld]` section:

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

As of MariaDB 11.5, the `character-set-collations` line is required. Without it, MariaDB uses the collation `utf8mb4_uca1400_ai_ci` for connections, even if the database and tables are set to `utf8mb4_general_ci`. The option is available as of MariaDB 11.2. Older versions such as MariaDB 10.11 LTS do not recognize it and do not start with this line; there, it is omitted.

The current settings are checked in the MariaDB console. The Relution database is selected first:

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

The values for `collation_server` and `collation_database` are `utf8mb4_general_ci`. Without `USE`, no database is selected (indicated by the prompt `MariaDB [(none)]`), and `collation_database` only shows the server default instead of the setting of the Relution database. If `collation_connection` is set to `utf8mb4_uca1400_ai_ci` on MariaDB 11.5 or later, the `character-set-collations` line is missing from the configuration. The complete configuration is described in the installation guide for Linux →.

For version 26.4.0

DatabaseChangeLogLock

The lock on the changelog table could not be removed. The Relution service is no longer starting or keeps rebooting (Docker). The log shows the following messages:

```
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.... []
```

The last message repeats periodically until the service finally terminates with a `timeout` and restarts automatically if necessary (Docker).

For version 26.4.0

Causes

At startup, the Relution service first checks if database updates need to be executed. To prevent two nodes from changing the database schema at the same time in cluster mode, a lock is always set in the `DATABASECHANGELOGLOCK` table for this purpose. This is released again after the check and/or the updates are completed.

If the Relution service is terminated in this state, this lock remains in place. The next time Relution is started, it waits for the lock to be released because the service assumes that another node is updating the database. If this is not the case after about 5 minutes, the service terminates with an appropriate error message.

This condition usually occurs when Relution terminates early during the execution of major database updates, as the startup process takes an unusually long time.

Native

To fix the issue, either remove the (only) entry from the `DATABASECHANGELOGLOCK` table or change the value of the `LOCKED` column from `1` to `0`. Depending on the database, `1` may also be displayed as `True` and should then be changed to `False`.

To update the database, the database's management tool or a free alternative (`BeeKeeper`, `DBeaver`, `HeidiSQL`, …) can be used. Depending on the database, the update may also be possible via the corresponding command-line tools. For example, in `DBeaver`:

```
TRUNCATE TABLE DATABASECHANGELOGLOCK;
```

The placeholders in angle brackets should be replaced with the values from the `application.yml` or `docker-compose.yml`.

Docker

For a Docker setup, the command to unlock the table can be executed from the server in the `/opt/relution/` directory as follows:

Long example

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

For version

Long example filled in:

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

Short example

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

Short example filled in

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

To avoid storing the password in plain text in the Bash history, the `-p` or `--password` option can be omitted when running the command without entering the password. This way, the database password will be requested interactively after submitting the command.

For version 26.4.0

Migrate MariaDB to PostgreSQL

This guide describes the process of migrating the database for a Relution instance within a Docker environment.

Prerequisites

Before starting the migration, ensure the following conditions are met:

- Disk Space: At least as much free space as the current MariaDB database size (1:1 ratio).
- S3 Storage: MinIO (or a compatible S3 storage) must be configured.
  Documentation to S3/SeaweedFS →
- Version: The Relution instance should be updated to version 26.0.0, but at least to version 5.31.0.

Data Backup (Optional)

If no virtual machine snapshots or external backups are available, perform a manual export and file backup.

Export MariaDB to a SQL file:

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

Backup configuration files:

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

Update Relution

Ensure the latest version is running:

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

Stop Services

Stop the Relution container to ensure data consistency during preparation:

```
docker compose down relution
```

Modify Docker Configuration

Update the `docker-compose.yml`. Add the services for `pgloader` and the new `database` (PostgreSQL), and adjust the `relution` block.

Add New Services

```
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
```

Adjust Existing Relution Block

Change the dependencies and add the migration argument:

```
  relution:
    image: relution/relution:latest
    restart: on-failure # Changed from always to on-failure
    container_name: docker_relution
    networks:
      relution-network:
        aliases:
          - relution-docker
    depends_on:
      - database # Changed from mariadb
    links:
      - database # Changed from mariadb
    environment: # replace old list notation (e.g. "- TZ=Europe/Berlin") if present,
don't mix it with the mapping notation
      TZ: "Europe/Berlin"
      RELUTION_ARGUMENTS: "--database-migration-only" # Newly added

volumes:
  mariadb:
  postgresql: # Newly added
```

For ver

pgloader Configuration

1. Download the file pgloader.load → into the directory `/opt/relution/`
2. Adapt the configuration to match the environment.

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

Initialize Database Schema

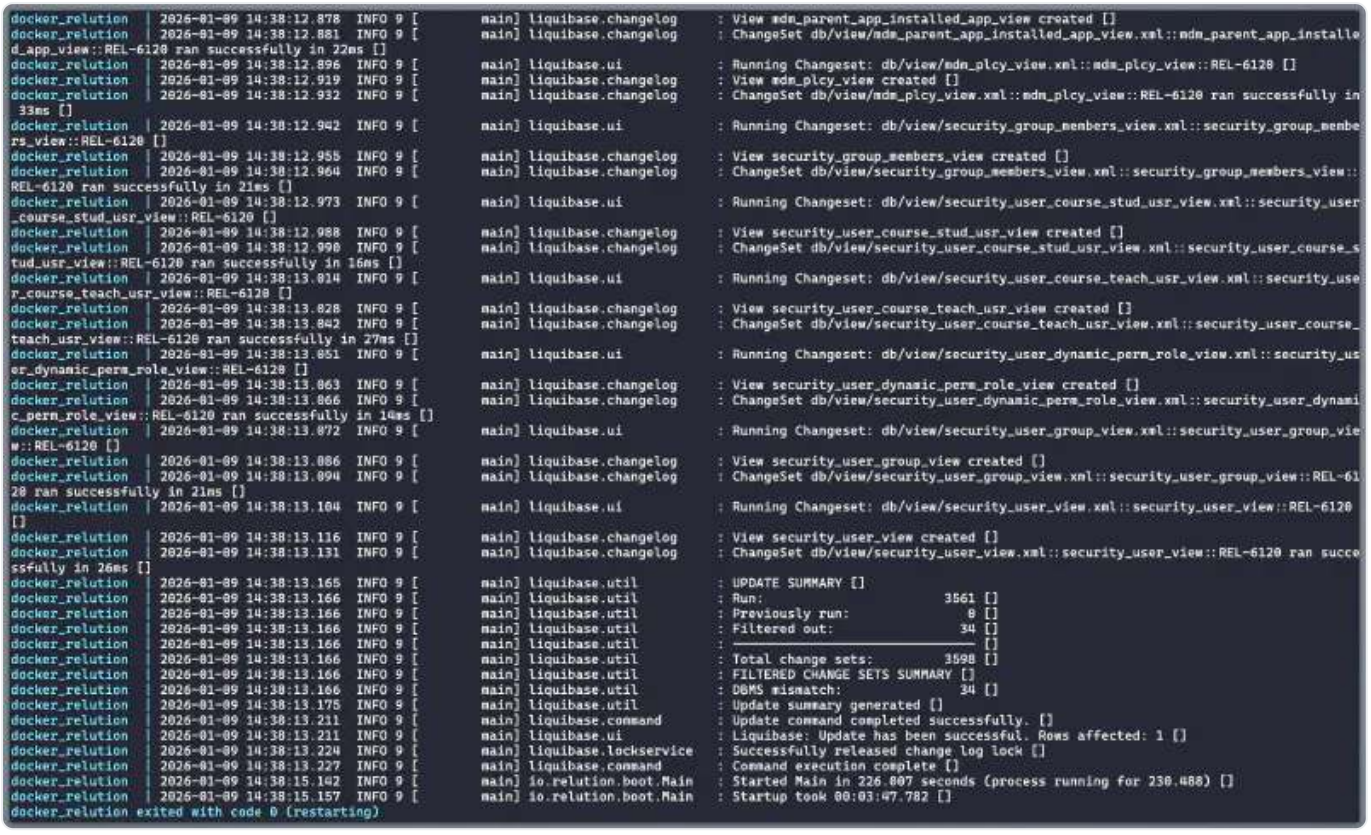
First, adjust the `application.yml` so that Relution recognizes the shift to PostgreSQL:

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

Now start PostgreSQL and Relution. Due to the `--database-migration-only` flag, Relution will only create the schema in PostgreSQL and then terminate.

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

The process is complete when the container exits with code 0: `docker_relution exited with code 0`



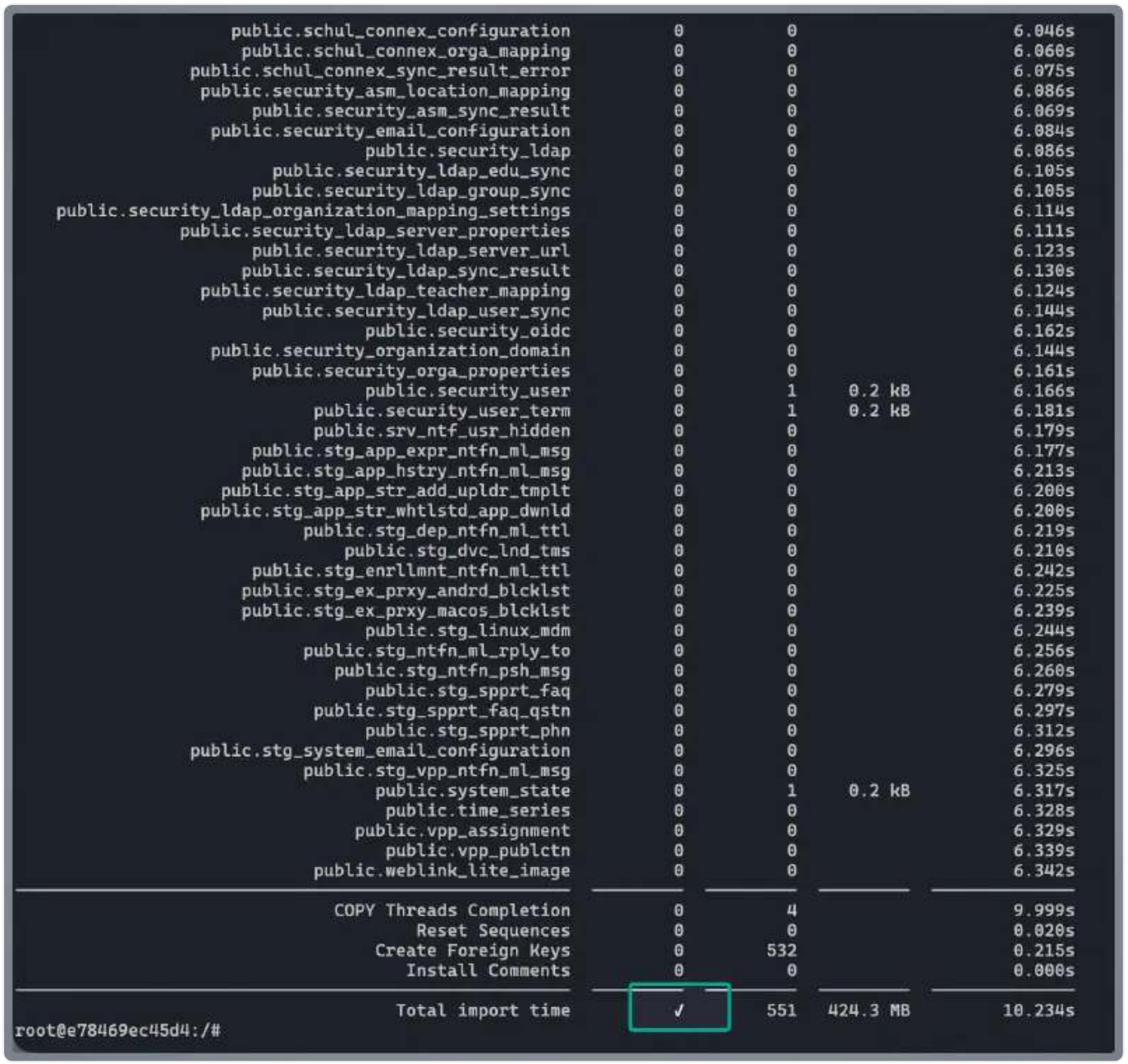
Execute Data Migration

Start the pgloader container and migrate the data from MariaDB to PostgreSQL:

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

Inside the container, run the migration command:

```
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:/#
```

Cleanup and Completion

After a successful migration, the temporary configurations and the old MariaDB container must be removed.

1. Remove from `docker-compose.yml`:
    - The entire `mariadb:` block under `services`.
    - The `pgloader:` block under `services`.
    - The `mariadb:` volume under `volumes`.
2. Adjust the `relution` block:
    - Change back from `restart: unless-stopped` to `restart: always`.
    - Remove the line: `- RELUTION_ARGUMENTS=--database-migration-only`.
3. Delete migration file:

```
rm pgloader.load
```

Restart Services: Shut down everything to remove orphaned containers and restart the system:

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

The migration is now complete, and Relution is running natively on PostgreSQL.

Migrate MSSQL to MariaDB

With Relution 5.25 the support for Microsoft SQL Server will finally be discontinued. The following instructions (valid from Relution version 5.24.2/ 5.25.0) describe how to migrate using the HeidiSQL GUI. If support is needed, please contact the Relution Helpdesk Team.

For version 26.4.0

Migration

1. shut down Relution
   1.1 Create new database and configure my.cnf cnf template →
   1.2 Create new database with HeidiSQL

2. connect old and new database in HeidiSQL

3. create schema in the new database

4. In the application.yml update the following values
   4.1 Change `database type` to `mariadb`
   4.2 Customize JDBC connection string

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

   4.3 Update DB username and password

5. Start Relution against the new DB with foreground.bat with + parameter

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

6. Exit Relution

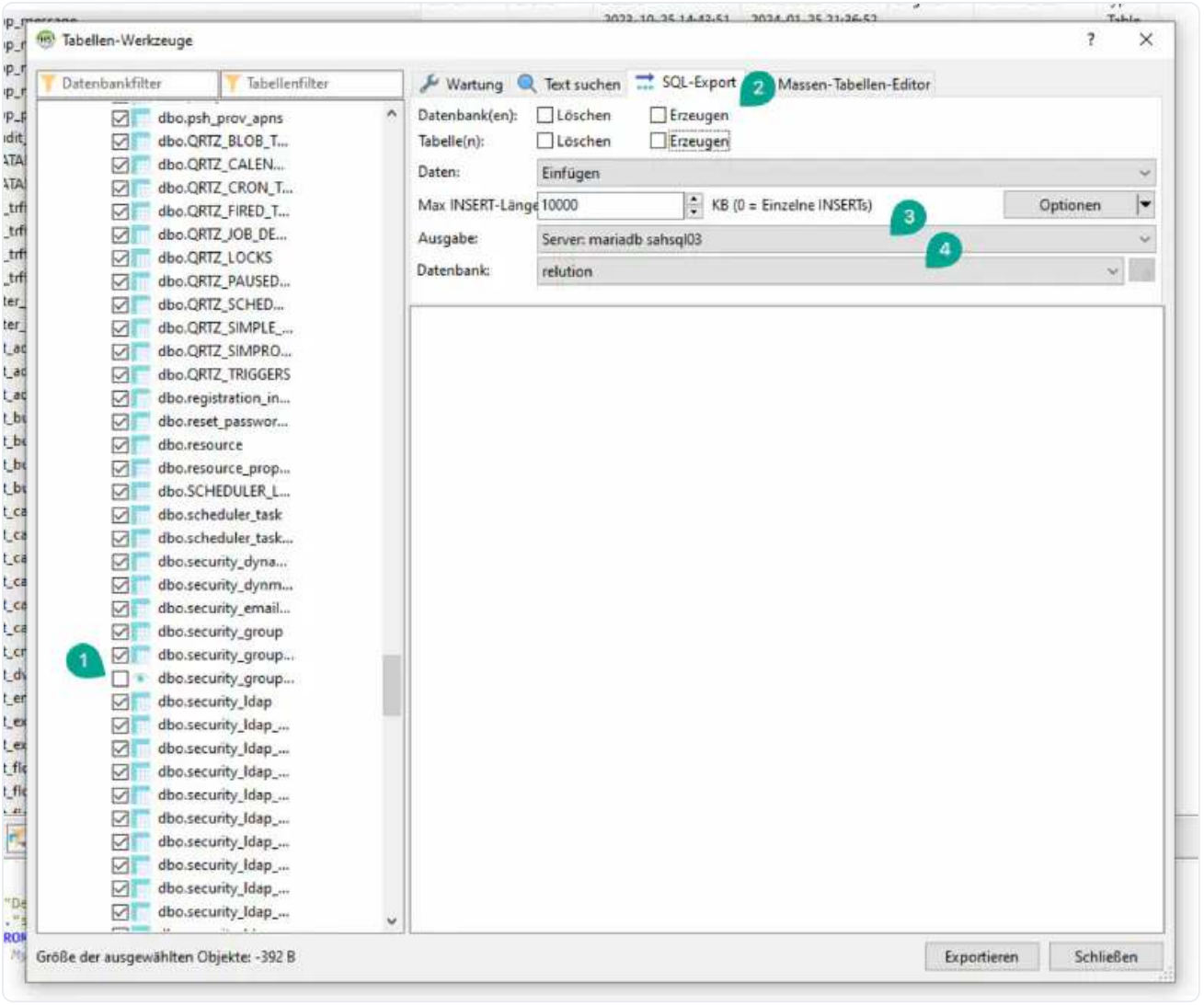
7. right-click on the old database

8. database export

9. databasechangelog + DatabaseChangeLockLock Table + deselect all views + JGROUPSPing

10. max INSERT length to 10k

11. deselect all databases and tables



12. output: New database Server
13. database: New database
14. start migration

After the migration

1. start Relution
2. check Relution log if the start works correctly
3. log in to Relution and check whether resources can be loaded
4. open Device Inventory (check whether the database views open)

Migration from Windows to Docker

This guide walks step by step through migrating an existing Relution installation on a Windows Server to a modern Docker-based installation on a Linux server.

> Please read each section in full before running any command.

What happens during this migration?

The current Relution installation runs on a Windows Server with a MariaDB database. The new setup runs on a Linux server in so-called “containers” (Docker). The difference that makes this migration necessary: Windows does not distinguish between uppercase and lowercase in file names and table names. Linux, on the other hand, does. That is why certain table names in the database must be converted to uppercase after the move – there is a ready-made script for this at the end.

The migration runs through these phases:

1. Create a backup (dump) of the database on the Windows Server
2. Prepare the new Linux server with Docker
3. Import the backup into the new database
4. Rename table names to uppercase
5. Start Relution and verify

For version 26.4.0

Prerequisites before starting

Make sure the following is available:

- Access to the Windows Server (directly on site or via Remote Desktop / RDP)
- The name of the Relution database – if unknown, ask the administrator or look it up in the existing Relution configuration file. Often the name is simply `relution`.
- The password of the MariaDB database user (usually `root` or a dedicated Relution user)
- A Linux server (Ubuntu 22.04 or 24.04 recommended) on which Docker and Docker Compose are already installed
- Access to the Linux server via SSH (a terminal program such as PuTTY on Windows or the built-in terminal on macOS/Linux)
- A file transfer program such as WinSCP → (free) to copy files from the Windows Server to the Linux server

Phase 1 – Create a backup on the Windows Server

In this step we create a complete backup copy of the Relution database as an SQL file. This file contains all the data and will be imported into the new environment later.

1.1 Open the Command Prompt as Administrator

1. On the Windows Server, press the key combination Windows key + R
2. Type `cmd` and press Ctrl + Shift + Enter (not just Enter) – this opens the Command Prompt with administrator privileges
3. Confirm the security prompt with Yes

1.2 Create the target folder for the backup

Enter the following command and press Enter:

```
mkdir C:\backup
```

This command creates the folder `C:\backup`, in which we store the backup file. If the folder already exists, a harmless message appears – just continue.

1.3 Find the database path

`mysqldump` is the program that creates the backup. It is located in the MariaDB installation directory. Check which path is correct on the system:

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

A folder named `MariaDB 10.6` or `MariaDB 10.11` should then be visible. Make a note of the exact version number – it is needed in the next step.

1.4 Create the database dump

In the following command, replace `10.11` with the actual MariaDB version number and `relution` with the name of the database, if it differs:

```
"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
```

After pressing Enter, a prompt for the database password appears. Enter it (the input is invisible – this is normal) and press Enter.

If no error appears and the normal input prompt reappears, the export was successful.

Brief explanation of the options used:

Option	Meaning
`-u root`	Log in as database user `root`
`-p`	Password is prompted interactively
`--single-transaction`	Backup without locking the database (ongoing operation remains possible)
`--routines`	Stored procedures are backed up as well
`--triggers`	Triggers are backed up as well
`--default-character-set=utf8mb4`	Character set for special characters and emojis

1.5 Verify the backup

Check whether the file was created correctly:

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

The file should appear with a size (typically several MB). If the file is 0 bytes, something went wrong – in that case run the command from 1.4 again and watch for error messages.

1.6 Transfer the backup file to the Linux server

Open WinSCP, connect to the Linux server (enter IP address, username and password) and copy the file:

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

If the folder `/opt/relution/` does not yet exist on the Linux server, create it first (see Phase 2, step 2.1).

Phase 2 – Prepare the Linux server

All of the following commands are run on the Linux server in an SSH terminal.

2.1 Create the working directory

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

The command `mkdir -p` creates the folder and all parent folders if they do not yet exist. With `cd` we switch into this folder.

2.2 Create the Docker Compose file

Docker Compose is a method for starting and managing several related programs (here: database + Relution) together. The configuration is stored in a file named `docker-compose.yml`.

Create the file:

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

The command `nano` opens a simple text editor directly in the terminal. Copy the following content into it in full:

For version 26.4.

Show full configuration example

Replace the three placeholders with secure passwords of choice:

- `HIER_ROOT_PASSWORT_EINSETZEN` → e.g. `Tr0mmelFeuer!92`
- `HIER_RELUTION_PASSWORT_EINSETZEN` → e.g. `Rel@ution#2024` (both occurrences must be identical!)

Save and close the file: Ctrl + O (save), then Enter, then Ctrl + X (exit).

2.3 Start only the database

Now we first start only the database container – not Relution itself yet. This is important so that on its first start Relution does not encounter an empty database and begin creating its own (incorrect) tables.

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

The option `-d` stands for “detached” – the container runs in the background and does not block the terminal.

2.4 Wait until the database is ready

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

This command displays the logs (log messages) of the database container in real time. Wait until the following message appears:

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

As soon as this message is visible, press Ctrl + C to stop the display. The database continues running in the background.

Phase 3 – Import the backup

If the dump file has not yet been transferred to the server, do so now (see Phase 1, step 1.6).

For version 26.4.0

3.1 Import the dump into the database

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

> There is no space between `-p` and the password. Replace `HIER_ROOT_PASSWORT_EINSETZEN` with the root password assigned in the `docker-compose.yml`.

A brief explanation of what happens here: `docker exec -i relution-db` means that we run a command inside the running database container. `mariadb ... < file.sql` imports the SQL file into the database.

The import may take a few minutes depending on the amount of data. If no error appears and the normal prompt reappears, the import was successful.

3.2 Verify the import

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

This command lists the first 30 tables of the database. Familiar table names should appear (e.g. `databasechangelog`, `qrtz_triggers`, etc.). If the list is empty or an error message appears, please repeat Phase 3.

Phase 4 — Rename table names to uppercase

As explained at the outset: Linux distinguishes between uppercase and lowercase, Windows does not. On Linux, Relution expects table names in uppercase. This step renames all affected tables.

Since a table cannot be renamed directly from `beispiel` to `BEISPIEL` (Linux sees this as the same name), the renaming runs in two rounds: first to temporary names (with `_tmp`), then to the final uppercase names.

version 26.4.0

4.1 Create the script file

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

Copy the following content into the editor in full:

> Show full configuration example

Save and exit: Ctrl + O, Enter, Ctrl + X.

4.2 Run the script

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

If no error message appears, the renaming was successful.

4.3 Verify the result

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

The output should now show table names in uppercase, for example:

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

Phase 5 – Start Relution

For version 26.4.0

Now that the database is correctly populated and prepared, we start the full stack including Relution:

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

5.1 Monitor the startup

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

Follow the output. On its first start, Relution performs various database checks – this can take 1–3 minutes. The startup was successful when a message like the following appears:

```
Started Relution in XX seconds
```

Exit the log view with Ctrl + C.

5.2 Open Relution in the browser

Open a browser and access Relution:

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

Replace `IP-ADRESSE-DES-SERVERS` with the actual IP address of the Linux server.

Common problems and solutions

“Table doesn’t exist” when running the rename script This means the dump import was not complete. Use `SHOW TABLES;` to check which tables are missing and repeat Phase 3.

Relution does not start / gets stuck in a loop Check the logs: `docker logs relution-app`. The most common causes are an incorrect database password in the `docker-compose.yml` or tables that have not yet been renamed correctly.

The dump file is 0 bytes The export command did not work. Check the path to `mysqldump.exe` and the database password.

Port 8080 is already in use Another program is using port 8080. In the `docker-compose.yml`, change the line `"8080:8080"` to e.g. `"8181:8080"` and then access Relution on port 8181.

WinSCP does not connect Make sure that the SSH service is running on the Linux server (`sudo systemctl status ssh`) and that the firewall allows port 22.

Summary of the most important file paths

File	Path on the Linux server
Docker Compose configuration	`/opt/relution/docker-compose.yml`
Database dump	`/opt/relution/relution_dump.sql`
Rename script	`/opt/relution/rename_tables.sql`

For version 26.4.0

Next steps after a successful migration

Once Relution is running and login succeeds:

- Check whether all devices, users and settings were transferred correctly
- Set up an SSL certificate (HTTPS) if not already present – guide: SSL certificate setup →
- Make sure that regular backups of the Docker volumes are set up
- Only shut down the old Windows Server once the new environment has run stably for several days

Service does not start - Linux

On Linux the Relution service cannot be started and via `systemctl status relution` these errors are output

```
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 can also be started normally via `relution-foreground.sh` and works as usual. The problem may be due to the fact that the `bash` is not the default shell of the operating system.

Adjust the relution service file

For this purpose a small adjustment can be made in the `Relution Services` file and the service should start again afterwards.

In the line `ExecStart` of the file `/etc/system/system/relution.service` `/bin/bash` must be added.
After that, the service can be started again.

```
ExecStart=/bin/bash /opt/relution/bin/relution-foreground.sh
```

Relution Logs

Docker does not write logs by default. Everything that can be read in the logs is contained in the container's `system log`. This is sufficient for most changes. It is recommended to provoke the error to make it visible just before working through the steps.

Find container ID

1. start a terminal and log in if necessary
2. Find out what name and ID the Docker has. Display container ID and name

```
sudo docker ps
```

The terminal should now display the following output

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

The information will be different from the one in the example. The name or the ID of the container can be used to start the log. In the example the name was used

Start log with container name

```
docker logs -f docker_relution
```

The `-f` option ensures that the log is always displayed continuously. Therefore, a lot of text is displayed quickly in the terminal. The log can be stopped with `CTRL + C`, then scroll up.

Save log to file

To save the logs to a file in the current path, use this command

```
docker logs -f docker_relution > my_logfile.txt
```

It is also possible to use an alternate path

```
docker logs -f docker_relution > /opt/relution/my_logfile.txt
```

To transfer the file to a local PC, use `Filezilla`, `WinSCP` or another `SCP client`

Log Rotation

Docker logs are inherently ephemeral. Sometimes it can be useful to retain them for a longer period. Below is an example based on a Rocky Linux 9 + Docker installation.

For version 26.4.0

Configure Log Rotation for Docker Host Logs

Docker stores its standard logs under `/var/lib/docker/containers/<container-id>/<container-id>-json.log`. To keep these logs manageable, Docker's integrated log rotation can be enabled via the `/etc/docker/daemon.json` file:

```
{
  "log-driver": "json-file",
  "log-opts": {
    "max-size": "10m",
    "max-file": "30"
  }
}
```

Afterward, restart the Docker service:

```
sudo systemctl restart docker
```

Rotate, Zip, and Move Logs Daily to the Relution Directory

For daily archiving, `logrotate` can be used. It must be installed on the Linux system afterward via:

```
sudo dnf install logrotate
```

First, a logs folder must be created:

```
sudo mkdir /opt/relution/logs
```

Then, a configuration file must be created under `/etc/logrotate.d/docker` with the following content:

> Replace the two WILDCARD words in the first line with `*`.

For 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
}
```

A log can be immediately created using the following test command:

```
sudo logrotate --force /etc/logrotate.d/docker
```

Subsequently, a log file should be stored in the `/opt/relution/logs` folder:

```
ls -lah /opt/relution/logs
```

Linux

If Relution was installed in the default directory `/opt/relution` logs can be found in `/opt/relution/log` The most recent log file is called relution.log, while archived log files are named `relution.log.<date>.gz` If Relution was installed in a different location, the log directory is found relative to its installation directory

---

Windows

If Relution was installed in the default directory `C:\Program Files\Relution` logs can be found in `C:\Program Files\Relution\log`. The most recent log file is called `relution.log`, while archived log files are named `relution.log.<date>.gz`. If Relution was installed in a different location, the log directory is found relative to its installation directory.

Adjust log level for advanced error analysis

If standard logs are not sufficient for troubleshooting an issue, the log level can be selectively raised to `DEBUG` (e.g. on the fly without a restart via the Web API or the system portal). A detailed guide can be found under Set log level →.

For version 26.4.0

Docker Fails to Start on EL10

The minimal and cloud images of RHEL, AlmaLinux and Rocky Linux 10 (EL10) lack a kernel module package that Docker requires for its network setup — in this case Docker does not start, and the Relution installation cannot continue. This guide describes how to install the missing package before the first Docker start.

> Only EL10 (version 10) is affected. On EL9 this step is not required — the package is already pre-installed there.

Problem

The minimal and cloud images of RHEL, AlmaLinux and Rocky Linux 10 are missing the `kernel-modules-extra` package. Without this package, iptables cannot load the kernel module `xt_addrtype`, which Docker needs for its bridge and NAT setup. The Docker service then fails to start and aborts with the following message:

```
failed to add jump rules to ipv4 NAT table: ... xt_addrtype
```

The output of `systemctl status docker` often shows only the follow-up error `Start request repeated too quickly` — the actual cause appears in `journalctl -xeu docker.service`.

Solution

The following steps are performed before the first start of Docker:

```
# 1. Install the module package matching the RUNNING kernel
sudo dnf install -y "kernel-modules-extra-$(uname -r)"

# 2. Load the modules
sudo modprobe xt_addrtype br_netfilter ip_tables

# 3. Make them persistent – loaded automatically on every boot
echo -e "xt_addrtype\nbr_netfilter\nip_tables" | sudo tee /etc/modules-
load.d/docker.conf

# 4. Start Docker
sudo systemctl reset-failed docker.service
sudo systemctl enable --now docker
```

Why These Two Points Matter

- Installing the versioned package (`kernel-modules-extra-$(uname -r)`): ensures that the modules match the *currently running* kernel. A plain `dnf install kernel-modules-extra` may provide the modules only for a newer, not-yet-booted kernel — in which case `modprobe` fails with `Module xt_addrtype not found` until the system is rebooted. If `dnf` instead reports no matching package for the currently running kernel (e.g. after a prior `dnf update` without a reboot), a reboot onto the most recently installed kernel is required before rerunning the command.
- **`/etc/modules-load.d/docker.conf`**: uses `systemd-modules-load.service` to ensure the modules are loaded automatically on every reboot. Without this file, the fix would be lost again after the next reboot.

Verifying That It Worked

```
sudo modprobe xt_addrtype && echo "OK – module loadable"
sudo systemctl is-active docker
sudo docker run --rm hello-world
```

If `modprobe` returns no error, the service reports `active`, and the test container prints `Hello from Docker!`, the step is complete.

For version 26.4.0

Set log level

In some cases the cause of a problem cannot be identified in the default log level. In this case the log level can be adjusted accordingly and the information output can be increased.

The log level can be set via the `application.yml`, the Web API or the system portal. The Web API takes effect immediately, requires neither a restart nor any additional configuration and is therefore the recommended way on a running instance. As of Relution 26.4, the system portal requires the corresponding actuator endpoint to be enabled once.

> The DEBUG log level should only be used for analysis purposes, as significantly more information is written to the log and the log grows accordingly. Once the analysis is complete, the log level is to be set back to INFO.

Logfile Location

Where to find log files for Docker, Linux, and Windows is described under Relution Logs →.

Activation of the system portal

In the `application.yml` in the Relution directory, add this section:

For version 26.4.0

```yaml
relution:
  spring-boot-admin:
    enabled: true
```

> Be sure to indent each line here (two spaces per level). It is recommended to deactivate the system portal again after finishing the work.

Enabling the actuator endpoints

As of Relution 26.4, only the health endpoint is exposed by default for security reasons. The instance view of the system portal therefore shows the `Details` section only. The `Logger` section appears once the corresponding endpoint has been enabled in the `application.yml` of the Relution server:

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

The list replaces the default configuration entirely. `health` has to remain part of it, as otherwise the health endpoint is dropped along with the status display of the system portal and the health checks of load balancers and cluster nodes.

A restart of the Relution server is required for the change to take effect.

Further sections of the system portal can be added individually following the same pattern:

Section in the 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`

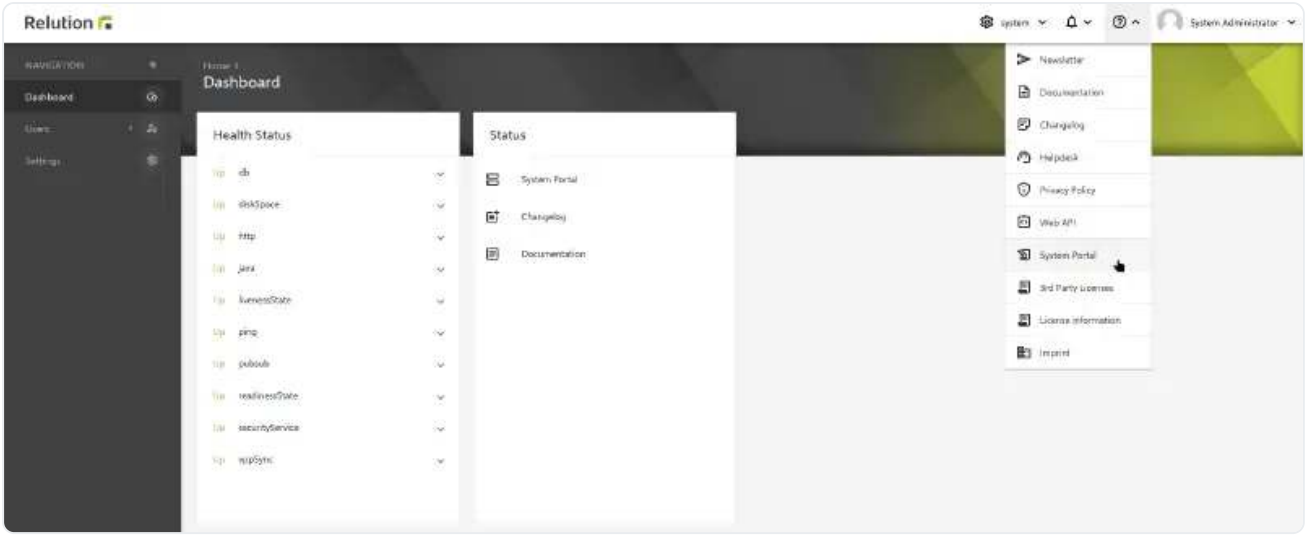
> The actuator endpoints are served on management port 8099 without authentication. This port must not be reachable from untrusted networks. The endpoints env, configprops and heapdump additionally expose configuration values and memory contents including credentials. Any endpoint enabled for an analysis is therefore to be disabled again afterwards.

Activation of the DEBUG Log in the System Portal

This requires an activated system portal as well as an enabled `loggers` endpoint, see the two preceding sections.

For version 26.4.0

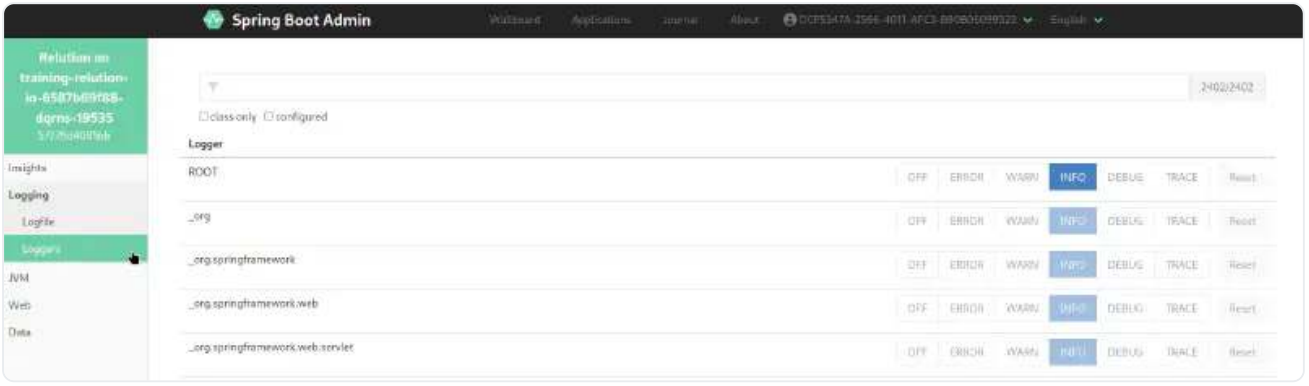
1. log in to Relution as system administrator. The default username is `admin`
2. go to `System Portal` in the system menu.



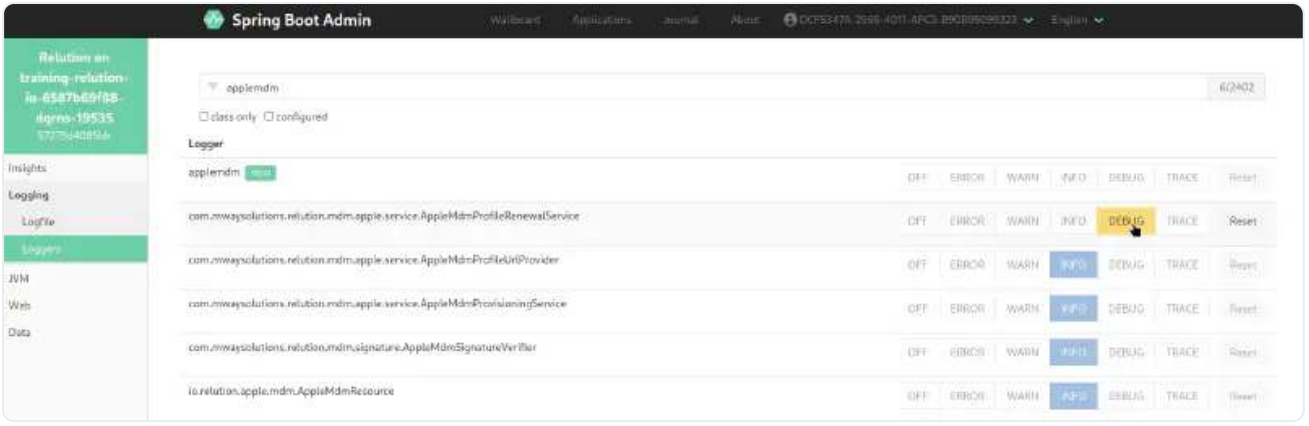
3. then call the associated instance. To do this, click on the box and not directly on the green link.



4. switch to the `Logger` section.



5. use the search to set the corresponding `Logger` to `DEBUG`. `ROOT` activates all `Loggers` and should therefore only be used in exceptional cases, as a lot of content is generated quickly. In the example the `AppleMDMResource` has been activated.



Note that the setting is directly active and no service restart is required. When restarting the Relution service or Docker container, the log will be set back to `INFO`.

Keeping the DEBUG log active beyond a restart

Since the `DEBUG` log is set back to `INFO` after a restart of the instance, it is not possible to log initial errors during the startup process, e.g. in the context of an LDAP connection, in the way described above. For this there is the possibility to define the log in the `application.yml`. This is loaded directly at startup and thus activates the `DEBUG` log.

Insert the following content directly into the first line at position 1.

Set ROOT to DEBUG

> Note that logging at the `ROOT` level may generate a lot of content quickly. This functionality should only be used in absolutely exceptional cases for short analysis activities. Note that there can be significant performance degradation here even with small installations.

It is recommended to activate one or more logs individually and targeted. To do this, simply add the individual `loggers` one below the other in the file:

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

For version 26.4.0

Multiple individual logs

```
logging.level.io.relution.security.ldap: DEBUG
logging.level.io.relution.apple.mdm.AppleMdmResource: DEBUG
```

In the example, LDAP functionality and `AppleMdmResource` would now be enabled in the `DEBUG` log. The names of the `loggers` can be looked up in the system portal as long as the `loggers` endpoint is enabled; otherwise they correspond to the package or class name shown in the log.

Setup Loglevel with a Logging User via the Web API

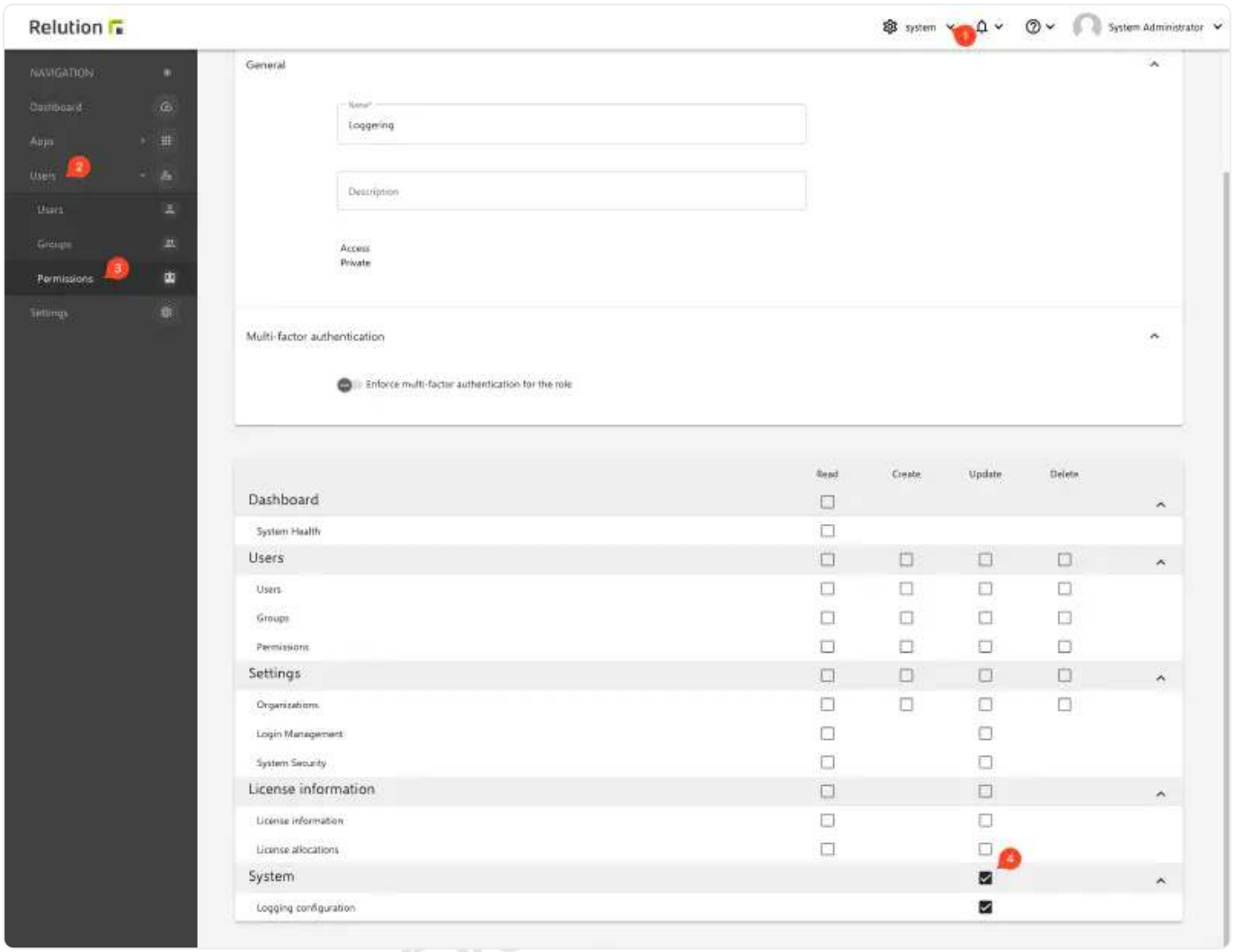
As of Relution 5.18, it is possible to create a special logging user on the system organisation, which can comfortably change the log level via the Web API. This saves the manual editing of the YAML configuration file as well as a restart of the server.

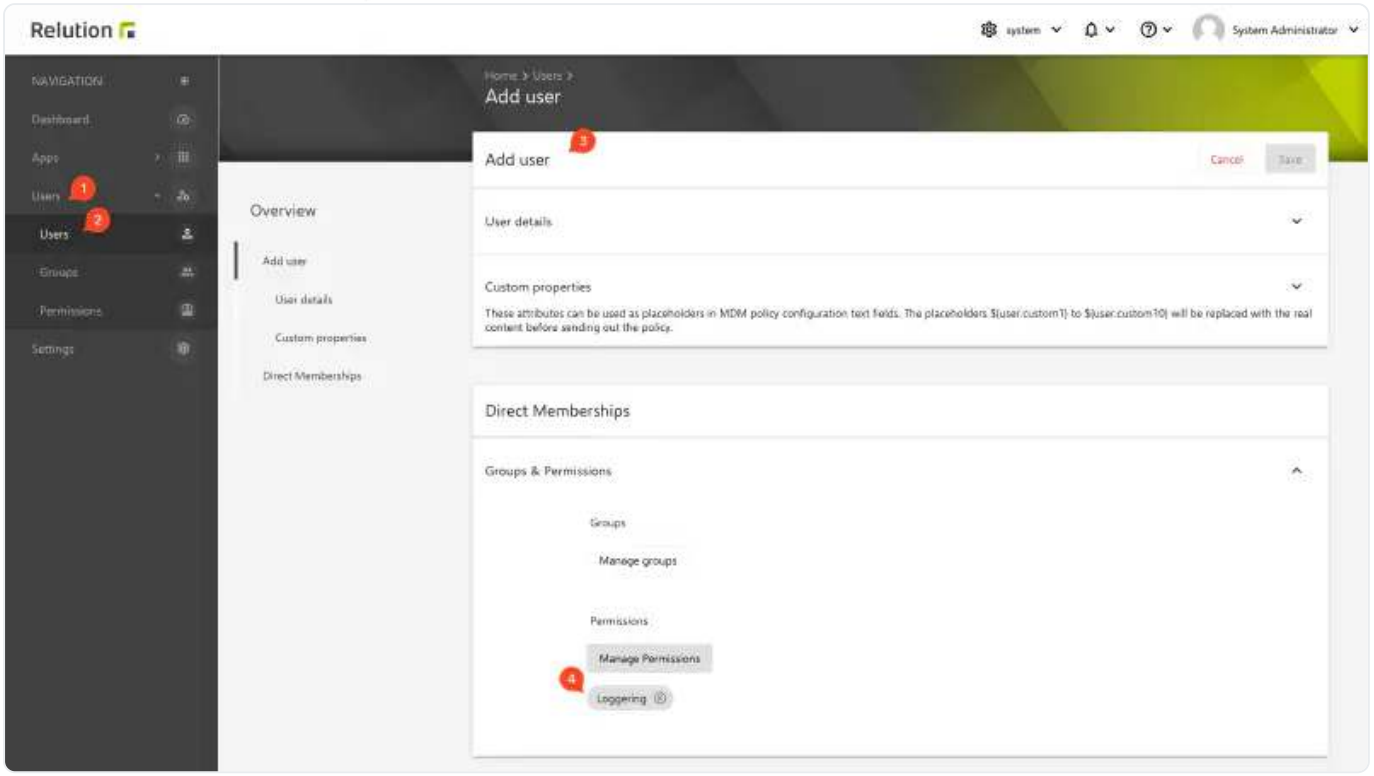
This path requires neither an activated system portal nor any enabled actuator endpoint and is therefore the recommended way to change log levels on a running instance. As in the system portal, the log levels are reset to their initial value when the instance is restarted.

For Version 26.4.0

1. create authorisation and user

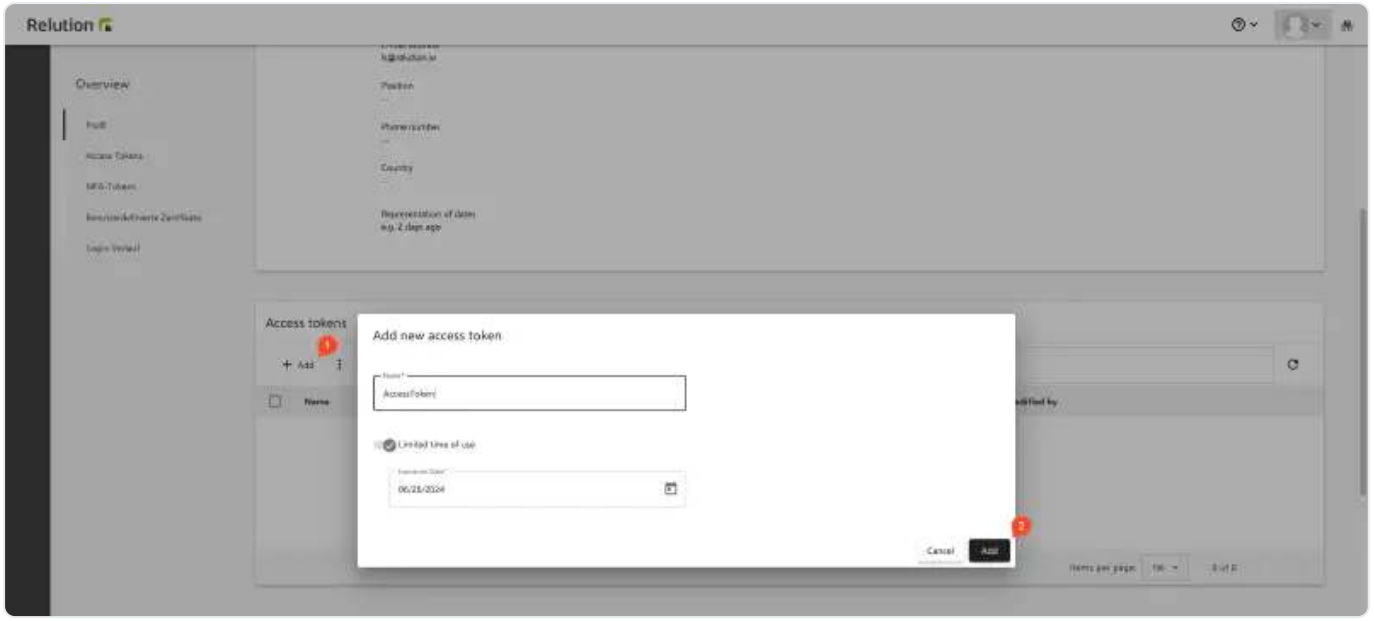
To create the logging user, a new authorisation must first be created on the system organisation, where the option “System > Logging configuration” is activated and saved. Then a new user can be created exclusively for the logging access, to which the previously created authorisation is assigned. Note: The system administrator has this authorisation by default.

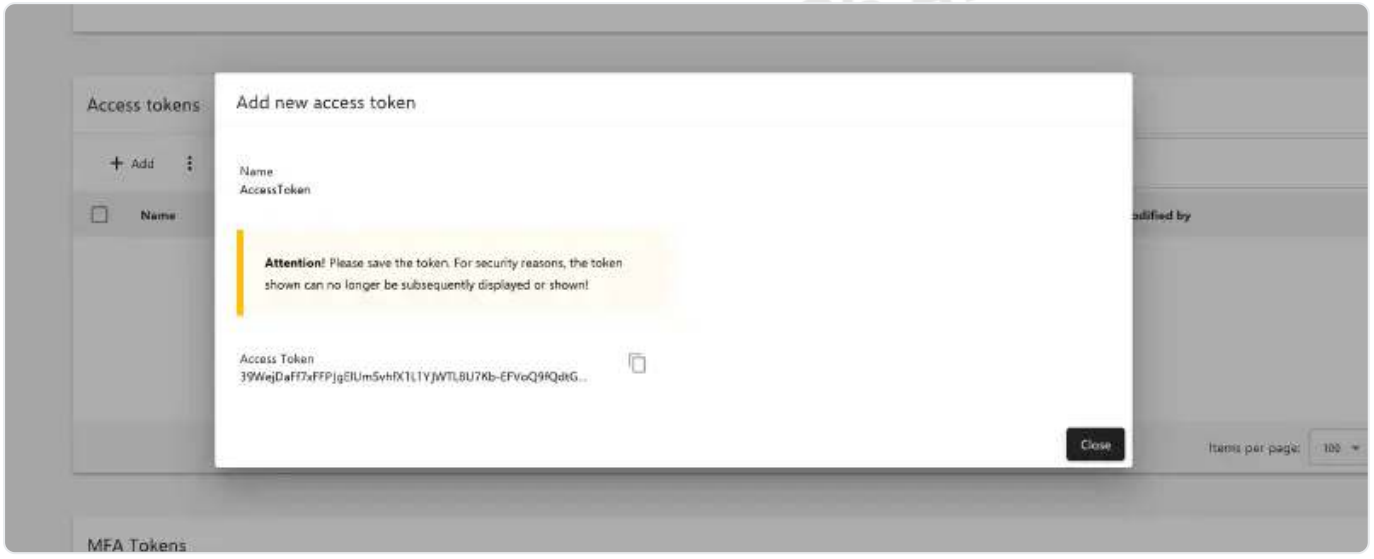

Relution
system
System Administrator
NAVIGATION
Dashboard
Apps
Users
Users
Groups
Permissions
Settings
General
Name*
Loggering
Description
Access
Private
Multi-factor authentication
Enforce multi-factor authentication for the role
Read
Create
Update
Delete
Dashboard
System Health
Users
Users
Groups
Permissions
Settings
Organizations
Login Management
System Security
License information
License information
License allocations
System
Logging configuration


Relution
system
System Administrator
NAVIGATION
Dashboard
Apps
Users
Users
Groups
Permissions
Settings
Home > Users >
Add user
Overview
Add user
User details
Custom properties
Direct Memberships
Add user
Cancel
Save
User details
Custom properties
These attributes can be used as placeholders in MDM policy configuration text fields. The placeholders ${user.custom1} to ${user.custom10} will be replaced with the real content before sending out the policy.
Direct Memberships
Groups & Permissions
Groups
Manage groups
Permissions
Manage Permissions
Loggering

2. create an Access Token

An Access Token can be created for this new user to facilitate handling. To do this, the user must first log in and create the token via the user profile. The Access Token is only displayed once, another token can be created if required.

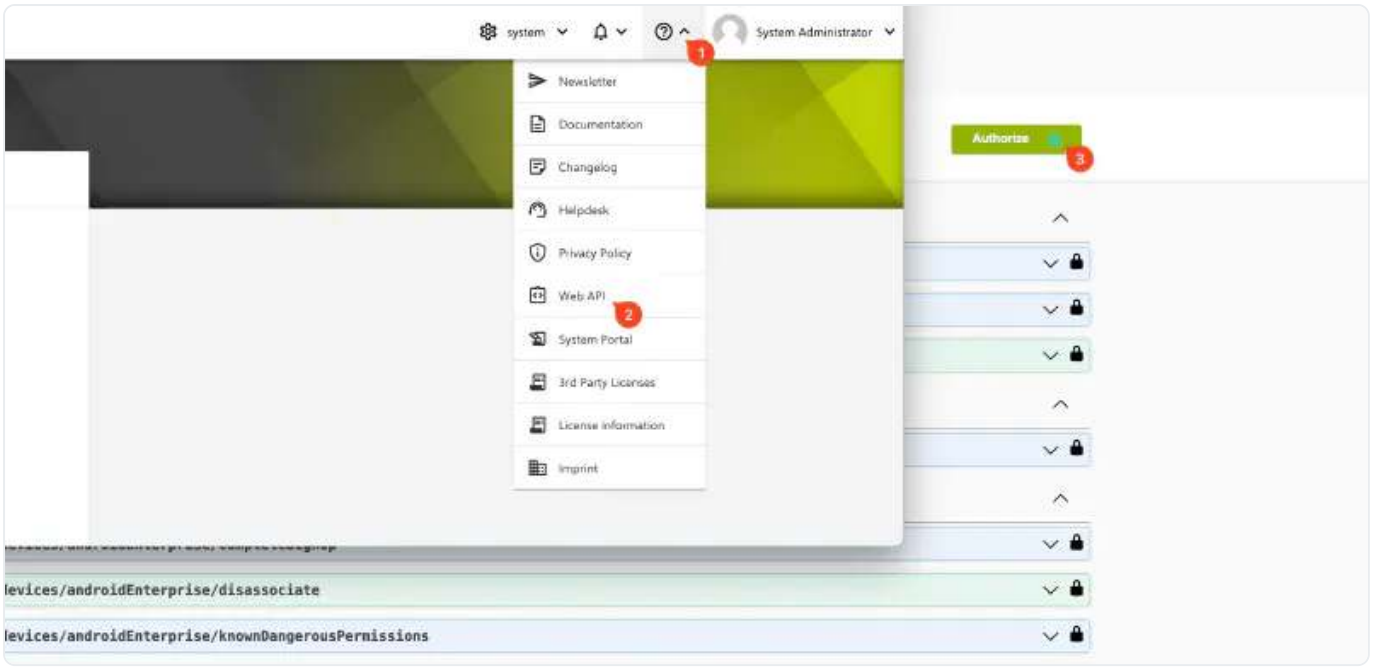


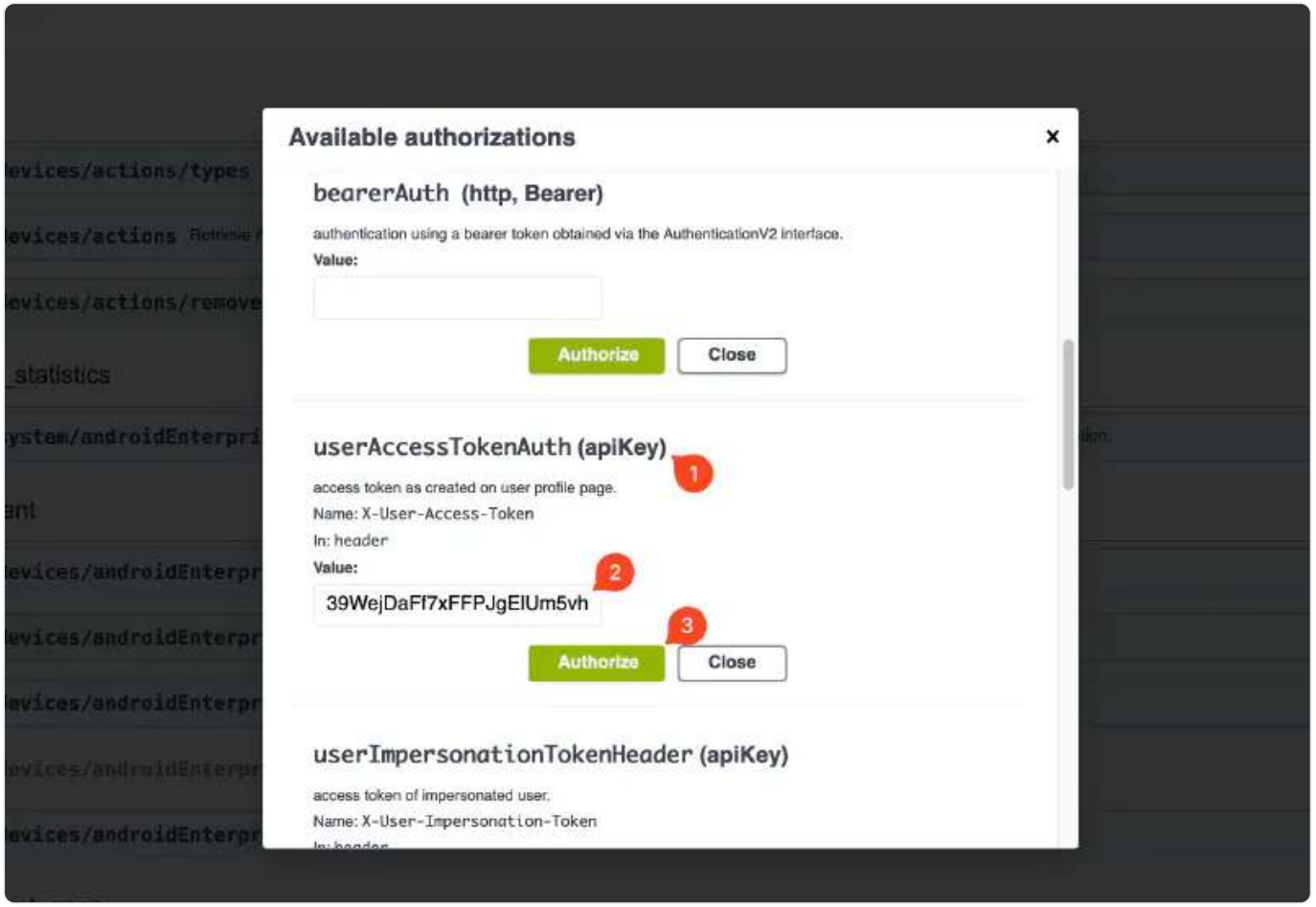


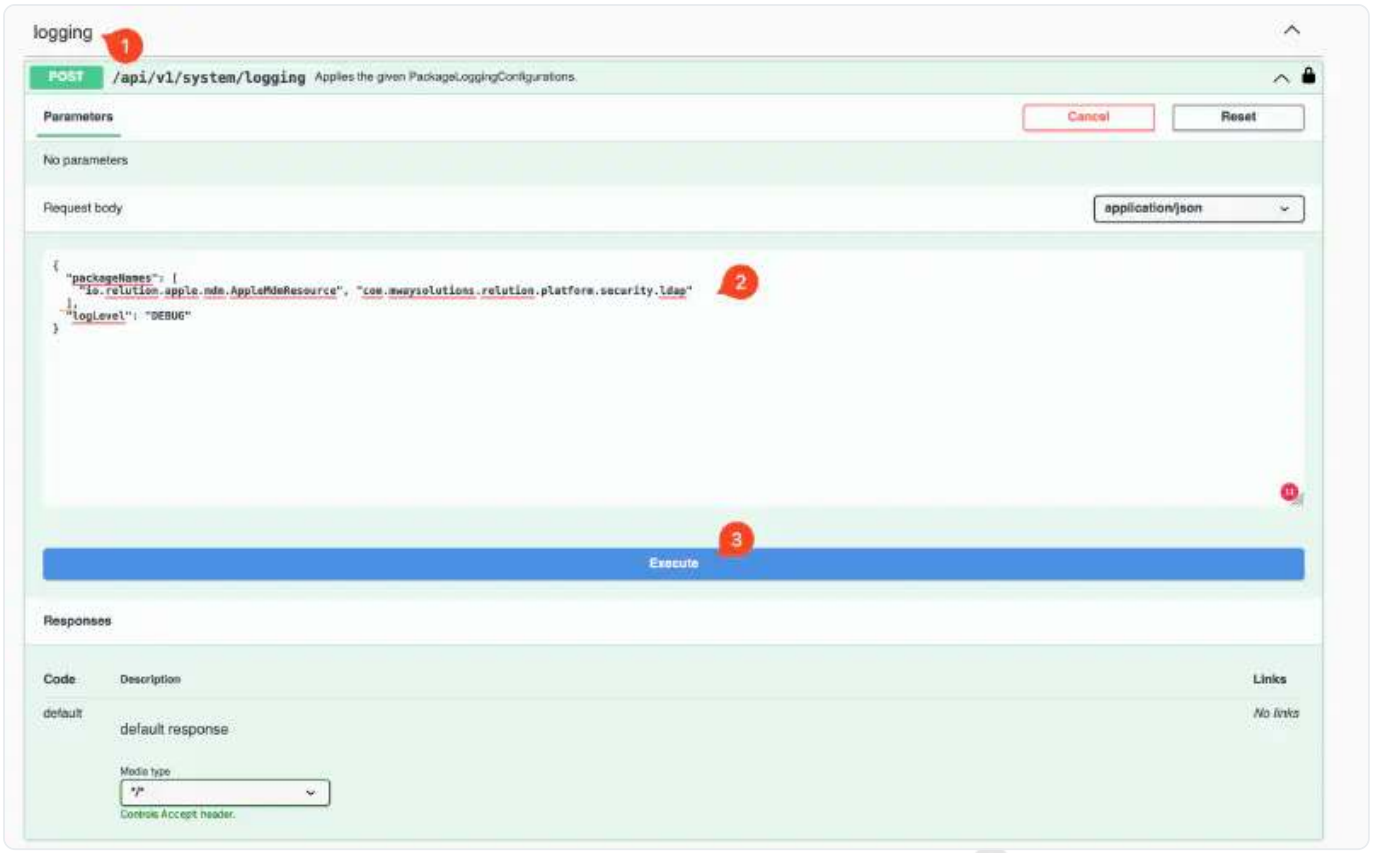
3. controlling the log level via the Web API

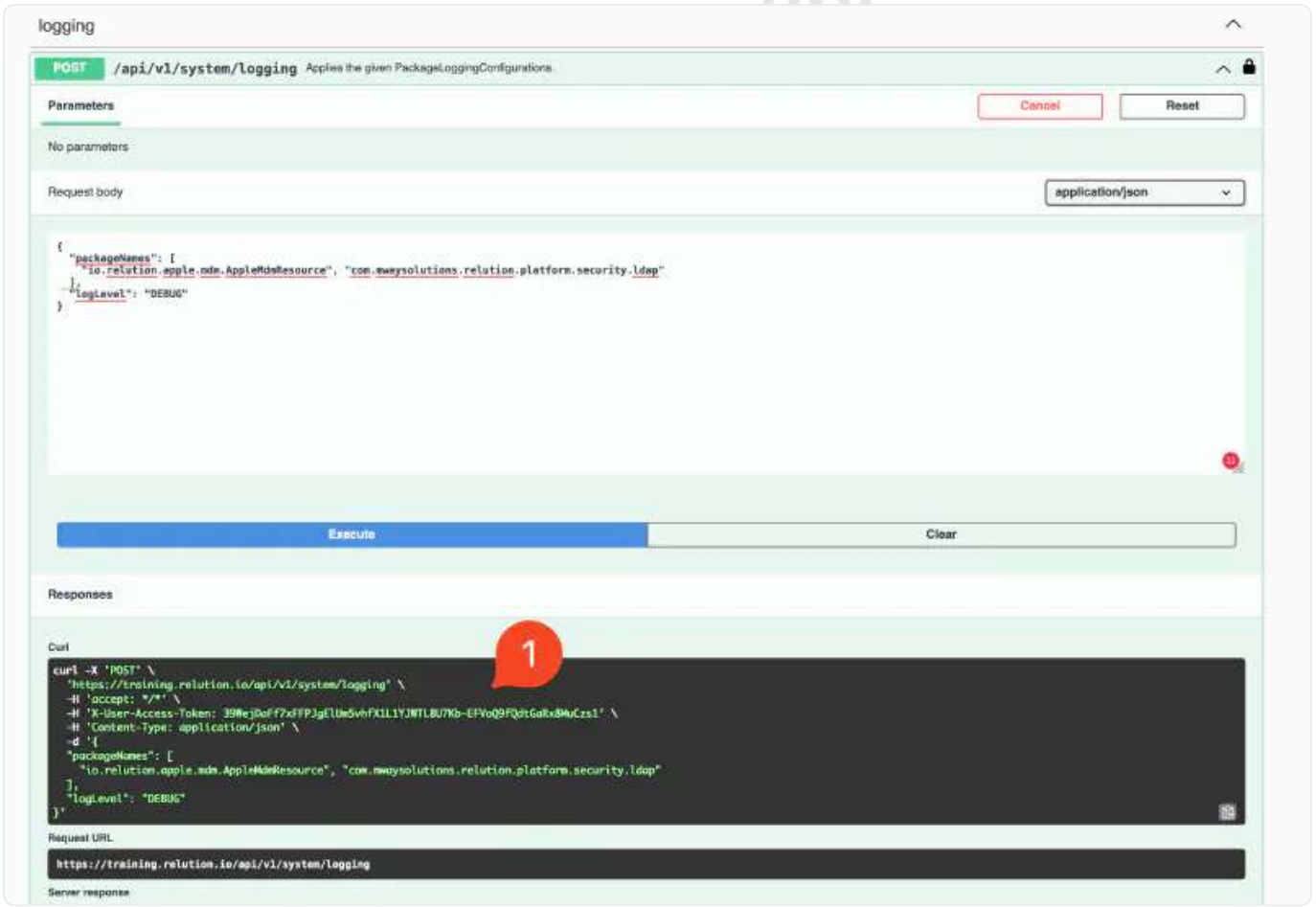
To control the log level via the Web API, the logging user can be accessed in the system organisation via the ⚙️ icon > Web API > Authorize. Here the access token of the logging user can be used to facilitate access and automatically add authentication at curl. In the item “userAccessTokenAuth” the token must be inserted and authorised. Note: Alternatively, log in with System System Orga Admin to skip entering the token.

At the point “logging”, the required logging points as well as the log level can be defined and executed. Successful execution is confirmed with code 204 and the executed curl command is displayed.


system
System Administrator
Newsletter
Documentation
Changelog
Helpdesk
Privacy Policy
Web API
System Portal
3rd Party Licenses
License information
Imprint
Authorize
1
2
3
levices/androidEnterprise/disassociate
levices/androidEnterprise/knownDangerousPermissions


Available authorizations
bearerAuth (http, Bearer)
authentication using a bearer token obtained via the AuthenticationV2 interface.
Value:
Authorize
Close
userAccessTokenAuth (apiKey)
1
access token as created on user profile page.
Name: X-User-Access-Token
In: header
Value:
2
39WejDaFf7xFFPJgElUm5vh
3
Authorize
Close
userImpersonationTokenHeader (apiKey)
access token of impersonated user.
Name: X-User-Impersonation-Token


logging
1
POST
/api/v1/system/logging
Applies the given PackageLoggingConfigurations
Parameters
Cancel
Reset
No parameters
Request body
application/json
{
"packageNames": [
"io.relution.apple.mdm.AppleMdmResource", "com.mwaysolutions.relution.platform.security.ldap"
],
"logLevel": "DEBUG"
}
2
3
Execute
Responses
Code
Description
Links
default
default response
No links
Media type
/
Controls Accept header.


logging
POST
/api/v1/system/logging
Applies the given PackageLoggingConfigurations
Parameters
Cancel
Reset
No parameters
Request body
application/json
{
"packageNames": [
"io.relution.apple.mdm.AppleMdmResource", "com.mwaysolutions.relution.platform.security.ldap"
],
"logLevel": "DEBUG"
}
Execute
Clear
Responses
Curl
1
curl -X 'POST' \
'https://training.relution.io/api/v1/system/logging' \
-H 'accept: */*' \
-H 'X-User-Access-Token: 39WejDoFf7xFFPJgElUm5vhfX1L1YJWTLBU7Kb-EFVoQ9FQdtGaKx8WuCzs1' \
-H 'Content-Type: application/json' \
-d '{
"packageNames": [
"io.relution.apple.mdm.AppleMdmResource", "com.mwaysolutions.relution.platform.security.ldap"
],
"logLevel": "DEBUG"
}'
Request URL
https://training.relution.io/api/v1/system/logging
Server response

In addition, it is possible to reset the logging to the default settings by triggering a reset or restore of the logging points.



4. controlling the log level via the curl command

It is also possible to control the log level via the curl command by saving the curl generated via the Web API as an alias or script for future use.

```
~ ❯❯❯ 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. use for support staff or other employees

To grant access to a user, for example a Relution support staff member, it is sufficient to, either pass on the token or the logging user's email address, which is linked to a valid Relution instance, to the Relution support team.

For version 26.4.0

Problem with update to 26.1

After updating to Relution 26.1, the Docker container no longer starts. The container log repeatedly shows the following error:

```
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)
```

Root Cause

Version 26.1 introduced changes to the user ID used in the Relution container due to updates securtity best practices. The existing internal temp directory (`/tmp`)in the Docker volume is now owned by the wrong user, preventing the Relution service from gaining write access at startup. Unfortunately, this cannot be solved automatically.

For Version 26.4.0

On startup, the service checks access to the temp directory:

- If it is not present, it will be created fresh with the correct permissions.
- If it already exists, the service attempts to clear it — which fails with incorrect ownership.

Solution

The volume will be recreated with the following command.

```
docker compose up -d --force-recreate --renew-anon-volumes --no-deps relution
```

Replace `relution` with the actual name of the compose service if a different one has been used.

After restarting, Relution will automatically recreate the `relution.tmp` directory with the correct permissions. The `Permission denied` error will no longer appear and the service will start normally.

Additional Notes

- This issue occurs only when updating from an older version to 26.1, as the directory already exists with outdated permissions.
- Fresh installations of version 26.1 are not affected.
- If the error persists after following these steps, check whether any additional volume mounts contain their own `tmp` directories.

For version 26.4.0

Server startup with a self-signed S3 certificate

After updating from a version earlier than 26.2 directly to Relution 26.4 or newer, the server no longer starts if the connected S3 object storage is reached over TLS using a self-signed or company-internal certificate. The following error appears in the log:

```
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)
```

Cause

During startup, Relution reads the JWT signer certificate from the configured object storage. If the certificate of the issuing CA is not registered as trusted, the TLS connection to the S3 endpoint fails and the startup is aborted.

The following factors interact here:

- Whenever an object storage is configured, resources are offloaded to it. This also affects certificates and therefore the JWT signer certificate.
- With Relution 26.2, certificates are classified as security-sensitive and are kept in the database permanently. Certificates that were already offloaded are automatically migrated back from the object storage into the database.
- With Relution 26.4, CA certificates are no longer stored in the container operating system but in the database, and are managed through the user interface (see CA certificate in Docker →). Adding the certificate therefore requires a running server, while the server in turn only starts once the certificate is already trusted.

If the update is performed in intermediate steps via 26.2 or 26.3, the signer certificate is back in the database after the reverse migration, so that the 26.4 startup no longer requires access to the object storage. Only when updating directly from a version earlier than 26.2 to 26.4 or newer does this reverse migration not take place, while at the same time the CA certificate can no longer be added through the operating system.

Solution

To allow the server to start, the affected signer certificate is removed from the database. On the next startup, Relution generates a new signer certificate and stores it in the database, so that no access to the object storage is required for the startup.

> A complete backup of the database is recommended before modifying the database.

Required steps:

For version 26.4.0

1. The Relution service is stopped.
2. The record of the signer certificate is removed from the database using the statement below.
3. The Relution service is started.

For PostgreSQL, the column name `usage` is enclosed in double quotes. In MariaDB, `usage` is a reserved keyword and is enclosed in backticks there.

PostgreSQL:

```
DELETE FROM mdm_crtfct WHERE "usage" = 'JWT_SIGNER_CERTIFICATE';
```

MariaDB:

```
DELETE FROM mdm_crtfct WHERE `usage` = 'JWT_SIGNER_CERTIFICATE';
```

Impact

A new JWT signer certificate is generated during the following startup. The existing login cookies become invalid as a result, so all users have to sign in again.

For version 26.4.0

After the server startup

Once the server has started successfully, the certificate of the internal CA is added so that the connection to the object storage is considered trusted again:

- Sign in to the global organization.
- Under `Settings` → `Certificates`, the certificate of the internal CA is uploaded (see Certificate management →).
- Under `Settings` → `TLS Trust configuration` → `Trusted certificates`, the uploaded certificate is selected from the certificate library via Add certificate.

> If this step is skipped, the server does start, but every access to the object storage keeps failing. As a result, native apps that were already uploaded can no longer be downloaded and app icons are not displayed.

The change is applied while the system is running; no further restart of the server is required. Afterwards the remaining security-sensitive certificates — such as the signer certificate for external services and the SCEP CA certificate — are moved from the object storage into the database as well.

Additional notes

- If the object storage is connected without TLS or with a publicly trusted certificate, the problem does not occur.
- The reverse migration of the certificates into the database is performed by a background job that runs once a day by default. When updating in intermediate steps, it must therefore be ensured that the migration has completed under 26.2 or 26.3 before updating to 26.4.
- The configuration of the object storage is described under Connect object storage →.

For version 26.4.0

Login: Access is forbidden

With Relution 26.4.0, the internal application server was switched from Undertow to Tomcat. If the reverse proxy (e.g. nginx or Traefik) runs on a different server than Relution itself, this can result in the following error during login:



The Relution server log shows a corresponding `ERROR` entry with the message `TLS required`.

Cause

For a login to succeed, the connection between the reverse proxy and Relution must satisfy two conditions at the same time:

1. The reverse proxy must communicate with Relution from an IP address classified as internal. By default, only the private IPv4 ranges `10.x.x.x`, `172.16.x.x` – `172.31.x.x` and `192.168.x.x`, as well as `localhost`, are considered internal.
2. The `X-Forwarded-Proto` header must be sent by the reverse proxy with the value `https`.

For version 26.4.0

Only when both conditions are met does Tomcat treat the incoming connection as secured by TLS. If the reverse proxy runs on a separate server with its own (external) IP address, the first condition is already not met. If the `X-Forwarded-Proto` header is missing or incorrect in addition to or instead of this, the connection is likewise not recognized as secure. In both cases, Relution aborts the login with `TLS required` in the server log, while the browser shows the message `Access is forbidden`.

Confirming the cause (optional)

To confirm the cause, DEBUG logging for the relevant Tomcat component can be enabled. To do this, add the following entry at the top level of the `application.yml`:

```
logging:
  level:
    org.apache.catalina.valves.RemoteIpValve: DEBUG
```

Afterwards, a new login attempt should be made. If an entry like the following then appears in the log, the reverse proxy's IP address is the cause: the request is not classified as trustworthy.

```
DEBUG ... ina.valves.RemoteIpValve: Skip RemoteIpValve for request
/api/device/v1/currentDevice/actions/next with originalRemoteAddr '<external-IP-of-the-
proxy>' []
```

If this entry does not appear but the error still occurs, the missing or incorrect `X-Forwarded-Proto` header is the cause instead, see Solution →.

> The log level should be removed or reset to INFO again once the analysis is complete, see Setting the log level →.

Solution

Depending on which of the two conditions from the Cause section is not met, one of the following two adjustments is required — both if necessary.

Trust the reverse proxy's IP address

For Relution to accept the reverse proxy's requests, its IP address must be explicitly registered as a trusted internal proxy. To do this, add the following entry at the top level of the `application.yml`:

Version 26.4.0

```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>` must be replaced with the actual, dot-escaped IP address of the reverse proxy, e.g. `194\.95\.62\.71`. For multiple proxy servers, additional IPs can be added, each separated by `|`.

The `application.yml` usually already contains other entries, for example for the system administrator, the external URL, or the database connection. The new `server` entry is its own top-level key next to the existing `relution` block, not a sub-item of it — even though a section also named `server` exists underneath `relution` (there, e.g., with `externalURL`). The following example shows a complete file with both blocks:

```
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%
```

Alternatively, the Relution server can be assigned a local/private IPv4 address through which it communicates internally with the reverse proxy. In this case, no additional configuration is required, since private IPv4 ranges are considered internal by default.

For version 26.4.0

Set the X-Forwarded-Proto header

In addition, the reverse proxy must forward the `X-Forwarded-Proto` header with the value `https` to Relution. The `location /` block of the nginx configuration must contain the following line for this:

```
proxy_set_header X-Forwarded-Proto $scheme;
```

This line is already included in the default `relution-nginx.conf` template. When using a custom or modified reverse proxy configuration, or if there is an additional proxy in front of it, check whether the header is set correctly and is not overwritten by an upstream proxy.

After adjusting the `application.yml` or the reverse proxy configuration, the Relution service or container (and, if applicable, the reverse proxy) must be restarted for the change to take effect.

Additional notes

- This issue primarily affects installations where the reverse proxy does not run on the same host as Relution.
- Relution installations from version 26.4.0 onwards are affected.
- The message `Access is forbidden` is a generic error message that is shown in the portal for a wide variety of requests rejected by the server. The solution described in this article only applies if the server log additionally shows the `ERROR` entry `TLS required`.
- See also: Docker installation: Nginx as an alternative to Traefik →

For version 26.4.0

Troubleshooting and help

If access to the Relution system administrator account has been lost and the password cannot be reset using the configured email address, it is also possible to reset the password from the database. This procedure requires write access to the database server and Relution's database.

Please try to reset the password via the `forgotten password?` link before trying to reset it from the database. See this option only as a last resort.

To reset the password, first log in via the command line or an administration tool to connect to the database. Then run the SQL script that is appropriate for the database server.

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';
```

Replace `password123` with the new desired password.

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';
```

Replace `password123` with the new desired password.

Server does not start

Please check the log files in the `log` directory, which is located inside the Relution installation directory.
If the problem cannot be identified independently, please open a support ticket and provide us with the logs.

Log files

Where to find log files for Docker, Linux, and Windows is described under Relution Logs →.

Performance analysis with Glowroot

New in 26.5

> This guide applies as of Relution 26.5.

In case of performance problems, Relution support may ask for an analysis using Glowroot →. Glowroot records which requests take how long and shows the result in a web interface of its own.

When running in Docker, Glowroot is not part of the image, it is downloaded automatically on startup as soon as `RELUTION_ENABLE_GLOWROOT` is set:

```
  relution:
    image: relution/relution:latest
    environment:
      - RELUTION_ENABLE_GLOWROOT=true
      -
RELUTION_GLOWROOT_ADMIN_JSON_BASE64=ewogICJ3ZWIiOiB7CiAgICAiYmluZEFkZHJlc3MiOiAiMC4wLjA
uMCIKICB9Cn0=
    ports:
      - '4000:4000'
```

The second variable merely contains the base64 encoded Glowroot configuration `{"web": {"bindAddress": "0.0.0.0"}}`. Without it, the interface can only be reached from inside the container. After restarting the container it is available on port 4000.

The recordings are kept inside the container and are lost as soon as it is recreated. For the duration of an analysis this is usually sufficient. To keep them, set `RELUTION_GLOWROOT_DIR` to a directory writable for UID `20001`.

> Only enable Glowroot for as long as the analysis takes. The interface on port 4000 is not protected by a password and reveals database queries, response times and stack traces. It must never be reachable from the internet.

To disable it, remove `RELUTION_ENABLE_GLOWROOT` again and restart the container.

Security notes

- Install the latest operating system and software updates and security patches
- Use strong passwords for administrator accounts
- Use long passwords for service-to-service communications, Passwords do not need to be used or remembered by humans
- Make sure the user account used to access LDAP has Read-only access
- Do not create accounts with weak passwords such as `password` or `test`
- Do not store passwords in files that are globally readable

For version 26.4.0

Local Exchange without SMG

Configuring a local Exchange server without SMG (Secure Mail Gateway) can easily fail. For this reason, we have identified common causes and recorded appropriate solutions. To check basic connectivity, there are four steps to perform.

Logfile analysis

The log from the reverse proxy (e.g. nginx) is needed for further analysis

- on Linux the log is located in the following directory `/var/log/nginx/relution_access.log`
- for Windows e.g. in the nGinx installation path `/nGinx/logs/relution_access.log`

If the mails are retrieved on the end device, the log should contain a reference to the following URL `/Microsoft-Server-ActiveSync`

If the entry /Microsoft-Server-ActiveSync is left behind the connection works.

Troubleshooting

If nothing is entered in the log, the URL must be entered in the browser whether it is generally accessible. `https://myexchange.com/Microsoft-Server-ActiveSync` If the URL is called, an entry must be left in the nginx log.

- If no entry is generated, the infrastructure must be checked.
- If the entry can be found, probably the settings of the Exchange configuration in the Relution policy are not set correctly or are invalid.

Checking the connection

A curl command can be used to check the connection from Relution to the Exchange server:

```
curl https://outlook.XXX.de/Microsoft-Server-ActiveSync --user Our-Exchange-host\\Exchangeuser@Domain.de:ExchangePWvomUser --verbose --http1.1 -i
```

The output may show a certificate error, as shown:

For version 26.4.0

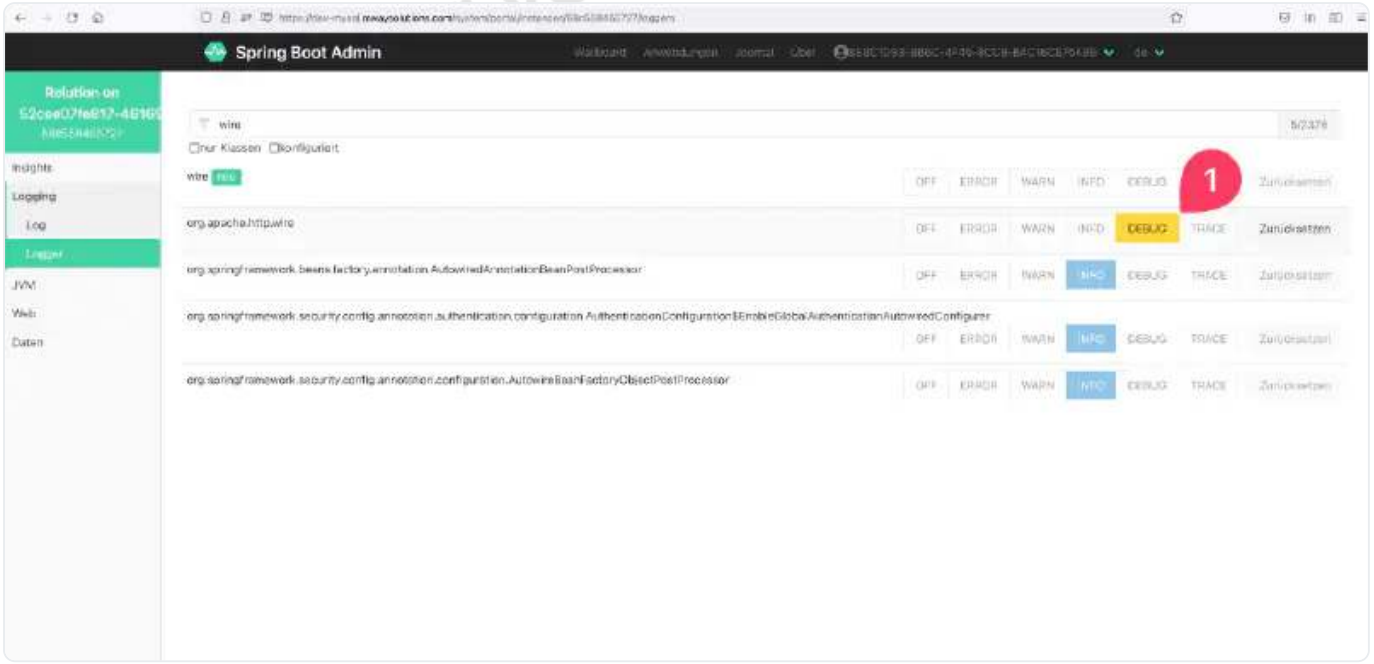
```
Trying 172.16.105.109:443....
Connected to outlook.XXX.de (172.000.000.000) port 443 (#0)
schannel: disabled automatic use of client certificate
ALPN: offers http/1.1
schannel: SEC_E_UNTRUSTED_ROOT (0x80090325) - *The certificate chain was issued by an
untrusted certificate authority.
Closing connection 0
curl: (60) schannel: SEC_E_UNTRUSTED_ROOT (0x80090325) - *The certificate chain was
issued by an untrusted certificate authority.
More details here: https://curl.se/docs/sslcerts.html
```

If the error message is displayed as above, the CA's certificate is not stored in the server's operating system, so depending on the operating system, the certificate must be installed accordingly.

Example for Relution in Docker →

Read out HTTPS communication

Setting the log level of the `org.apache.http.wire` logger to `DEBUG` makes the HTTPS communication between Relution and the Exchange visible in the log file. The available ways to set the log level — Web API, `application.yml` or system portal — are described under Set log level →. The system portal route shown in the screenshot below requires the corresponding actuator endpoint to be enabled → as of Relution 26.4.

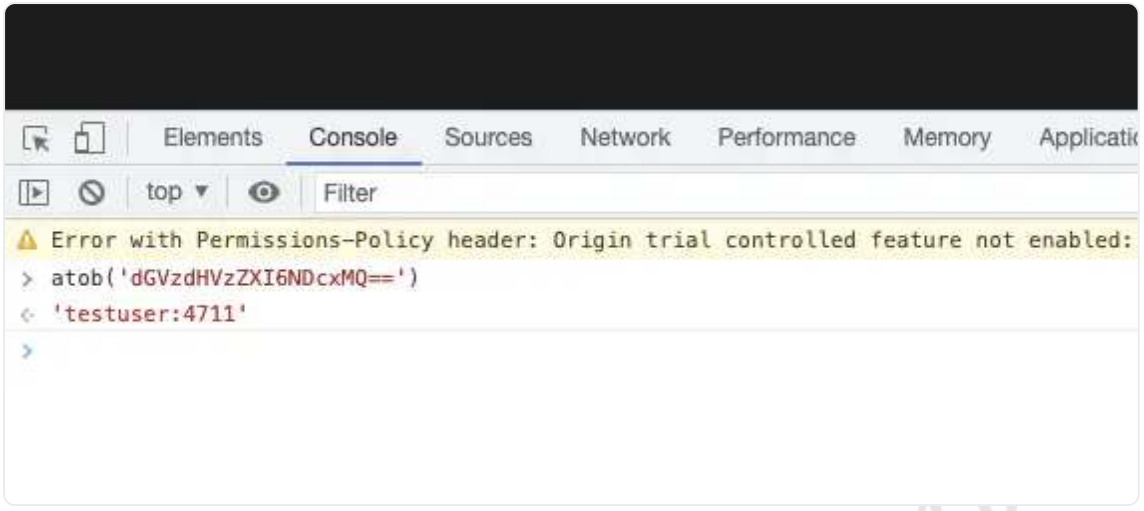


A communication must be triggered by the device to fill the log with hints about the cause. The log level must be set back to `INFO` after the analysis.

Evaluate log

Subsequently, the increased log level can be searched for conspicuous clues. For example, if the user and user credentials are not correct, the login fails and a 401 Unauthorized message is entered, which may look like this in basic Auth:
`dGVzdHVzZXI6NDcxMQ==`

This can be decoded in the browser console to compare the transmitted password and the user
`atob('dGVzdHVzZXI6NDcxMQ==')`



SMG is not functional with Outlook365, Microsoft has deactivated Basic Auth for this and is using OAuth2

Deprication of Basic Auth →

For version 26.4.0

Announcements and Hints

Software in End-Of-Life (EOL)

For security reasons, Relution does not support software which has already reached its end of life (EOL), since no security patches will be provided any more.

Announcements and Deprecations

- Update to 26.4.0+: 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 base image: Ubuntu instead of AlmaLinux: Starting with Relution 26.4.0, the Relution container image is based on Ubuntu instead of AlmaLinux.
- Secure Mail Gateway: Starting with Relution 26.4.0, using the Secure Mail Gateway feature requires a dedicated standalone service — without it the feature will no longer be available. In 26.3, the new mode can already be activated optionally using a feature toggle. For migration guidance, see Secure Mail Gateway →.
- Update to 26.1: Before upgrading to version 26.1 or higher, a 26.0.x version must be installed and started at least once. If any 26.0.x version is already running, updating to 26.0.3 specifically is not required. Background: Relution 26.1 only supports database upgrades from version 26.0, so a 26.0.x version is required as an intermediate step. Additionally, updating to 26.1 may cause the Docker container to fail to start due to a permission issue on the temp directory. See Problem with update to 26.1 → for the solution.
- Object Storage: For installations using MinIO as the local S3-compatible storage provider, we recommend a migration to SeaweedFS, because MinIO has ceased development. A guide for this is available at Object Storage Migration →.
- Device groups: As has been announced previously, Relution 26.0 will automatically migrate organisations to device groups. Support for the legacy functionality will be removed. This version will also finally drop all rule sets, which have been replaced by device group actions.
- Java: Starting with version 5.35, Relution will require *Java 21*. With 26.0, starting Relution on older Java versions is no longer possible.
- MariaDB: Relution 5.30 requires *MariaDB 10.11 or higher*. Please note that *support for MariaDB in general will only be available until the end of 2027.*
- PostgreSQL: Relution 5.29 requires *PostgreSQL 14 or higher*. Using *PostgreSQL 18* is recommended.

New handbook articles

An overview of new features from the last three versions, linking to the corresponding handbook articles.

For version 26.4.0

Version 26.5

On Premises Installation

- Troubleshooting and help → Performance analysis with Glowroot
- Server-Side Encryption (SSE-C) → Option C: Key as a file
- Relution Shield (Add-on) → Set up a technical user and create an API access key{#create-technical-user}

General

- Dashboard
- Teacher → Web links and browsing restrictions
- Advanced placeholders → User certificates
- Profile for ADE → Minimum OS version
- Device groups → Education groups

Apple macOS

- Recovery Lock → Verify Recovery Lock
- Relution Decon (content filter)

Education

- Education groups

Android Enterprise

- Link Organization → Repair signup

Settings

- Certificate Pool
- TLS Trust Configuration → Certificate pinning (Apple enrollment)
- Meta Organizations
- OIDC with Entra → Redirect URI for device enrollment
- Relution as Identity Provider
- OIDC with Workspace → Redirect URI for device enrollment

For version 26.4.0

Version 26.4

On Premises Installation

- CA certificate in Docker → Adding certificates via the user interface
- Login: Access is forbidden
- Secure Mail Gateway → Mandatory component as of 26.4.0

General

- Self-Service Portal → Show location on a map
- Profile for ADE → User authentication during enrollment

Apple iOS

- Software Update → Managed Software Updates

Apple macOS

- Recovery Lock → Set Recovery Lock
- Software Update → Managed Software Updates

Android Enterprise

- Locate Android Device → Viewing location in the Self-Service Portal

Windows

- Configure Companion

Settings

- Global Organization → Organization switcher
- TLS Trust Configuration
- OIDC with Entra → Add redirection URI
- OIDC with Workspace → Scoped redirect URIs
- Secure Mail Gateway → Configuration of the Secure Mail Gateway

---

Version 26.3

On Premises Installation

- APNS Push Certificates → Migration from the Previous Process
- Server-Side Encryption (SSE-C)
- Secure Mail Gateway → Feature toggle for on-premise installations (26.3)

Get started

- Manage Apple devices → Certificates

Apple iOS

- Intelligence Settings
- External Intelligence Settings
- Keyboard Settings
- Siri Settings

Apple macOS

- Intelligence Settings
- External Intelligence Settings
- Keyboard Settings
- Siri Settings
- Migration Assistant → Settings Declaration

Apple visionOS

- Intelligence Settings

Settings

- Organization Certificates

For version 26.4.0

Technical Changelog

This page contains the technical changelog and is intended for an experienced audience. The release notes containing a lot more explanation are available details →.

Generally recommended version

Please note that it can take some time until versions listed here are made available via `latest`. This is done after the version has passed additional quality gates.

Version currently available via `latest`: 26.5.4 (at 20.10.2026)

Before Updating to Relution 26.1

A 26.0.x version (for example the latest version 26.0.3 →) must be installed and started at least once before upgrading to version 26.1 or higher. If any 26.0.x version is already running, updating to 26.0.3 specifically is not required.

Background: Relution 26.1 only supports database upgrades from version 26.0. A direct upgrade to 26.1 or higher without first installing and starting a 26.0.x version is therefore not supported.

Additionally, updating to version 26.1 may cause the Docker container to fail to start due to a permission issue on the temp directory. See Problem with update to 26.1 → for the solution.

For version 26.4.0

Announcements

See section Announcements and Hints →.

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]

For 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

For 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

For 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]

For 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]

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]

For version 26.4.0

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]

For 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

For 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 the 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

For 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]

For 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

For version 26.4.0

2026-06-08

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]

For 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]

For 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]

For 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]

For 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

For 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]

Version 26.0.3

2026-02-11

For Version 26.4.0

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]

For 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

For 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]

Fixes

For version 26.4.0

- 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]

Full 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]

For 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]

For 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]

For 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]

For 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]

For 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]

For 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 back to the 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

2025-08-12

For version 26.4.0

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]

Updates

For version 26.4.0

- 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

For 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]

For 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]

Updates

For version 26.4.0

- 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]

Fixes

For version 26.4.0

- 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]

For 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

For 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]

Fixes

For version 26.4.0

- 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]

For 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

For 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]

For 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]

Fixes

Current version 26.4.0

- 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]

Version 5.28.3

2024-12-23

Updates

For version 26.4.0

- 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]

For 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]

Updates

For version 26.4.0

- 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

For 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]

---

for 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]

For 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]

For 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]

For 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]

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]

For version 26.4.0

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]

For 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

For 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]

Fixes

For version 26.4.0

- 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

For 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]

For 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

For 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]

For 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

For 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

For 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

- 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

For version 26.4.0

- 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]

For 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]

For 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. Rule set configurations should be migrated 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

For 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

For 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

- 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]

For Version 26.4.0

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

For 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

For 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]

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

For version 26.4.0

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]

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

For version 26.4.0

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

For 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

For 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]

For 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]

For 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]

For 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]

For 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]

Version 5.18.0

2023-06-09

New

For version 26.4.0

- 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]

For 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]

For 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]

For 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]

For 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]

For 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

For 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]

For 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

For 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]

For 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]

For 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

For 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]

For 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]

For version 26.4.0

Version 5.13.2

2022-10-20

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

For 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

For version 26.4.0

- 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]

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

- 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

For version 26.4.0

- 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

For 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]

For 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]

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

For version 26.4.0

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

For 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

For 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]

For 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

For 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

For 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]

For 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

For 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

For 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]

Fixes

For version 26.4.0

- 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]

For 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]

For 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

For 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]

For 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]

For 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

Updates

For version 26.4.0

- 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]

For 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]

For 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

For 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]

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]

For version 26.4.0

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

For 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]

Version 5.1.4

2022-05-31

Updates

For Version 26.4.0

- 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]

For 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

For 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]

For 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

For 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]

For version 26.4.0

Known Issues

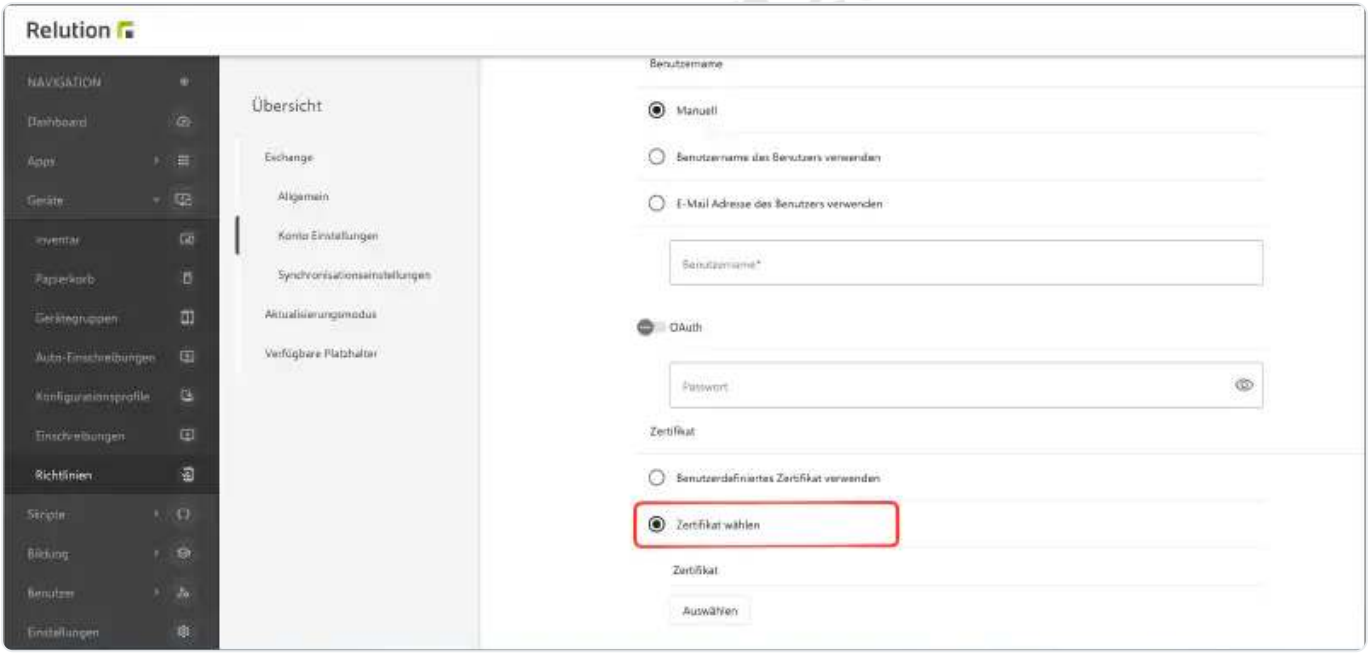
Exchange policy: No user certificate of subtype Exchange

When a policy with an Exchange configuration is applied, the Change policy action fails in the device actions. The following message is displayed:

```
At least one sub action failed: ErrorCode: -, Message: No user certificate of subtype Exchange found for user <username>.
```

The cause is the Use user certificate setting in the Certificate section of the Exchange configuration. With this option, Relution looks for a user certificate of subtype Exchange for the device user. If no such certificate exists for the user, the account cannot be deployed.

Solution: In the applied Exchange configuration, the Select certificate option is set in the Certificate section. No certificate needs to be selected; the configuration can be saved directly.



The same applies to the S/MIME certificates further down in the Exchange configuration. If S/MIME signing or encryption is enabled, the S/MIME signing certificate and S/MIME encryption certificate sections appear there with the same choice. If one of these sections is set to Use user certificate, Relution additionally looks for a user certificate of subtype S/MIME signing or S/MIME encryption, and the action fails with the corresponding message if none exists. In this case, the Select certificate option is set in these sections as well.

More information: Exchange configuration →

Shortcuts as a required app

Apple changed the bundle ID of the `Shortcuts` app. The older VPP listing with the bundle ID `is.workflow.my.app` can no longer be installed on devices running iOS 26 or later, because iOS actively rejects the installation with the error `AppBlacklisted`. If this older listing is included in the `Required Apps` list, the deployment keeps restarting without the installation ever completing successfully.

Typical symptoms:

- Affected iOS devices are displayed as `non-compliant` in the device inventory.
- `Shortcuts` is correctly listed under `Installed apps`.
- The app deployment keeps restarting but never completes successfully.
- The device log shows the message `This app can no longer be installed on this version of the OS.` together with the error code `AppBlacklisted`.

Workaround: The outdated VPP app with the bundle ID `is.workflow.my.app` is removed from the `Required Apps` list, and the corresponding VPP assignment is deleted.

> The current `Shortcuts` app with the bundle ID `com.apple.shortcuts` should not currently be added to the `Required Apps` list as a replacement, since Relution still treats Shortcuts as a system app that cannot be installed. If `Shortcuts` is genuinely missing on individual devices, it can instead be installed separately by distributing an Apple App Store app (Manage App Store apps →).

For version 26.4.0

Error when updating to Relution 26.1

After updating to Relution 26.1, the Docker container no longer starts. The following error appears repeatedly in the container log:

```
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)
```

Cause and solution: Problem with update to 26.1 →

Server startup fails with a self-signed S3 certificate

After updating from a version earlier than 26.2 directly to Relution 26.4 or newer, the server no longer starts if the connected S3 object storage is reached over TLS using a self-signed or company-internal certificate. The following error appears in the log:

```
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)
```

Cause and solution — including the required re-login of all users: Server startup with a self-signed S3 certificate →

Prometheus metrics are not exposed

As of Relution 26.4, only the health endpoint is exposed by default for security reasons; the Prometheus endpoint (`/actuator/prometheus`) is disabled. Prometheus monitoring therefore does not receive any metrics until the endpoint has been enabled once in the `application.yml`.

Cause and solution: Enabling Prometheus metrics in Relution →

Log levels cannot be changed via the system portal

As of Relution 26.4, only the health endpoint is exposed by default for security reasons. The system portal therefore shows the `Details` section only; the `Logger`, `Environment`, `Metrics` and `Threads` sections appear once the corresponding endpoints have been enabled in the `application.yml`. Independently of this, log levels can still be changed via the Web API.

For version 26.4.0

Cause and solution: Enabling the actuator endpoints →

OIDC + Entra ID

- OIDC authentication with Microsoft Entra ID was reconfigured according to our documentation.
  The configuration itself is correct, but login does not work immediately after setup.
  Users receive an error message after logging in with their Microsoft credentials:



Solution / Workaround

Only after restarting the Relution server does OIDC login work as expected.

Backups with iOS 26.4

- When restoring backups from iOS 26.3 or earlier to a device with iOS 26.4 installed, the Device Management state is lost.

shared iPad

- On Shared iPad, as of iOS 26, it is not possible to create or save local files in Guest Mode. We have opened a case with Apple regarding this, and to expedite the process, feel free to open a case with Apple → and inform our support team.
  - Workaround: Create and edit files through a connected file share. paed.ML x Relution →

Apple ID signing

> The problem is solved by Apple with iOS 26.2.

- Signing in through system apps with an Apple ID is possible, even though the restriction *Modifying accounts allowed* is disabled.

New Apps

- New Apps and the bundle IDs to block
  - Preview → `com.apple.Preview`
  - Games → `com.apple.games`
  - Tipps → `com.apple.tips`

For version 26.4.0

Relution Agent 5.19.0

> The issue (1) is resolved with Relution Agent 5.19.2. The version has been released by Apple!

There are currently two problems with Relution Agent version 5.19.0.

1. In some cases, an error may occur when logging in to Relution Shared Device. This is displayed after login. The error message reads ‘Bad state: Stream has already been listened to.’ As a workaround, simply press the Home button on the iPad. The user should be logged in and the device should be usable as normal.

2. All apps with an available update are displayed in the App Store. This is a display error.

---

iOS Wallpaper

> The problem is solved by Apple with iOS 18.5.

There is currently an issue with the deployment of Wallpapers the Problem can occur on all iOS Device where a Wallpapere policy is deployed. The issue can’t be reproduced the whole time but occur when a policy change occur on the device. We created a Workaround with the Relution Server Version 5.29.1 but the problem can still occur in some cases. We already created a Ticket with Apple to solve this Problem as quickly as possible.

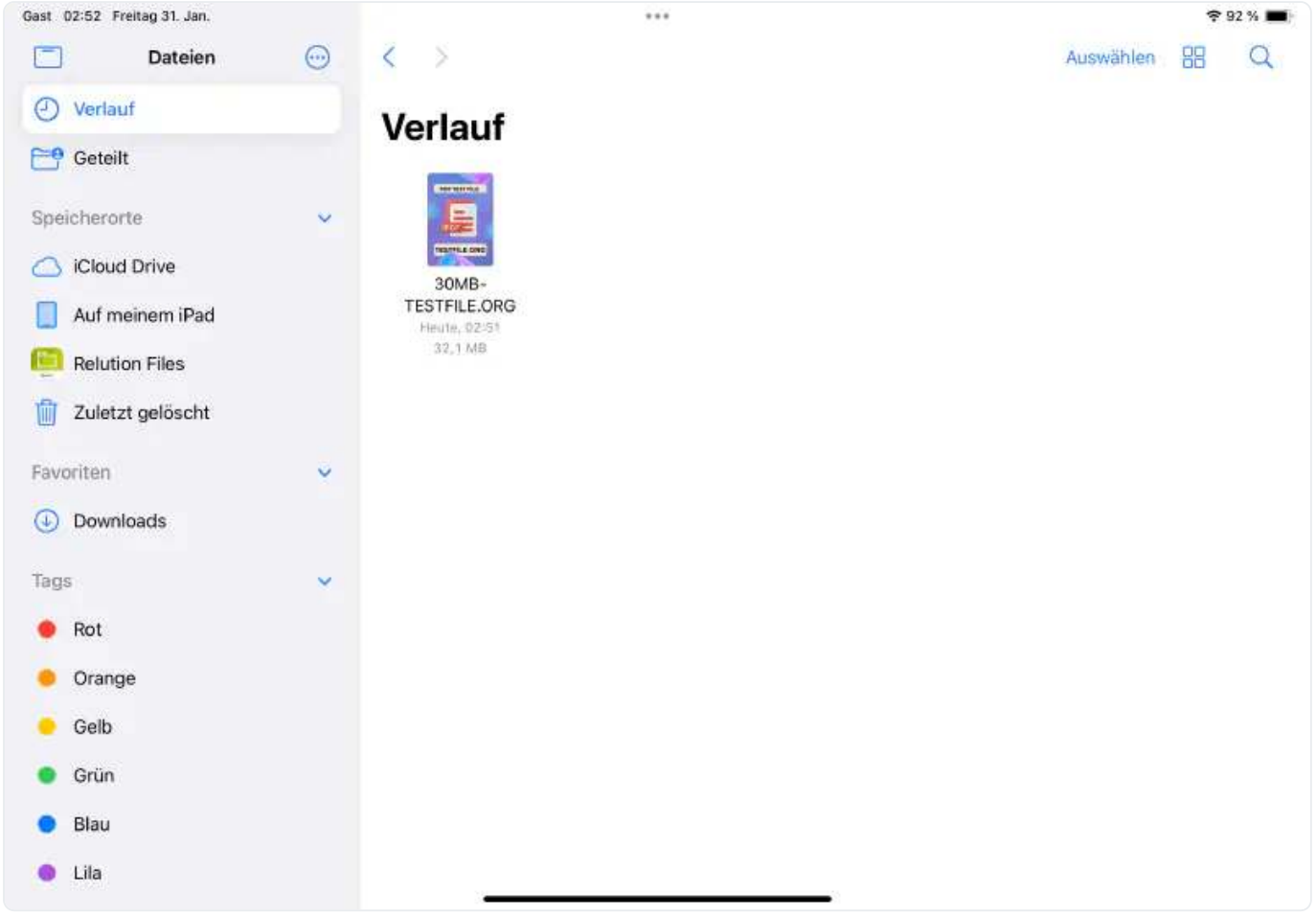
The other solution for the problem would be to create a Device group where the device is only for a brief moment and where the wallpaper is deployed. After the wallpaper is deployed the Wallpaper wont be withdrawn from the device but the policy will. Which shouldn’t result in the mentioned Wallpaper Problem.

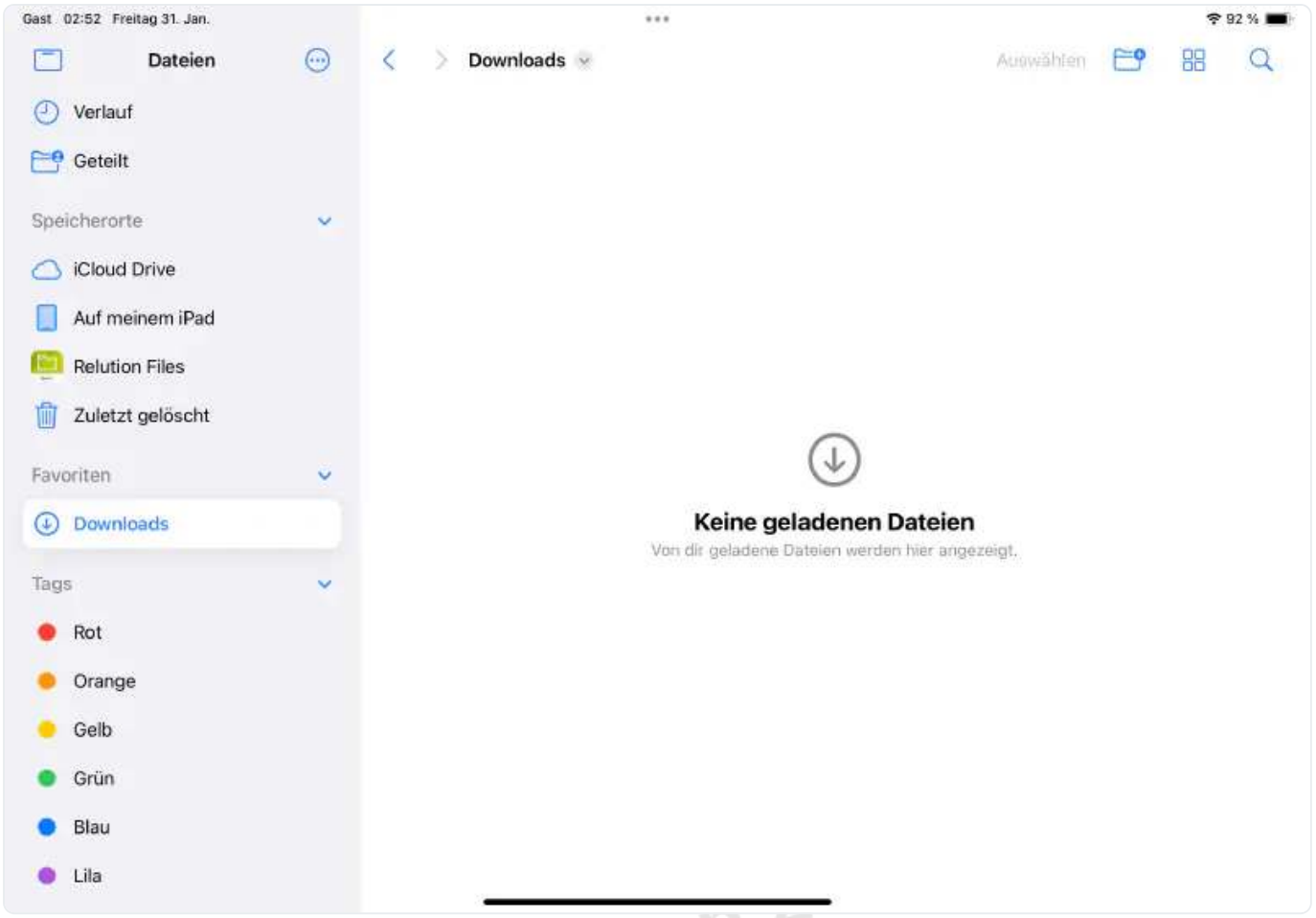
Apple Files App

There is currently an error in the Files app on Apple shared iPads (tested with iOS 18.2 and 18.3).

> The share and the use of the Apple Files app works on non-shared devices.

The bug is also noticeable in that downloaded files are missing from the Downloads folder. When data is opened, it is visible in the Downloads folder until the Apple Files app is closed and reopened.





The problem has been fixed in Relution Server 5.32. Here, a new parameter can be configured in the file sharing settings. To do this, change the Extension type from Modern to Classic.

Issues with SMB Access in iOS 18

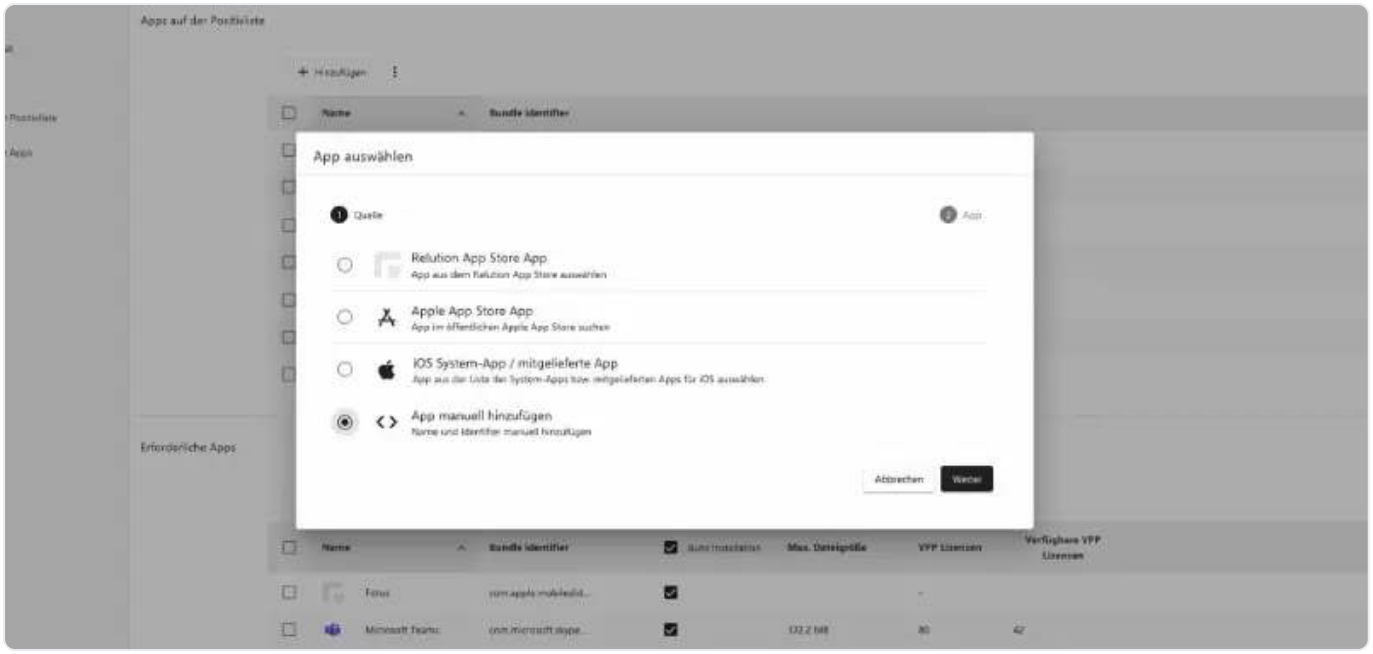
There is a known issue in iOS 18 that can cause problems when writing to SMB shares. This is a bug that occurs independently of Relution and is related to a problem within iOS 18 itself. Apple is aware of the issue, and we recommend keeping an eye on upcoming updates from Apple, as a solution may be included in a future iOS release.

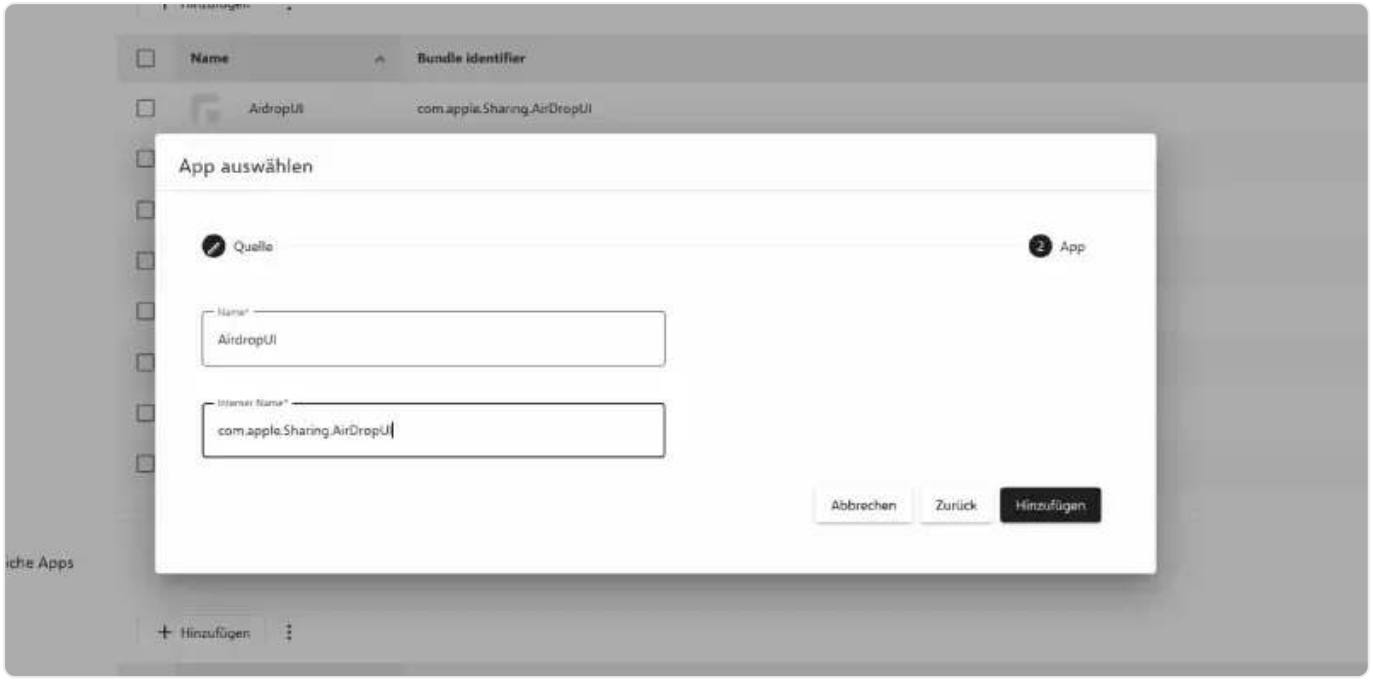
Airdrop

In iOS 18, there may be difficulties with Airdrop, as the new bundle identifier for the Airdrop UI must be stored positively in the app compliance. The correct identifier is:

```
com.apple.Sharing.AirDropUI
```

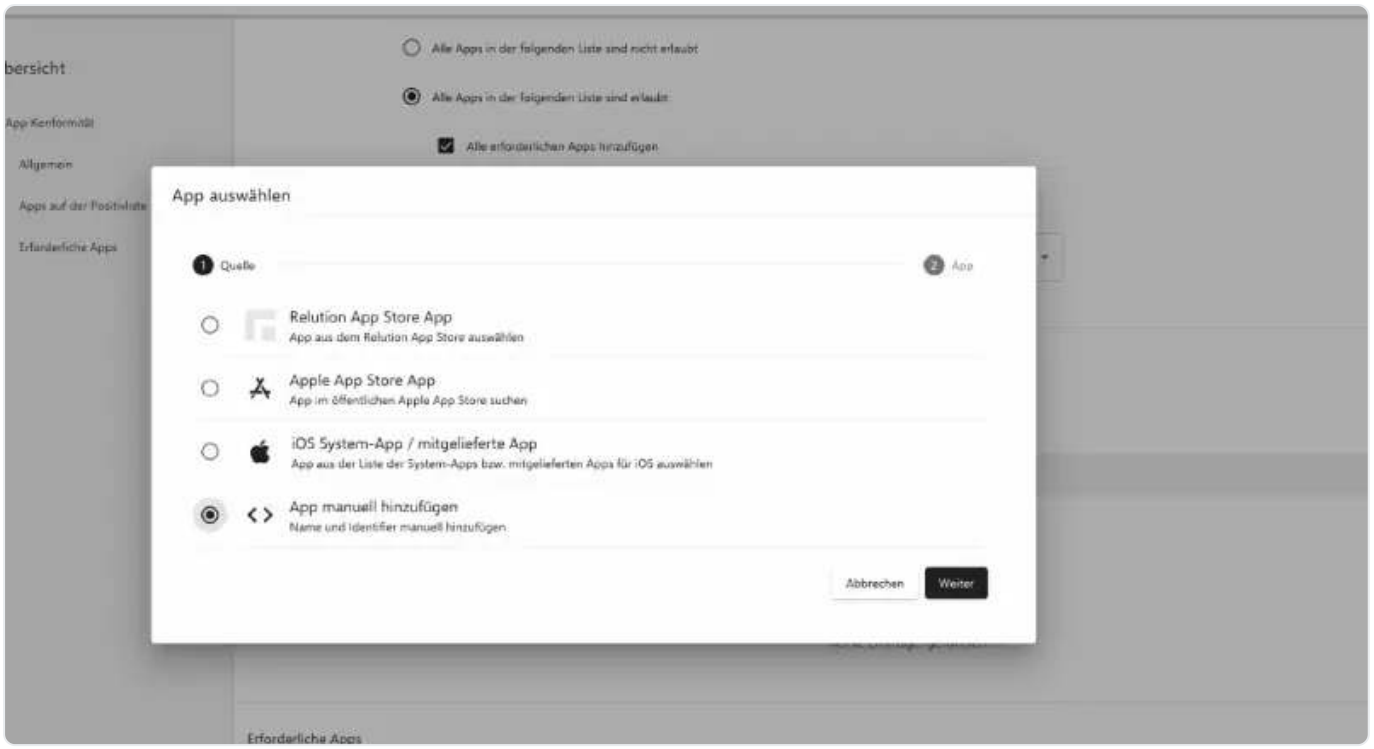
Please note that the bundle identifier is case-sensitive.

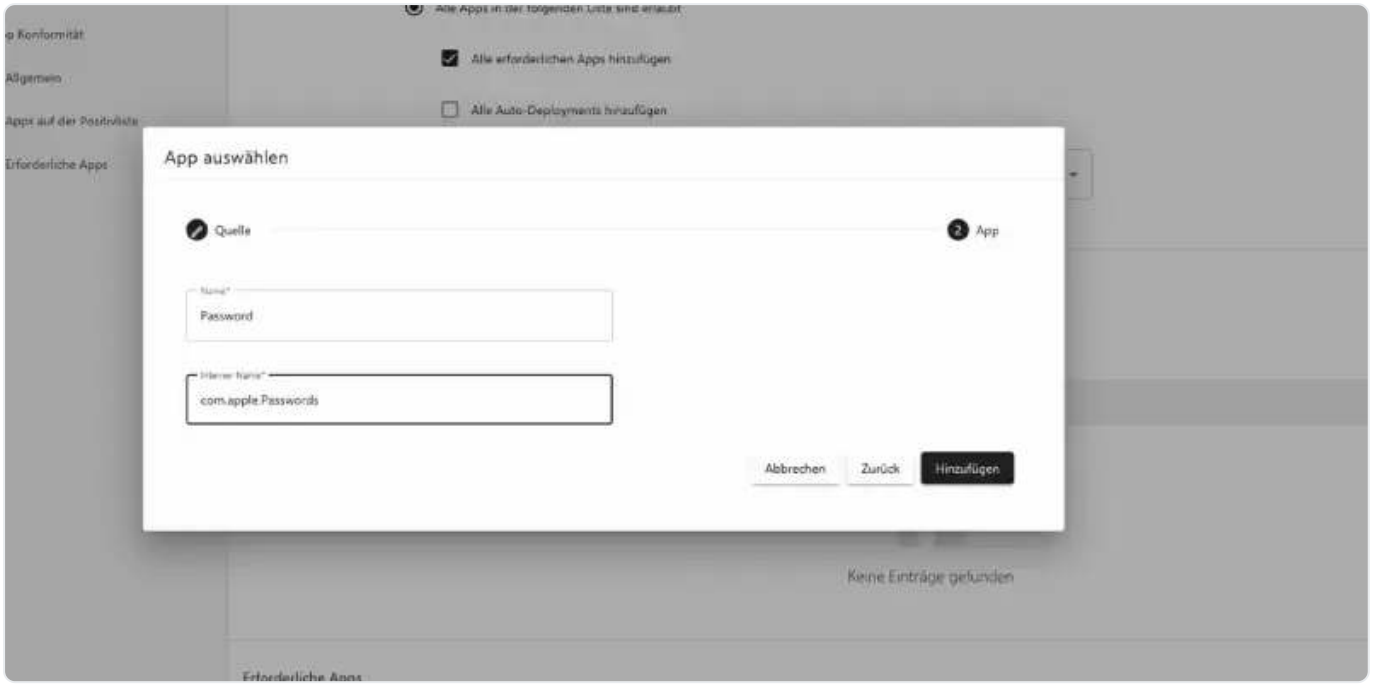




Password app

With iOS 18, Apple has introduced a new system app that serves as a password safe. If a positive list of approved apps is defined via app compliance, the new bundle identifier of the password app must also be stored here in order to allow it correctly.





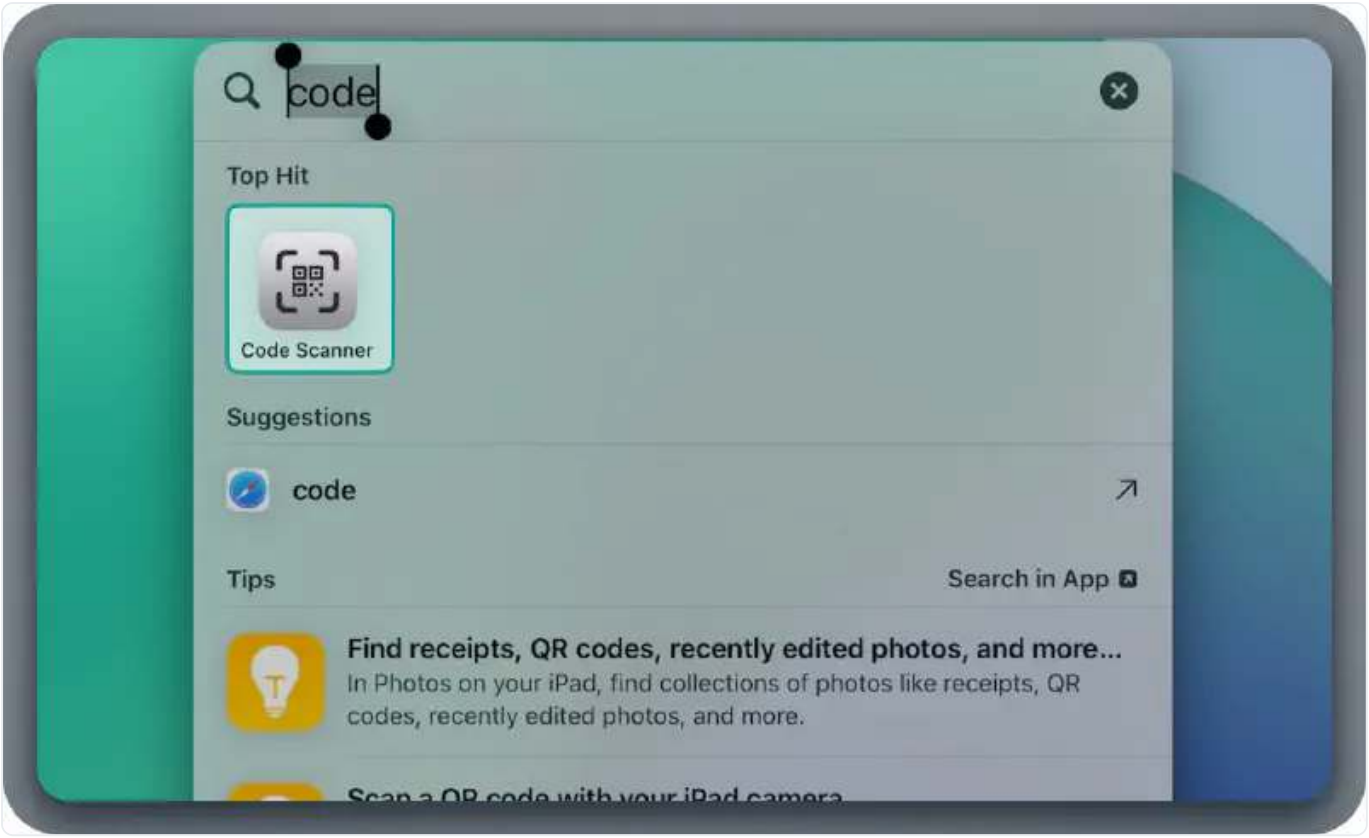
QR code scanner

Another known problem concerns the QR code scanner in iOS 18 with devices from generation 9. The bundle identifier has been shortened here. The current identifier is:

```
com.apple.BarcodeScanner
```

To fix this, the positive list must be added manually in the app compliance. The name is irrelevant here; it is only important to enter the bundle identifier mentioned above.

Devices smaller than generation 9 must use the separate app `Code Scanner`. This can be called up by calling up the Spotlight search from the home screen from top to bottom and searching for `Code`.



Slow login on shared devices

With iOS 17.x, setting the restriction configuration Allow iCloud Keychain synchronization to No causes the login on shared devices to be slowed down.

To bypass this behavior, the item Allow iCloud Keychain synchronization must be set to yes in the applied configuration of the ‘Restriction’.

Lack of storage space on iOS devices

On iOS devices, despite sufficient memory for app installations, a message may appear that there is not enough memory available. This is also displayed accordingly in the system settings.

The problem is caused by using the policy configuration `Shared iPad settings`. Repeated logins and logouts of guest users on the shared device can cause this error to occur spontaneously.

To avoid the occurrence of this problem, it is recommended not to use the policy. Alternatively, at least the two points Storage space quota and Number of users should be avoided.

For affected devices, it is necessary to reset them to factory settings.

For version 26.4.0

Vulnerability Disclosure Policy

1. Introduction

Relution is committed to the security of our products, services, and the data entrusted to us by our customers. We recognize that independent security researchers play a valuable role in identifying vulnerabilities that may otherwise go undetected.

This policy describes how security researchers can engage in authorized vulnerability discovery activities, how to report findings to us, and what they can expect from us in return. We value the work of security researchers who act in good faith to help us maintain a secure environment for our users.

This policy may be updated from time to time. The effective date and version number will be updated accordingly. We encourage researchers to review this policy before conducting any testing.

2.1 In Scope

The following assets are within the scope of this policy:

- The Relution platform and its associated services hosted at domains operated by Relution
- Web applications and portals operated by Relution under `*.relution.io`
- The Relution Docker containers published to Docker Hub
- Mobile applications published by Relution on official app stores
- Public APIs documented at https://live.relution.io/web-api/index.html (registration → required)
- The Relution website → and related web pages, such as Relution Hub →.

For Version 26.4.0

2.2 Out of Scope

The following targets are not authorized for testing under this policy:

- Relution Software operated by our customers, partners, or third parties
- Other Systems, networks, or applications operated by our customers, partners, or third parties
- Third-party services integrated into our platform (e.g., payment processors, identity providers, analytics services)
- Physical premises and facilities of Relution GmbH

If it is unclear whether a target is in scope, contact us at security@relution.io → before conducting any testing.

3.1 Authorized Activities

When conducted in accordance with this policy, the following activities are explicitly authorized:

- Analysis of publicly accessible information related to our systems (e.g., DNS records, SSL certificates, publicly available documentation)
- Testing for common web application vulnerabilities (e.g., injection flaws, authentication weaknesses, access control issues, security misconfigurations)
- Examination of API endpoints for security weaknesses
- Analysis of client-side code served by our web applications
- Given they were published by Relution and were legitimately obtained through official distribution channels:
    - Analysis of Docker containers and their contents
    - Reverse engineering including decompilation of mobile applications and Java archives and respective class files

---

3.2 Conditions for Authorization

To remain within the scope of this authorization, researchers must:

1. Act in good faith with the sole purpose of identifying and reporting security vulnerabilities
2. Minimize harm: avoid actions that could impact system availability, data integrity, or other users
3. Stop upon discovery: once a vulnerability has been confirmed, cease further testing and report the findings; do not attempt to demonstrate impact by accessing additional data or systems
4. Protect data: do not access, copy, modify, or delete data belonging to other users; if such data is inadvertently accessed, stop immediately, do not save or share it, and include this information in the report
5. Maintain confidentiality: do not disclose vulnerability details to third parties until we have had reasonable opportunity to address the issue and coordinated disclosure has been agreed upon

---

For version 26.4.0

3.3 Prohibited Activities

The following methods and behaviors are not authorized under any circumstances, even against in-scope targets:

- Any form of social engineering, phishing, vishing, pretexting, or similar activities against Relution employees or users
- Physical intrusion or physical access attempts
- Denial of service (DoS/DDoS) attacks or any testing intended to degrade service availability
- Automated vulnerability scanning at volumes or frequencies that could impact system performance
- Accessing, downloading, or otherwise exfiltrating customer data, personal data, or confidential business information
- Modifying or deleting data in any system
- Uploading malicious code, backdoors, or persistent access mechanisms
- Attempting to pivot from a discovered vulnerability to access additional systems or data
- Spam or unsolicited bulk messaging
- Sharing access credentials, vulnerability details, or proof-of-concept code with third parties
- Public disclosure of vulnerabilities before coordinated disclosure has been agreed upon

---

4. Legal Position

When security researchers comply fully with this policy, Relution commits to:

- Not pursue civil legal action against researchers for activities conducted in accordance with this policy
- Not refer researchers to law enforcement for activities conducted in accordance with this policy
- Work in good faith with researchers who report vulnerabilities to us
- Provide confirmation of authorization upon request for researchers who wish to document their authorized status before commencing testing

This policy constitutes authorization from Relution as the operator of the systems described in Section 2.1. We have established this policy in good faith to protect researchers acting in good faith.

However, this policy cannot and does not guarantee immunity from criminal prosecution. We strongly encourage researchers to document their activities thoroughly and request written confirmation of authorization from us before beginning testing if they have any concerns.

---

5. Use of Personal Data

The personal data transmitted in the context of reporting vulnerabilities is used exclusively for the purpose of investigating and remedying the vulnerability and is subject to the data protection regulations in accordance with the General Data Protection Regulation (GDPR) and the German Federal Data Protection Act (BDSG).

6.1 How to Report

For version 26.4.0

Please submit vulnerability reports via PGP-encrypted email to: security@relution.io →

Our PGP public key is available at keys.openpgp.org →. The key fingerprint is: `3594163819E19D4D9FDA35F78BDAB6171E0A12DF`.

We also maintain a security.txt →.

6.2 What to Include

To help us understand and address the issue efficiently, please include:

- Description of the vulnerability and its potential impact
- Affected system(s): URLs, application names, version numbers where applicable
- Step-by-step reproduction instructions
- Proof of concept: screenshots, logs, or code samples that demonstrate the vulnerability (without including real user data)
- Assessment of severity and potential impact
- Contact information for follow-up questions (may be pseudonymous, if preferred)
- Any sensitive data encountered: if personal or confidential data was inadvertently accessed, describe what was seen without including the data itself

Please submit reports in German or English.

6.3 What Not to Include

- Do not include actual customer data, personal data, or credentials in the report
- Do not attach malicious payloads or functional exploit code that could cause harm if mishandled

---

7. Response and Disclosure

Upon receiving a report, we will acknowledge receipt within five business days and start to validate and triage the reported vulnerability.

Please allow us reasonable time to address the vulnerability: We request a minimum of 90 days from the initial report before public disclosure. This allows us to validate and remediate the issue, verify the fix, and roll it out to all systems and customers.

We might request additional information through the established channels, and will keep researchers informed about the progress of the investigation and remediation.

If the vulnerability has been confirmed, an internal `RVD` identifier number will be created to identify it in communication and later Security Advisories →.

Once the vulnerability has been remediated, we will coordinate on disclosure timing and details.

---

8. Recognition and Rewards

For version 26.4.0

We do not currently operate a monetary bug bounty program. We may establish such a program in the future and update this policy accordingly.

As of today, researchers who report valid vulnerabilities in accordance with this policy are eligible for:

- Public acknowledgment on our Security Advisories page → page (with consent)
- Credit in security advisories related to the reported vulnerability (with consent)
- A letter of appreciation suitable for professional portfolios (upon request)

Appendix: Vulnerability Examples

These examples are meant to illustrate which types of vulnerabilities are in or out of scope of this policy.

Qualifying Vulnerabilities

- Remote code execution
- SQL injection and other injection vulnerabilities
- Authentication or session management flaws
- Authorization bypasses and privilege escalation
- Cross-site scripting (XSS) with demonstrated impact
- Cross-site request forgery (CSRF) with demonstrated impact
- Sensitive data exposure
- Security misconfigurations with clear impact
- Server-side request forgery (SSRF)
- Insecure direct object references

Non-Qualifying Issues

The following are generally not considered qualifying vulnerabilities:

- Vulnerabilities requiring physical access to a user's device
- Vulnerabilities in third-party applications or services
- Social engineering attacks
- Denial of service vulnerabilities (please report these, but they are not eligible for recognition under this policy due to the testing limitations)
- Issues identified by automated scanners without demonstrated exploitability
- Missing security headers without demonstrated impact
- Clickjacking without demonstrated sensitive action
- Self-XSS (user can only execute script in their own session)
- CSRF on non-sensitive functionality
- Information disclosure of non-sensitive data
- Software version disclosure without associated vulnerability
- Theoretical vulnerabilities without proof of concept
- Issues already known to us or previously reported

For version 26.4.0

Security Advisories

This page provides an overview of security vulnerabilities identified in our products, including their internal REL identifier and associated CVE identifiers (if present) and detailed disclosure information. We follow a coordinated vulnerability disclosure process → and publish full advisory details once patches are available and the disclosure window has expired. Our goal is to ensure transparency, support secure deployments, and help customers stay protected by keeping their systems up to date.

Relution is implementing a coordinated vulnerability disclosure process → starting 2026, and subsequent advisories created in the scope of that process will be published here.

Subscribe to our newsletter → to get notified about security vulnerabilities and other important information.

RVD-2026-6: Unauthenticated Access in Relution Server

Field	Value
Identifier	`RVD-2026-6`
CVE	not assigned
Affected component	Relution Server
Affected versions	up to `26.5.3`
Fixed in	`26.5.4`
Published	October 20, 2026
Status	Update available

Relution Server 26.5.4 fixes a vulnerability that may allow access without prior authentication.

We recommend that all customers with on-premises installations update to version **`26.5.4`** or later promptly.

All cloud instances operated by Relution have already been updated; no action is required for cloud customers.

Further technical details will be published here once the update has been widely rolled out.

RVD-2026-5: Brute-Force Vulnerability in Relution Server

Field	Value
Identifier	`RVD-2026-5`
CVE	not assigned
Affected component	Relution Server
Affected versions	up to `26.5.1`
Fixed in	`26.5.2`
Published	October 19, 2026
Status	Update available

Relution Server 26.5.2 fixes a vulnerability that may allow unauthorized access through automated guessing (brute force).

We recommend that all customers with on-premises installations update to version **`26.5.2`** or later promptly.

All cloud instances operated by Relution have already been updated; no action is required for cloud customers.

Further technical details will be published here once the update has been widely rolled out.

For version 26.4.0

RVD-2026-4: Database Access Vulnerability in Relution Server

Field	Value
Identifier	`RVD-2026-4`
CVE	not assigned
Affected component	Relution Server
Affected versions	up to `26.5.2`
Fixed in	`26.5.3`
Published	October 16, 2026
Status	Update available

For version 26.4.0

Relution Server 26.5.3 fixes a vulnerability that may allow authenticated users unauthorized access to database contents.

We recommend that all customers with on-premises installations update to version **`26.5.3`** or later promptly.

All cloud instances operated by Relution have already been updated; no action is required for cloud customers.

Further technical details will be published here once the update has been widely rolled out.

RVD-2026-3: Code Execution in Relution Server

Field	Value
Identifier	`RVD-2026-3`
CVE	not assigned
Affected component	Relution Server
Affected versions	up to `26.5.2`
Fixed in	`26.5.3`
Published	October 16, 2026
Status	Update available

Relution Server 26.5.3 fixes a vulnerability that may allow authenticated users to execute code under certain circumstances.

We recommend that all customers with on-premises installations update to version **`26.5.3`** or later promptly.

All cloud instances operated by Relution have already been updated; no action is required for cloud customers.

Further technical details will be published here once the update has been widely rolled out.

For version 26.4.0

RVD-2026-2: Permission Issue in Relution Server

Field	Value
Identifier	`RVD-2026-2`
CVE	not assigned
Affected component	Relution Server
Affected versions	up to `26.5.2`
Fixed in	`26.5.3`
Published	October 16, 2026
Status	Update available

Relution Server 26.5.3 fixes a vulnerability that may allow authenticated users unauthorized access.

We recommend that all customers with on-premises installations update to version **`26.5.3`** or later promptly.

All cloud instances operated by Relution have already been updated; no action is required for cloud customers.

Further technical details will be published here once the update has been widely rolled out.

For version 26.4.0

RVD-2026-1: Permission Issue in Relution Server [REL-13078]

Field	Value
Identifier	`RVD-2026-1`
CVE	not assigned
Affected component	Relution Server
Affected versions	`5.32` - `26.4.1`
Fixed in	`26.4.2`
Published	August 13, 2026
Status	Update available

For version 26.4.0

Relution Server 26.4.2 fixes a permission issue that may affect authenticated users.

We recommend that all customers with on-premises installations update to version **`26.4.2`** or later promptly.

All cloud instances operated by Relution have already been updated; no action is required for cloud customers.

Further technical details will be published here once the update has been widely rolled out.

Security optimization

Relution is a powerful tool with which users sometimes have extensive authorisations on managed devices. The system should therefore be optimally protected against unauthorised access. The Relution portal can be optimised in terms of security at various points with built-in functions. Added to this is the targeted distribution of necessary authorisations.

Use a secure password

If a new user account is created in Relution, a complex password is suggested here. This can be accepted or changed. In any case, make sure the password complies with the complexity recommendation of the BSI →.

Add a second factor for authentication

Relution supports login with a second factor. Users must configure this themselves for their own account. To do this, click on the user name > Profile at the top right. An MFA token for an authenticator app or email verification can be stored there. Be sure to use this function!

For version 26.4.0

Use access token

In Relution, an access token for using the API can also be stored in the user account profile. This token offers the advantage that no username/password combination needs to be stored in plain text in scripts. In addition, the token can be given an expiry date to ensure that it is not active for longer than is really necessary.

Configuring IP Access Rules & Fail2Ban

In the Global Organisation, both IP access rules and Fail2Ban can be configured under `Settings` → `System Security`.

This allows defining rules such as blocking an IP address for a certain period after a number of failed login attempts (e.g. 10).

IP access rules generally control from which IP addresses or networks a login is allowed or blocked. Both single IPs and entire ranges can be defined.

> Before configuring, it should be verified which IP address is used to connect to the server, to avoid an accidental lockout.

Meaning of status values

Allowed

- Login is currently possible
- Is automatically set as soon as a login attempt occurs (even if unsuccessful)
- Mainly used for visibility and logging

Permanently allowed

- IP address is explicitly whitelisted
- Takes precedence over other rules
- Remains permanently active
- Recommended for trusted locations (e.g. office or VPN)

Blocked

- IP address is temporarily blocked
- Can be unblocked at any time

Permanently blocked

- IP address is permanently blocked
- No login possible anymore
- Useful for clearly unwanted access attempts

For version 26.4.0

Use of IP ranges

The so-called CIDR prefix defines how large the IP range is that a rule applies to.

Prefix	Meaning
`/32`	Exactly one single IP address
`/24`	A typical network (e.g. company network)

Basic rule:
The smaller the number, the larger the covered IP range.

CIDR examples

- `192.168.1.10/32`
  → Affects exactly one single device
- `192.168.1.0/24`
  → Affects all devices from `192.168.1.1` to `192.168.1.254`

Example: Block everything except allowed IPs

Define trusted IPs

- Define own or known networks
- Configure them as “Permanently allowed”
- Examples:
  - Office network
  - VPN access

For Version 26.4.0

Create global block rule

- Create a rule covering all remaining IP addresses
- Example: `0.0.0.0/0` (covers all IPs worldwide)
- Status: “Permanently blocked”

> Before activating the global block rule, make sure that the IP address used to connect is correctly set as permanently allowed.

Security optimizations for enrollments

The link and QR code of an enrollment act like an access key: as long as the enrollment is valid, it can be used to enroll a device in Relution. The device then receives the policies and rulesets linked to the enrollment – which may include Wi-Fi credentials, certificates or access to company services. Open enrollments should therefore be kept to a minimum.

- Keep the validity short: When an enrollment is created, Valid until is set to seven days in the future by default. The period should not be longer than actually required for the planned enrollment. If the time is not sufficient, enrollments that have not yet been used can be extended later via Extend Enrollments – long validity periods as a precaution are therefore not necessary.
- Prefer single-use enrollments: By default, each enrollment can only be used for a single device. A Multi-use enrollment, on the other hand, allows any number of devices to be enrolled until the expiration date, limited only by the available licenses. It should therefore only be used specifically for larger rollouts and combined with a particularly short validity.
- Delete enrollments that are no longer needed: Open enrollments that are no longer required – for example after a rollout has been completed or if a device is not enrolled after all – should be deleted under `Devices` → `Enrollments`. Devices that have already been enrolled via a multi-use enrollment remain enrolled. For Android Enterprise, the associated enrollment token is also deleted at Google, so the QR code no longer works.
- Do not share links and QR codes publicly: Enrollment links are only sent to the intended recipients and are not published on the intranet, in wikis or via large mailing lists. Printed QR codes are destroyed after the rollout.
- Review enrollments regularly: The list under `Devices` → `Enrollments` shows, based on status and Valid until, which enrollments are still open. In addition, the device inventory should be checked for unexpected devices.
- macOS: profile removal password: For macOS enrollments, Use profile removal password can be enabled. The MDM profile can then only be removed from the device with an automatically generated password.

Manage permissions

Relution offers twelve authorisation preconfigurations as standard. Check which functions are active in which authorisation preset. To do this, click on `Users` → `Permissions` and pay attention to the entries that have been created by the system. These roles cannot be edited. However, new authorisations can be created at any time, enabling the necessary functions for individual users on a fine-grained basis. The authorisations correlate with the user groups created by Relution.

For version 26.4.0

Create organizations

Relution is multi-tenant, meaning a realistic representation of school or company structures is possible. After installation, the first login occurs at the global organization level. From there, additional tenants can be created.

This article explains step by step which actions need to be taken and what to pay special attention to.

Creating an Organization

1. Log in with the created administrator `admin` and the system password.
    - On a user's first login, the EULA must be accepted.
2. In the Global organization, navigate in the sidebar to `Organizations` → `Add`.

General Information

- Organization data
    - If the organization, company, or institution is not listed, select the nearest available address.

For version 26.4.0

Organization

- Name
    - Used for general display in Relution and can be changed later.
- Unique organization identifier
    - Cannot be changed later (relevant to the database).
- Organization Type
    - Defines whether the organization is created as a standalone organization (Standalone), as a Meta Organization (Meta) or as a sub-organization of an existing Meta Organization (Sub). For Sub, the parent Meta Organization is selected as well. Details under Meta Organizations →.
- Sender address
    - The email address the server uses as the sender when sending emails (e.g., when creating new enrollments or when certificates expire).
- Reply-to address
    - Optional address inserted into the Reply-To field. If a user replies to a registration email, this address will be used as the recipient instead of the original sender (depending on the mail client).

Management

- Manage members
  - Add existing members to the organization.
- Create administrator
  - Create a new administrator for this organization.

Summary

A summary of all entered or selected items is displayed.

Licenses

- Without a limit, the created organization can use all licenses of the global instance until they are exhausted.
- The limit can be set, removed, or adjusted later. → Menu `?` → `License Information` (top right next to the username).

For version 26.4.0

Manage Apple devices

The operating systems iOS, macOS and tvOS were developed exclusively for Apple devices. Relution provides a set of features to configure and control Apple devices. Here, one can learn more about how to get started managing Apple devices.

Certificates

New in 26.3

Before enrolling Apple devices, make sure that an APNS (Apple Push Notification Service) certificate is configured on the server.

As of Relution 26.3.0, new installations must provide their own APNS certificate before devices can be enrolled. The self-service wizard in `Settings` → `Organization Certificates` guides through the setup. Instances already running before this version continue to operate with a certificate provided by Relution for now.

Set up APNS push certificates →

Enrollment

To be able to manage an Apple device, it must be enrolled in Relution. To do this, a so-called MDM profile is installed on the device. Three different types of enrollment are available for Apple devices.

For version 26.4.0

iOS enrollments →
macOS enrollments →
tvOS-enrollments →

Supervised Mode

Supervised Mode allows to distinguish Apple devices owned by the employer from personal devices. We recommend putting the devices into Supervised Mode for unrestricted management and use of all MDM features. This allows restrictions to disable many features not needed for use in a school or work environment. To learn more about putting the Apple device in this mode, one has to click on the link below.

DEP devices are always supervised. Add devices to DEP using Apple Configurator →

Relution Agent

Relution Agent is always automatically installed on Apple devices during enrollment. It is not necessary for device manageability, but provides a variety of additional useful features for users.

It is recommended to have a sufficient number of device-based VPP licenses for the app available, in this case the installation can run without any user interaction. Otherwise users need to login in with their Apple accounts in the App Store, so no VPP licenses are required for app installation.

Separate business and personal data

`Managed Apps` Apps that are deployed to Apple devices through Relution are called managed apps. One can retain control over these apps and can remove them and their associated data as needed. For iOS and macOS devices, one can configure managed apps through the Managed App policy configuration.

`Managed Accounts` For iOS and macOS devices, Relution lets set up email and other accounts and manage them independently of personal accounts. With Relution, the following accounts can be configured:

- Email
- Exchange
- CardDAV
- CalDAV
- Subscribed calendars
- Google Accounts (iOS devices only/).

Data separation takes place within the operating system for Apple.

Manage apps

For version 26.4.0

The apps which are wanted to be used on the Apple devices, should be selected and the apps that are not relevant should be blocked or removed. A large number of Apple devices can be managed, distributed and removed efficiently on a large number of Apple devices at the same time.

App Management →

App Licenses

Every app that is installed on Apple devices through the Public App Store must be licensed. It does not matter if the app is free or not. The license can be obtained either via the user currently logged in via Apple ID or, if working without Apple IDs, via the Apple Volume Purchase Program (VPP). For VPP, access to an Apple School/Business Manager is required. For native apps, this is not necessary.

One can install the apps on Apple devices without users manually initiating the installation, as long as the Apple devices are monitored, i.e. in supervised mode.

App installation without user input →

VPP (Volume Purchase Program) apps can be installed on Apple devices that are supervised without user input. Learn more about VPP:

VPP setup in Relution →
Roll out VPP apps →

Block or positive list for iOS and tvOS

The block or positive list feature in Relution allows administrators to block certain apps on iPhones, iPads, and Apple TVs and allow installation of important apps. This feature prevents the installation of unwanted apps and hides installed apps that are already on devices from users if necessary. Click on the link below to learn more about blocking or allowlisting apps.

App compliance for iOS →
App compliance for tvOS →

Single App Mode for iOS

Single App Mode can be enabled on iPhones and iPads, restricting devices to a single app and blocking all others. It should be noted that the devices must be monitored (supervised) to enable single app mode.

Single App Mode for iOS →

Web link

The webclip looks like an app icon that links to a website when clicked. Just a label and an URL have to be specified.

Add weblinks via policy →
Add web links and place via homescreen layout for iOS →

For version 26.4.0

Protect MDM profile from deletion

Prevent removal of MDM profile from device settings by enrolling devices through Apple Device Enrollment Program (DEP).

Profile for ADE →
Auto enrollment →

Network configuration and security

Maximum network security can be achieved by setting up appropriate configurations. With Relution, WiFi settings can be configured for all Apple operating systems. In addition, VPN (Virtual Private Network) and per-app VPN settings can be configured for iOS and macOS devices. Cellular (Access Point Network) settings can be configured for iOS devices.

Restrictions

The policy configuration of restrictions limits Apple devices in functionality. It is important to note the type of enrollment, as many restrictions only take effect on supervised devices (supervised).

Go to restrictions →

System updates

One can update Apple devices to the latest operating system version if the devices are supervised.

Administrators can also defer updates for supervised devices for up to 90 days. During this period, users will not be prompted to update devices to the latest OS version. This allows organizations to check for errors/problems or to check the compatibility of deployed applications with the latest OS versions.

Restrictions →

Content filtering

The web content filtering feature can be used to prevent access to specific web pages in the organization.

Content Filter →

Homescreen Layout for iOS

The apps can be arranged on the homescreen of the iPhone or iPad as well as in the Dock, and be placed in folders that can be created manually or automatically.

Homescreen Layout for iOS →

For version 26.4.0

Manage Android Enterprise

Android Enterprise is an initiative by Google, aimed at improving the management and security of Android devices in enterprises. It is a set of tools, APIs, and services that enable enterprises to manage Android devices more efficiently and ensure the security of enterprise data on those devices.

Prerequisite

Before Android devices can be enrolled via Android Enterprise, the Relution organization must first be linked to a Google organization. The link is established under `Settings` → `Device platform specific` → `Android Enterprise`.

Link Organization →

Enrollment

Multiple enrollment options are available for Android Enterprise. Devices can be enrolled manually, via a QR code, or automatically via Android Zero Touch or, for Samsung, via Knox Mobile Enrollment (KME).

KME → and Zero Touch →
Enrollment types →
Enrollfully-managed-device →
Work-profile →
Fully-managed device with personal profile →

For version 26.4.0

Relution Agent and Relution Companion

Relution Agent and Relution Companion are always automatically installed on Android Enterprise devices during enrollment. Both are not mandatory for device manageability, but provide a variety of additional useful features for users. With Relution Companion for Android Enterprise, it is possible to install certificates on the devices and perform device location.

Separate business and personal data

Android Enterprise offers excellent options for separating business and private data. Here, the user can work with a `Work Profile`, which can be installed on private devices. Alternatively, a personal profile can be activated on fully managed devices, in which users can log in with a private Google account and use the device privately without almost any restrictions, without private and business content getting mixed up.

Manage apps

Android Enterprise does not allow native apps to be installed on devices. All apps must come from the Managed Google Play Store. Custom APKs can be uploaded there and made available in the organization as long as the app's package name is unique to Google.

Manage apps →

> There is currently no way to distribute paid apps with Android Enterprise.

Configuration can also be stored via the app management. These are for pre-configuring individual apps to roll out mail profiles or other settings, for example. The possible configurations have been built in by the app manufacturer. We cannot provide any support here in the event of any malfunctions.

Homescreen Layout and Kiosk Mode

With the Homescreen Layout policy, Relution offers the activation of the Kiosk Mode with a launcher specially developed by Relution. This allows the installation of a wallpaper as well as the arrangement of apps on the homescreen or in folders.

Kiosk Mode →

For version 26.4.0

Restrictions

On Android Enterprise devices, many restrictions can be enabled with Relution.

> It is possible to make devices permanently unusable with restrictions. For example, a ban on a factory reset cannot be overridden.

Restrictions →

Runtime permissions

The runtime permissions can be used to allow users to answer permission questions. Standard but user-defined permissions can be configured here.

Runtime permission management →

Manage Windows devices

In Relution, devices with Windows 10/11 can be managed. Depending on the variant, different functions are available. The largest range of functions is available with Pro, Education or Enterprise licenses. In contrast to domain policies, Relution can perform actions and apply policies on Windows devices even if they are not in the local network. Here, an Internet connection is sufficient.

Enrollment

Windows devices can be enrolled in three different ways.

Manual Enrollment →
Bulk Enrollment →
Auto Pilot Enrollment →

Auto Pilot requires a P2 Premium license in Microsoft Azure.

> For manual enrollment and bulk enrollment, the user must have administrative privileges.

For version 26.4.0

Relution Companion

Relution Companion is always automatically installed on Windows devices during enrollment. However, this does not work on this variant due to limited features in Windows Home. The Relution Companion allows running Powershell scripts and installing MSI and EXE files.

Windows Companion →
Windows Home Limitations →

Manage apps

Relution allows apps from the Windows Store and native apps from the Relution App Store to be installed on Windows devices. Native apps must be uploaded to Relution and configured, depending on the format. MSIX- files must be self-created and signed with a certificate to allow installation. EXE and MSI files require installation and uninstallation parameters. These can be found either on the vendor's website or on tech blogs.

Create MSIX files→
Use EXE and MSI files in Relution →
SilentinstallHQ →

Figuring out the correct configuration parameters is often a time-consuming procedure. Relution support can only provide very limited support here.

Certificates

Certificates can be loaded directly onto the Windows device via the corresponding policy configuration. Here, it is also possible to select the appropriate certificate store.

Certificates →

Restrictions

On Windows devices, many restrictions can be activated with Relution. Here, one can define whether the MDM profile can be removed by the user or whether the computer can be reset.

Restrictions →
Protect MDM profile →

Other configurations

There are other configurations available, for example WLAN and VPN profiles, kiosk mode and configuration for Windows Shared PC.

For version 26.4.0

Manage whiteboards

The use of Android-based whiteboards is increasingly popular in schools, companies, and other organizations. To manage these devices efficiently, Relution provides a comprehensive solution specifically designed for the centralized management of Android whiteboards from various manufacturers.

Manufacturer-Dependent Functionality

The functionality for managing whiteboards depends on the endpoints provided by each manufacturer. These endpoints determine which control and configuration options can be used via Relution.

Examples:

- Specific settings
- Firmware updates
- Security policies

Available functions depend on the features supported by each manufacturer.

For version 26.4.0

Easy Integration via Android Classic

Whiteboards can be manually enrolled into the Relution platform. This is done using the Relution Companion, which guides devices through step-by-step enrollment.

Once successfully registered, the full functionality of Relution becomes available. Configurations and policies can be flexibly set up and applied to the devices via the platform.

Wide Support for Numerous Manufacturers

A variety of manufacturers are already supported by Relution. A complete list of currently compatible manufacturers can be found Android Classic Integrations →.

The list is continuously updated as additional manufacturers are integrated.

Advanced Options with Android Enterprise

In addition to Android Classic whiteboards, Relution offers advanced options via Android Enterprise.

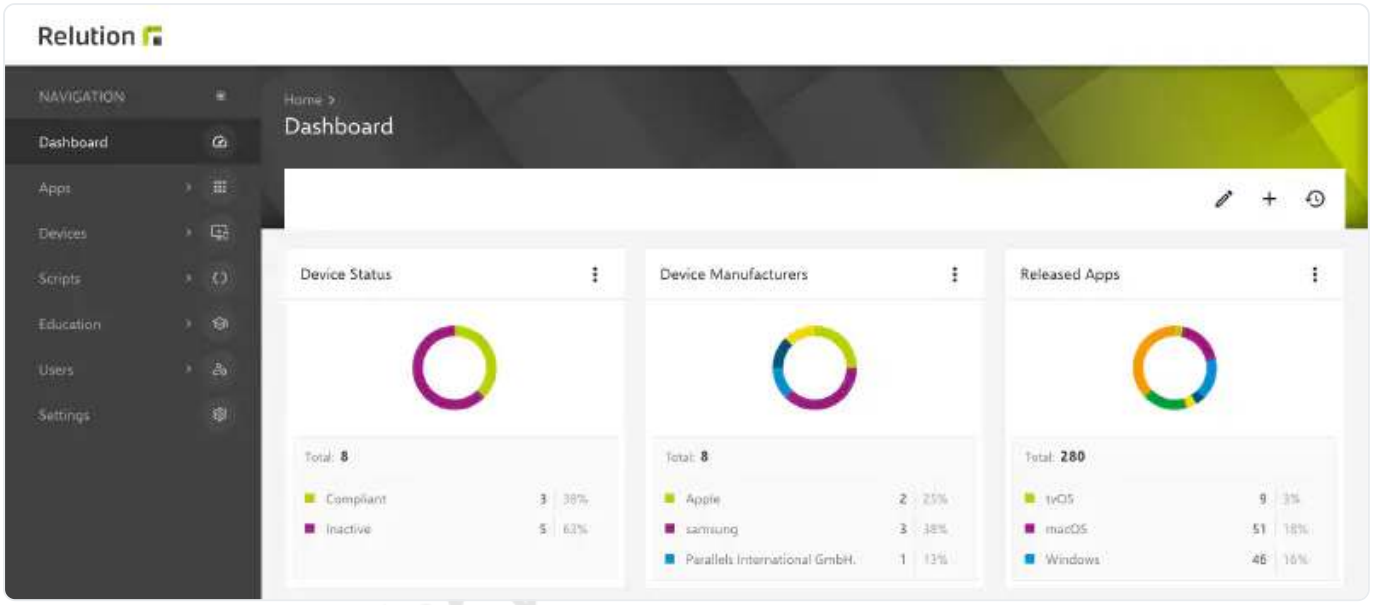
This platform provides additional, standardized functions for comprehensive device management. Relution extends the Android Enterprise capabilities specifically for interactive whiteboards, combining standard features with manufacturer-specific whiteboard functions.

A full overview of the available Android Enterprise extensions can be found EDLA Extensions →.

Dashboard

The dashboard is the start page of the Relution portal and summarizes the current state of an organization: devices, apps, policies, enrollments, certificates and the system status are presented as tiles. The page is reached through Dashboard in the side navigation.

The individual tiles are referred to as widgets. Each widget shows one evaluation as a chart, a table or a status overview. The scope of the dashboard is not fixed: widgets can be added, adjusted, moved and removed.



One shared dashboard per organization

A dashboard belongs to the organization, not to an individual user account. Layout changes as well as added or deleted widgets are therefore visible to all users of that organization. A personal dashboard visible to a single account only is not available.

When the tenant is switched, the dashboard of the active organization is loaded. The values shown always refer to the organization the session is currently working in.

> Because the dashboard applies organization-wide, deleting a widget and restoring the default dashboard affect all users of the organization as well.

Default dashboard

Without any customization, a preconfigured default dashboard is provided. Which widgets it contains depends on the type of organization.

Present in every organization are Device Status, Device Manufacturers, Device Models, Operating Systems, Devices, Device Ownership, Devices in roaming mode by country, Policies, Released Apps, Certificates, System certificates and Knox Service Plugin Feedback.

Depending on the organization, further widgets are added:

- Open Enrollments — in every organization except the global organization.
- Organizations — in organizations with sub-organizations as well as in the global organization.
- Health Status — in the global organization only.

As long as the default dashboard is unchanged, the restore action is disabled and a note points out that the default dashboard is already in use. Once the layout has been saved or a widget has been changed, the result becomes the organization's own dashboard.

Customizing the layout

The Reorder widgets icon (pencil) activates the editing mode. In this mode widgets can be moved and resized with the mouse; the grid rearranges the remaining tiles automatically.

Changes are applied through Save Dashboard Changes and discarded through Deny Dashboard Changes. Both actions are confirmed in a dialog, because the result applies to all users of the organization. When no change is pending, a note on the save icon points out that there are no changes to save.

For version 26.4.0

Adding widgets

Add new Widget opens the Create Widget dialog. It is divided into the Select Chart Type area for custom evaluations and the Predefined Widgets area for fixed tiles.

Custom widgets based on metrics

The form of presentation is the starting point. The Select Chart Type area offers Bar Chart, Stacked Bar Chart, Pie Chart and Table Chart.

After the selection, the widget form opens with the Widget Configuration section. All fields shown there are required:

- Name — the label of the tile.
- Entity — the data source: Devices, Apps, Device Groups, Enrollments or Policies. Only those entities are selectable for which the current user account holds a read permission; the remaining ones do not appear in the list.
- Field — the attribute used for grouping, for example operating system or manufacturer. This field is omitted for table charts.
- Display entities by — for the stacked bar chart only: the second attribute the series are derived from. It has to differ from Field.
- Columns — for table charts only: the selection of the displayed columns.

The Metric Filter section allows the data basis to be restricted further, for example to one platform or one device status.

The Preview button shows the result of the configuration next to the fields before it is saved; a name is not required for this. If the selected combination returns no values, a note above the fields states that no suitable data was found.

Predefined widgets

The Predefined Widgets area provides evaluations that cannot be expressed through the metric configuration:

- Health Status — availability of the Relution system components, shown as Up or Down.
- Organizations — overview of the accessible organizations, from which the tenant can be switched.
- Knox Service Plugin Feedback — feedback from the Knox Service Plugin.
- System certificates — expiration date of the organization's APNs push certificate for managing Apple devices and of the built-in push certificate of the Relution Agent (see APNS Push Certificates →).

Only those predefined widgets are offered for which the required read permissions exist (see Permissions). Their evaluation is fixed and cannot be adjusted through the widget form. Each type can be placed on the dashboard only once; a tile already in use is disabled in the dialog and marked as Already added.

Editing, refreshing and removing widgets

Every tile provides a Widget options menu. It contains Delete, Edit and Refresh: Refresh reloads the widget's data, Edit opens the configuration in the widget form, Delete removes the tile from the dashboard. For predefined widgets and the Certificates widget, Edit is omitted because their evaluation is not configurable. Delete and Edit are only shown with the permission to update dashboards; on the default dashboard, the permission to create dashboards is required as well. The menu is not available in editing mode, nor for widgets whose data is not covered by a read permission.

Removal is confirmed in a dialog. Widget and configuration are deleted permanently and for all users of the organization; restoring an individual widget is not possible. The Certificates widget is not offered in the Create Widget dialog; once deleted, it can only be brought back by restoring the default dashboard.

For version 26.4.0

Restoring the default dashboard

Restore default Dashboard brings back the initial configuration. All customized widgets are deleted permanently. This action cannot be undone either and affects all users of the organization.

Navigating from widgets to the lists

Widgets are linked to their corresponding overviews. Clicking a chart segment opens the matching list — the Inventory overview →, for example — and applies the selected value there as a filter or as a search term. For a stacked bar chart, both attributes of the clicked segment are carried over. In table widgets, clicking a row opens the detail page of the respective object, provided a detail view exists for that data type. In the Certificates widget, clicking a row opens the certificate list with the certificate name as search term.

This navigation is disabled in editing mode so that moving a tile does not accidentally trigger a page change.

If a widget returns no data, the tile offers a matching button next to the note, for example Create Enrollment, Create Device Group, Create Policy, App Store or, in the Certificates widget, Add Certificate. The button is only shown with the permission for the respective action.

Permissions

Access to the dashboard and its customization is controlled by the permissions in the Dashboard section:

- Displaying the dashboard requires the Read permission.
- Editing the layout, saving changes, adding widgets as well as editing and deleting individual widgets require the Update permission.
- While the default dashboard is active, the first customization creates the organization's own dashboard. The Create permission is additionally required for this step.
- Restoring the default dashboard requires the Delete permission.

If one of these permissions is missing, the corresponding icon in the header is disabled and a note on it names the missing permission. Without any of the Create, Update and Delete permissions, the header is not shown at all. Assigning permissions is described in the article Permissions →.

Independently of this, widgets only display data covered by a read permission. Where this is not the case, a note is shown instead of the evaluation, recommending that the required permissions be requested from the administration; for custom widgets, it names the affected entity.

Each predefined widget requires a read permission of its own. It determines whether the widget is offered in the Create Widget dialog and whether it displays data on the dashboard:

26.4.0

Widget	Required permission
Health Status	Read in the System Health section (global organization only)
Organizations	Read in the Organizations section (global organization) or Sub-Organizations (meta organization)
Knox Service Plugin Feedback	Read in the Policies section
System certificates	Read in the Organization Certificates section

Limitations

The following limits apply when planning a custom dashboard:

- One dashboard per organization. User-specific dashboards within the same organization are not possible.
- Limited number of widgets. By default, 30 widgets are allowed per dashboard. Once the limit is reached, a note on the add icon states the current and the maximum number.
- Limited number of filters per widget. By default, 20 filters are allowed per widget. If the filter configuration exceeds this value, the widget cannot be saved until filters have been removed.
- Predefined widgets are immutable and can be added only once each.
- Knox Service Plugin Feedback requires a configured Android Enterprise connection; otherwise the widget remains without data.
- Organization scope of the data. The data of the active organization is evaluated.
- Deletions are final. Neither a removed widget nor a dashboard replaced by a restore can be brought back.

Both numeric limits are default values and can be adjusted on the server. In an installation configured differently, the notes in the portal state the values that apply there.

For version 26.4.0

Agent

The Relution Agent monitors the compliance status of each device, provides apps via the Relution Store, and supports multi-user mode (iOS) across various devices. These comprehensive features enable smooth and centralized management of all devices, whether in schools or demanding enterprise environments.

Through seamless integration, the Relution Agent creates an efficient platform that optimizes both security and productivity in mobile device management.

Relution Agent for iOS

The Relution Agent is automatically installed on all managed devices and serves as the central application for Mobile Device Management (MDM) features. A key security measure is that the Relution Agent cannot be removed from the device by the user as long as the MDM profile is installed. This ensures constant presence and reliability of MDM functions.

> The Relution Agent app is part of the Relution platform and can only be used with the Relution backend component and appropriate credentials. Installation should be coordinated with the IT administrators of the organization.

For version 26.4.0

App Features

- Display device compliance status
- Install and update relevant apps
- Uninstall unnecessary apps
- View, request, and add apps and web links
- Relution Shared Device (for multi-user devices)
- iBeacon, GeoFence, and zone detection
- Display messages from the MDM system on the device
- Device login via QR code / MFA token
- Display device information
- Enable push notifications
- Enable biometric authentication for device login

Portal Notices

For iOS devices, two agent-related notices may appear in the portal, visible in the device's policy view in the Device Default row:

1. `Relution Client App bounding` – `Relution Agent is not installed`
2. `Push service` – `Push must be enabled for the Relution App`

The `Relution Client App bounding` notice is resolved once the Relution Agent is installed and appears in the device's list of installed apps. If the app is missing, Relution automatically triggers its installation again at the next device update. The `Push service` notice is resolved by opening the Relution Agent app and allowing notifications. Relution removes resolved notices from the view.

Relution Agent for Android Enterprise

The Relution Agent is an integral part of the Relution platform and only usable with the Relution backend component. It is automatically installed on all managed devices and serves as the central application for MDM features. It is protected against uninstallation, and Relution automatically preconfigures it with the device's connection data.

App Features

- Display device compliance status
- Install and update relevant apps
- Uninstall unnecessary apps
- Display available apps from the Google Managed Play Store
- Display messages from the MDM system on the device
- Device login via QR code / MFA token
- Display device information
- Enable push notifications
- Enable biometric authentication for device login

Relution Agent for Windows

The Relution Agent for Microsoft Windows provides basic functionality and is available in the Windows Store. Users with the required permissions (at least `Appstore User`) can view Windows apps provided by the administrator via the Relution portal. Administrators can manage app requests. If the Agent is distributed from the Store via Relution, Relution automatically writes the connection configuration to the device registry (`HKLM\SOFTWARE\Relution\Relution Agent`).

For version 26.4.0

Relution Agent for macOS

With Relution 5.25.0 →, the Relution Agent was released for macOS. This allows providing information directly to users of managed devices.

As with iOS, the Relution Agent can be installed from the App Store. On managed macOS devices, Relution installs the Relution Agent automatically if licenses for the app are available via Apps and Books (VPP in the portal). If the Agent is later missing from the device, Relution installs it again. Without such licenses, Relution does not install the Agent on macOS automatically.

App Features

- Display device compliance status
- Install and update relevant apps (managed devices)
- Display messages from the MDM system on the device
- Display device information
- Enable push notifications

Installing Apps via the Relution Agent

To install and display apps via the Relution Agent, a user must be assigned to the device. This user can be a dummy user if only the app functionality is required.

The user must be a member of the system group `[ORGA] Appstore User` or `[ORGA] Device Manager`, either directly or through a group that is itself a member (e.g. Teacher, Developer, App Reviewer, Content Manager, Administrator). Alternatively, an appropriate permission can be created and assigned.

Which apps appear in the Agent is determined by the permissions of each app; group membership alone is not sufficient. By default, new apps contain the Appstore User and Device Manager groups in the User role. If a custom template is active under `Settings` → `App Store`, its groups apply (App Store Default Permissions →). Members of the `[ORGA] Student` group only see apps in the Agent if they are also members of Appstore User or are entered in the app's permissions.

New Users

User Management → During creation, the user can be assigned directly to a group or permission.

Existing Users via System Group

Members are assigned to the `Appstore User` group under: `Users` → `Groups` → `[ORGA] Appstore User` ([ORGA] = Unique name of the organization in upper case)

Existing Users via Permission

Permissions →

For Version 26.4.0

Companion & Daemon

The Relution Companion App is available for various platforms. It not only expands functionality but also simplifies the smooth setup of devices. As a connecting element, the app creates a functional bridge between operating systems and the Relution platform.

On macOS devices, this role is handled by the macOS Companion. On the Mac, it runs as the Relution Daemon service.

The versions of the companion apps installed on the devices are shown under `Settings` → `Relution Client Apps`. The macOS Companion (switch Enable macOS companion) and the device user change of the Windows Companion (switch Enable device user change) are also switched on and off there.

Companion for Android (Legacy)

Android Legacy is an older method for managing Android devices, previously known as `Device Administrator`. For enrollment and configuration of Android Legacy devices, the Relution Companion is essential: it is installed from Google Play or as an APK before enrollment, and the enrollment itself runs through it, see Manual enrollment →.

The app not only expands functionality but also provides core Mobile Device Management (MDM) capabilities. This integration allows for seamless management of older Android devices, improving usability and efficiency.

If the option Withdraw Android legacy devices in case the device administrator permission is not granted is enabled under `Settings` → `Device Management`, Relution removes the Companion and thus the management if the device administrator permission is not granted or is revoked later. The option has no effect on Android-based whiteboards.

For version 26.4.0

> With the introduction of more advanced approaches such as Android Enterprise, the Legacy model is no longer considered the preferred method for managing Android devices.

Companion for Android Enterprise

The Relution Companion for Android Enterprise is installed automatically during enrollment and is mandatory for the enrollment process. Its installation type cannot be overridden in the policy.

The Companion expands device capabilities with additional features, such as the location tracking of lost devices.

Furthermore, it enables the distribution of certificates to devices via the Relution Portal (see Certificate →). Relution also uses the Companion to set the Wallpaper → and to provide the root certificate for Relution Decon (content filter) →.

Companion for Windows

The Relution Companion for Windows is an exclusive Windows service that is automatically installed on all Windows devices managed by Relution, except devices running Windows Home Edition and devices whose edition is not recognized (see Windows Companion →).

Unlike standard applications, it is not available in the Windows App Store or the Relution App Store. Equipped with administrator rights, the Relution Companion is designed solely for administrators and operates silently in the background, without direct interaction with end users.

When configuring Windows devices, Configuration Service Providers (CSPs) are typically used to provide access to specific Windows system settings. While useful, these CSPs have certain limitations in configuration options.

The Relution Companion for Windows overcomes these limitations by significantly extending the configuration options, allowing for more comprehensive customization.

The behavior of the Companion (including log level, time limits for actions and app installations, server communication and user change on login) is controlled via the Windows Companion policy configuration, see Configure Companion →.

Companion for Whiteboards

Depending on the management type, Relution provides dedicated companion apps or extensions for whiteboards.

For version 26.4.0

Android Classic

Thanks to the Relution Companion, it is possible to efficiently manage Android-based whiteboards from different manufacturers. This is done through the manual enrollment of the devices via the Relution Companion.

After enrollment, the whiteboards can be centrally managed through policies and actions in Relution.

The available functionality depends on the endpoints provided by each manufacturer.

An overview of all Android Classic integrations is available under Manufacturers →.

Android Enterprise

Relution also provides the ability to manage interactive whiteboards via Android Enterprise. To use the additional whiteboard features, one of the EDLA extensions is required.

An overview of the EDLA extensions is available under EDLA extensions →.

macOS Companion (Relution Daemon)

The macOS Companion (installed on the device as Relution Daemon) was specifically designed for macOS devices to enable the execution of scripts and the installation of .dmg files.

The daemon is installed automatically as soon as a device is enrolled. Requirements:

- Enable macOS companion is switched on under `Settings` → `Relution Client Apps` (default: enabled).
- The Mac runs macOS 12 or later.
- The Mac is not user-enrolled (User Enrollment).

On other Macs, scripts cannot run and .dmg files cannot be installed. If the option is disabled, the daemon is uninstalled from all enrolled Macs.

If the macOS Companion is missing on a Mac that meets these requirements, Relution records a compliance violation for the device with the notice `The MacOS companion is not installed!`.

The Script policy configuration and the Execute shell script action are only available when the macOS Companion is enabled, see Overview → and Install native macOS apps →.

For version 26.4.0

Assets

The Relution Assets App enables borrowed devices to be easily returned using a QR code scan. For this, the Relution Assets App must be installed on a managing device (e.g. the administrator's smartphone or tablet), and the Relution Agent App must be installed on the borrowed device.

Users sign in to the Assets App with a Relution user account of the organization; if multi-factor authentication is set up for the account, it is requested during sign-in. The account requires read permission for devices as well as read and edit permissions for lendings. Shared logout + return additionally requires permission to edit devices, and resetting to factory settings requires permission to run this device action.

Instructions for returning: How to return a borrowed device

The following steps are required to return a loaned device:

Loaned device

1. Open the Relution Agent App
2. Open the side menu (hamburger menu)
3. Open device information
4. QR code must be visible

For version 26.4.0

Managing device

1. Open the Relution Assets App
2. Scan the QR code from the loaned device
3. After scanning, up to 3 options are available, depending on whether it is a 1:1 device or a device with Relution Shared Device:

- Return device: Ends the lending period without further changes
- Reset to factory settings + return device: Wipes the device and ends the lending period
- Shared logout + return: Only available for devices with the Relution Shared Device → policy on which a user is currently signed in. Logs out this user, thereby removes the user assignment of the device, and ends the lending

After the return

After successful execution, the Relution Portal shows the lending as no longer active (column Active); the return date is shown in the column Returned.

Learn more about the device lending system in Relution: Lending →

Files

The Relution Files App is a mobile app for iOS and Android devices that enables the integration of local file shares. These file shares can be provided via SMB or WebDAV protocols.

The app is particularly useful for businesses and schools that want to manage their data securely and centrally. By integrating local file shares, users can access relevant documents and content.

With the Relution Files App, shares set up via the Relution Portal can be accessed. Alternatively, additional shares can also be configured directly in the app. The built-in file explorer provides access to directories, and various files can be opened in the system applications.

Additionally, the integrated camera can be used in the Relution Files App to save images directly to the network share, instead of the Apple Photos app. This helps to enhance data protection.

Manual Setup

The manual setup of file shares in the Relution Files App is intuitive and easy to perform. Only a few mandatory fields need to be filled in; after entering them, the connection can be tested and established using the Test button.

sion 26.4.0

Field	Description
Display Name	Any name to assign to the share
URL	WebDAV or SMB URL for the file share
Username	Username of the user for the file share
Password	Password of the user for the file share
Extension Type	Type of integration into the Apple Files App (iOS only)

> iOS only: The Extension Type must be set to either `Modern` or `Classic`. Depending on the iOS version and device usage (shared), the file share may not appear correctly in the Apple Files App. Files Bug →

Managed Setup

Documentation for the managed setup can be found under Relution Files for iOS → and Relution Files for Android →.

In the managed setup via the Relution File Shares policy configuration, the Extension Type (iOS only) is set to Modern by default. On Android, Relution automatically installs the app as a required app as soon as an Android Enterprise policy contains this configuration.

User Operation

After successful setup, the app's file browser can be used to navigate the share. Users can also add or edit folders within the share.

The integrated camera can be used to store images in compliance with data protection directly on the share.

Once configured, the file share can be used directly via the built-in Files app on both iOS and Android devices.

For version 26.4.0

Parent

The Relution Parent App enables parents to manage their children's devices – without schools losing control. The school administration retains the ability to individually configure the setup process of the Relution Parent App or to sever the connection between the Parent App and the student device at any time.

Using the Relution Parent App, parents can restrict or re-enable the use of installed apps on their child's device.

Parent App Compatibility

The Relution Parent App is compatible with parents' iOS and Android Enterprise devices. The student devices to be controlled can also be Android Enterprise or iOS devices.

A special highlight is the cross-platform functionality: Parents with Android Enterprise devices can manage iOS devices – and vice versa. This means maximum flexibility when using different device combinations.

Setup

For version 26.4.0

The Relution Parent App is compatible with the Relution Server from version `5.23.0`. For a student device to be connected:

- the device must be an iOS or Android Enterprise device,
- the Relution Agent → must be installed at least in version `5.15.0`,
- the device must be supervised,
- and the user of the student device must have the permission to pair.

This permission can be found under: `Relution Parent App` → `Allow pairing` → `Create` It can be added to an existing role or assigned via a new role.

To manage pairing requests, the administrator needs the Parent App Links permission in the Settings area: Read to view, Update to approve and edit, Delete to remove entries.

Linking Student Devices with the Parent App

To ensure that only authorized parents can perform a pairing, every connection must be approved by the administrator. A free-text field allows for mapping individual pairing processes (e.g., school ID, class name, etc.).

Student Device

On the child's device, the `Device Information` → `Parent App` section is opened in the Relution Agent App. A QR code is generated there, which is scanned by the parents' Relution Parent App.


04:29 Thu 11 Dec
100 %
Device information
Device
Service
Parent App
Location tracking
Parent App
Scan the QR code below in the Relution Parent App
Create a link for this device in order to connect via Parent App

> If the Parent App section is not displayed, either the Agent is older than version `5.15.0`, the device is not an iOS or Android Enterprise device, or the user of the student device lacks the `Relution Parent App` → `Allow pairing` permission.

The QR code and the invitation are valid for 24 hours from the creation of the QR code.

A maximum of 5 entries under `Parent App Links` is possible per student device. All entries count except those with the status Expired, i.e. including Open, Invited, E-mail confirmed, Established and Deleted by parent. A QR code whose 24-hour validity has passed keeps the status Open and still counts. Once the limit is reached, the administrator must first delete an entry under `Parent App Links`.

Parents

Parents download the Relution Parent App from the Google Play Store or Apple App Store. After agreeing to the privacy policy, the app can be used immediately.

The QR code is scanned with the Parent App's integrated scanner or any QR code app (e.g., camera app).

For version 26.4.0

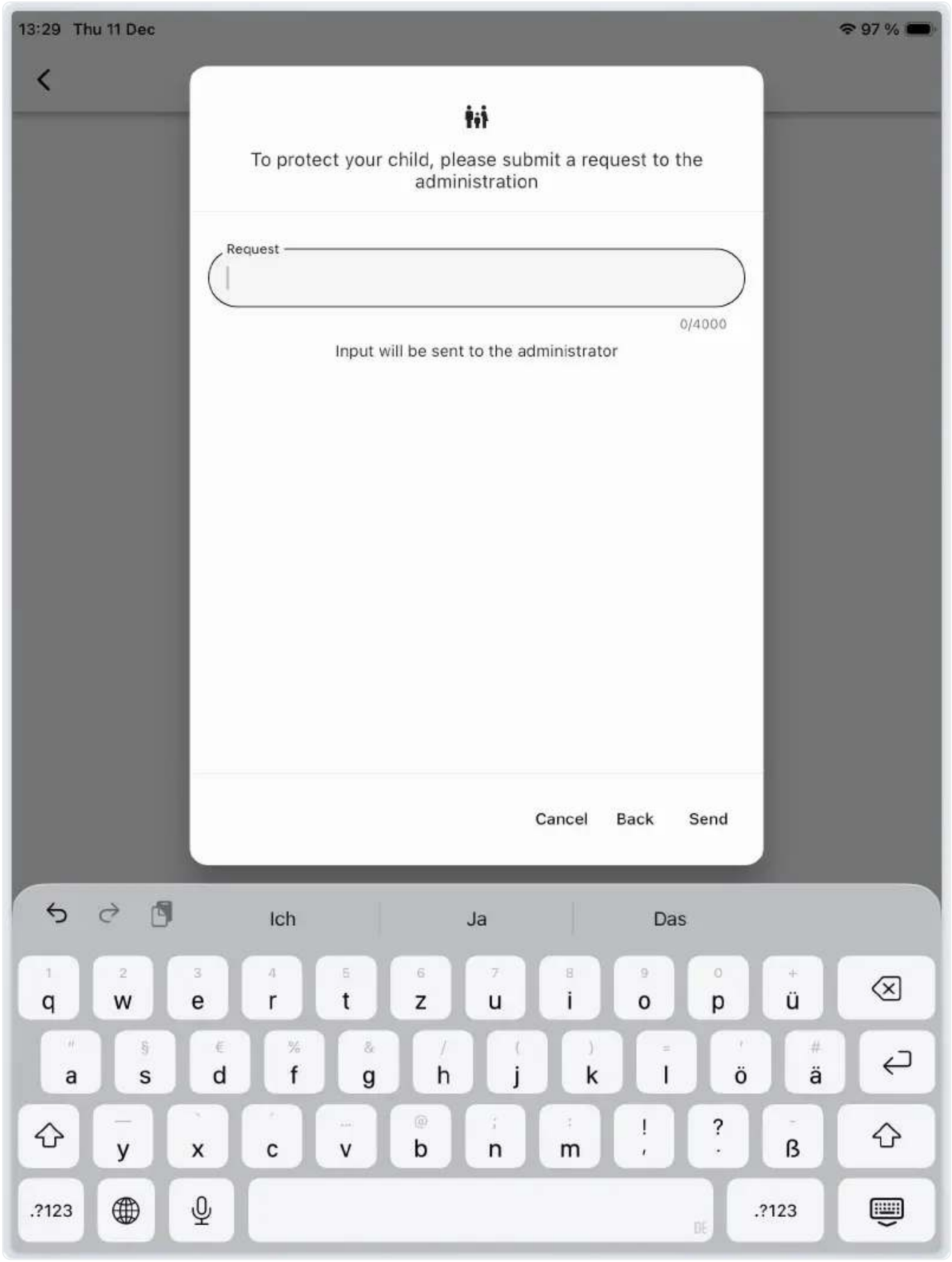


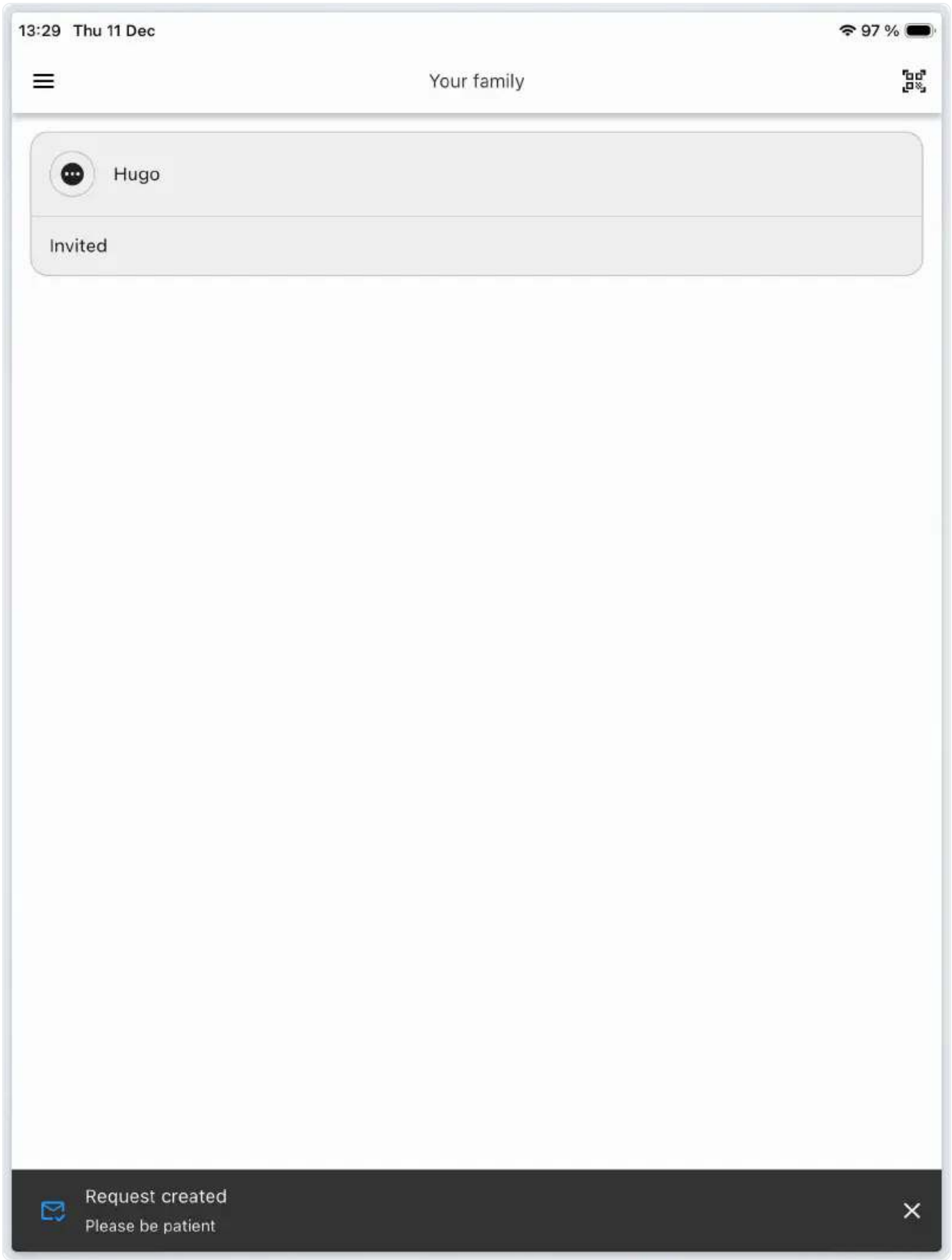
After the scan, parents must:

- give the device a name,
- provide a valid email address (must be confirmed),
- optionally add a free text for additional information.

For version 26.4.0

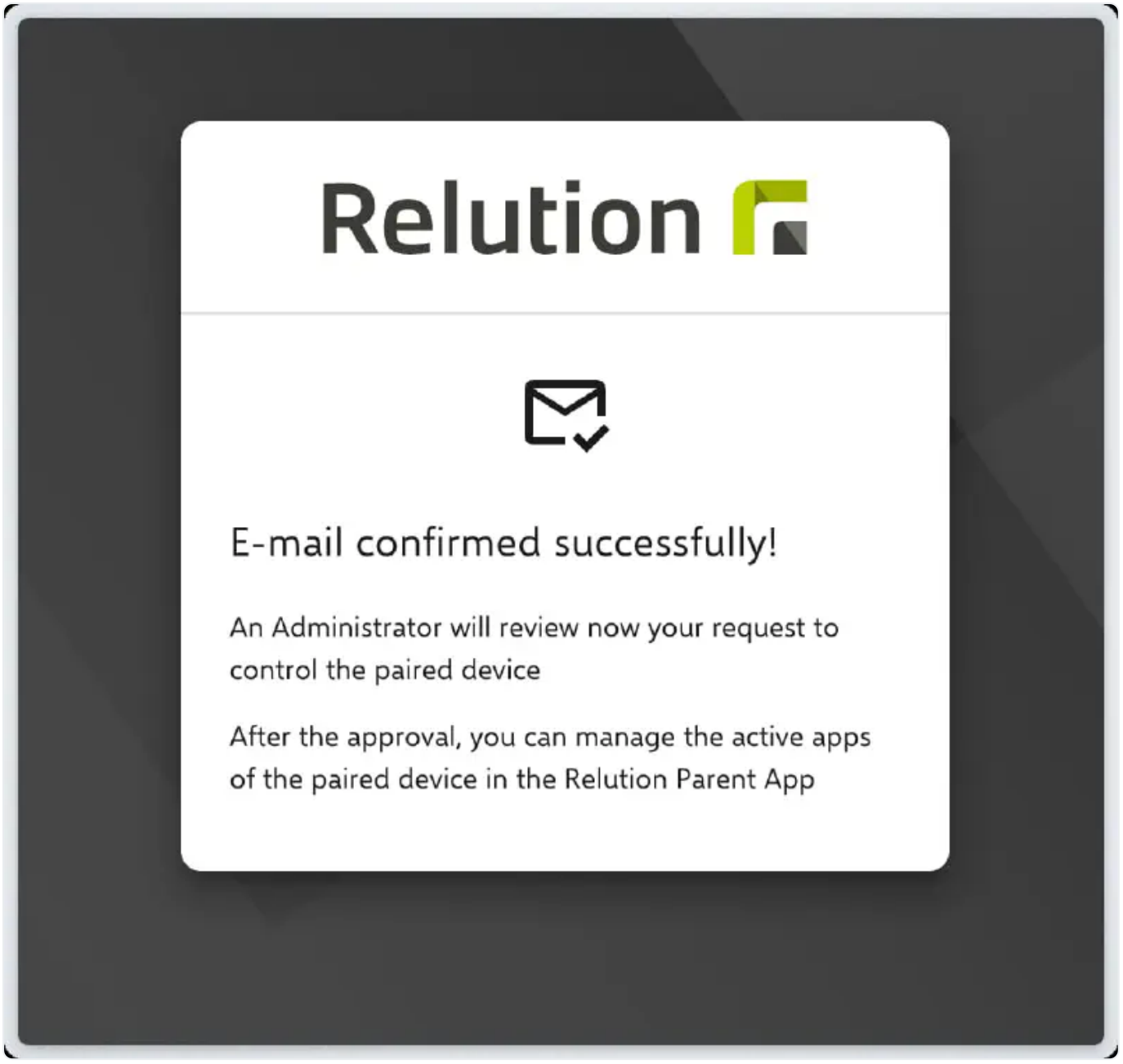

13:29 Thu 11 Dec
97 %
Add child
Give your child's scanned device a name and e-mail address
Name of child's device
For identification of the device in the app
E-Mail address used for confirmation
Enter an E-Mail address for access
Cancel
Next


13:29 Thu 11 Dec
97 %
To protect your child, please submit a request to the administration
Request
0/4000
Input will be sent to the administrator
Cancel
Back
Send
Ich
Ja
Das


13:29 Thu 11 Dec
97 %
Your family
Hugo
Invited
Request created
Please be patient

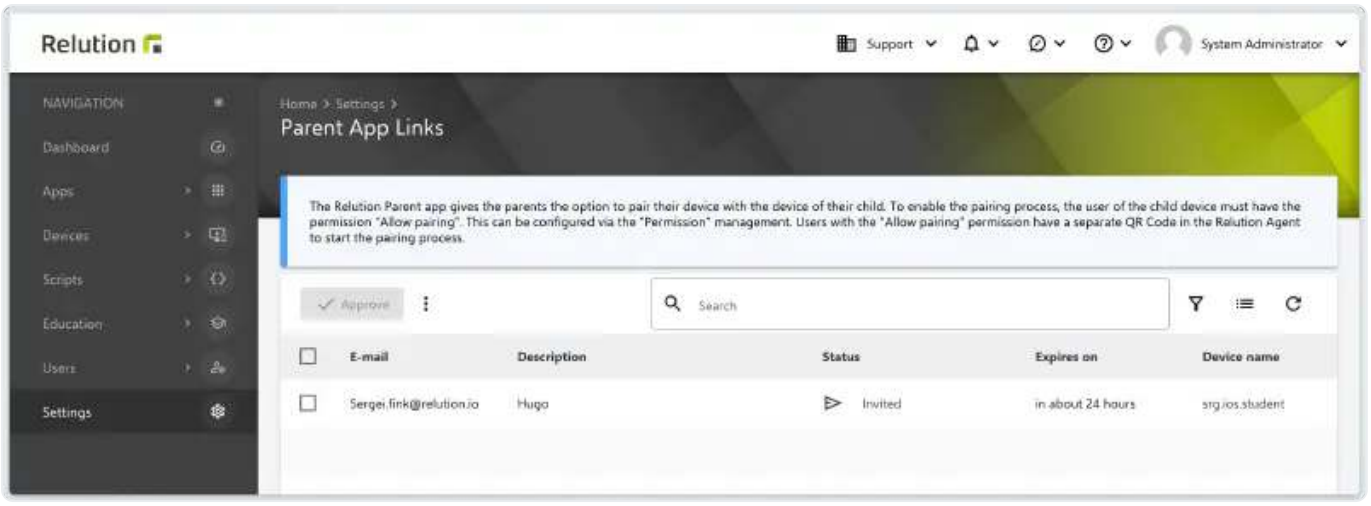
> If an error occurs when submitting the request, the QR code may have expired or already been used. In this case, the Parent App section in the child's Relution Agent should be refreshed.

After submitting, the parents receive an email with an eight-digit confirmation code and a confirmation link. After successful confirmation, the status changes to E-mail confirmed. If the confirmation code is entered incorrectly ten times, the entry receives the status Expired and can no longer be confirmed.



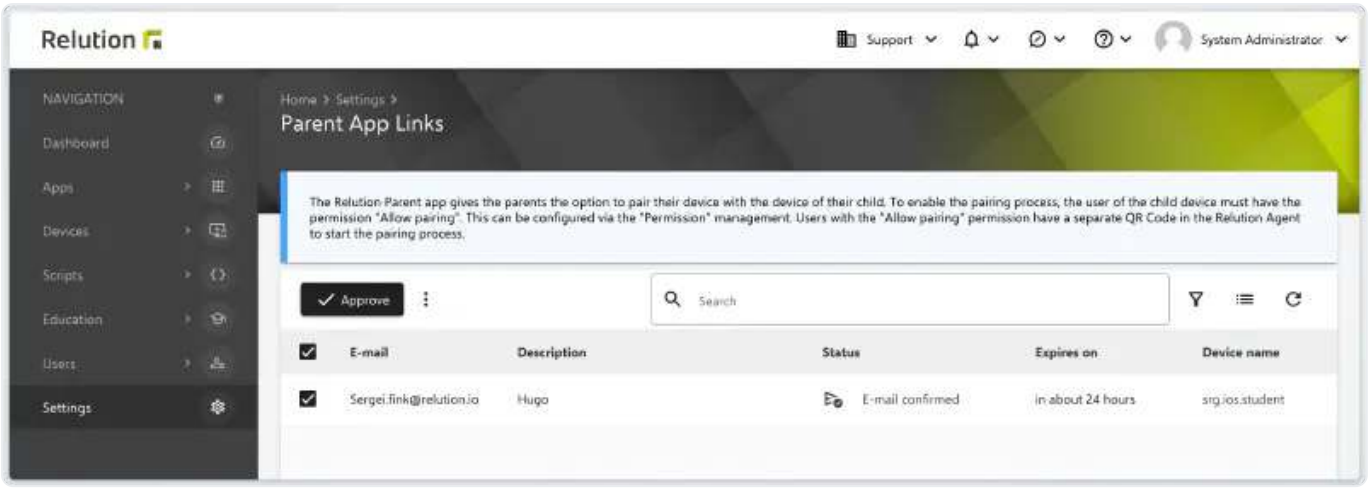
Administration

All pairing requests are displayed under `Settings` → `Device Management` → `Parent App Links`. The pairings of a single device can also be viewed in the device details under `Devices` → `Inventory` in the Parent App Links tab (iOS and Android Enterprise only).



The Expires on column shows the expiration time for entries with the status Open and Invited. After expiration, the entry keeps the status Open or Invited but can no longer be continued. The default filter of the list hides entries with the status Expired.

As soon as the parents have confirmed their email address (status E-mail confirmed), the administrator can approve the pairing via Approve. Several selected entries can be approved at once, provided they all have the status E-mail confirmed. The description of an entry can be changed via Edit in its context menu.



There is no separate action for denying a request: a request is denied by removing the entry via Delete. An existing pairing can also be deleted at any time. The parent then loses the authorization to control the child's device. If no other pairing with the status Established remains for the device, all restrictions set by parents are lifted. The same applies when the parents remove the pairing in the Parent App.

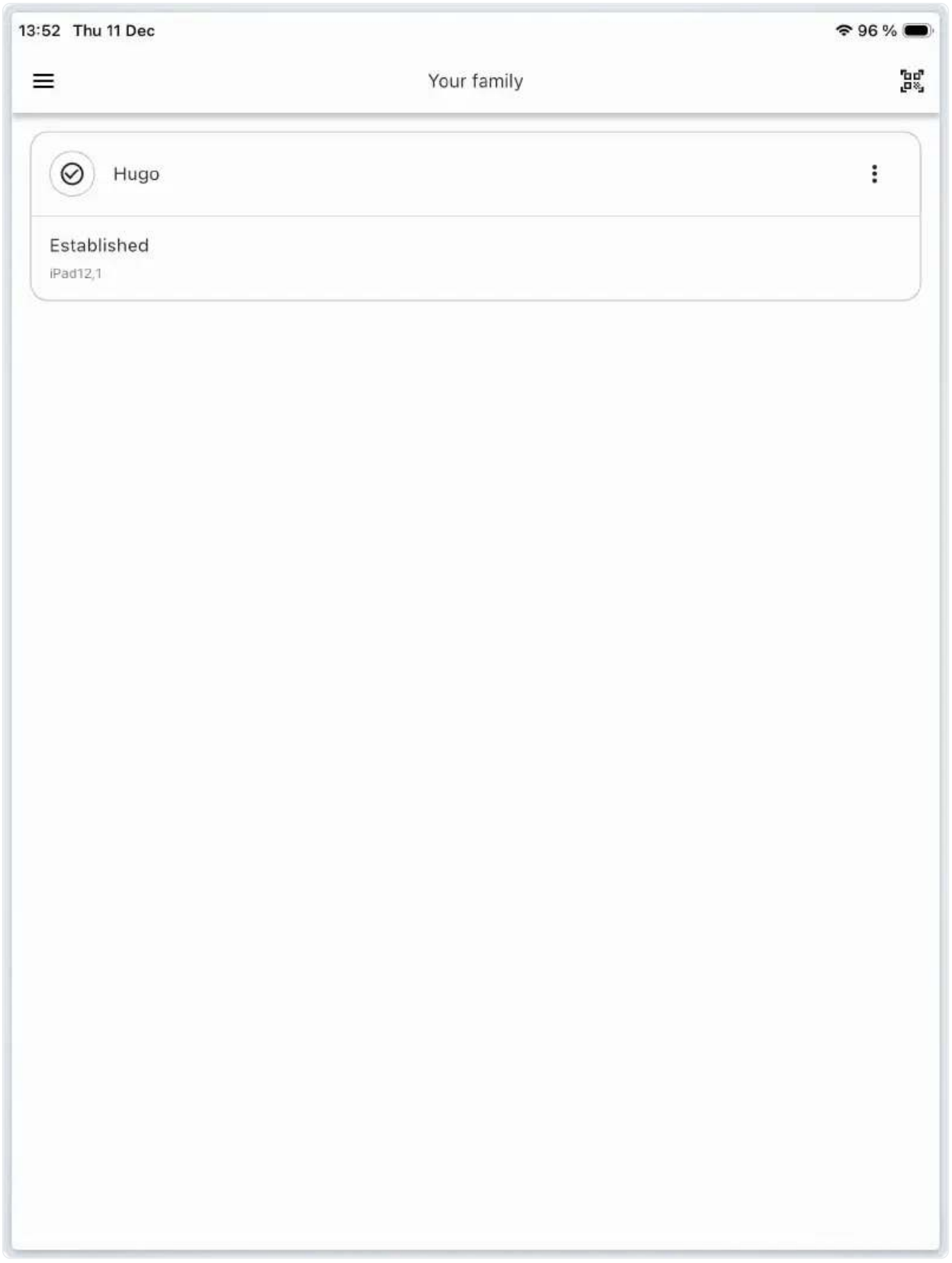
Possible Pairing Statuses

Status	Description
Open	QR code has been created but not yet scanned.
Invited	QR code has been scanned, but email not yet confirmed.
E-mail confirmed	Email has been confirmed, pending administrator approval.
Established	Pairing has been approved by the administrator.
Expired	The email confirmation failed too often because of a wrong confirmation code (10 attempts). The pairing can no longer be confirmed.
Deleted by parent	Pairing has been removed by the parents.

Using the Parent App

For version 26.4.0

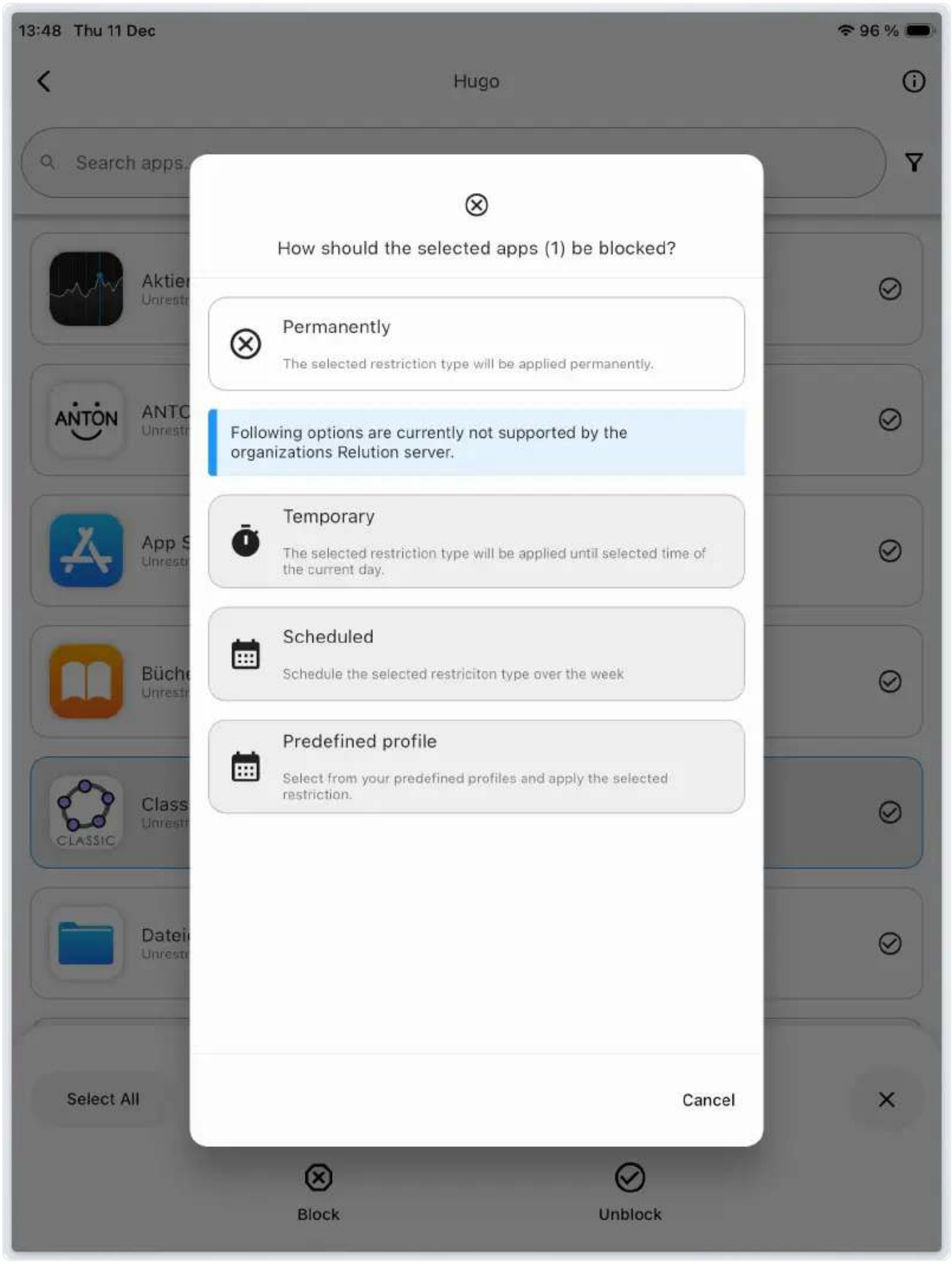
Upon launching the app, parents see all linked devices on the homepage. The current status of the pairing is visible below the assigned device name.



As soon as the school has approved the connection, parents can:

- view the installed apps on the child’s device,
- block or unblock individual apps,
- temporarily or scheduled block and unblock individual apps
  From Relution 26.0.0
- apply the changes by confirmation.

For version 26.4.0


13:48 Thu 11 Dec
96 %
Hugo
Search apps
How should the selected apps (1) be blocked?
Permanently
The selected restriction type will be applied permanently.
Following options are currently not supported by the organizations Relution server.
Temporary
The selected restriction type will be applied until selected time of the current day.
Scheduled
Schedule the selected restriciton type over the week
Predefined profile
Select from your predefined profiles and apply the selected restriction.
Cancel
Select All
Block
Unblock

If a parent restriction overlaps with a lesson restriction, the lesson always takes precedence.

Applying Restrictions

Starting with Relution Server 26.0.0 and Relution Parent 26.0.0, parents have the option to apply time-based restrictions. They can choose from three types:

1. Permanent
    - The restriction is applied indefinitely and permanently overrides any previously selected restriction (including its type).
2. Temporary
    - The restriction remains active until the specified time on the current day. If the selected time has already passed, the next day is used instead.
    - After it expires, the previously configured restriction (including its type) is automatically restored.
    - Temporary restrictions only override other temporary restrictions and revert to the previously active restriction afterward.
    - Perfect for situational restrictions, such as during study or quiet periods.
3. Scheduled
    - The restriction is active during the specified schedule. Outside of this schedule, the inverted restriction applies.
    - To simplify reusing schedules, they can be saved as profiles in Relution Parent and reused as needed.
    - Changes to a profile do not affect restrictions that have already been applied; they must be reapplied to the desired apps.

The current time-based restriction is displayed as an icon and in text form for each app.

For version 26.4.0

Notes

- If an allowlist is active on an iOS student device, it takes priority over the Parent App. The allowlist can come from the App compliance configuration (List type Allowlist — The apps below are allowed) or from the Restrictions configuration (Allowed App Bundle IDs).
- An active lesson also takes priority over restrictions set by parents.
- The Relution apps on the student device (e.g., Relution Agent, Relution Companion, Relution Teacher) cannot be blocked by parents.
- Starting with iPadOS 26, system apps (e.g., Safari, Books) are made available to the Parent App on the child's device. This feature is not available on earlier iPadOS versions.

Error Messages

- Error Message 500
  In this case, sending an email from the Relution Server is not possible. Email sending is set up in the `Global` organization under `Settings` → `Email Configuration` and checked there in the Test email configuration area (see Mail dispatch →).

Teacher

The Relution Teacher App (iOS, Android & Windows, and since Relution 5.24 also as a web app) allows teachers to create lesson-specific profiles with which apps, device functions, and web links can be prepared and managed for lessons.

It also enables the definition of participant groups and the control of lessons.

Thanks to integration with Apple Classroom and Samsung Classroom Management → (separate license required), comprehensive control is also possible during lessons – completely without an Apple Account on student devices.

Prerequisites for use

To use the Relution Teacher App, a Relution Education license is required.

In addition, classes with the corresponding students and teachers should be created (`Education` → `Classes`).

The teacher requires at least the `Education` → `Use Teacher App` permission. It is included in the system group [organization unique name] Teacher (e.g. `UIT Teacher`), which is assigned in the user account under Groups & Permissions in the Groups field; alternatively, it can be granted via a role in the Permissions field.

iOS, Android Enterprise and ChromeOS devices are supported as student devices.

For version 26.4.0

Structure

The content for the student device is defined by a profile. In addition, participants are defined and the duration is set. The lesson can then be started.

Profiles

Profiles define what the device is equipped with for the lesson.

The teacher can choose between private and public profiles. The latter can be used by all teachers in the organization. Editing and deletion remain reserved for the creator.

For the exam profile (iOS, ChromeOS), the wallpaper is additionally set.

Apps, web links, system apps, and certain restrictions can be defined in the profile.

Apps should not be installed only when the profile is applied in order to minimize setup time for the lesson. When using exam mode, a default wallpaper should be set in a separate policy. To keep students permanently in Wi-Fi or prevent disabling Bluetooth, a separate policy is also recommended.

Managing participants

For the lesson, a preconfigured class can be selected. Missing students can be removed directly from the lesson. This ensures that the profile is only distributed to the devices of present students.

Alternatively, an ad-hoc class can be created. In this case, all students of the organization are available for selection.

For recurring ad-hoc groups, it is recommended to define custom classes via the portal or assign students to multiple classes.

Setting lesson duration

A profile is time-limited – e.g., until the end of the current lesson.

Under Lesson Settings →, individual lesson times can be configured.

Starting and controlling lessons

Only one lesson per teacher can run at a time. When a lesson is started, other unfinished lessons of the same teacher are ended or deleted. If students are already taking part in another active lesson, a notice appears; if the lesson is started anyway, they are removed from the other lesson.

If the Limit lesson to timetable option is enabled in the Lesson Settings →, lessons cannot be started outside the timetable.

During a running lesson, teachers can adjust participants, change the remaining time, and manually end the lesson. When ending the lesson, shared iPads (Shared iPad) can be signed out; during a running lesson, this is also possible for individual shared devices.

The profile is removed from student devices after the defined time has elapsed or when the lesson is ended.

When the lesson is ended manually, Relution sends the changes to the student devices immediately; after the defined time has elapsed, within about one minute. Blocked websites and lesson restrictions are lifted as soon as the change reaches the device. If a device is not reachable at that time, it receives the change as soon as it is reachable again. Apps installed for the lesson are not uninstalled in the process.

> The arrangement of apps and folders cannot be saved, as removing profiles changes the structure of the home screen and synchronizes it again.

Creating lesson templates

Lessons can be saved as personal or shared templates to reuse them quickly.

A lesson template includes the following settings:

For version 26.4.0

Type of lesson template

- Personal template (private)
- Use only for the creator of the template
- Shared template (shared)
- Use of the template for all teachers

Private templates without an owner (e.g., after the teacher has been deleted) are deleted automatically every day at 01:00.

Exam mode (iOS, ChromeOS)

- Exam mode
- Sets a purple wallpaper with the text “Klausur” (or “Exam” if the server’s default language is English) on the students’ iOS and ChromeOS devices, so that it is clear at a glance whether the device is in the desired state.
- On iOS, the wallpaper cannot be changed during the exam, and Spotlight search does not show internet results.
- After the exam ends, Relution sets a default wallpaper. On iOS, this does not happen if a policy already defines a wallpaper for the lock and home screen.

Single app mode

For version 26.4.0

- Puts the device (Android or iOS) into single-app mode.
- Exactly one app must be selected in the lesson for this.
- In addition, device functions can be restricted in single app mode, e.g. touch, rotation, volume buttons, ringer switch, sleep/wake button and auto-lock on iOS, and e.g. power button, system navigation, status bar, device settings and keeping the screen on while charging on Android.

Apps allowed during the lesson

- Here a selection of apps can be defined that are available to students during the lesson.

Device functions during the lesson

- Allow camera (Android + iOS)
- Allow screenshots (Android + iOS)
- Show Safari and web links (iOS)
- Use web links to filter web content (iOS)
- Show Messages app (iOS)
- Allow spelling assistance (iOS)
- Allow AirDrop (iOS)
- Enforce Bluetooth (iOS)

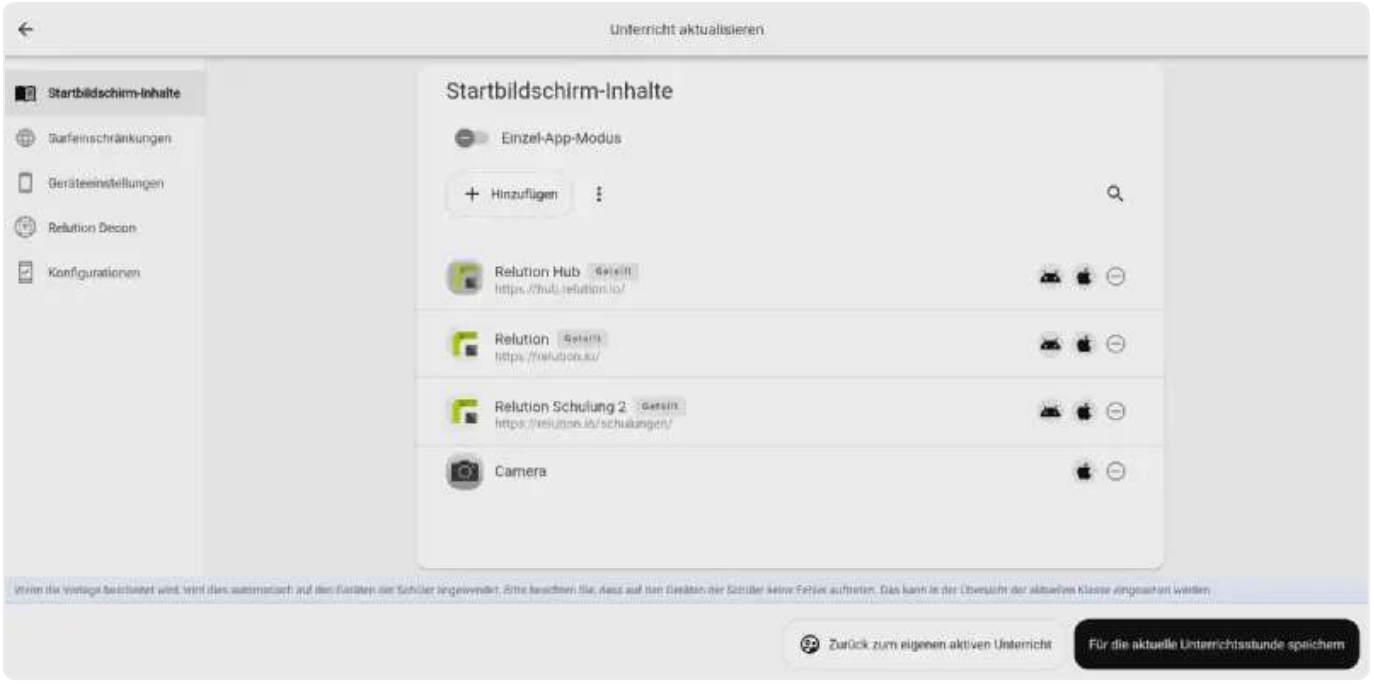
Alternatively, it can be specified that no lesson-specific restrictions are applied for the lesson.

Web links and browsing restrictions

New in 26.5

Web links can be used in a lesson template in two independently configurable ways:

- Under Homescreen content, web links are placed as shortcuts on the students' home screen for the duration of the lesson. Further web links can be added via Add.
- Under Browsing Restrictions, URLs act as an allow list for the web content filter (iOS). The Use URLs as web content filter toggle enables filtering. When it is switched off, browsing is unrestricted and the listed URLs have no effect.

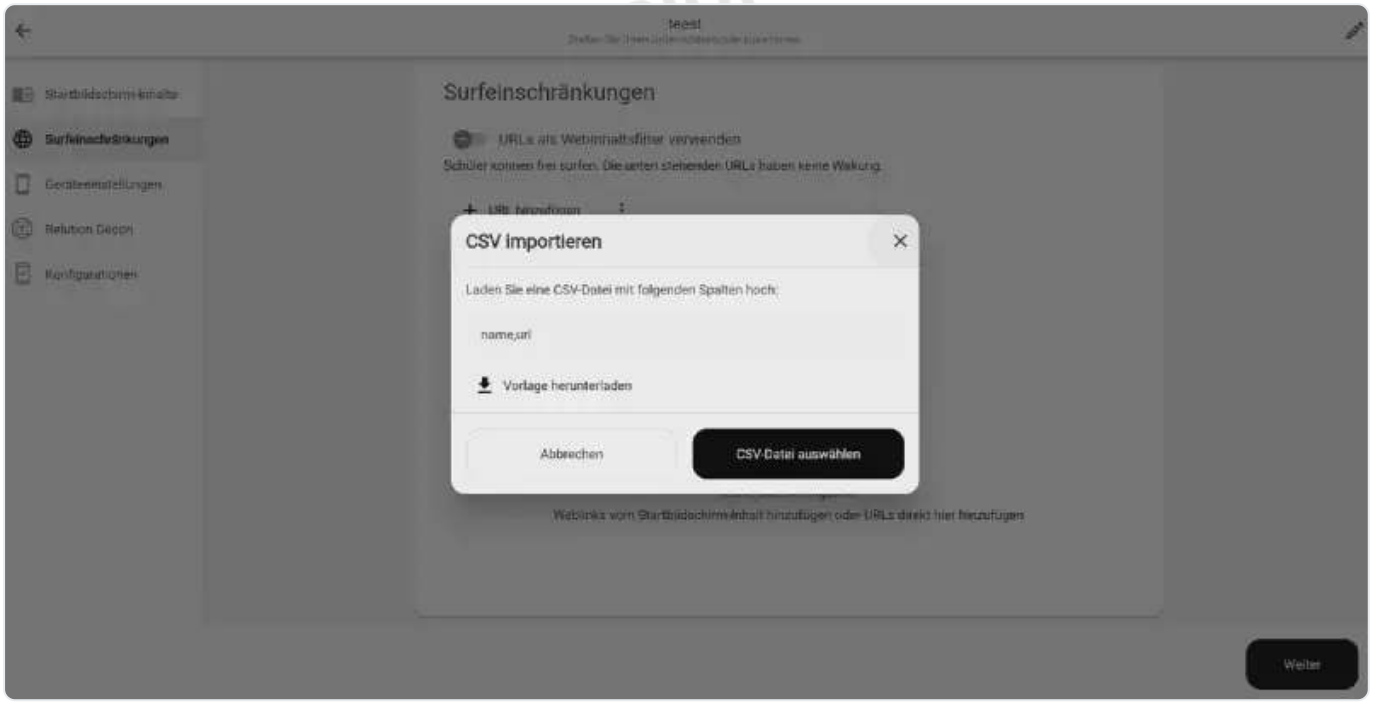


In the browsing restrictions list, the Active column defines for each URL whether it is allowed in the web content filter, and the Home Screen column whether it additionally appears as a shortcut on the home screen. An entry can thus serve purely as an allowed URL without appearing on the home screen. When the web content filter is enabled, an inactive URL does not appear on the home screen either. URLs can be added directly via Add URL; web links already created under Homescreen content can also be adopted.



Importing web links via CSV

Using the three-dot menu → Import CSV, a list of web links can be uploaded as a CSV file. The file contains the columns `name` and `url`; a matching template is available via Download template.




```
name,url
Wikipedia,https://wikipedia.org
```

App Store settings

- Allow Google Play Store (Android)
- Show App Store (iOS)
- Show iTunes Store (iOS)

Relution Decon

- Enable Relution Decon (license required. In addition, a Decon policy must be assigned to student devices in Relution)
- BPjM list
- Safe search
- Filter type
  - Off
  - Age restriction
    - 0+
    - 6+
    - 12+
    - 16+
  - Categories
    - Adult content
    - Advertising
    - Communication
    - Social media
    - Entertainment
    - Music
    - News
    - Shopping
    - Work
    - Education
    - Generative AI
    - Phishing
    - Miscellaneous

For version 26.4.0

More about Relution Decon →

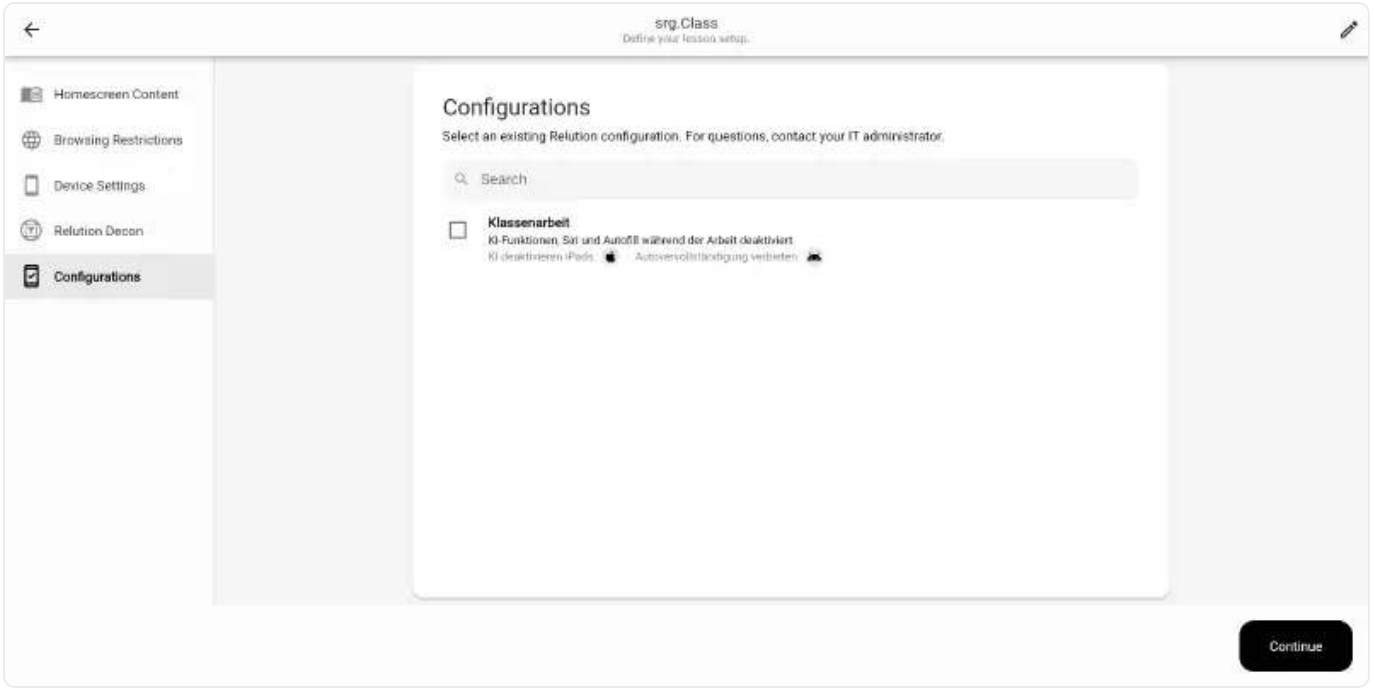
In addition, separate lists of allowed and blocked websites can be defined for the lesson. The active web links of the lesson are automatically adopted as allowed websites. The Categories filter type and the 12+ age level are preset.

Note: For the duration of the lesson, the otherwise active Decon configuration is overridden.

Configurations

In Relution Teacher, Configurations are the education groups that have been created and assigned policies in the portal: Education groups →.

In the lesson template, one or more configurations can be selected in the Configurations area; the name, description and linked policies are shown for each. When the lesson starts, the linked policies are applied to the student devices and removed again when it ends.



Selecting configurations requires the read permission `Education` → `Lesson Device Groups`. Without this permission, no configurations are displayed.

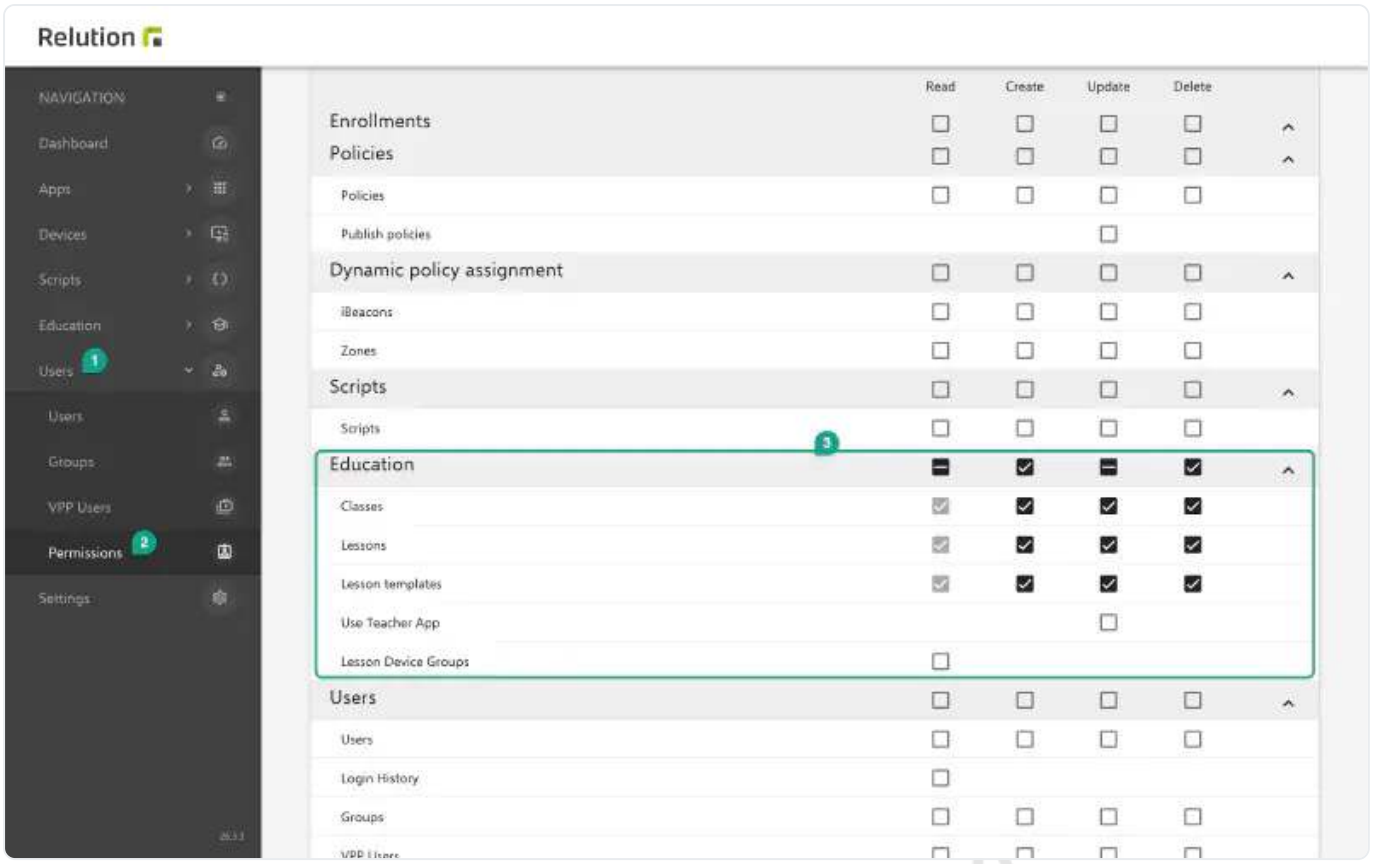
For version 26.4.0

Admin mode for lesson overview

For the admin view in the app, at least read permission `Education` → `Lessons` is required.

The admin has access to all lessons in their organization. These can be viewed and additional information can be obtained in case of issues.

With the Update permission for `Education` → `Lessons`, the lesson can be edited (add/remove students) and ended early.



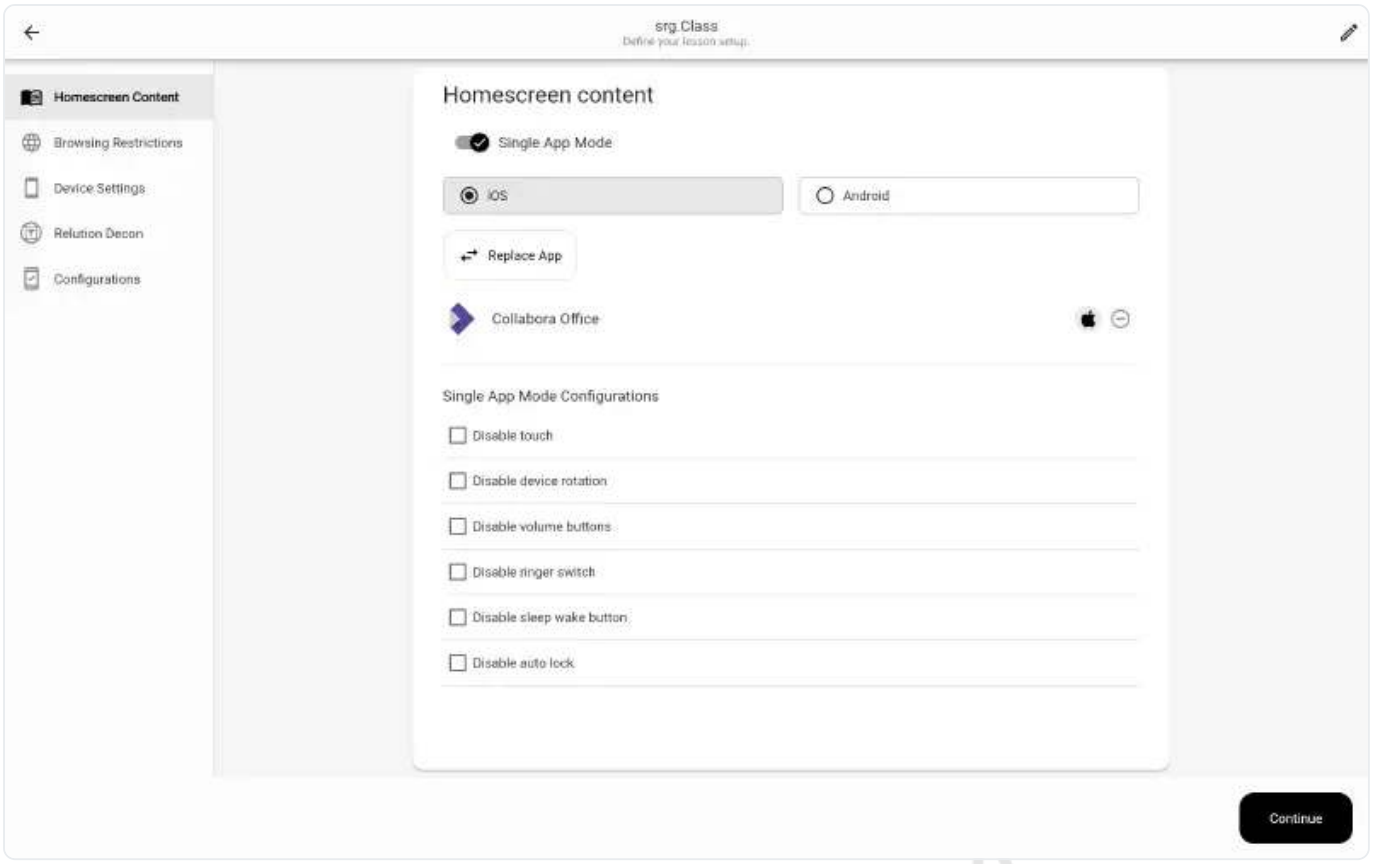
For version 26.4.0

Relution Teacher as a web app

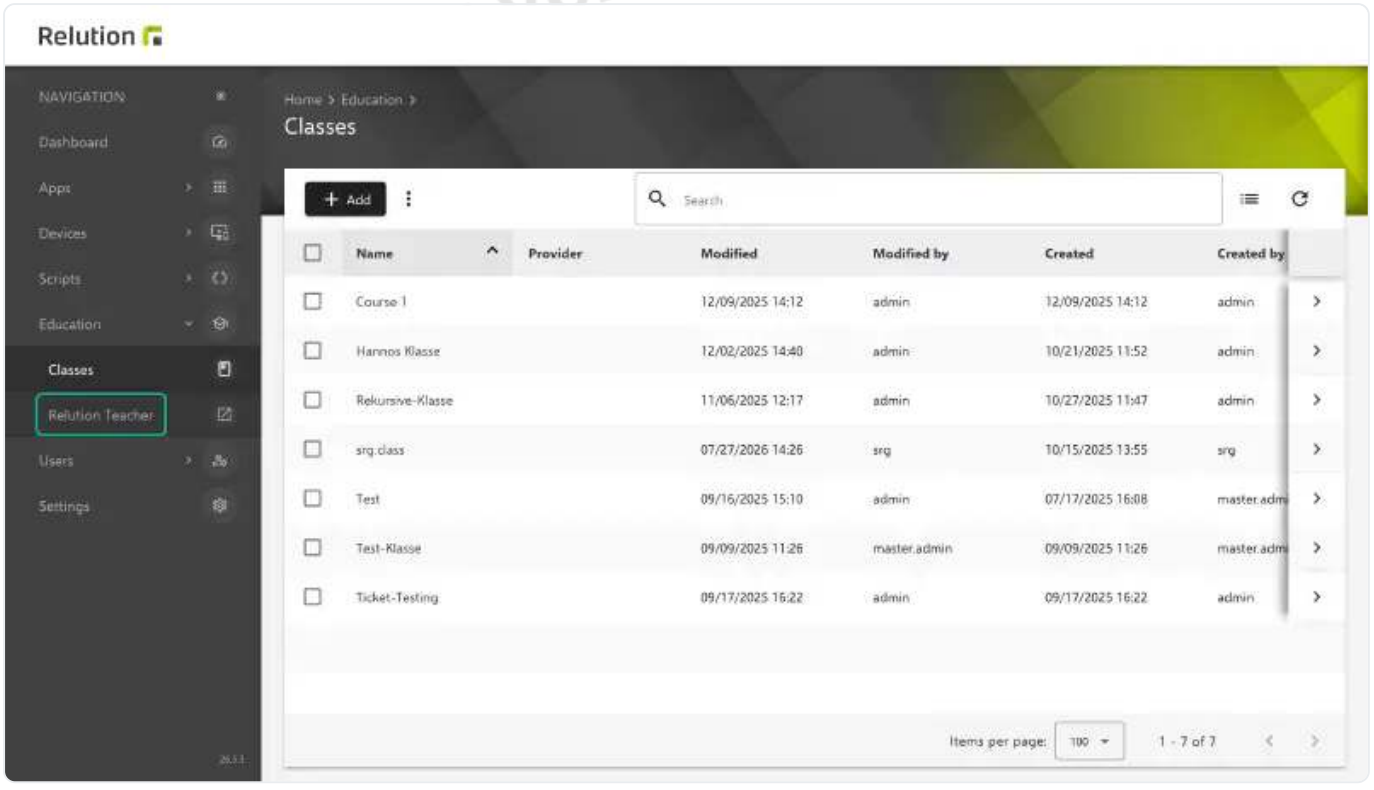
Since Relution Server 5.24, the Relution Teacher web app is available.

Teachers can now create, start, and control lessons directly from a browser window in the same way as on iOS and Android.

This seamless integration enables smooth and efficient lesson organization that meets the requirements of modern educational environments.



The web app is accessible in the navigation menu under `Education` → `Relution Teacher` and opens in a new browser tab. The menu entry only appears with the `Education` → `Use Teacher App` permission.



Multitenant feature for teachers with multiple schools

The multi-tenant capability of Relution Teacher allows teachers to extend the functionality of Relution Teacher across multiple organizations.

This is especially useful when teachers work at multiple schools that manage their student devices via the same Relution instance.

Configuration

To enable access to multiple Relution organizations, the following steps are required:

- The login takes place in the `Global` organization.
- In the Relution portal, the corresponding user (teacher) is searched for and edited in the `Users` section.
- The user is added to the system user groups of the additional organization(s), e.g. the [organization unique name] Teacher group.

After configuration, the desired organization can be selected in the Relution Teacher App as well as in the Relution Teacher web interface via the side menu. Only organizations in which the teacher has the `Education` → `Use Teacher App` permission are available for selection.

Additionally, in the `Global` organization under `Education` → `Classes`, the Organization column shows which Relution organization each class belongs to.

For version 26.4.0

Note

When applying a lesson via Relution Teacher, the user's individual home screen layout is discarded.

Technically, it is currently not possible to save the user's app arrangement and reapply it after the lesson ends.

It is possible to centrally define a layout via Home Screen Layout configuration so that a consistent state can be enforced across all devices.

Homescreen Layout →

Lesson Settings

Under `Settings` → `Education` → `Lesson settings`, the time frame within which teachers can start lessons via the Teacher App → is defined. This page is only visible with an Education or Free license.

The Lesson settings permission in the Settings area is required: Read to view, Update to change. Without Update, the page is read-only. Added, edited and deleted lesson schedules only take effect once the page is saved via Save.

Lesson Schedules

This section contains the list of lesson schedules with Name, Description, Start time, and End time. Name is required, Description is optional. Lesson schedules must not overlap, which also applies when editing. A start time that falls exactly on the end of another lesson schedule also counts as an overlap, so at least one minute of spacing is required. The end time must be later than the start time.

By default, the list is pre-filled with 14 lesson schedules (1. Stunde to 14. Stunde, 07:45 to 21:05), Monday to Friday are set as lesson days, the time zone is UTC and the timetable limitation is switched off.

General Settings

- Override system wide settings: Only visible for tenant organizations. Allows deviating from the system-wide lesson settings. If the option is switched off, all fields are locked and lesson schedules can neither be added nor edited; changes in the system organization are applied automatically. When switching back to the system-wide settings, the values of the system organization apply again.
- Time zone: The time zone the configured lesson schedules refer to.
- Limit lesson to timetable: When enabled, lessons can only be started in the Teacher App on the selected Lesson Days, no earlier than the start of the first lesson schedule and with a planned end time no later than the end of the last lesson schedule. Breaks between individual lesson schedules are not blocked.
    - Lesson Days: Becomes required once the limitation above is enabled. Defines on which weekdays lessons may take place.

Access to Profile Images for Apple Education Configurations

Controls whether Relution may access users' profile images to supply Shared iPad login and Apple Classroom with the stored profile images. Enabled by default. When set to Disabled, Relution does not serve profile images to Shared iPad and Apple Classroom.

Profile images are only served to devices with an Apple Education configuration, and only for users who are members of a class in this configuration.

For version 26.4.0

Homescreen

The Relution Homescreen App is a launcher that allows administrators to remotely customize the home screen of fully managed Android Enterprise devices. The app replaces the pre-installed launcher and is centrally configured via the Relution Home Screen Layout configuration in an Android Enterprise policy. It is automatically installed on devices when the policy is applied.

The app only replaces the pre-installed launcher on fully managed devices (Device Owner). With the other Android Enterprise enrollments, the app receives the configured layout but is not set as the launcher. This configuration is not available for Android Legacy.

The app provides a variety of features to customize the home screen:

- Theme customization
- Wallpaper selection
- Choosing and arranging the displayed apps

Configuration

The Relution Home Screen Layout configuration includes the following settings:

- Layout: Theme (Light by default or Dark), Grid size (Auto, 4x4, 5x4 (default), 6x4) and Screen orientation (Automatic by default, Landscape, Portrait).
- Wallpaper: image file and, optionally, a Text on wallpaper with Text color (hex value, default `#ffffff`).
- Constraints → Allowed Apps: Display only apps from layout (default) or Display all apps. With Display only apps from layout, only the apps from the layout are available on the device.
- In the layout editor, apps, folders and web links are arranged via drag & drop on pages and in the dock; folders are not possible in the dock. Apps can also be added manually via their package name; the new item then appears on the first page. On the device, the layout is locked and cannot be changed by the user.

Further details on the configuration can be found in the Kiosk Mode → article.

> The Relution Home Screen Layout configuration is only available if no Kiosk Mode configuration is applied. It is not possible to use both configurations simultaneously. Only one of the two can be added within a policy; with multiple policies, the policy priority decides.

With Relution Education, the server automatically uses the Homescreen App with the lesson's apps on Android Enterprise student devices during a lesson, even without a configuration of its own. Lessons in single app mode are excluded.

Unmanaged Devices

The Relution Homescreen Layout App is also freely available for unmanaged devices on the Google Play Store.

Google Play Store Link →

For Version 26.4.0

Relution Decon (content filter)

Starting with version 5.27, Relution for iOS enables the setup of a DNS-based content filter. This feature ensures a secure and focused internet experience by restricting access to selected websites and apps. With AI-powered content categorization, Relution Decon also provides a comprehensive parental control filter with advanced configuration options.

What is Relution Decon?

Relution Decon is an AI-powered add-on for iOS, iPadOS, macOS and Android Enterprise that filters content in real-time, creating a safe digital environment. Using DNS-based content control, Decon blocks unwanted websites and apps, allowing users to work and learn in a protected, distraction-free space.

Relution Decon uses a DNS proxy to forward all requests to the Decon server. Websites are classified and either allowed or blocked according to policy rules. All data transfers are SSL-encrypted, ensuring user activities remain secure.

Decon App

For version 26.4.0

The Decon app is automatically deployed on iOS, iPadOS, macOS and Android Enterprise devices when the policy is installed. It monitors device DNS requests and ensures that only approved content is accessible.

App features:

- Activates a system-wide DNS proxy, which cannot be disabled by the user
- Displays the current status of Relution Decon
- Provides insight into blocked websites and applied filter categories

> Recommendation: For Apple devices, ensure sufficient Apps and Books licenses (VPP in the portal) for the app before deployment.

Configure VPP →
Relution Decon on the Apple App Store →

Decon Policy

In the device policy, the configuration is created via `Add` → `Relution Decon`. This policy automatically installs the Decon app on the devices and acts as a proxy for all DNS requests.

Policy configuration is completed upon publishing. Without a valid Relution Decon license, the form shows a notice and the configuration cannot be saved. On macOS, the configuration is only available with device enrollment.

If an iOS or macOS policy already contains a DNS Proxy configuration, Relution Decon does not set up its own DNS proxy; the device receives a compliance notice.

The settings are described in detail in the platform articles Relution Decon for iOS →, Relution Decon for macOS → and Relution Decon for Android Enterprise →.

Policy configuration hierarchy (highest to lowest priority)

1. Allowed apps (iOS/iPadOS and macOS only)
2. Blocked apps (iOS/iPadOS and macOS only)
3. Permitted domains
4. Blocked domains
5. Filter Type (blocked categories or age level)

The Relution apps (Relution Agent, Relution Teacher, Relution Files, Relution Assets, Relution Decon) as well as the addresses of the Relution server and the Decon server are always allowed.

Decon in Relution Teacher

Decon can be selected and managed in class profiles with Relution Server 5.32.0 and Relution Agent 5.19.0. Student devices must have a Decon policy assigned.

Teacher →

Note: The otherwise valid Decon configuration will be overwritten for the duration of the lesson.

For version 26.4.0

Filtering

In the Filtering section, the required Filter Type field determines how websites are filtered:

- Off: Filtering takes place neither by category nor by age level.
- Categories (default): The categories to be blocked are selected individually (see table).
- Age level: Filtering is based on an age level (0+, 6+, 12+ or 16+, default 12+).

In addition, the BPJM list and Safe search toggles are available. Entries under Permitted domains can enable access to content that has been classified as inadmissible by the BPjM.

If several Decon configurations are used on one device, the strongest filtering automatically takes effect: filters by age level take precedence over filters by category, and configurations without filtering are ignored. Blocked categories are merged (a category is blocked as soon as one configuration blocks it); with several age levels, the strictest applies. Domain and app lists are merged as well.

Category Classification

Relution Decon automatically assigns each website to a category. With the Categories filter type, administrators define under Blocked categories which categories are blocked. By default, only Adult is blocked.

Category	Description	Examples
Adult	Sites inappropriate for youth	Pornography, Violence, Weapons, Drugs, Gambling, Adult Entertainment, Adult Shopping, Dating, Google Safe Search
Advertisement	Advertising websites	Ad providers
Communication	Communication services	Email, Messenger, (Video) Calling
Social Media	Social media content	Facebook, Instagram, TikTok, etc.
Entertainment	Entertainment websites like streaming or games	Movies, Games, Videos
Music	Music streaming services	Spotify, Tidal, etc.
News	News and magazines	News, Weather
Shopping	Online shops (excluding adult content)	Amazon, eBay, etc.
Work	Work-related websites	Office, File Sharing, Intranet
Education	Learning websites	Wikipedia, Google Scholar
Generative AI	AI-specific websites	ChatGPT, Perplexity.ai, etc.
Phishing	Potential phishing websites	Potential scams, Data theft
Misc	Everything else	Remaining sites

Allow and Block Lists

- Permitted domains / Blocked domains: Specific domains can be allowed or blocked independently of categories. Only the domain should be specified, not the path. Domains with wildcards as well as IPv4 and IPv6 addresses are possible. The number of blocked domains should be limited to about 500.
- Allowed apps / Blocked apps: Apps can have internet access controlled; base functionality remains unless internet connection is required. The app lists are only available in policies for iOS/iPadOS and macOS, not for Android Enterprise.

In addition, Relution adds the domains allowed and blocked organization-wide under `Settings` → `Relution Decon requests` to every Decon configuration. These domains do not apply during a lesson with Decon.

Advanced DNS Configuration

The advanced DNS configuration is not available in Android Enterprise policies.

DNS servers on the device: Alternative DNS servers can be configured if the Relution Decon DNS is unavailable. Fallback: Cloudflare Families DNS (1.1.1.3).

DNS servers on the Relution Decon server: Replaces the default DNS of the Decon server. IP addresses (UDP) or DNS-over-HTTPS (DoH) such as Zero or Quad9 are possible.

Privacy

In Android Enterprise policies, the Privacy section offers the Auto accept data disclosure option. It accepts the data disclosure in the Decon app on behalf of the user.

Limitations

- Caching: Blocks and policy changes may take up to 1 minute to take effect.
- Path independence: DNS works at domain level; subpages cannot be distinguished.
- App blocking: Only internet access is blocked; basic functions and cached content remain available.

For version 26.4.0

App Management

Relution offers comprehensive Mobile App Management (MAM) functionality, enabling centralized management of all supported apps — cross-platform and efficient.

Supported platforms and app formats:

- iOS & iPadOS: apps from Apps and Books (VPP in the portal) and native apps (`.ipa`)
- macOS: apps from Apps and Books and native apps (`.dmg` , `.pkg`)
- Android: Google Play Store apps, Managed Google Play Store apps (Android Enterprise) and native apps (`.apk`)
- Windows: Microsoft Store apps and installation packages in the formats `.msix` , `.msixbundle` , `.appx` , `.appxbundle` , `.msi` , `.exe` , and via Winget
- Web links: can also be managed and provided centrally

Relution allows unified and flexible management of all applications within an organization.

For native apps, using the Relution App Store is mandatory, whereas apps from Apps and Books or from manufacturer stores can optionally be managed through it.

Overview of the Apps Menu

For version 26.4.0

The Apps Menu in Relution is divided into the following sections:

- App Store - Relution's own app store for all supported apps and formats mentioned above.
- Requests - App requests from end users that can be approved by administrators or app managers.
- Categories - Allows apps to be categorized, e.g., for educational purposes.
- Purchased Apps - Overview of all apps from Apps and Books, including VPP tokens and synchronization options.
- Media - Overview of all books obtained via Apps and Books and of self-uploaded files, e.g., PDFs.

App Store Explained

The Relution App Store serves as a central repository for all supported apps across various platforms.

It provides an overview of available apps based on Name, Platforms, Status, Modified, and additional criteria. Additional columns can be displayed via the hamburger menu.

Using the add button, apps can be integrated from their respective manufacturer stores or uploaded natively. The following sources are available: Native app, Weblink, Windows Store app, Google Play Store app, Managed Google Play Store App (Android Enterprise), Apple App Store App and Winget Store app. The Managed Google Play Store App (Android Enterprise) source only appears if Android Enterprise is connected in the organization.

Sections in the App Store

When opening an added app, extended configuration possibilities and actual MAM functionalities become accessible.

- Information
    - Overview with current status and version (Development, Review, Release, Archive)
    - Description of the app (retrieved from the respective manufacturer store)
    - Changelog of the app (retrieved from the respective manufacturer store)
    - Additional Information such as internal app name or version
- Settings
    - General
        - Update automatically – only for store apps; refers to metadata from the respective manufacturer store (weekly updates)
        - Categories – allows the app to be categorized, e.g., for educational purposes
        - Responsible Person – assigned person or role for the app
        - Support Contact – contact address for app support
    - Permissions
        - Owner – owner of the app
        - Reviewer – permissions for app review
        - Developer – permissions for app development
        - Users – users or groups approved here can use or install the app
- Auto Deployments – specify users or groups that should automatically receive this app. The tab only appears once a version in the Release status exists; for macOS only for apps from Apps and Books.
- Scripts – only for Windows apps in `.msi` or `.exe` format
- Version assignments and App permissions – only in the global organization for local apps
- History – timeline of app updates and versions
- Devices with this App – overview of all devices where this app is installed

For version 26.4.0

Requests

Via the Relution Agent → or the Portal, users can request desired apps.

This enables the authorized user or administrator to approve apps, delete requests, adjust the status, and procure Apps and Books licenses if necessary.

This requires the App requester enabled toggle under `Settings` → `General Organization Settings` in the App Requests area. It is enabled by default and is not available in the global organization. If it is switched off, the Requests menu item is missing and no apps can be requested.

Categories

Admins and authorized users can create categories for apps and add respective apps to them, making them easier and faster to locate within the Relution Teacher App.

Purchased Apps

A dedicated overview for apps from Apps and Books for iOS, iPadOS, and macOS, including a manual sync function if required.

It allows filtering via VPP tokens and offers an overview of total license count, available licenses, and assigned licenses. Clicking on a specific app allows assigning licenses directly to devices, users, or groups. Further licenses can be purchased via the Purchase app context menu.

With a public VPP token, the assignments shown refer only to the current organization, while the total license count refers to all organizations.

Media

A dedicated overview for media from Apps and Books for iOS, iPadOS, and macOS, including a manual sync function if required.

It allows filtering via VPP tokens and provides an overview of total license count, available licenses, and assigned licenses. Clicking on a specific medium allows assigning licenses directly to devices, users, or groups.

Additionally, other media such as PDF or EPUB files can be distributed. They are added via Upload new PDF or ePUB and replaced via Update media content. Uploading is only possible if a VPP token is available in the organization. Further books can be purchased via Purchase books from Apple Store.

Processing App Requests

Requested apps are placed in the Review status. Without an active app release workflow, owners and reviewers of the app, i.e. by default the members of the App Reviewer group, can release or reject the requested version directly. Users with delete permission can remove the request. Optionally, a multi-step release process can be set up whose steps can be restricted to requested apps.

For version 26.4.0

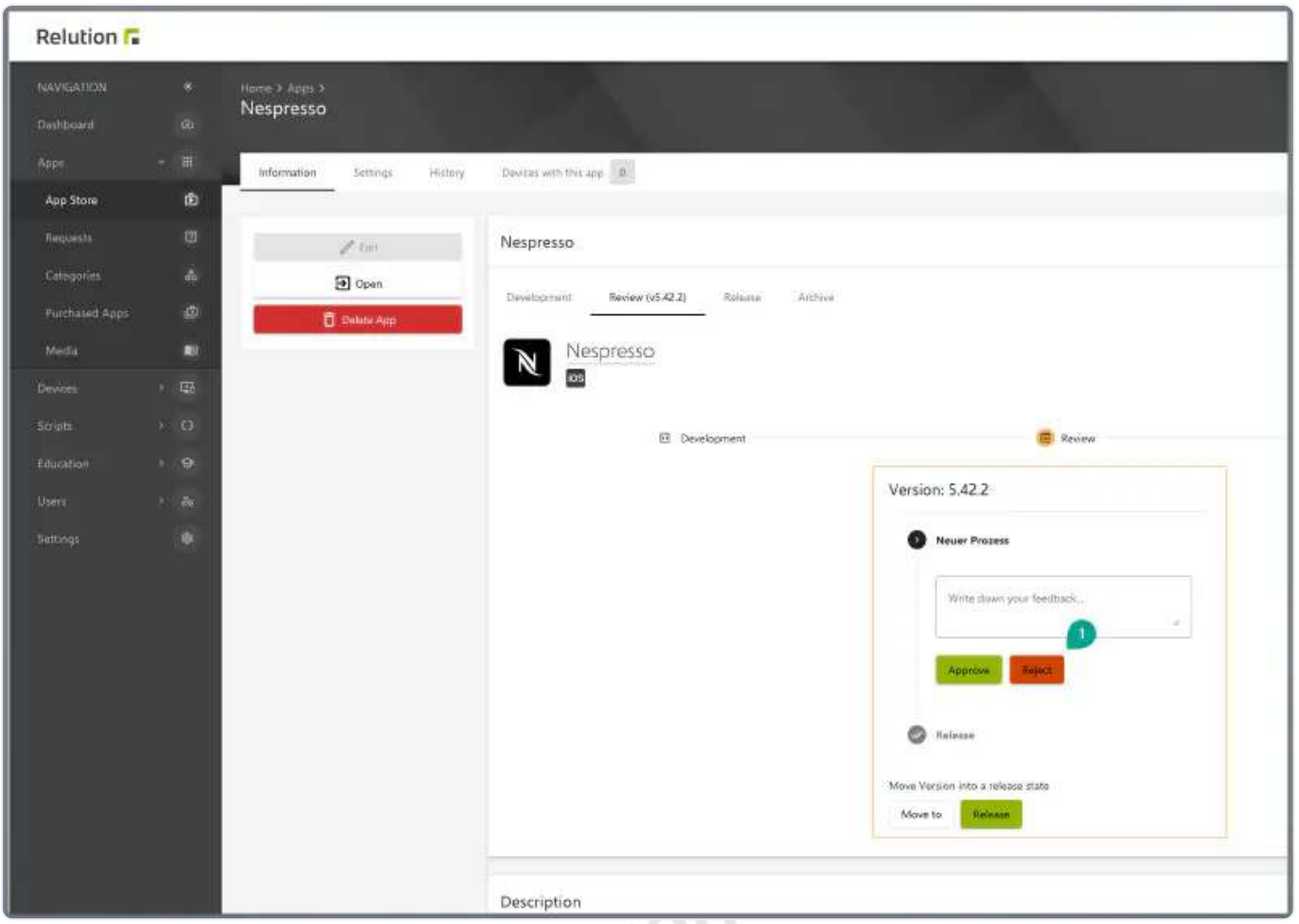
Setting Up the Process

An optional release process is configured under `Settings` → `App Release Workflow`. For details on individual release steps, responsibilities, and automated date arrangement, see App Release Workflow →.

Managing App Requests

Requested apps can be managed via the sidebar under the following menu item: `Apps` → `Requests`

In this section, pending requests can be reviewed and subsequently approved or rejected.



For version

App Store Default Permissions for New Apps

In Relution, the default permissions for new apps can be defined under `Settings` → `App Store`. This is particularly useful if apps should be explicitly available only to a specific group of users by default.

Default Configuration for New Apps

As long as the Enable toggle is switched off, new apps receive the following default assignment:

- Users: Appstore User and Device Manager
- Developers: Developer
- Reviewers: App Reviewer

After switching it on, all roles are initially empty and must be filled via App uploader or Assign User or Group. Without an assignment in the User role, new apps are not available to App Store users. After switching the toggle off and on again, the template is empty again.

When active, the app uploader is not allowed to assign individual permissions for an uploaded app. Instead, the defined default permissions are applied automatically. Users with the Appstore Manager role (including administrators) are exempt: for their uploads, the default permissions are only pre-filled and can be adjusted individually during upload.

Example: Configuration for the User Role

Within the settings, the following options are available for assignment:

1. App uploader: If active, the uploading user is automatically assigned to this role. If a user is assigned as the owner, they have the permission to modify all settings for the app.

2. Assign User or Group: Alternatively, a specific user or a predefined group can be defined for the use of the app.

For version 26.4.0

App Release Workflow

Under `Settings` → `App Release Workflow`, the steps an app version must go through before reaching the Release status can be defined. The process applies to versions in the Review status. Without an active process, any user with the Owner or Reviewer permission on the app can release a version directly. In the default app permissions, the organization's App Reviewer system group is entered as Reviewer.

Creating Release Steps

A release process consists of any number of freely sortable steps. Each step supports the following settings:

- Name and Description
- Type:
  - Standard – a regular release step.
  - Arrange go live date – adds a date-arrangement step to the version (see below).
- Responsible person or group: If none is set, the app owner is automatically responsible. If a user entered as responsible is deleted, responsibility passes to the organization's Appstore Manager group.
- Enforce this step: When enabled, the version must go through this step. As long as this step or a later step is enforced, the version cannot be moved directly from Review to Release. App owners with the Appstore Manager role, which administrators have automatically, are exempt.
- Conditions: A step can be restricted to specific apps (For certain apps), app types (Native, Public, Weblink), platforms (iOS, Android, macOS, Windows, tvOS), Price types (Paid/Free), specific App operations (Create/Update), or exclusively to requested apps (Only requested apps). If specific apps are selected, the app type, platform, price type and Only requested apps conditions no longer apply. If Only requested apps is enabled, the app type selection no longer applies.

For version 26.4.0

> A step that already has versions assigned to it can be neither edited nor deleted.

If the last release step is deleted, the release process is deactivated automatically.

Release with an Active Process

When the release process is active, every version in the Review status is assigned to the first matching step. Only the responsible person or the members of the responsible group, as well as app owners, can approve the current step. After approval, the version moves to the next matching step.

Once the last step has been approved, the version is published and receives the Release status. If a Go Live date in the future is set for the version, it is published automatically on that date.

For native apps, a preferred date can be entered in the Go Live date field for versions in the Development or Review status. While a step of type Arrange go live date is in progress, the date cannot be changed.

Arrange Go Live Date

If the process includes a step of type Arrange go live date, the uploader and the responsible person jointly propose a release date in the app's version detail view. Once both sides have agreed, the date is adopted as the Go Live date. If further steps follow in the process, the version first goes through them. After the process is complete, it is published automatically on the agreed date.

Enabling/Disabling the Process

The entire release process can be enabled or disabled via the 3-dot menu:

- Enable Workflow: All versions in the Review status are moved into the first matching release step. If a version was already in a step before, its release history is restored. Enabling is only possible once at least one step has been created.
- Disable Workflow: Owners and reviewers of the app, and therefore by default also the members of the App Reviewer group, can release versions directly again.

Providing a Native App in the Relution App Store

Relution supports the provision of native apps and installation packages, for example IPA, PKG, DMG, APK, MSIX, MSIXBUNDLE, APPX, APPXBUNDLE, MSI and EXE files. This also allows different versions of an app, such as developer or test versions, to be provided specifically and tested in advance.

For version 26.4.0

Under `Apps` → `App Store`, the Native app source is chosen via Add and confirmed with Next.

The desired installation package is uploaded via Select.

Once the installation package has been uploaded, the form is opened via Add details. In the General section, the Release status is selected in the Release status field. The status name appears as a tooltip on the respective icon. The Release status is only available to app owners. A version created directly in the Release status does not go through a release process.

Apps with the Release status can be downloaded by all authorized users via the Relution App Store.

This area also shows the version name as well as the creation and modification date of the app.

Finally, the entries are applied via Save in the upper right corner.

After saving, an overview of the stored app is displayed. Among other things, it shows the platform for which the app is available as well as further information and settings.

The Relution App Store also shows the type of app and the platform for which it is provided.

Providing a Developer or Test Version to Specific Users

If a further version of the same app – for example a developer or test version – is to be provided only to specific users, it is created in the Review status.

The desired app is opened in the Relution App Store and a new version is created via Add new version.

The new version is then uploaded as a native app as described above. In the General section, the Review status is selected in the Release status field and the changes are saved.

As a result, the version is not visible to regular App Store users. Review versions are only visible to persons with the Owner, Reviewer or Developer permission on the app, and to administrators. The access always applies to all review versions of the app, not to a single version.

Access via the App Permissions

Individual testers are given access specifically via the app itself: In the app's Settings tab, the person is entered under Reviewer or Developer in the Permissions section via Users and Groups. As a Developer, the person sees review versions but cannot release them. However, they can edit review and development versions and delete the app. The Permissions section is available to app owners.

Access via the App Reviewer Group

Alternatively, the user is added to the organization's App Reviewer system group. To do so, the user is opened under `Users` → `Users`, and the Manage groups button is selected in the Groups & Permissions section. The group is assigned there. Its name begins with the organization name. If the organization is called "Support", for example, the group is named Support App Reviewer.

Members of this group are entered as Reviewer in the default app permissions. They therefore see the review versions of all apps whose permissions contain the group. If a template for the default permissions is active under `Settings` → `App Store`, this only applies if the group is included in it (App Store Default Permissions →).

> As Reviewer, the members of the App Reviewer group may also release versions of these apps, i.e. move them from Review to Release or Development. If no app release workflow is active, this happens without any further check. For individual testers, the Developer permission on the app is therefore the more targeted approach.

For version 26.4.0

Users without any of these permissions only see versions with the Release status. Users with access to review versions additionally see the Review area in the top bar of the Relution App Store.

See also Processing App Requests → for reviewing requested apps afterward.

User Management

Relution features an internal user management system that supports creating user accounts manually or adding them via external providers. Some key points and special considerations are explained below.

Users Overview

- Each user is created within a single organization in Relution.
- A user cannot belong to multiple organizations simultaneously.
- Multi-tenant support is available for administrative accounts, but the user account always resides in the original tenant.
- All user accounts are stored in the database.
- Email addresses must be unique; this is checked across all organizations on the server. User names must be unique within an organization.

Adding User Accounts

There are several ways to add user accounts:

1. Manual account creation
2. CSV file upload
3. Integration with external providers (e.g., LDAP → or Microsoft Entra ID →)

For version 26.4.0

The context menu of the user list also offers Invite users (invitation by email) and Create multiple users. Both entries require the permission to create users.

1. Manual Account Creation

- In the Users section, clicking Add opens the input form.
- All required fields must be filled in: user name, password, given name, surname (up to 50 characters each) and email address.
- With the Disable password based authentication option, no password is set. Sign-in is then only possible via an external identity provider (e.g. OpenID Connect or SAML) or an API token. The option can only be set when the account is created and cannot be reverted afterwards.
- The Custom properties section (collapsed by default) provides 15 fields with up to 255 characters each. Fields 1–10 can be used as placeholders `${user.custom1}` to `${user.custom10}` in policy configurations; fields 11–15 are stored but not substituted as placeholders.
- Permissions and groups should be defined as needed.
- More information about permissions can be found in the article Permissions →.

Create multiple users creates up to 50 user accounts at once. The user name must contain the placeholder `%N`, which is replaced by an ascending number (default `user-%N`); the start value is set in the Start of %N field.

2. CSV File Upload

The CSV import function is available for importing multiple user accounts. The complete process, including the template, preview, and optional group or permission assignment, is described in the article CSV Import →.

> Passwords stored in the CSV must meet the password policy under `Settings` → `Login Management`, in particular the Minimum password length. Rows with non-compliant passwords are not imported.

3. Integration with External Providers

- When using an external provider (e.g., LDAP →, Microsoft Entra ID →), the provider is always the leading system.
- Imported content is updated automatically if it changes on the provider side.
- The fields user name, given name, surname, email address, position, phone and country are locked in the portal, as they will be overwritten during the next synchronization.
- During login, Relution always authenticates against the configured LDAP →. If the connection is unavailable, the user cannot sign in.

The configuration of the connection is explained in detail in the articles on the individual providers. For schools, the OneRoster Interface → and SchulConnex Import → connections are also available.

User Groups

For version 26.4.0

User groups are managed under `Users` → `Groups`. Groups bundle user accounts — for example, to assign permissions via group membership. Permission roles → can be assigned to individual users as well as to groups — members receive the permissions of their groups.

- Add group: A new group is created via Add in the group overview.
- Manage members: Members are added or removed via Manage members in the group details. Both user accounts and other groups can be members of a group (nested groups). For groups synchronized by a provider (e.g. from LDAP), the members are read-only.
- Delete: Groups that are no longer needed can be deleted from the group list.
- System groups: They cannot be deleted; their name and description cannot be edited, and other system groups cannot be added as members.

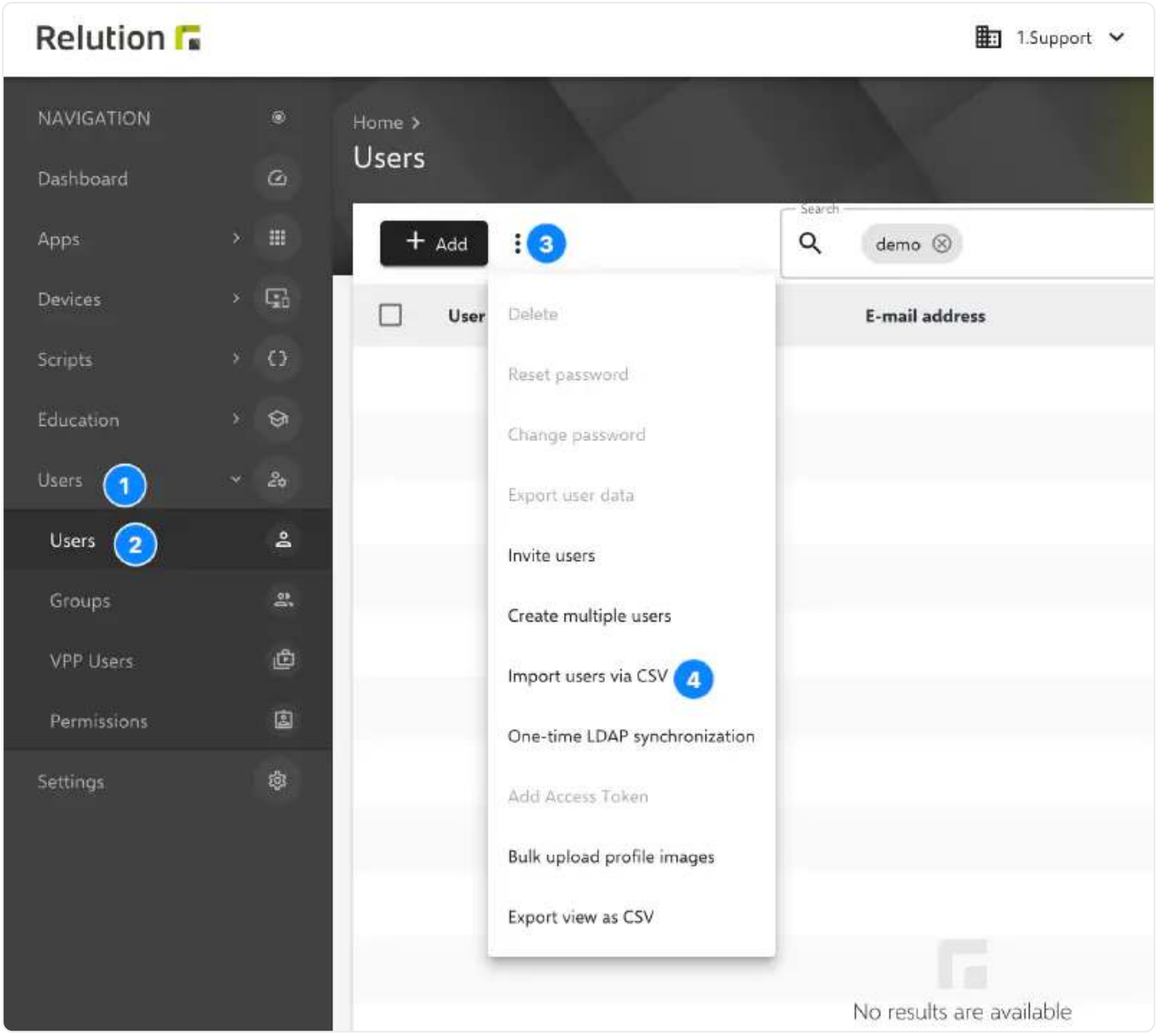
The group memberships of an individual user can also be managed in the user details in the Direct Memberships area under Groups & Permissions via Manage groups.

CSV Import

To manage a large number of users efficiently, the CSV import function can be used. It requires the permissions to create and to update users. The following steps are required:

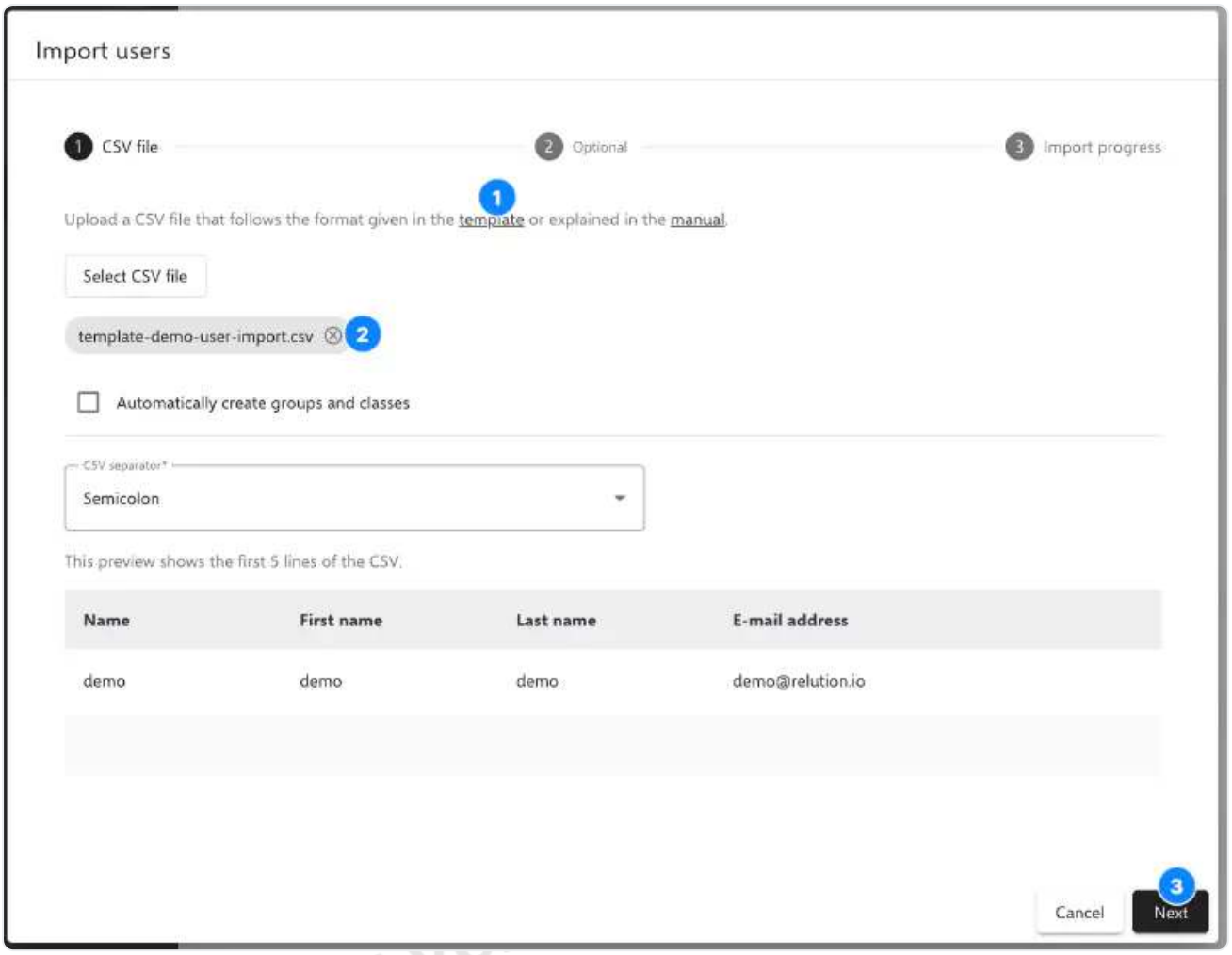
For version 26.4.0

1. Access the Menu: The Users navigation point in Relution is opened.
2. Start Import: In the 3-dot menu, Import users via CSV starts the import.

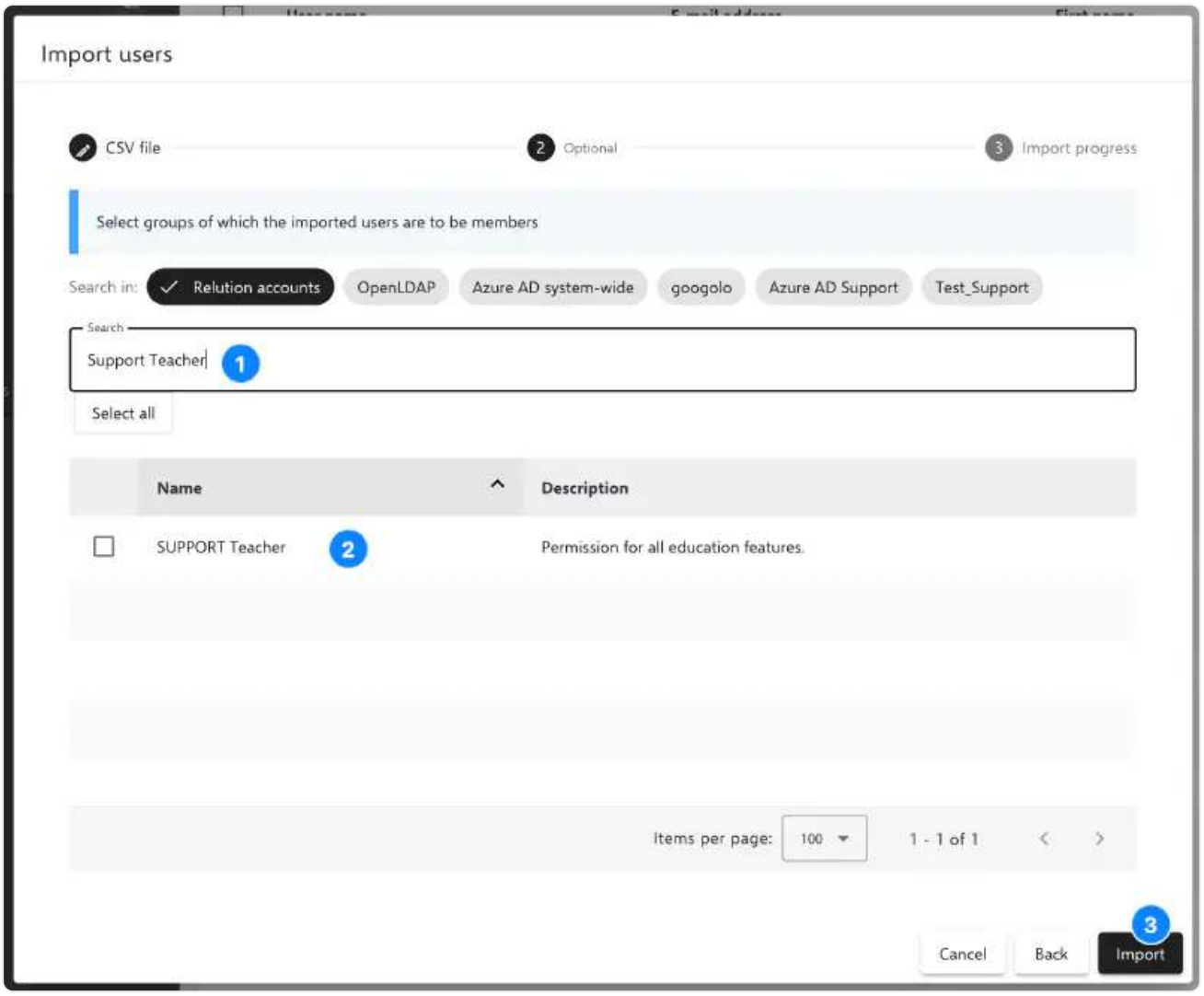


3. Use Template: The provided CSV template is downloaded. It uses the separator selected in the CSV separator field (Comma or Semicolon) and contains the columns `name`, `email`, `givenName`, `surname`, `password`, `disablePasswordAuthentication`, `phone`, `position`, `country`, `managedAppleId`, `locale`, `permissions`, `memberOfGroups`, `teacherOfClasses` and `studentOfClasses`.
4. Edit Data: The file is opened in an editor of choice and the required values are entered.
5. Upload File: The edited CSV file is uploaded back to Relution in the CSV file step. This step also contains the option Automatically create groups and classes (see below).

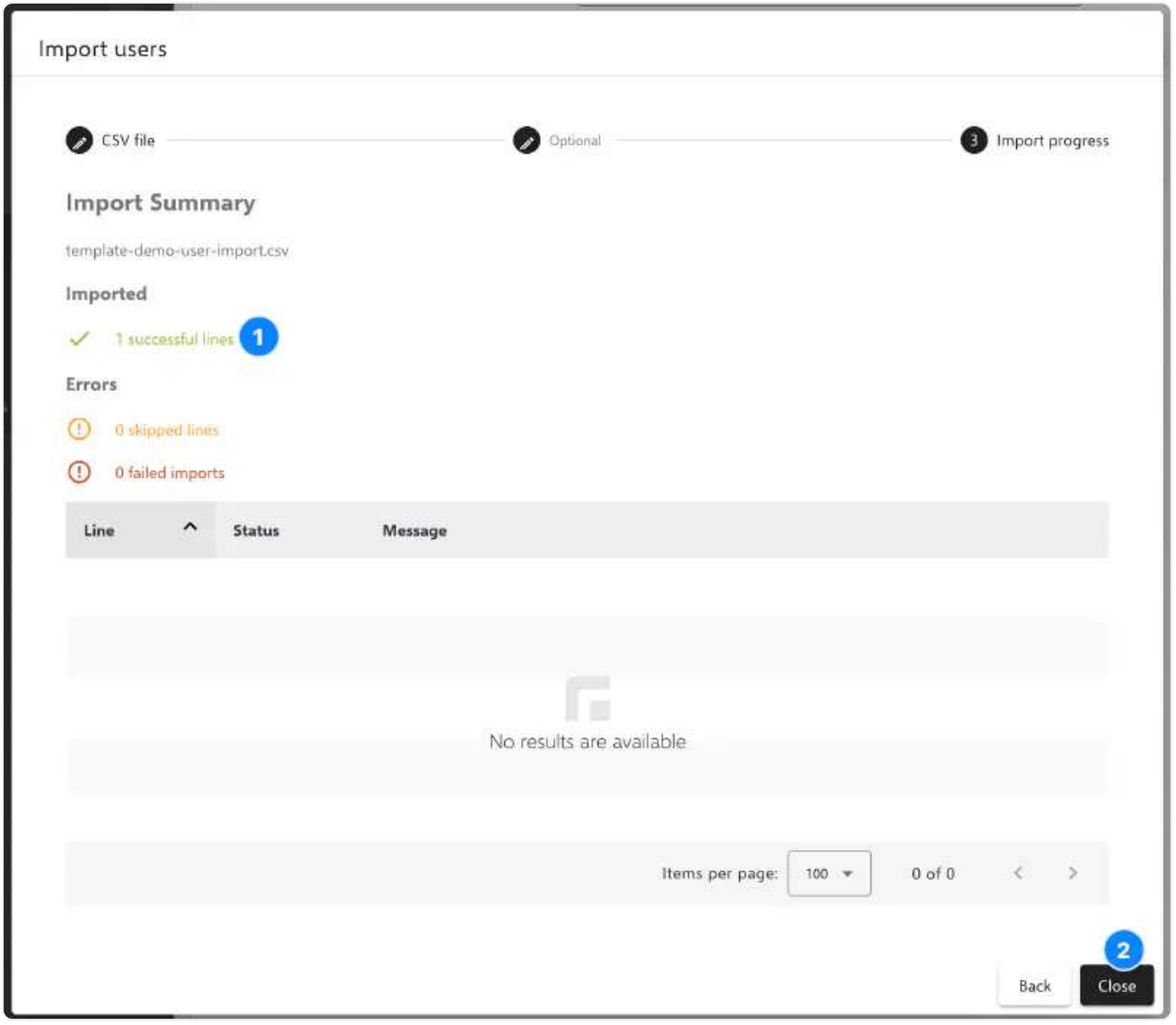
6. Review: The Preview shows the first 5 rows for verification.



7. Assignment (Optional): Users can be added directly to existing groups during this process. This step is only shown with the permission to read groups.



8. Completion: The import progress shows the current status. The summary distinguishes successful, skipped and failed lines and lists the message for each line.



Important Configuration Notes

- Password Policies: If fixed passwords are defined, they must comply with the password policy of the respective organization. For example, if the policy requires at least 8 characters, the import will fail for any users whose passwords contain fewer characters.
- Class Assignment: Teachers and students are assigned to classes via the `teacherOfClasses` and `studentOfClasses` columns. Multiple classes in one cell are separated by `|`. Membership in a group (e.g. `UIT Teacher`) does not assign anyone to a class. A class is only saved if it then has at least one teacher and at least one student; for existing classes, the previous members count as well. Otherwise, this class is listed as skipped in the import report, while the users themselves are still imported. A class that does not exist yet is only created if the option Automatically create groups and classes is enabled; otherwise, the line is reported as failed.
- Group Assignment: Groups (e.g. the system groups `UIT Teacher` and `UIT Student`) are assigned via the `memberOfGroups` column, permissions from `Users` → `Permissions` (e.g. `Self service portal - read access`) via the `permissions` column. The exact name is decisive in each case. The organization's system groups carry its unique name as a prefix, e.g. `UIT Teacher`; self-created groups are entered with their own name. If the name of a permission is entered in `memberOfGroups`, the import fails for this line with a message that the group could not be found; if Automatically create groups and classes is enabled, a new, empty group with this name is created instead.
- Updating Existing Users: The CSV import can also be used for already existing user accounts. Matching accounts are identified by the `name` column (username) within the same organization and updated with the values from the CSV file instead of being created again. The email address is not used for this matching. Users managed by an external provider (e.g. a directory service) are skipped. Imported users are always activated.
- Empty Columns During an Update: If a column exists in the CSV file but its value is empty for a given row, the corresponding field of the existing user is cleared. The columns `permissions`, `memberOfGroups`, `teacherOfClasses` and `studentOfClasses` are an exception: an empty cell leaves the existing assignments unchanged. A filled-in value, however, replaces the previous assignments completely; permissions and groups not listed are removed, as are classes not listed in which the user is entered as teacher or student. The groups additionally selected in the import dialog are added in any case. For all other columns: columns whose existing values should remain unchanged must be removed from the CSV file entirely rather than just left empty.
- Password During an Update: If the `password` column is empty or omitted for an already existing user, that user's current password remains unchanged. For newly created users without a password value, no password is generated automatically; an initial password needs to be set for them in a separate step.
- SSO-only Sign-in: The `disablePasswordAuthentication` column only takes effect when a user is created; during an update, the previous value is kept.

Behavior in Practice

A few concrete examples for updating existing users via the CSV file:

- The **`email`** column is present but left empty for a row: The user's existing email address gets deleted. To keep it unchanged, the `email` column must be removed from the CSV file entirely.
- The **`memberOfGroups`** column is present but left empty for a row: The user's existing group memberships remain unchanged. If the cell contains `UIT Teacher` instead, the user is afterwards only a member of this group and of the groups selected in the import dialog.
- How an existing user is recognized during an update: Exclusively by the `name` column (username) within the same organization — the email address plays no role in this.
- The **`password`** column is left empty: For an already existing user, the current password remains unchanged, regardless of whether the column is missing or just empty. For a newly created user, no password is generated automatically in this case.

Naming Example:

- Organization Name: `User-Import-Test`
- Unique Organization Name: `UIT`
- User Groups: `UIT Student`, `UIT Teacher`

A CSV file with one teacher and one student, each assigned a group via the `memberOfGroups` column and the class `10a` via `teacherOfClasses` or `studentOfClasses`, could look as follows:

```
name;email;givenName;surname;permissions;memberOfGroups;teacherOfClasses;studentOfClass
es
teacher1;teacher1@uit-school.com;Jane;Teacher;;UIT Teacher;10a;
student1;student1@uit-school.com;Sam;Student;;UIT Student;;10a
```

Multiple groups, permissions or classes within the same cell are separated by a pipe character (`|`), for example `UIT Teacher|UIT Student`. This applies to the columns `memberOfGroups`, `permissions`, `teacherOfClasses` and `studentOfClasses`. A semicolon can also be used as a separator within the cell; however, since it may already separate the columns themselves depending on the chosen CSV separator, using `|` is recommended for unambiguous results. A comma does not separate values within a cell.

Automatic Creation of Missing Groups and Classes

Relution can automatically create classes and user groups that do not yet exist during the CSV import. This requires the option Automatically create groups and classes to be enabled in the first step (CSV file). The option is disabled by default and can only be enabled with the permissions to create groups and classes. Without this option, lines with groups or classes that do not exist are reported as failed. Permissions from the `permissions` column are never created automatically; they must already exist. The following points apply:

- Precision: The exact spelling of the name is decisive; a different spelling results in a new group or class.
- Whitespace: Leading and trailing spaces around group, class and permission names are removed automatically during import.
- Managed Classes: Classes synchronized by an external provider are skipped during the import.

Common Reasons for a Failed Import

A common reason for a failed CSV import is an email address that is already assigned to another user account on the server. Email addresses must be unique across the entire server, regardless of which organization the respective user belongs to.

For version 26.4.0

Education function

Relution's innovative education feature makes it easier to prepare classes by seamlessly integrating them into the Relution Teacher App. This feature allows teachers to easily start and manage classes. Relution classes are made up of teachers and students, each with specific permissions. The clear structure and user-friendly interface of the Relution platform makes the organization and delivery of lessons more efficient. More information about the education function and other features of Relution is available on the website at www.relution.io.

> The Education menu item is only displayed in organizations with a valid Education or Free license. It contains the entries Classes and Relution Teacher; Relution Teacher opens the Teacher web app directly.

Create users

New users are created in the Users menu item and assigned the corresponding authorizations. The available creation methods (manual creation, CSV upload, LDAP synchronization) as well as the rule on unique e-mail addresses are described in the article on user management.

User Management →

For version 26.4.0

Assign Permissions

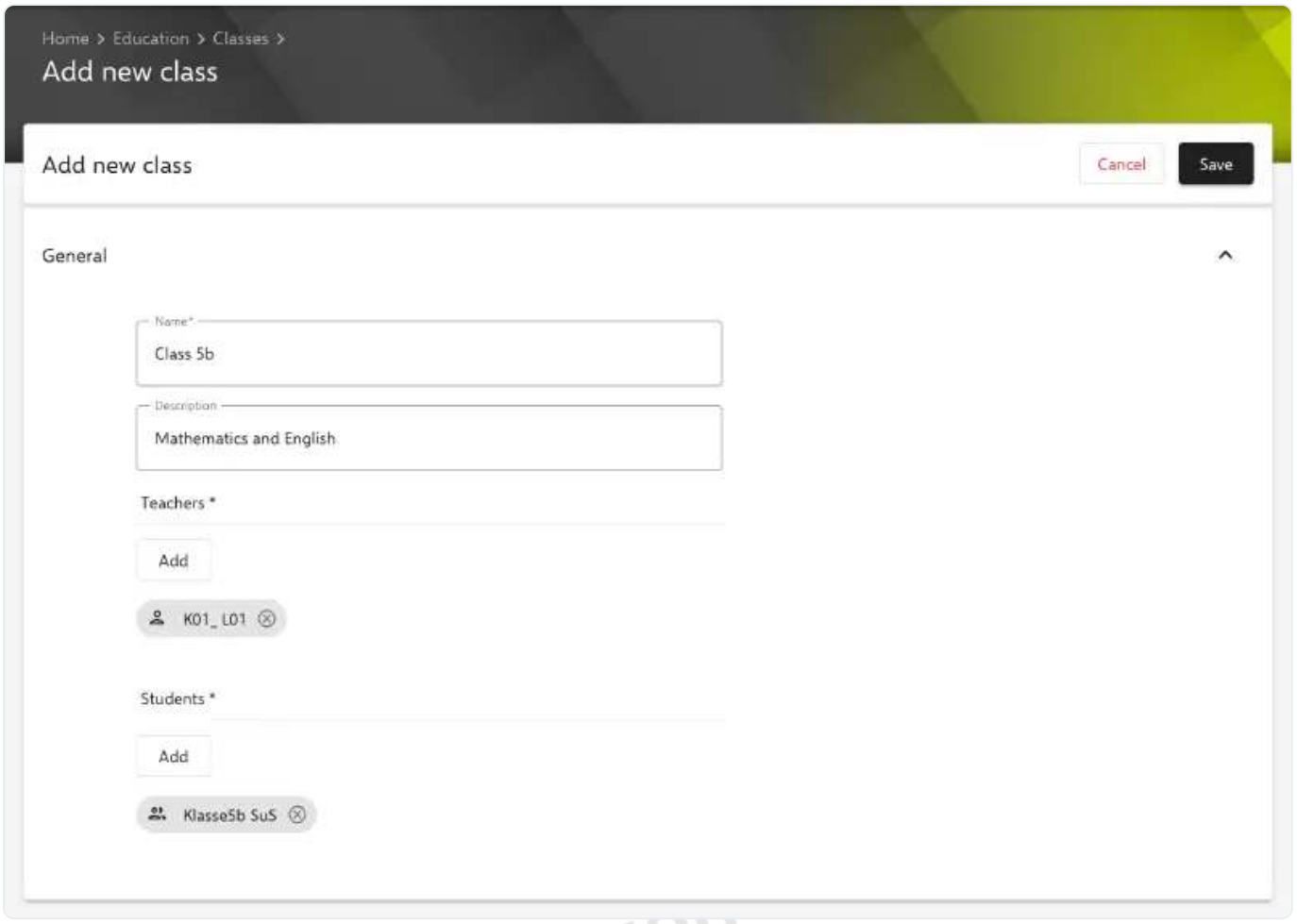
In the menu item `Users` → `Groups`, groups can be assigned to existing users. Two important standard groups are already stored: `<ORGANIZATION> Teacher` and `<ORGANIZATION> Student`. The group name starts with the unique name of the organization in capital letters, e.g. `SCHOOL Teacher`. These groups are not created in the system organization.

The two groups differ both in terms of their rights and the scope of their functions. For example, starting a lesson via the Relution Teacher App is reserved for the Teacher group; students (Student group) do not have this right. The system groups `Device Manager` and `Appstore Manager`, and therefore also `Administrator`, are members of the Teacher group and inherit its rights. This clear distinction makes it easier to manage users and ensures that rights are assigned according to the respective tasks and responsibilities.

If several user accounts are to be given `Teacher` or `Student` at the same time, the assignment can also be done directly during the CSV import, see CSV Import →.

Create Classes

In the menu item `Education` → `Classes`, classes can be created manually and assigned to users according to their role. The Name is required; in the global organization, the target organization is selected as well. Teachers and students can be assigned as individual users or as entire groups. A class must consist of at least one teacher and one student (each as a user or group) in order to be created correctly.



For efficient administration, there is the option to create multiple classes quickly and easily using the CSV upload function. The most convenient solution is synchronizing classes from an external system, as it enables automatic updating and uniform management of classes. In addition to LDAP, the following interfaces are available for this purpose:

- SchulConnex Import →
- OneRoster Interface → (e.g. for Untis/WebUntis)
- Apple School Manager import →

Classes synchronized via such an interface are read-only in the portal and are maintained exclusively in the source system.

Using Relution Teacher and/or Apple Classroom

The classes created can be easily prepared for teaching using the Relution Teacher App. More details about this process are available in the article about the Relution Teacher App.

Teacher →

To control the devices during lessons, the Apple Classroom App can also be used. More information is available in the article on the Apple Classroom App.

Apple Classroom →

In summary, it can be said that the Relution Teacher App is used to prepare lessons, while the Apple Classroom App enables control during the lesson.

For version 26.4.0

Permissions

Relution allows permissions to be configured very precisely and in a fine-grained manner. This ensures that for each use case, a specific permission set can be created without giving users more functionality than necessary.

A permission can also enforce multi-factor authentication (MFA) for all users who have this permission. In addition, permissions can be made available to all organizations from the Global organization, and to all sub-organizations from a meta organization.

Overview of Permissions

Under `Users` → `Permissions`, default permissions are already available, e.g. Administrator, Teacher or Student. They apply globally to all organizations, correspond to the system groups and are linked to them. In the list, they are marked in the System column. These default permissions are managed automatically and cannot be modified, deleted or exported.

However, it is always possible to create new custom permissions.

> Permissions are additive, meaning that all permissions assigned to a user account are combined.

For Version 26.4.0

Configuring Permissions

In the Permissions category, a new entry can be created by clicking Add. The Name is mandatory (up to 255 characters); a Description (up to 4000 characters) is optional. Almost every function available in the Relution Portal can be assigned individually.

Typically, there are four options: Read, Create, Update, and Delete. If an option requires another one, the required option is enabled automatically and locked, e.g. Create requires Read.

For example, a user can be given an account with read-only permissions, preventing them from making changes to the system.

Device actions can also be configured individually.

- Example: All actions are allowed except for device location tracking.
- Another use case: A user may only renew the tokens for Apps and Books (VPP in the portal) and Automated Device Enrollment (ADE, DEP in the portal) but not make any other changes. For Apps and Books, this requires the Update option in the Volume Purchase Programm (VPP) entry; for ADE, the Create option in the Apple Automated Device Enrollment entry. There is no Update option for ADE; with Create, the user can also add new ADE server accounts.

Enforcing Multi-Factor Authentication

With the Enforce multi-factor authentication for the role option, all users with this permission must sign in using MFA. The Multi-factor authentication section only appears if at least one MFA method is enabled under `Settings` → `Login Management`. Since the default permissions cannot be modified, a custom permission is required for this. Details can be found in the article Multi-factor authentication →.

Scope

The Scope column shows where a permission applies: Local (only in the own organization), Meta (in all sub-organizations of a meta organization) or Global (in all organizations). New permissions are created locally.

In the Global organization, the context menu entry Set visibility to global makes selected permissions available in all organizations; in a meta organization, Set visibility to meta makes them available in all sub-organizations. This does not assign the permission to anyone; it only becomes available for selection there.

Exporting and Importing Permissions

Via the context menu of the list, selected permissions can be saved as a JSON file with Export permissions and read in again with Import permissions, e.g. in another organization. Imported permissions are always created locally. Default permissions cannot be exported.

Linking Permissions to User Accounts

In the user account, a permission is assigned in the Direct Memberships area under Groups & Permissions: the Manage Permissions button in the Permissions field opens the selection.

Permissions can also be assigned to a group in the same way. All members of the group then receive them, including via nested groups.

For version 26.4.0

Assigning Permissions During CSV Import

Permissions can also be assigned when creating multiple user accounts through the CSV import. The import process itself is described in CSV Import →.

The assignment can be done in three ways:

- In the `permissions` column of the CSV template, permissions are entered per row using their exact name, e.g. `Teacher` or `Student`. Multiple entries are separated by `|`.
- In the `memberOfGroups` column, groups are entered using their exact name, e.g. the system group `[Organization] Teacher`. The user account receives the group's permissions through the group membership.
- In the optional Groups step of the import dialog, one or more existing groups are selected. All imported user accounts become members of these groups in addition to the groups from `memberOfGroups`. This step is only visible with read permission on groups.

An unknown name in `permissions` causes the affected row not to be imported. The same applies to `memberOfGroups` unless the Automatically create groups and classes option is enabled; with this option, a new, empty group without permissions is created.

> The names of the system groups include the unique name of the respective organization, e.g. [Organization] Teacher or [Organization] Student. The corresponding default permissions are named without this prefix, e.g. Teacher or

Student.

For version 26.4.0

Self-Service Portal

As of version 5.22, Relution has a self-service portal. Here Relution users can view their own devices, carry out individual actions and request details.

Requirements

Two default permissions are available for using the self-service portal. They are created automatically during an update to Relution 5.22 or when the database is created. To make the Self-Service Portal available to users, they must have the appropriate permission and have linked at least one device to their user account.

Granting permissions

Under `Users` → `Permissions`, `Self service portal - full access` and `Self service portal - read access` are available as templates. Depending on the requirements, these must be linked to the desired accounts.

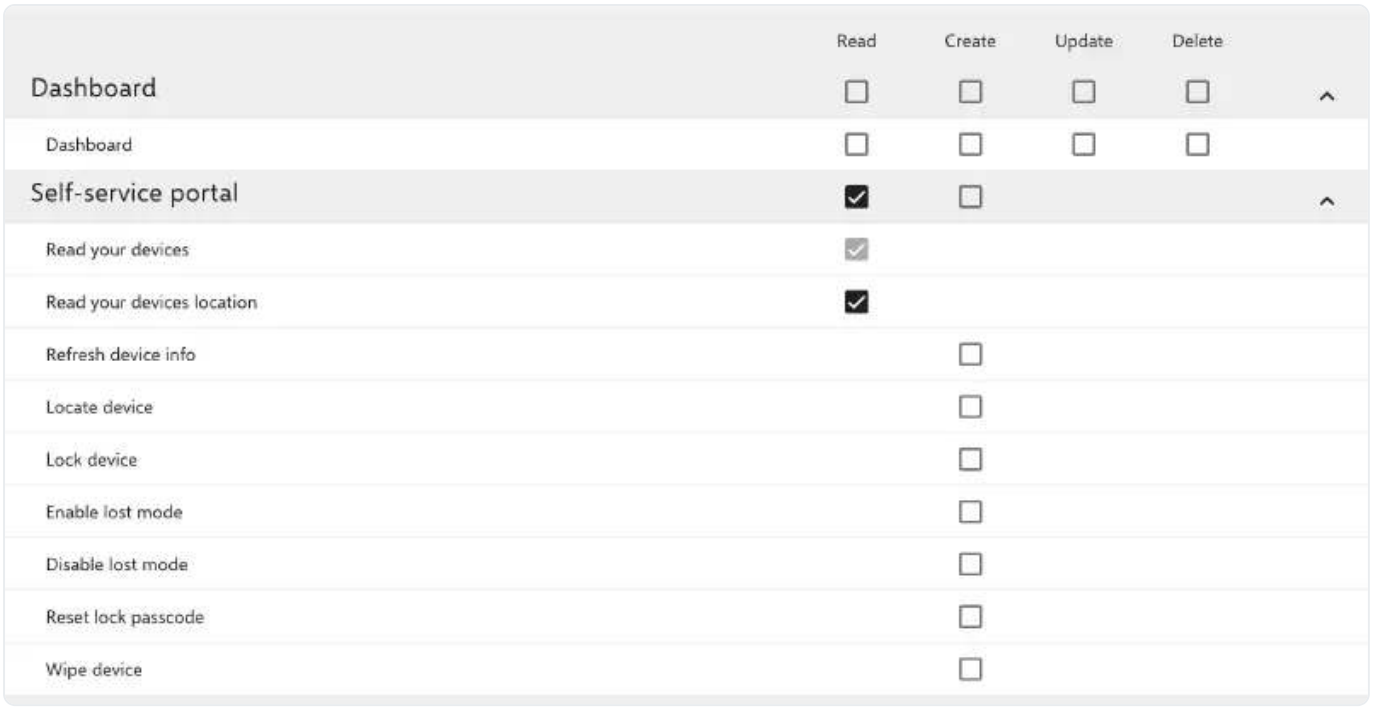
- `Self service portal - read access` only allows viewing the user's own devices and refreshing their device information.
- `Self service portal - full access` additionally allows reading the location, locating the device, enabling and disabling lost mode, locking the device, resetting the lock passcode, and wiping or deleting the device.

For version 26.4.0

For custom permissions, the individual rights are available in the Self-service portal category, e.g. Read your devices, Read your devices location and a separate right for each action.

The assignment is done as follows:

1. Under `Users` → `Users`, the relevant user account is opened.
2. In the Direct Memberships area under Groups & Permissions, Manage Permissions in the Permissions field opens the selection.
3. One of the above permissions is selected there.
4. Save applies the assignment.



Linking a device to the user account

A user account can be linked to a device either by importing a CSV file, by configuring the enrolment accordingly before enrolment or manually.

For the manual method, it is only necessary to select the device from the inventory and select the Change device user icon from the toolbar.

For version 26.4.0

The Self-Service Portal

If a person logs in to the Relution portal with the corresponding user account, the self-service function is available. Users who only have self-service permissions are taken directly to the Your devices page after signing in; administrators reach it via the profile menu at the top right.

Since Relution 26.5.0, signing in to the Self-Service Portal uses a dedicated scope (`/api/selfService/`). If OpenID Connect with scoped redirect URIs is used for this, the corresponding redirect URI must be registered with the identity provider, see OIDC with Entra → or OIDC with Workspace →.

For each device, basic information is displayed, e.g. battery status, status, last connection, platform, owner, model, serial number, operating system, enrollment date and lost mode status. The following functions are also available:

- Enable / disable lost mode
- Locate device
- Show location on a map
- Wipe device
- Lock device
- Reset lock passcode

Wipe device opens the Remove dialog. There, a choice is made between resetting the device to factory settings and Delete (removing the device from the MDM). The Refresh device informations of all visible devices button on the Your devices page queries the information of all displayed devices again; by default, a new query is possible at the earliest 5 minutes after the last refresh.

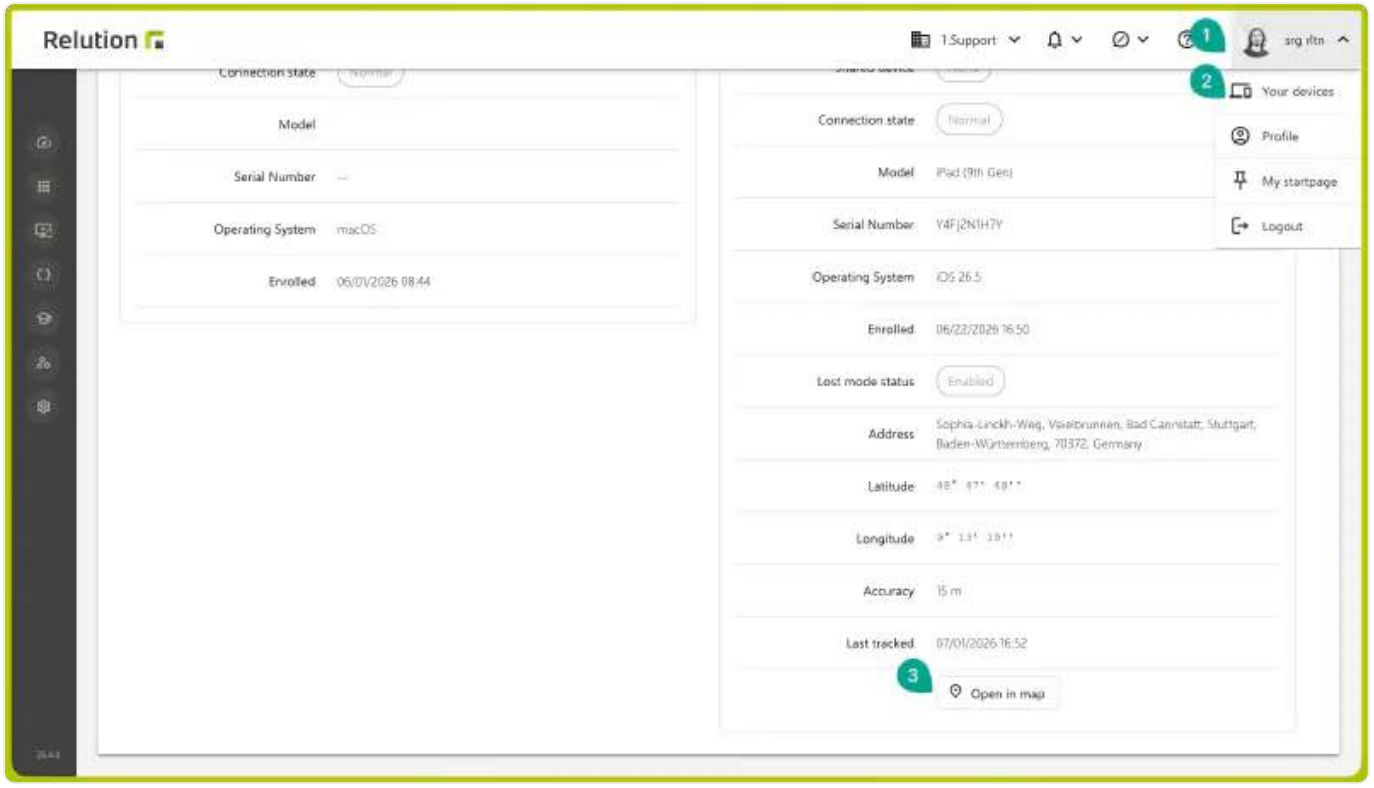
The available functions may vary depending on the device platform. On iOS devices, lost mode and locating are only available on supervised devices, and locating additionally only while lost mode is enabled. While a device is being deleted or retired, the actions are locked. The functions can also be restricted via permissions.

Show location on a map

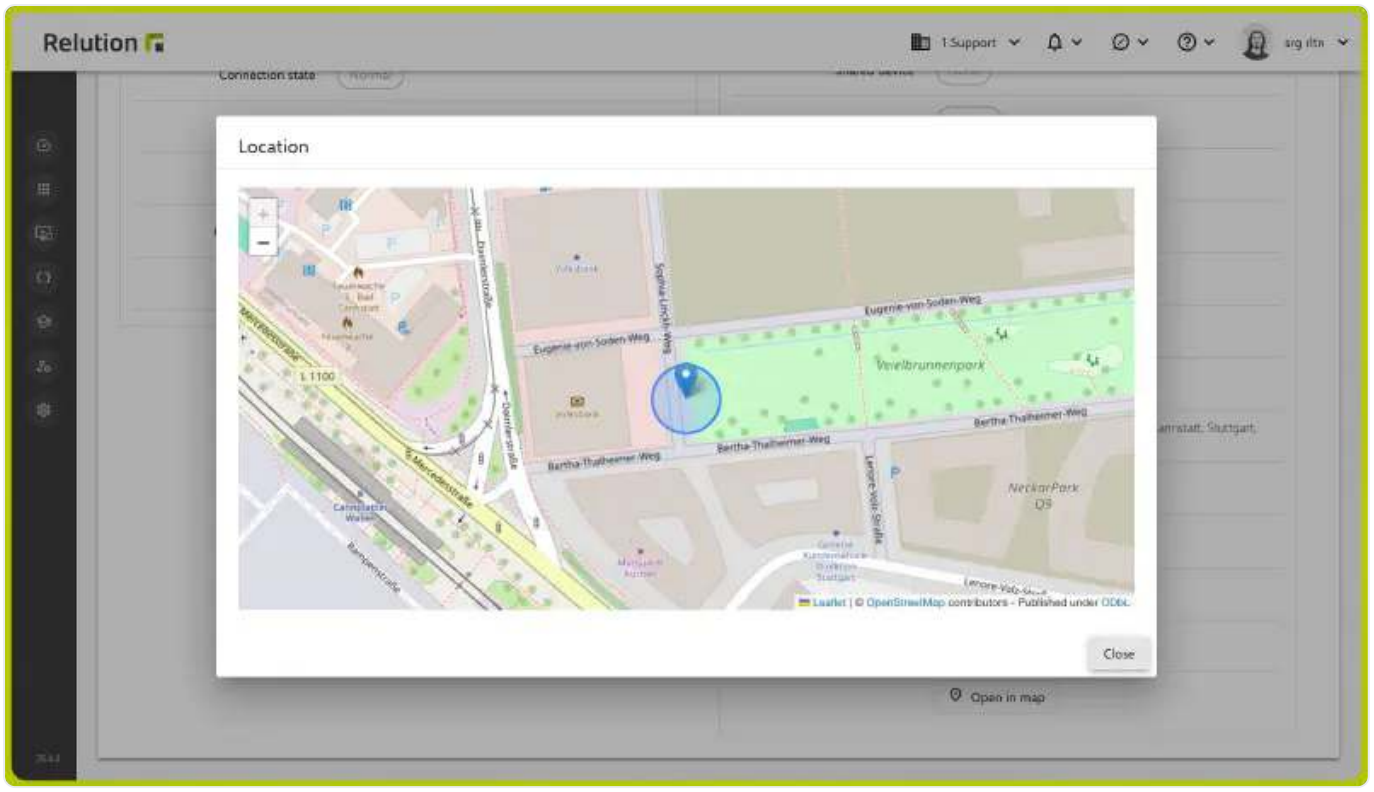
New in 26.4

Users with the corresponding permission can display the last known location of their device directly on a map.

1. The profile icon in the top right corner opens Your devices.
2. In the relevant device, Open in map in the location section opens the map.



The last known location is then displayed on a map view.



This requires the Read your devices location permission. It is included in `Self service portal - full access`, but not in `Self service portal - read access`. Without it, the location section is not displayed. The location section is available for iOS, Android (including Android Enterprise) and Windows devices; on iOS devices only if the device is supervised and lost mode is enabled. No location is displayed for macOS and ChromeOS devices.

For Android Enterprise devices, activated location services as well as the corresponding permission of the Relution Companion are also required; see Locate Android Device → and Location Services →.

For version 26.4.0

Advanced placeholders

Placeholders such as `${user.email}` or `${device.model}` are used in several places in Relution, for example in device names, certificates, Exchange accounts or app configurations. The underlying template engine `FreeMarker` provides additional functions that allow placeholders to be customized further.

Substrings

The notation `[start..*length]` extracts only a portion of a value: at most `length` characters from position `start`. Counting starts at `0`. If the value is shorter, correspondingly fewer characters are inserted; if it is empty, none. This requires `start` not to lie beyond the end of the value; otherwise the substitution fails as with `[start..end]` (see the note below).

- `${user.givenName[0..*1]}` → first letter of the given name
- `${device.model[0..*2]}` → first two characters of the device model

Example:
`${user.givenName[0..*1]}${user.surname[0..*1]}-${device.model[0..*2]}-${(device.custom1)!"00000"}` results in `MM-iP-00042` for a user account “Max Mustermann” with a `custom1` value of `00042` on an `iPad12,1`.

> The alternative notation `[start..end]` (e.g. `[0..0]`) requires the value to extend at least to position `end`. If the value is set but shorter or empty, the substitution fails and none of the placeholders in the affected text are replaced. The same applies to `[start..*length]` if `start` is greater than the length of the value.

For version 26.4.0

Default value for unset fields

If a field is not set, a default value can be provided using the `!` operator: `${(device.custom1)!"00000"}`. If the custom field `custom1` is not set, `00000` is used instead of the placeholder remaining empty. A value that is set but empty, however, counts as present: the default value does not apply and the placeholder remains empty.

Case conversion and character replacement

Using `?lower_case` or `?upper_case`, a value is converted entirely to lower or upper case. With `?replace("old", "new")`, individual characters or character sequences can be replaced, for example to resolve umlauts for systems that do not allow special characters in user names:

`${user.surname?lower_case?replace("ä","ae")?replace("ö","oe")?replace("ü","ue")?replace("ß","ss")}`

> This function is particularly relevant for macOS enrollments with user authentication, as special characters in the local account name can cause script deployments to fail.

Using the local part of an email address

To use only the part before the `@` sign of `${user.name}` (or `${user.email}`), several variants are available:

- `${user.name?keep_before("@")}`
- `${user.name?split("@")[0]}`
- `${user.name[0..user.name?index_of("@")-1]}`

If the value contains no `@`, the first two variants return the complete value, while the third one fails. `?keep_before` is therefore recommended.

User certificates

New in 26.5

Placeholders of the form `${user.certificate.…}` insert the certificates stored on the user profile (section User Certificates) into a configuration as a base64-encoded string — for example into a managed app configuration whose fields expect a certificate as a base64 string. The placeholder is resolved when the configuration is transferred to the device, based on the user assigned to that device.

For version 26.4.0

Three selection forms are available:

Placeholder	Resolution
`${user.certificate.EXCHANGE}`	Certificate of the subtype with the longest remaining validity
`${user.certificate.EXCHANGE["my-certificate"]}`	Certificate with exactly this name (case-sensitive); if there are several with the same name, the one with the longest remaining validity
`${user.certificate.EXCHANGE[device.serialnumber]}`	Certificate name computed from another placeholder

The subtype is the Category selected for the certificate on the user profile. The subtype is not case-sensitive.

Category on the user profile	Subtype
General certificate	`GENERAL_CERTIFICATE`
WiFi	`WIFI`
Exchange	`EXCHANGE`
VPN and apps	`VPN`
S/MIME Encryption	`SMIME_ENCRYPTION`
S/MIME Signing	`SMIME_SIGNING`

Certificate names in square brackets

For computed names, the inner placeholder is written without the surrounding `${…}`, i.e. `[device.serialnumber]` instead of `[${device.serialnumber}]` — nested `${…}` expressions are not supported. For names consisting only of letters, digits and underscores, the dot form `${user.certificate.EXCHANGE.iPhone}` also works.

> Certificate names containing other characters (e.g. hyphens or spaces) must be specified in the bracket form with quotation marks. An expression such as `${user.certificate.EXCHANGE.my-certificate}` is interpreted as an arithmetic operation and causes the entire configuration to be delivered without any placeholders substituted.

For version 26.4.0

Password for PKCS#12 certificates

For password-protected PKCS#12 certificates (e.g. an S/MIME identity), the import password is delivered via the reserved key `password`:

- `${user.certificate.SMIME_SIGNING.password}`
- `${user.certificate.SMIME_SIGNING["my-certificate"].password}`

For certificates that are not PKCS#12 containers, the value remains empty. Since `password` is a reserved key, a certificate that is itself named `password` cannot be selected via placeholders — both the dot form and the bracket form resolve to the password in this case. A different certificate name should be used instead.

Output format

Regardless of the uploaded file format (PEM or DER), the placeholder always yields the base64-encoded DER form of the certificate. PKCS#12 containers are delivered base64-encoded as stored, so together with the password they can be imported directly by the receiving app. Other certificate types are also delivered as stored.

Example of a managed app configuration for an email client with S/MIME signing:

```
<key>SMIMECertificate</key>
<string>${user.certificate.SMIME_SIGNING}</string>
<key>SMIMECertificatePassword</key>
<string>${user.certificate.SMIME_SIGNING.password}</string>
```

Availability

User certificate placeholders are intended for configurations whose content is delivered to the device of the assigned user, in particular managed app configurations (iOS/macOS, Android Enterprise), Knox configurations (Android Enterprise, Samsung KNS), custom configuration profiles (`.mobileconfig`) and Windows custom CSP. In these configurations, the portal also lists them under Available placeholders. They are not resolved (the placeholder remains empty) in device names, i.e. when renaming devices and in device name configurations for Apple and Windows, in Android Enterprise lock screen and support messages, work account setup and setup actions, in script environment variables, or in webhook actions of device groups. They are not supported for Linux configurations. In custom configuration profiles (`.mobileconfig`), the placeholder can only be used in string fields, not in data fields; in managed app configurations, both work.

If no certificate can be determined — for example due to an unknown subtype, a name that does not exist, or a missing user assignment — the placeholder remains empty and the configuration is still delivered. Details about the cause are recorded in the server log.

Notes

For version 26.4.0

> Function names and their casing must be used exactly as described. The Relution Portal does not show a preview of the resolved value; it is therefore recommended to test the combination on a test device before rolling out the configuration.

Which base placeholders (e.g. `${user.email}` , `${device.serialnumber}`) are available in a specific configuration is shown in the configuration form or the respective dialog in the Available placeholders section. Clicking an entry copies it to the clipboard.

Values that are not set are inserted as an empty string. If, however, the evaluation of an expression fails — for example a slice `[0..0]` of a value that is set but empty or an unknown function name —, this does not only affect the individual placeholder: the entire text of the field or configuration is delivered unchanged, i.e. with all `${…}` expressions unreplaced. The cause is logged in the server log.

OneRoster Interface

Starting with Relution 26.2, the OneRoster interface is implemented in the portal for users. This interface allows the synchronization of users and classes, for example, from Untis or WebUntis, with Relution. The feature can be found under `Settings` → `User Management` → `OneRoster`.

> Currently, Untis/WebUntis only supports one organization/tenant in Relution. Therefore, it is recommended to integrate the OneRoster interface directly into the target tenant. Alternatively, the interface can also be integrated into the global organization, where schools can be mapped via IDs. However, this requires support from the user management application.

Setting Up the OneRoster Interface

A new connection is created in the overview `Settings` → `User Management` → `OneRoster` via Add.

General Settings

For version 26.4.0

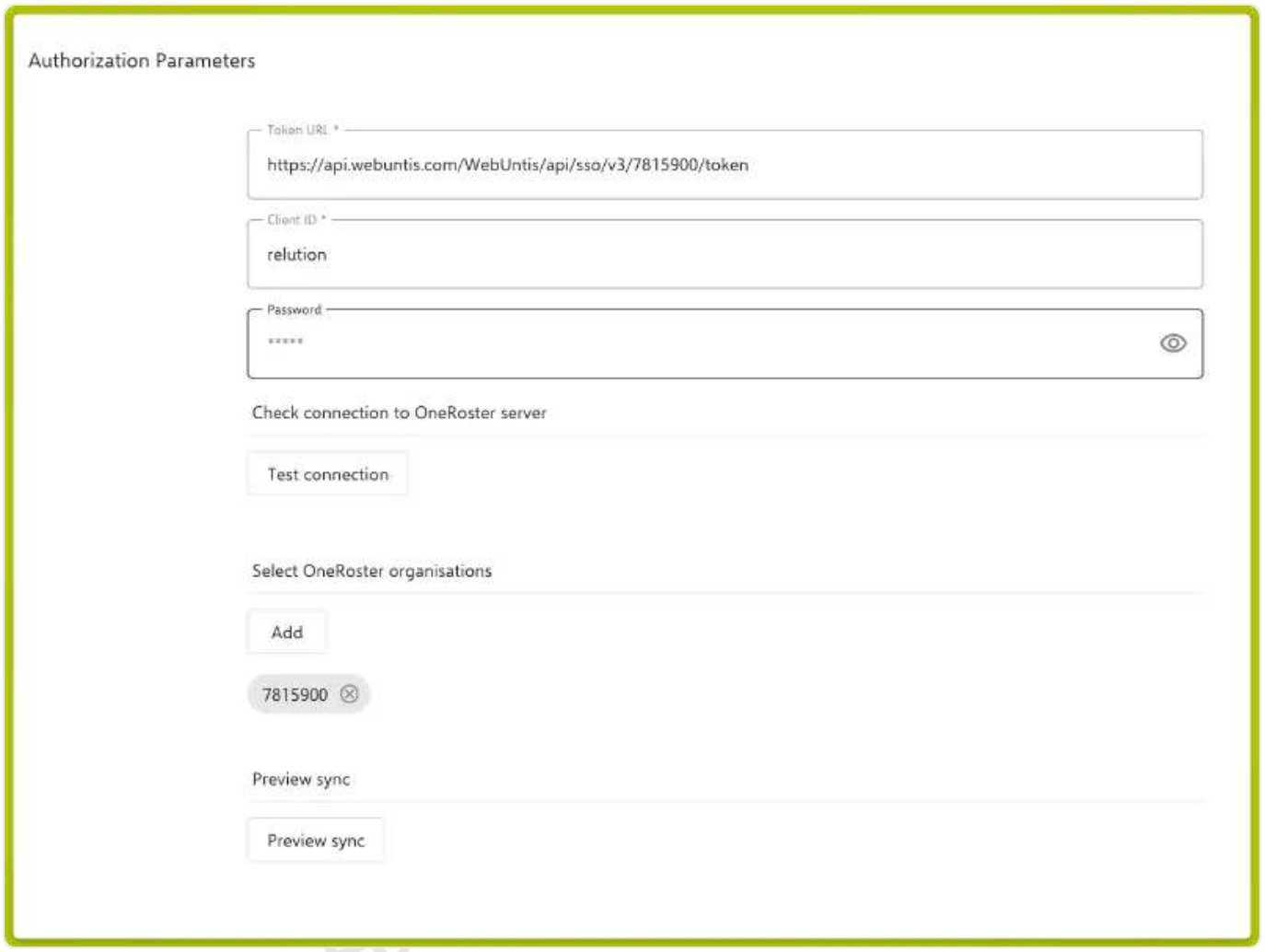
1. Provider name: Unique name for the connection. The name must not be used by any other provider configuration and cannot be changed after saving.
2. Enabled: This switch turns the interface on. For a new connection, it is turned off; as long as it is disabled, no synchronization takes place.
3. Host: URL of the OneRoster server.



Authorization Parameters

- Token URL: URL for token authentication.
- Client ID: Client ID for authentication.
- Password: The corresponding client secret. For a saved connection, the field shows `*****`; if it is left empty, the stored password remains in effect. If Host or Token URL is changed, the password must be entered again, otherwise Relution rejects the connection test and saving.

The Test connection button tests the connection to the OneRoster server as soon as all required fields are filled in.



Select Organizations

- In a tenant, the OneRoster organizations to be synchronized are selected in the Authorization Parameters section via Add next to Select OneRoster organisations. The button becomes active as soon as all required fields are filled in.
- In the global organization or a meta organization, the Organization mappings section is shown instead. There, OneRoster organizations are mapped to the individual Relution organizations.
- Preview sync shows the classes to be synchronized, together with their teachers and students, beforehand. The preview is available as soon as at least one organization is selected or mapped.

Without a selected OneRoster organization, the synchronization fails.

Synchronization Settings

- Synchronize classes: Imports classes from OneRoster. The option is enabled by default.
- Action for missing users: Defines what happens to previously synchronized users that are no longer returned by the OneRoster server: `None` (default), `Deactivate` or `Delete`. This setting always applies, even if Synchronize classes is disabled.
- Action for missing classes: Defines what happens to previously synchronized classes that no longer exist in OneRoster: `None` (default) or `Delete`. This setting only applies if Synchronize classes is enabled.

If a synchronization run returns no users or no classes at all, Relution does not execute the respective action. This prevents all objects from being deactivated or deleted in case of a connection or configuration error.

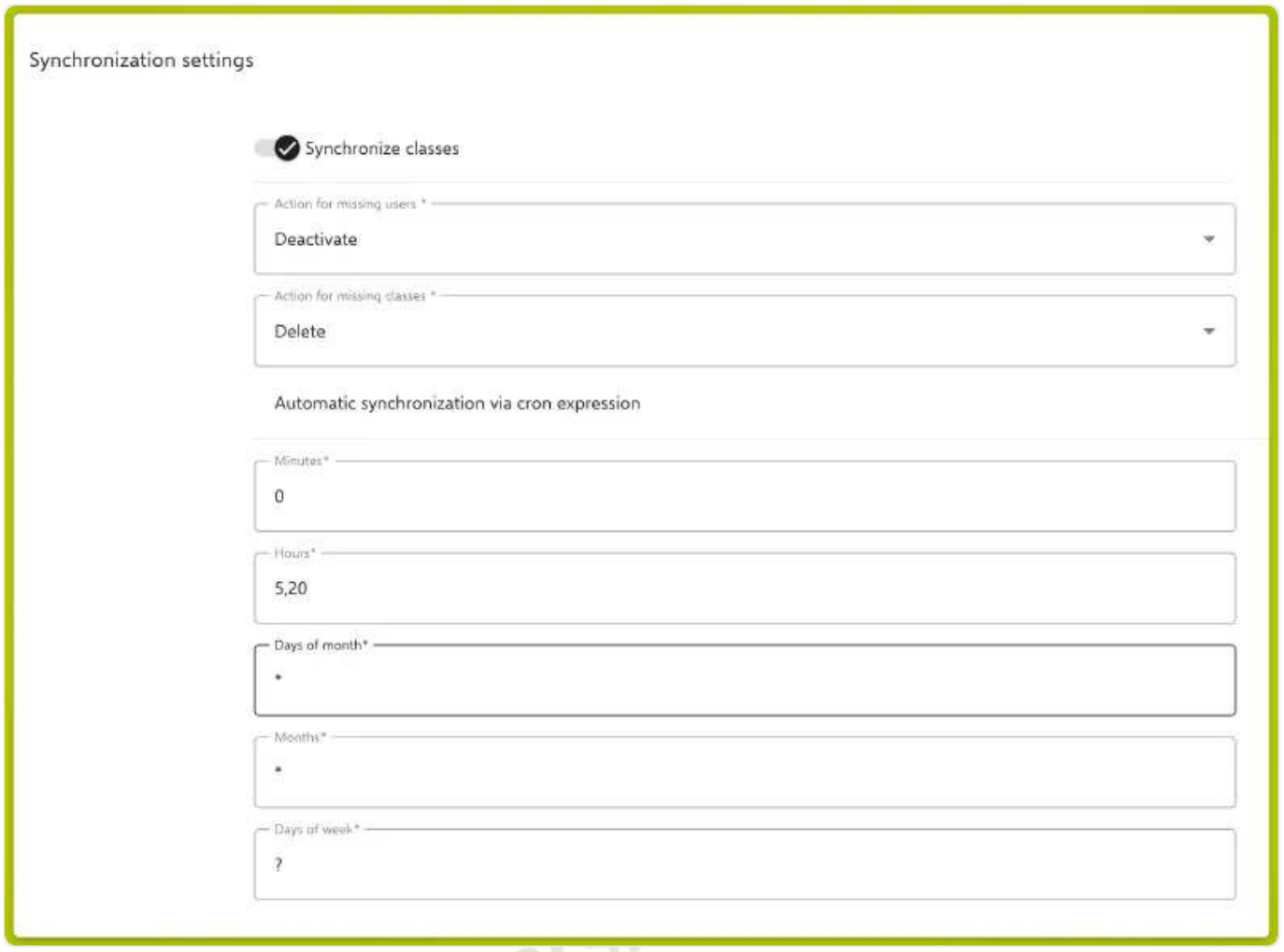
Synchronized users are automatically assigned to the organization's system group `<ORGANIZATION> Teacher` or `<ORGANIZATION> Student` and to a group of the provider. As login name, Relution uses the username from OneRoster, alternatively the email address or an identifier from OneRoster.

Automatic Synchronization

Automatic synchronization is defined using cron syntax. By default, it runs daily at 5:00 and 20:00.

- Minutes: Minute at which the synchronization runs.
- Hours: Hour of the synchronization.
- Days of month, Months, Days of week: Further restrictions of the synchronization interval.

For version 26.4.0



For ver

Checking Synchronization

Once the connection has been saved, it can be opened in the overview. The detail view lists the sync results separately for users and classes: it shows when the next planned synchronization is due and when the last one was completed, whether the synchronization was successful, the Status message and the number of synced, missing and failed objects. Clicking the number under Sync Errors shows the individual errors and thus their cause.

In the header of the detail view, the Sync icon triggers a manual sync run at any time (requires the permission to update users or classes). Edit and Delete are also available there.

> Most synchronization errors occur due to missing users in a class. Relution requires at least one student and one teacher to create a class. In addition, users are skipped during synchronization if their username is already taken in the organization, their email address is already taken in Relution, or they have no email address.

SchulConnex Import

Relution supports synchronizing identities and educational context data via SchulConnex (a German school data exchange standard). The feature can be found under `Settings` → `User Management` → `SchulConnex` and automatically synchronizes users, group roles and classes/courses from the underlying school administration software. In the SchulConnex Imports overview, a new configuration is created via Add.

SchulConnex is used for import only. Imported users sign in to Relution via a different login method, e.g. an identity provider.

General

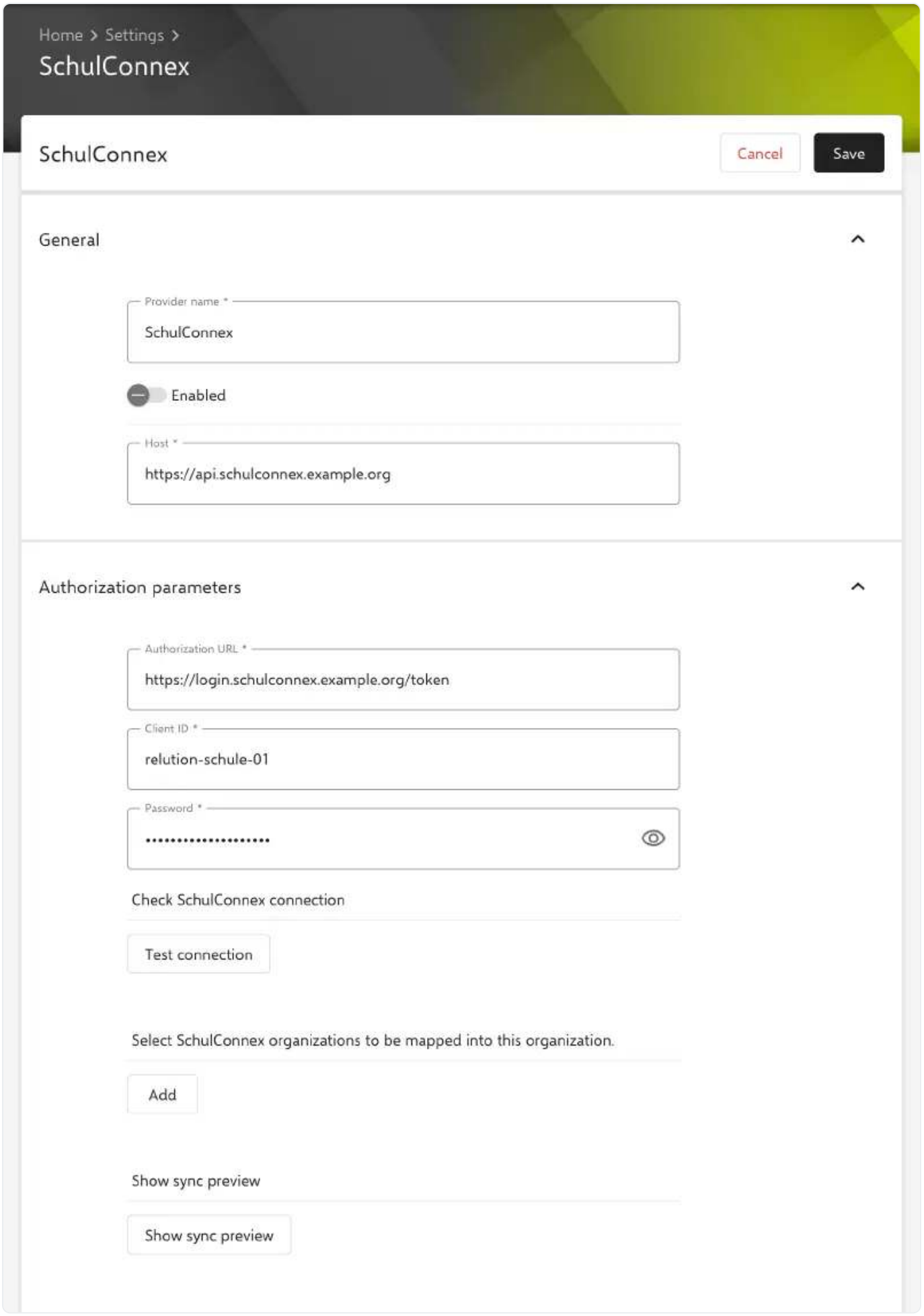
1. Provider name: Unique name for the configuration. The name must not be used by any other provider configuration and cannot be changed after saving.
2. Enabled: Turns synchronization on. For a new configuration, the switch is turned off; as long as it is disabled, no synchronization takes place.
3. Host: URL of the SchulConnex server.

Authorization Parameters

- Authorization URL: URL used for OAuth authentication.
- Client ID: Client ID for authentication.
- Password: Client secret of the SchulConnex client. For a saved configuration, the field shows `*****`; if it is left empty, the stored secret remains in effect. If Host or Authorization URL is changed, the secret must be entered again, otherwise Relution rejects saving, the connection test and the sync preview.

The connection can be tested via the Test connection button (label Check SchulConnex connection) as soon as all required fields are filled in correctly.

For version 26.4.0


Home > Settings >
SchulConnex
SchulConnex
Cancel
Save
General
Provider name *
SchulConnex
Enabled
Host *
https://api.schulconnex.example.org
Authorization parameters
Authorization URL *
https://login.schulconnex.example.org/token
Client ID *
relution-schule-01
Password *
Check SchulConnex connection
Test connection
Select SchulConnex organizations to be mapped into this organization.
Add
Show sync preview
Show sync preview

Organization Mapping

- On a regular organization, the SchulConnex organizations to be incorporated are selected directly (1:1 mapping).
- On the global organization or a meta organization, multiple Relution organizations can be managed at once: for each Relution organization, a dedicated set of SchulConnex organizations is assigned via a mapping wizard. Each SchulConnex organization and each Relution organization can only be mapped once.

Show sync preview shows upfront which classes/courses would be imported, along with their teacher and student counts.

Synchronization Settings

- Synchronize classes: Enables the import of classes/courses (enabled by default).
- Action, when a user is removed in SchulConnex: Defines what happens when a previously synchronized user no longer exists in SchulConnex: `None` (default), `Deactivate` or `Delete`.
- Action, when a class is removed in SchulConnex: Defines what happens to classes removed in SchulConnex: `None` (default) or `Delete`.
- Automatic Synchronization: Schedule via cron syntax (minutes, hours, days of month, months, days of week). By default, synchronization runs twice daily at 5 AM and 8 PM.

In addition to automatic synchronization, a sync run can be triggered manually at any time via the Sync icon in the header of the configuration's detail view (requires the permission to update users or classes).

For version 26.4.0

Role Mapping

SchulConnex group roles are automatically mapped to the organization's system groups `<ORGANIZATION> Teacher` and `<ORGANIZATION> Student` on import:

- Teachers: Roles `LEHR`, `KLLEIT`, `FOERD`, `VLEHR`, `GLEIT`
- Students: Roles `LERN`, `GMIT`

Only SchulConnex groups of type class or course are evaluated. The role `SCHB` is not assigned to any group. In addition, all imported users are assigned to a group of the provider.

Checking Synchronization

After a sync run, the results can be reviewed in the configuration's detail view. For users and classes separately, it shows the next planned synchronization, the time of the last completion, whether the synchronization was successful, the Status message and the number of synced, missing and failed objects. Clicking the number under Sync Errors shows the individual errors.

> A class/course is only created if it contains at least one student and one teacher. Skipped classes are counted as errors.

If a person has no email address on file, the SchulConnex person ID is used as the login instead. If a user with the same email address or username already exists, the import for that person is skipped and reported as an error.

If authentication fails (e.g. an expired secret), the entire sync run for the configuration is aborted, since the credentials apply to all mapped organizations at once.

Other errors, such as a timeout, only abort the synchronization of the affected mapped organization. For this organization, the actions for removed users and classes are not executed; the remaining organizations are fully synchronized. In this case, the sync run is reported as failed.

For version 26.4.0

Profile pictures

Relution allows storing profile images for existing users within the platform. This feature provides particular advantages in the Apple ecosystem, such as for the Classroom app or simplified login on Shared iPads.

When a user has a profile image assigned, teachers can more easily identify students within the Apple Classroom app. Additionally, the feature simplifies the login process on Shared iPads: users can select their class and click on their profile image to log in.

It is important to note that the profile images remain stored on Relution servers and are not synchronized with Apple servers.

Prerequisites

- Existing users in Relution
- Square images (recommended: `256x256` or `512x512` pixels)
- Maximum image size: `300 KB`

Configuration

For version 26.4.0

- The images are named after the user name of the respective user. The file name without extension is decisive; it must exactly match a user name.
- All images are combined into a `.zip` file. macOS metadata files (`._*`) are ignored.
- Under Users, the three-dot menu opens the Bulk upload profile images option. This requires the permission to update users.
- After the `.zip` file has been uploaded, a summary shows for each image whether it is valid and which violations exist, e.g. no or several matching users found, image not square or too large.
- Only valid images are assigned; an existing profile image is overwritten. Invalid images are discarded.

Individual profile images (JPEG or PNG) can also be uploaded in the user details in the Profile image field. Users can change their own profile image in their profile via the edit icon on the avatar.

Notes

For teachers to manage users in the Classroom app, classes must be defined in Relution. This is also required for simplified login on Shared iPads. Shared iPad additionally requires Managed Apple Accounts (Managed Apple ID in the portal) to enable login.

Profile images are only delivered if, under `Settings` → `Education` → `Lesson settings`, access is set to Enabled (default) in the Access to profile images for apple education configurations section, and the user is a member of a class of the device's Apple Education configuration; see Lesson Settings →.

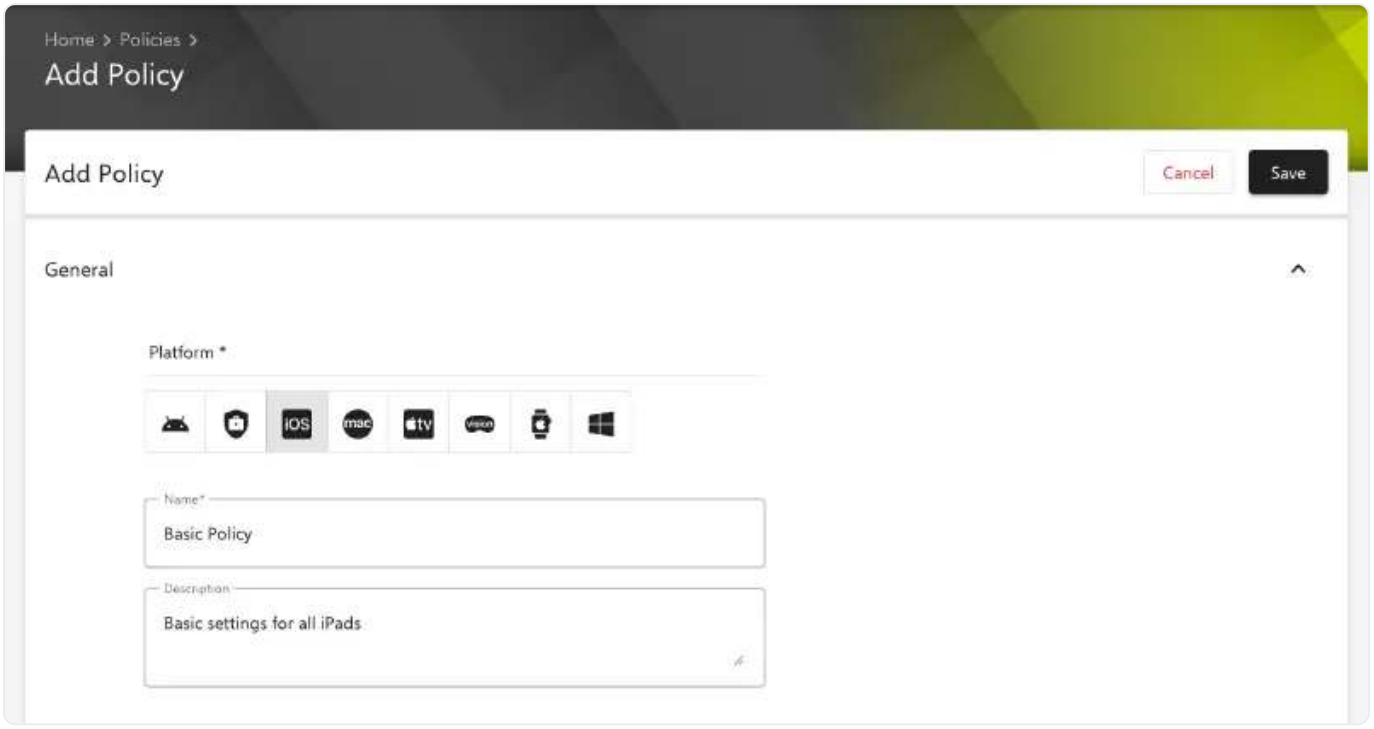
Policies explained

A policy is a collection of one or more configurations. Each policy can be applied to one or more devices at the same time. In addition, one or more policies can be associated with each device.

Create

Policies are platform dependent. When creating them, care must be taken to determine which platform a policy is created for. For example, an iOS policy cannot be subsequently changed to an Android or Windows policy. Within the Apple operating systems, a distinction is also made between iOS, macOS, tvOS, visionOS and watchOS policies and likewise cannot be subsequently changed over.

In the side menu under `Devices` → `Policies`, there will be the overview of the policies that have already been created. One can create a new policy via the Add button. At this point, a target system must be specified and a name has to be given.

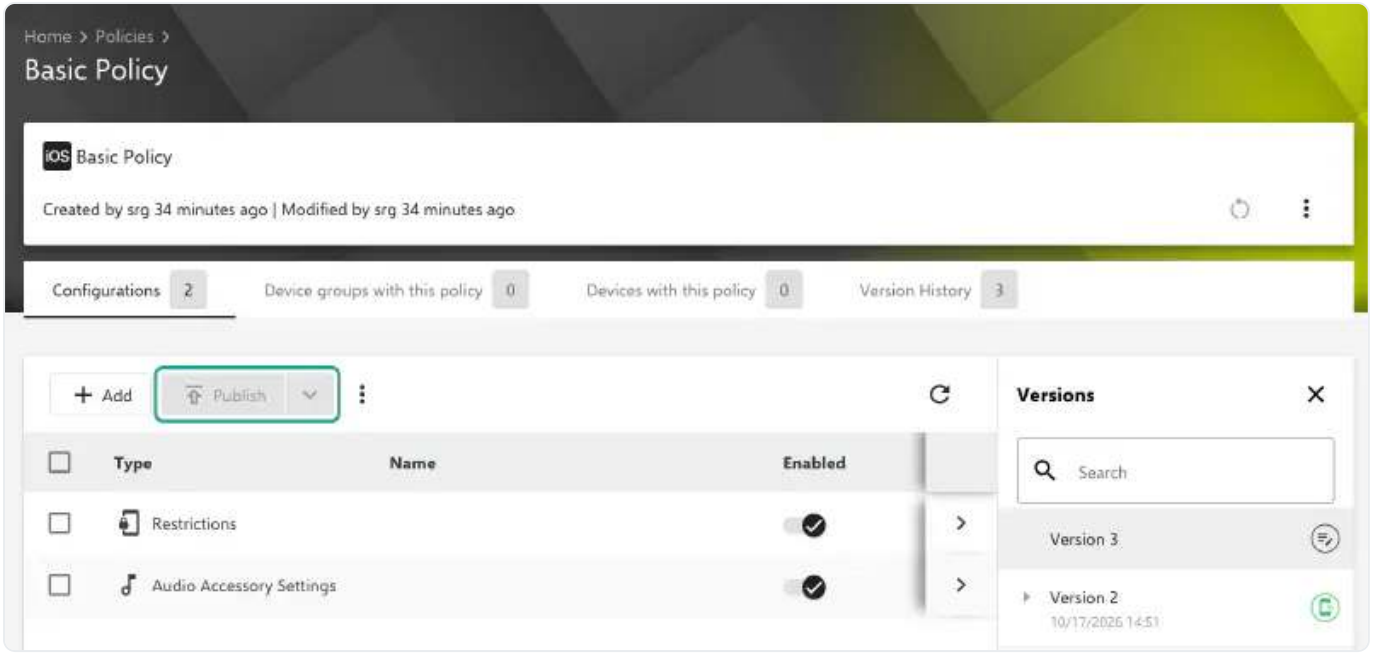


Clicking Save creates the new policy.

Policy Versioning

All changes to a policy only take effect after a Publication. This process allows all configurations to be made and checked for completeness without the changes becoming active directly on linked devices.

Once all changes have been made and are ready to be applied to the devices, the version is published via the Publish button. The button is located in the action bar of the configuration list, to the right of Add. Only a version that has been changed since its creation and contains at least one enabled configuration can be published.



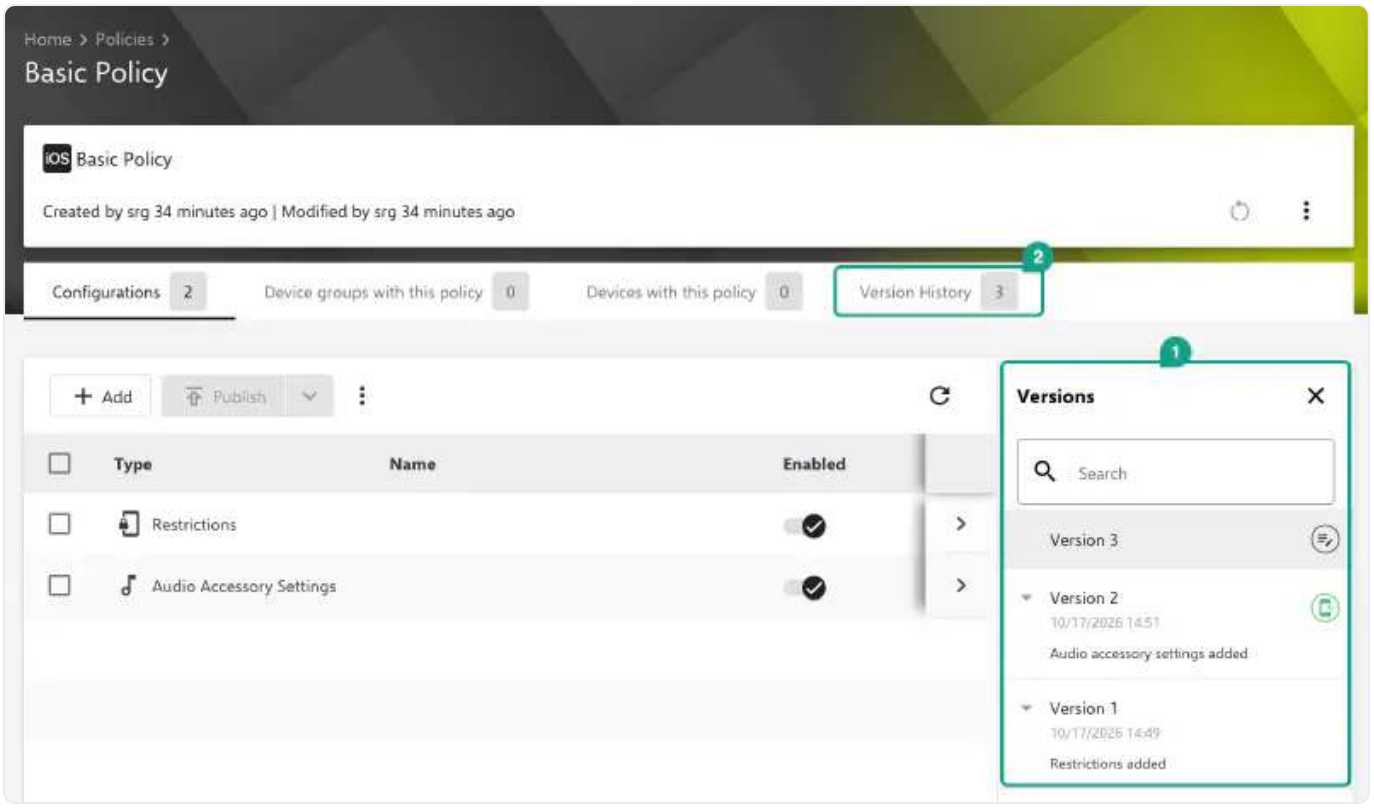
The menu of the Publish button offers two variants:

- Publish on all devices: The version is applied to all devices the policy is assigned to.
- Publish on test devices: The version is published as a test version (state Test) and is only applied to the devices of the device groups that use the test version. These device groups are selected in the following dialog, provided that no device group uses the test version yet. All other devices keep the previously published version. A test version can later be applied to all devices via Publish.

For version 26.4.0

The Versions Sidebar

The Versions Sidebar is used for a quick view of already published policies.



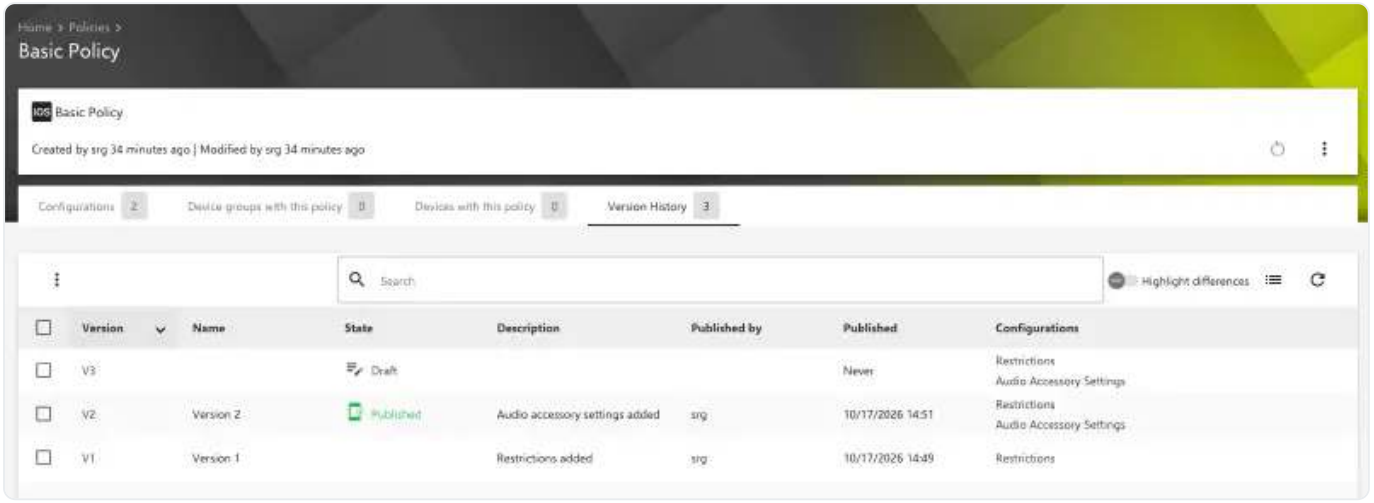
The following indicators are shown here:

- Pencil Icon (Pen): Marks the current Draft – this is the latest, but still unpublished version of the policy.
- Green Mobile Phone Icon: Identifies the currently published policy and thus the one applied to the devices.
- Blue Flask Icon: Identifies a test version that is only applied to the selected test device groups.
- Version Information: When publishing a new version, a Name and a Note (Description) can be specified. These are displayed directly in the sidebar to quickly document and track changes.

For version 26.4.0

Version History

For detailed tracking of all changes, there is also the Version History tab.



In this overview, all policy versions are clearly listed, including the following details:

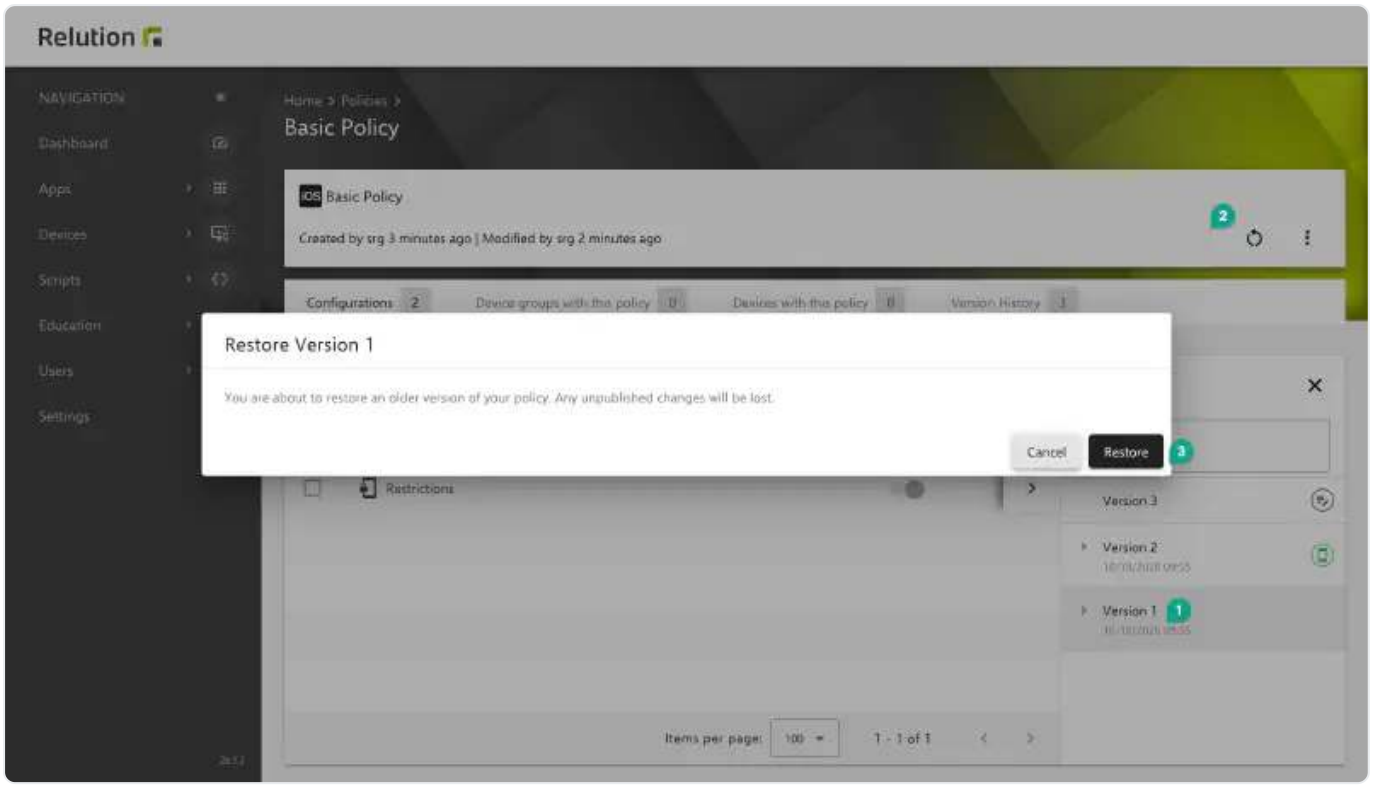
Column	Description
Version	The unique identifier of the version (e.g., V4).
Name	The assigned version name.
State	The state of the version: Draft, Published or Test. For outdated versions, the column remains empty.
Description	The note/comment added upon publication regarding the changes.
Published by	The user who published the version.
Published	Date and time of publication.
Configurations	All configurations of this version. The Highlight differences switch marks configurations added, changed and removed compared to the previous version.

The columns Modified by and Modified on are hidden by default and can be shown via the column selection.

Restoring Policies

An older version of a policy is selected in the Versions sidebar (1) and restored as a new draft using the Restore as draft version button (2) in the policy header. Alternatively, the function is available on the Version History tab. After confirming with Restore (3), the current draft is replaced by a copy of the selected version; all unpublished changes are lost. The policy must have at least one other version besides the draft.

For version 26.4.0



Priorities

For version 26.4.0

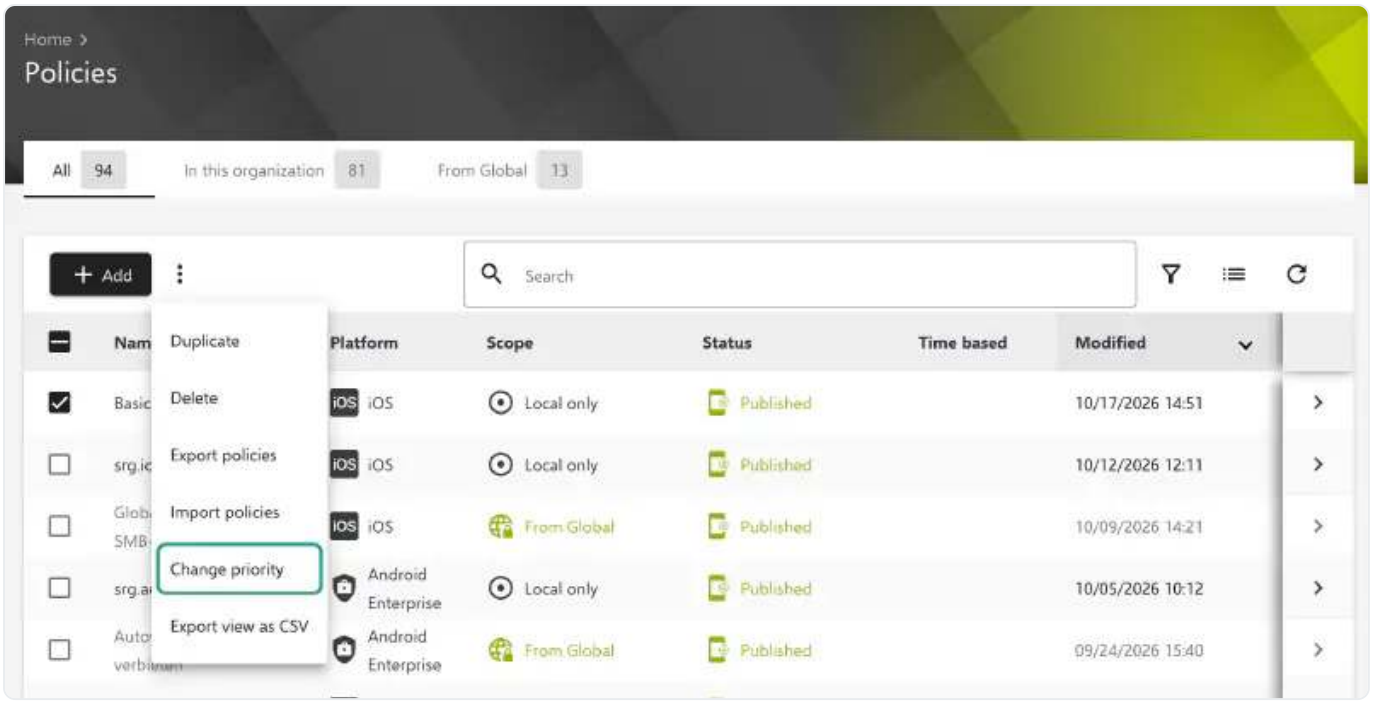
Policies have priorities. The lower number trumps the higher one. So priority 2 wins against priority 3. The priority number only applies within the same level: Global policies → always take precedence over policies shared by a meta organization →, and these in turn take precedence over the policies of the organization itself. A local policy with priority 1 therefore does not override a global policy.

Each platform has its own priority list. So there can be policies with priority 1 multiple times - each for iOS, macOS, tvOS, visionOS, watchOS, `Android Classic/ Legacy`, `Android Enterprise` and Windows.

If a configuration type that can only be created once per policy (e.g. the restrictions for `Android Classic/ Legacy`, `Android Enterprise` and Windows) occurs in several policies with different priorities, only the configuration from the policy with the highest priority is used. The configurations of the lower-priority policies are not merged, but ignored completely. If a function is allowed in the restrictions of a policy with priority 2, but prohibited in one with priority 4, it remains allowed.

Some of these configuration types, however, are transferred to the device from all policies together, e.g. the restrictions for iOS, macOS and tvOS; the device then applies the more restrictive setting in each case. Configurations that can be created multiple times (e.g. Wi-Fi or certificates) are combined from all policies. If two entries collide (e.g. Wi-Fi profiles with the same SSID), the one from the policy with the higher priority applies.

The priorities are changed in the policy overview via the 3-dot menu and the Change priority entry.



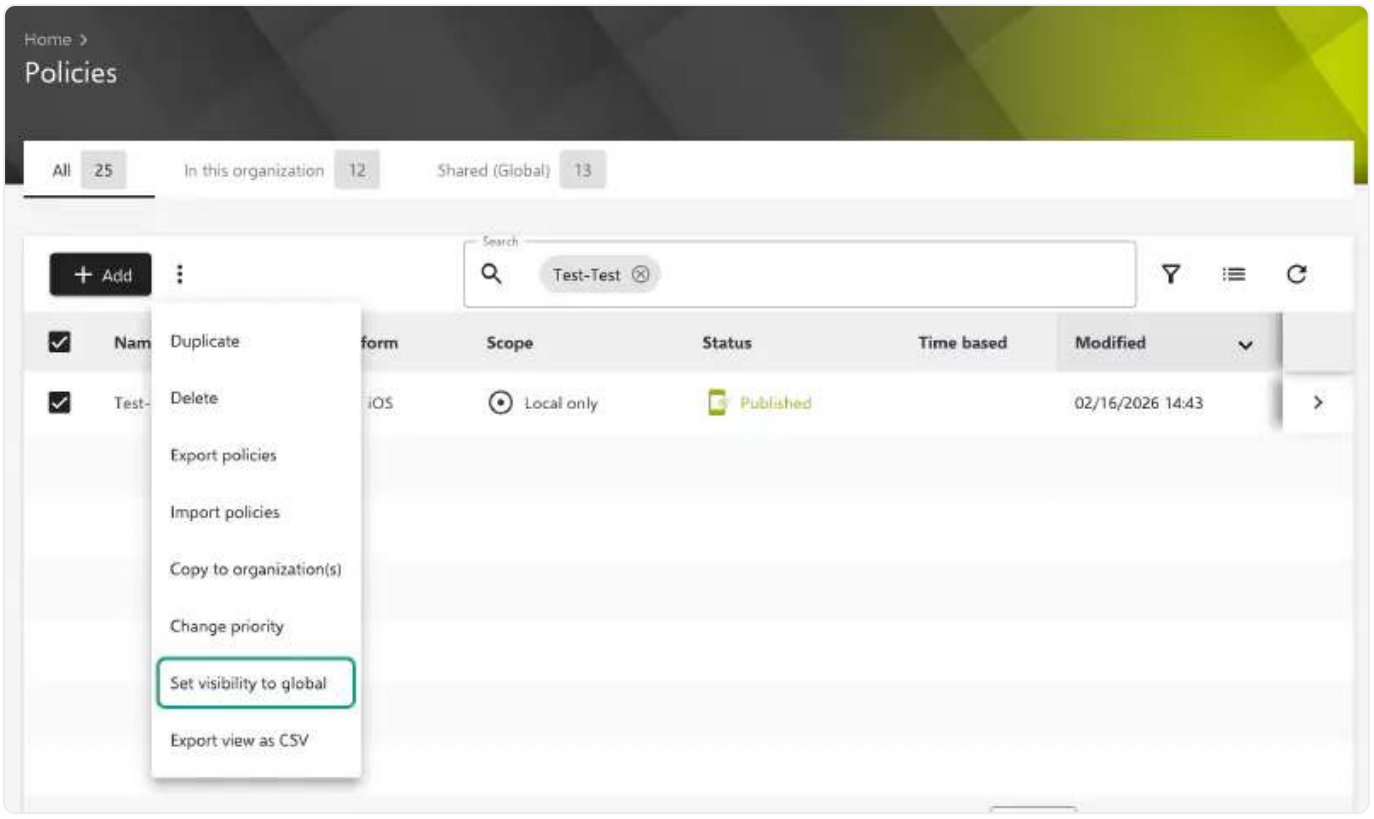
Global policies

Now and then, it can be useful to be able to apply identical configurations in several organizations of Relution. To do this, global policies can be created and shared in the Global organization →. These policies can be edited normally in the Global organization, but are only available as read-only in the other organizations.

A published version of the policy is required for sharing. The policy is then selected in the overview and shared via the 3-dot menu with Set visibility to global (in the detail view of the policy: Set policy visibility to public). This sharing cannot be undone. In meta organizations →, Set visibility to meta is available accordingly; the policy is then available as read-only in all subordinate organizations.

> Global policies are not available for Android Enterprise.

For version 26.4.0



In the overview, the Scope column shows whether a policy is shared: In the Global organization, shared policies are marked with Shared, in the other organizations with From Global (or From Meta for policies of a meta organization). Policies that are not shared are marked with Local only.

For version 26.4.0

Deactivate Policies

As of Relution 5.33, it is possible to deactivate policies for individual devices. Previously, device groups always had to be cloned and adjusted to temporarily remove a device from a policy assignment. This is now easily possible via `Navigation` → `Devices` → `Inventory` → `the device` → `Policy`. To do this, the corresponding policy must be selected and can be deactivated/activated via the 3-dot menu.

Policy Status

The policy status is displayed in the header box on the device details page. The following statuses can occur:

- `UNKNOWN = Problem`
  - The status of the device policy is unknown
- `NONE = None`
  - No policy is applied to the device
- `SENT = None`
  - A policy has been assigned to the device, but it has not yet been applied
- `APPLIED = Active`
  - A policy is being applied to the device
- `UPDATE = Active`
  - A new version of the policy has been sent to the device, but the device has not yet updated it
- `CHANGE = Info`
  - Another policy has been sent to the device, but the device has not yet changed the policy
- `REMOVED = Info`
  - The policy has been unassigned from the device, but the device has not yet removed the policy

For version 26.4.0

Device groups

The device group function has been available in Relution since version 5.21.0. This allows devices to be automatically assigned to groups based on various device properties. The device groups can then be used to assign policies that are delivered automatically.

Accessing device groups

Device groups are located under `Devices` → `Device Groups`. This page provides an overview of the existing groups and allows new groups to be created.

A device group is a link between devices and policies. This link can be created either manually or automatically based on certain device properties.

Policies are linked to devices exclusively via device groups; direct linking is no longer possible. Device groups can also trigger actions based on events or on a schedule: Device group actions →

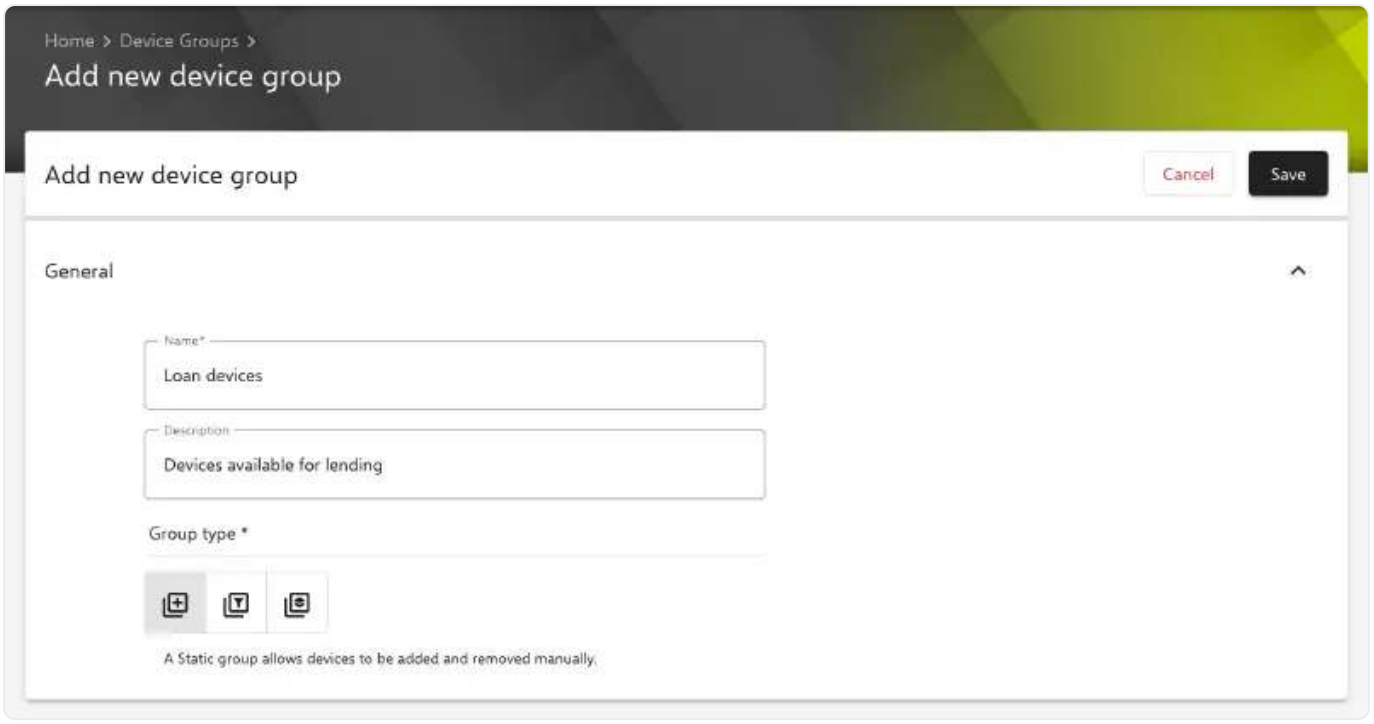
Creating new device groups

A new device group is created by clicking Add. A name and (optionally) a description are assigned to the group. The Group type can also be selected. Here the options Static and Dynamic are available; with an Education or Free license, Education is also available. Dynamic is preselected.

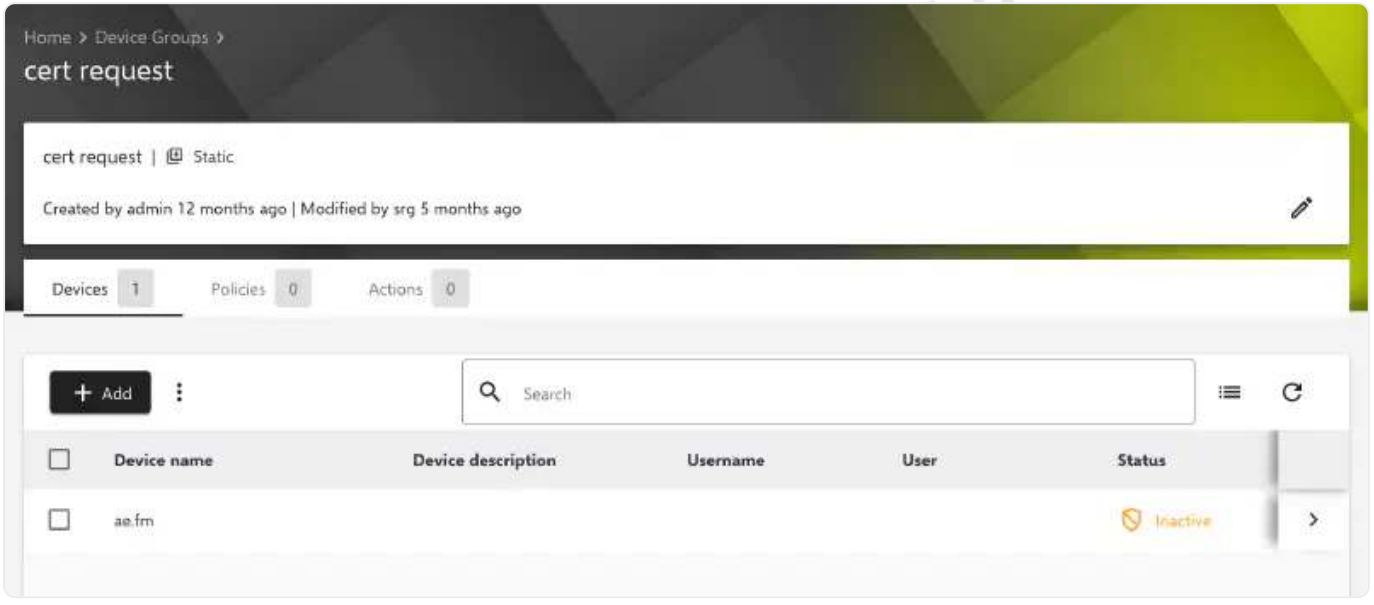
For version 26.4.0

Static groups

Static groups allow manual linking between devices and policies.

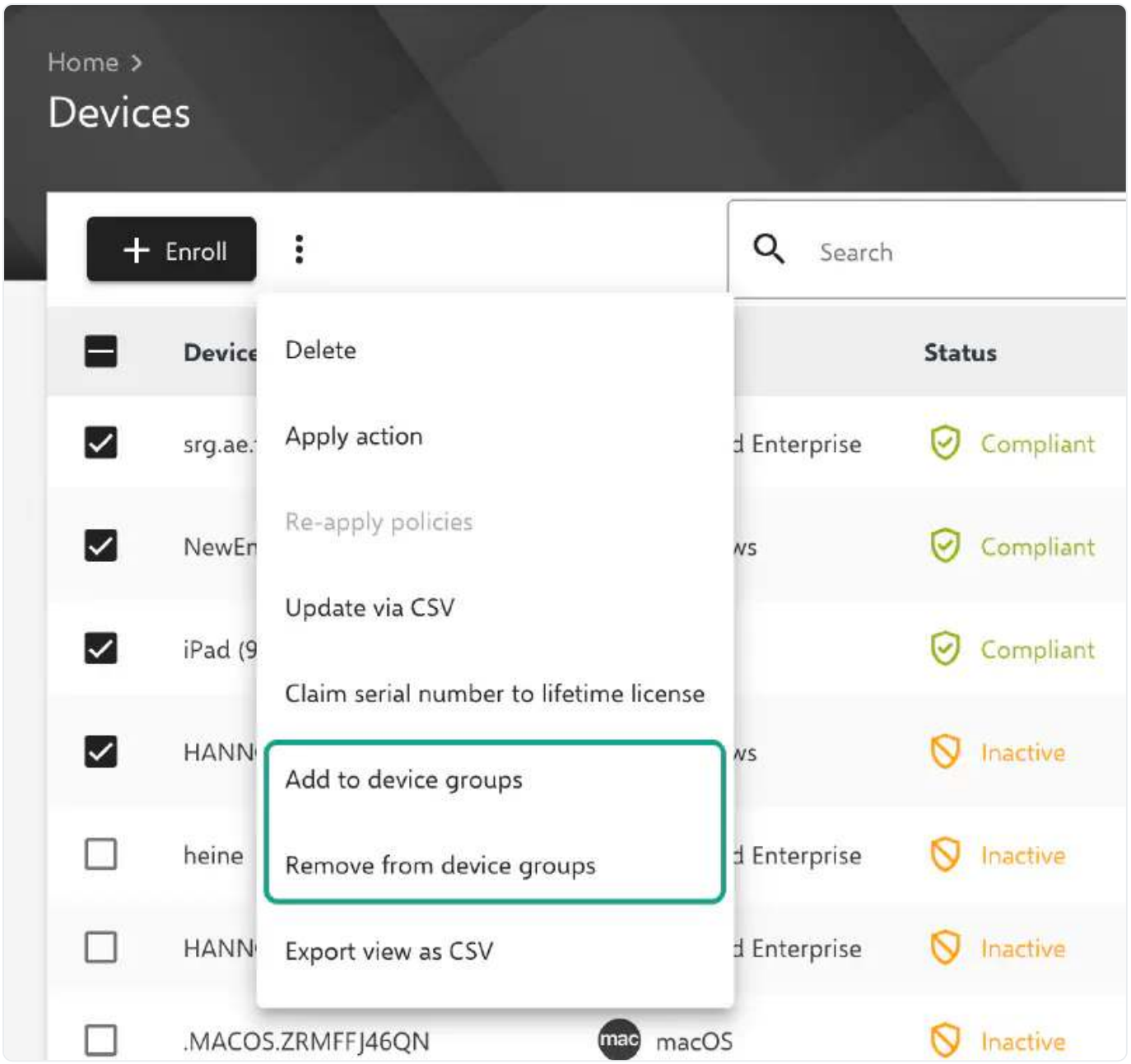


After the group is created, devices and policies can be added. Only policies that have been previously published, can be linked.



Bulk Adding Devices

With Relution 26.1.0, it is possible to directly add multiple selected devices from the inventory or auto-enrollments to an existing static group or remove them from it, which also assigns or withdraws the associated policies. The 3-dot menu provides the entries Add to device groups and Remove from device groups for this purpose.

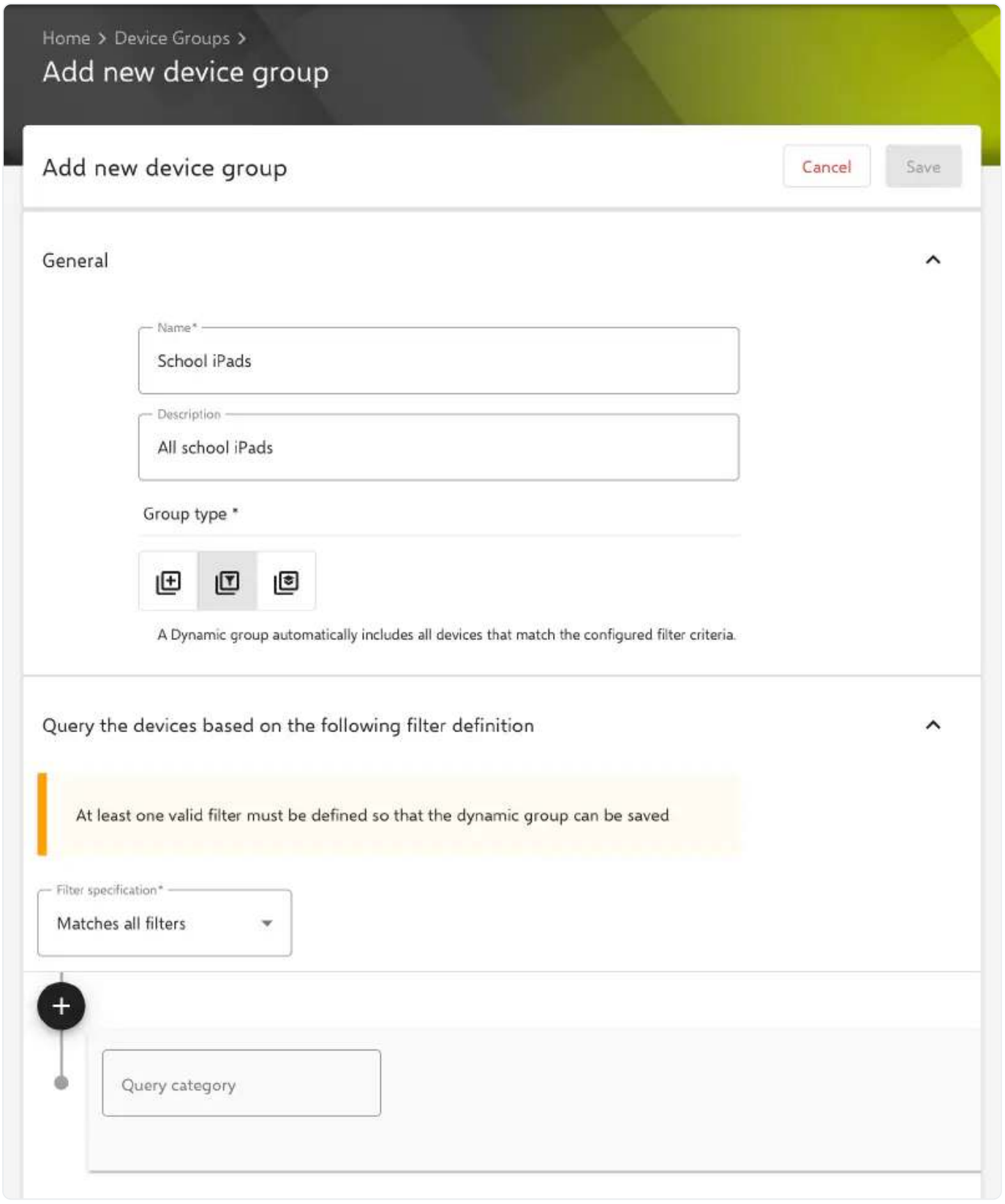


Devices can already be assigned to static groups during enrollment: enrollments and auto-enrollments provide the Static device groups field for this purpose.

Dynamic groups

In dynamic groups, filters must be defined based on which devices are automatically assigned to the group. This happens automatically in the background. For filters on user groups or classes (courses), it can take up to an hour until changes take effect in the group; prompt evaluation is only guaranteed for Relution Shared Device logins and logouts. There is no direct manual influence on the content of these groups.

In the Device preview section, clicking Update shows how many and which devices the group contains with the current filters. If saving an existing dynamic group changes the number of devices, Relution asks for confirmation before saving.



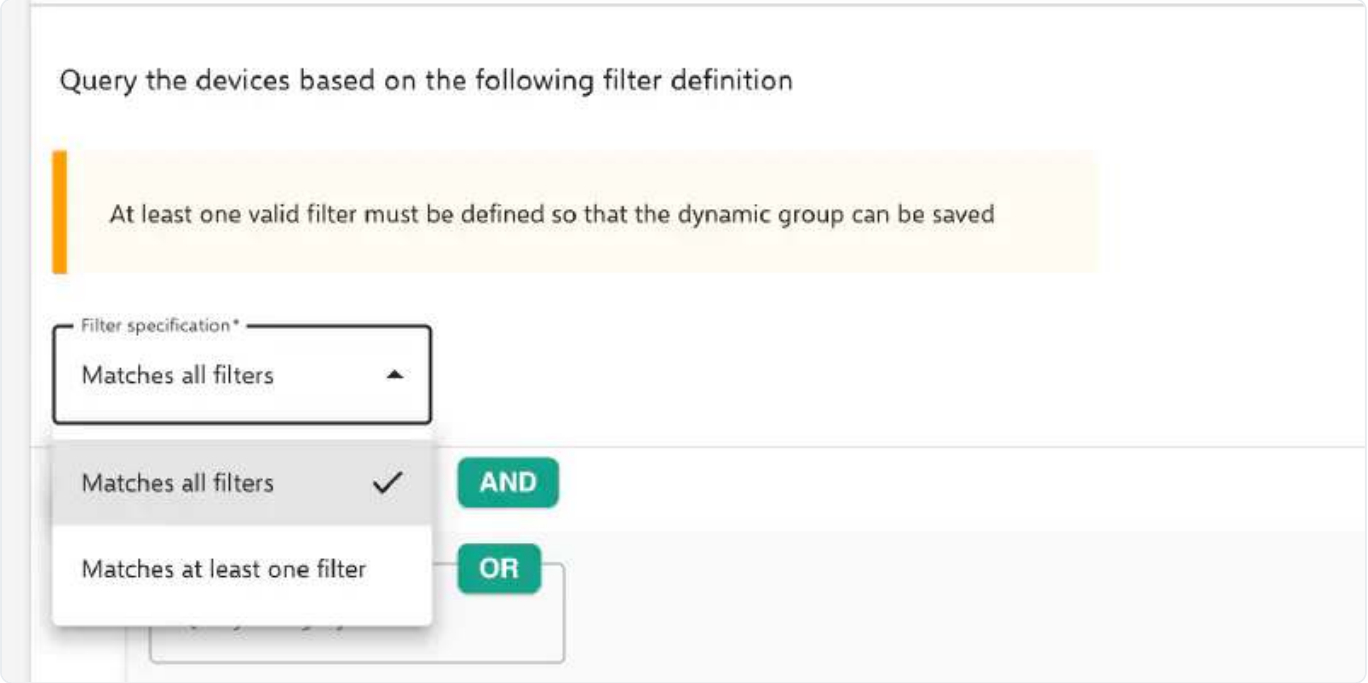
This is a complex tool that requires concentration to operate. Careless actions can quickly lead to undesirable results. Dynamic groups should be used with particular caution for infrastructural policies. It must be ensured, for example, that no Wi-Fi policy is revoked when the device status changes.

Caution: When a device loses its membership in a dynamic device group, the policies assigned through this group are withdrawn. If Uninstall auto-installed required apps if no longer required is enabled in an affected app compliance policy, the apps are removed together with their local data. The group membership is restored automatically as soon as the filter condition applies again, the app data is not.

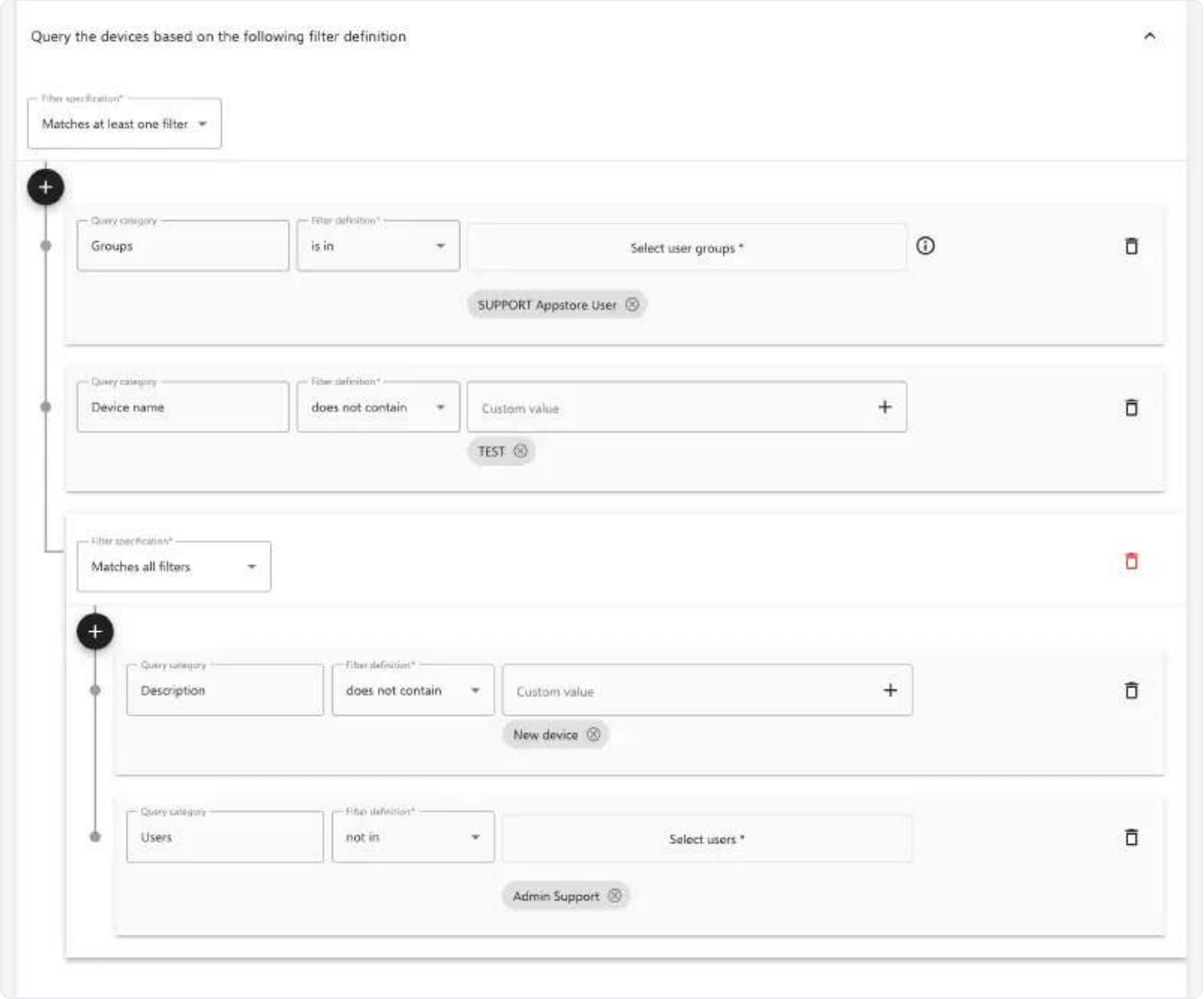
Almost all filterable properties can change without any action by an administrator: they are reported by the device or taken over from Apple, Google, Microsoft or the identity provider. Custom fields 1–5 as well as the device name and description are also reset when the device is enrolled again.

For policies with automatic uninstallation, it is therefore advisable to use static device groups or to disable automatic uninstallation for apps that hold user data.

The Filter specification field offers the options Matches all filters (AND) and Matches at least one filter (OR). Via the plus icon, Add filter creates further filters and Add group creates nested filter groups. Each filter group has its own Filter specification, which allows conditions to be bracketed as in the following example.



In the example, a filter has been defined from several properties and filter specifications.



The filter integrates the following devices:

- The linked user must be a member of the `SUPPORT Appstore User` group.

OR

- The device name does not contain `TEST`.

OR

- The description does not contain `New device`.

AND

- The user is not `Admin Support`.

Alternatively, the filter could be described like this:

```
Groups = "SUPPORT Appstore User" OR Device name DOES NOT CONTAIN "TEST"
OR (Description DOES NOT CONTAIN "New device" AND User NOT "Admin Support")
```

The filter specifications behave like ordinary logical functions.

For example, to avoid accidents, the serial number of a single device can also be added as a fixed filter value to apply the policy only to that device and verify that the result is as expected.

Dynamic Device Groups with Group Filter

As of version 5.33, Relution supports the use of device groups as filters within dynamic device groups. This allows existing static or dynamic groups to be used as conditions in new groups – either to include or specifically exclude devices. For this filter type, Device group is selected under Query category and at least one existing device group is added as a condition. The filter definitions is in, not in and all of (device is a member of all selected groups) are available. The group currently being edited is not offered for selection.

Advantages of the Group Filter

- More precise target group formation, e.g., `all iPads except test devices`
- Less maintenance effort, as policies no longer need to be manually duplicated
- Clearer management of policies, profiles, and actions

With the new filter type, one or more other device groups can be included in or explicitly excluded from a dynamic group. For example, a test group can easily be filtered out of a dynamic production group without the need to configure additional criteria.

For version 26.4.0

Working with dynamic device groups requires careful planning:

- No mutual dependencies between groups
- No accidental removal of critical baseline configurations, such as Wi-Fi profiles
- Policy changes are always tested with pilot devices first

Misconfigurations can otherwise lead to unwanted device loss from groups or even endless loops.

Education groups

New in 26.5

The Education group type automatically applies the linked policies to the devices of participating students for the duration of a lesson. Membership results from the active lessons in Relution Teacher; manual device assignment is not possible. Details under Education groups →.

Duplicate Device Groups

As of Relution 5.33, device groups can be duplicated to enable faster and more convenient management. To do this, one or more desired device groups can be selected under `Devices` → `Device Groups` and duplicated via the 3-dot menu. A query will follow asking what should be duplicated from the original device group. The following options are available:

- Include device group actions (only with the permission to create device group actions)
- Include devices (static groups only)
- Include filters, if disabled a static group will be created (dynamic groups only; if disabled, a static group without devices is created)
- Include policies

If only one group is duplicated, the dialog also asks for the Name of the device group duplicate. When several groups are duplicated, the duplicates are automatically named `<original name> - duplicate`.

Delete Device Groups

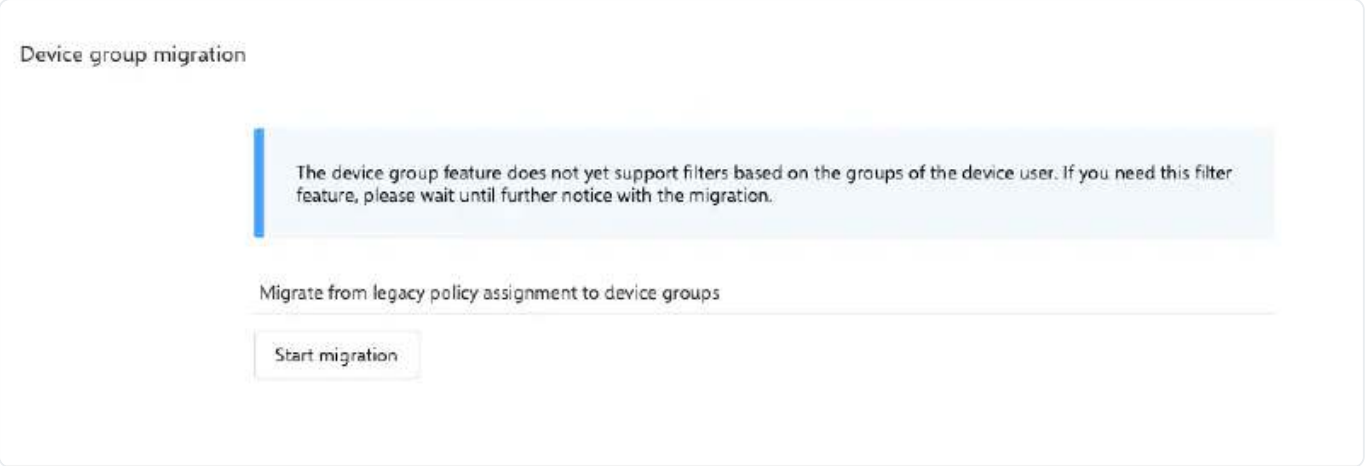
Device groups that are no longer needed can be selected under `Devices` → `Device Groups` and deleted via the 3-dot menu. Deleting a group leaves the devices enrolled. However, policies that were assigned to the devices only through this group are withdrawn. If Uninstall auto-installed required apps if no longer required is enabled in an affected app compliance policy, the apps are removed together with their local data.

For version 26.4.0

Activate Device Groups

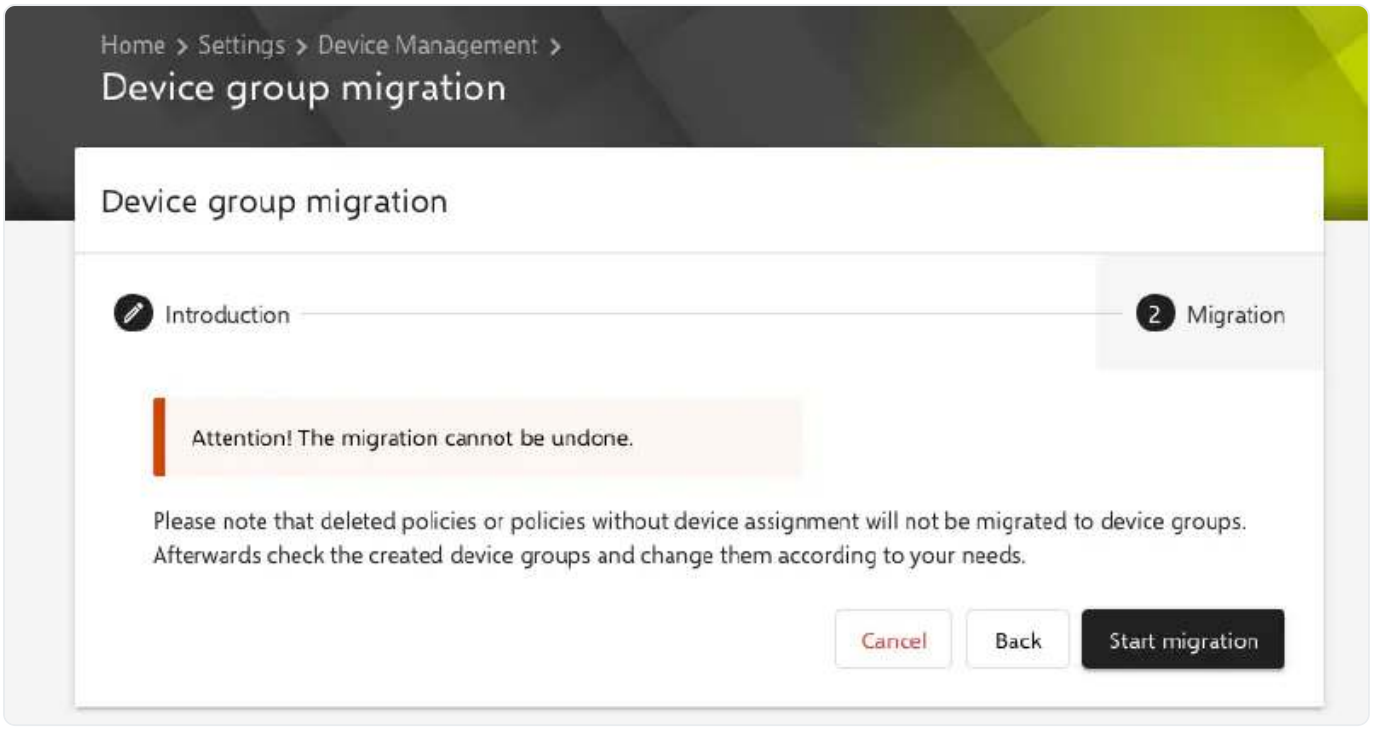
Outdated as of Relution 26.0.0 — device groups have been enabled by default since then.

In older versions, the device groups feature has to be enabled manually. This can be done via `Settings` → `Device Management` → `Device group migration`. The associated policy assignment to device groups cannot be undone.



After clicking Start migration, a message about the upcoming changes is displayed. It should be read carefully before clicking Next.

In the following dialog, the migration can finally be executed.



For version 26.4.0

Distribute User-Based Policies

In Relution, policies are assigned to device groups by default. However, with dynamic device groups and user-based filtering, policies can also be specifically linked to an individual user or an entire user group.

The principle works as follows:

1. A dynamic device group is configured with a user filter.
2. As soon as the corresponding user (or a member of the user group) is assigned to the device as device user, the device is automatically added to this device group. The assignment usually takes place during enrollment or manually in the device details.
3. The policies assigned to the device group become active and are applied to the device.
4. If the assignment is removed or another user is assigned, the device leaves the group again – the policies are deactivated.

> Signing in on the device only changes the device user in these cases: on Relution Shared Devices (sign-in and sign-out) and on Windows devices with device user change enabled in the Windows Companion. On Windows, the sign-in assigns the user; the user remains assigned until the next sign-in.

Details can be found in the articles Relution Shared Device → and User change on login →.

Requirements

- Users are created in Relution and, if necessary, assigned to a user group
- Devices are enrolled and can be assigned to a user
- Permissions in the respective organization to create device groups, to read users or groups (without this permission, the selection in the filter is disabled) and to assign policies

For version 26.4.0

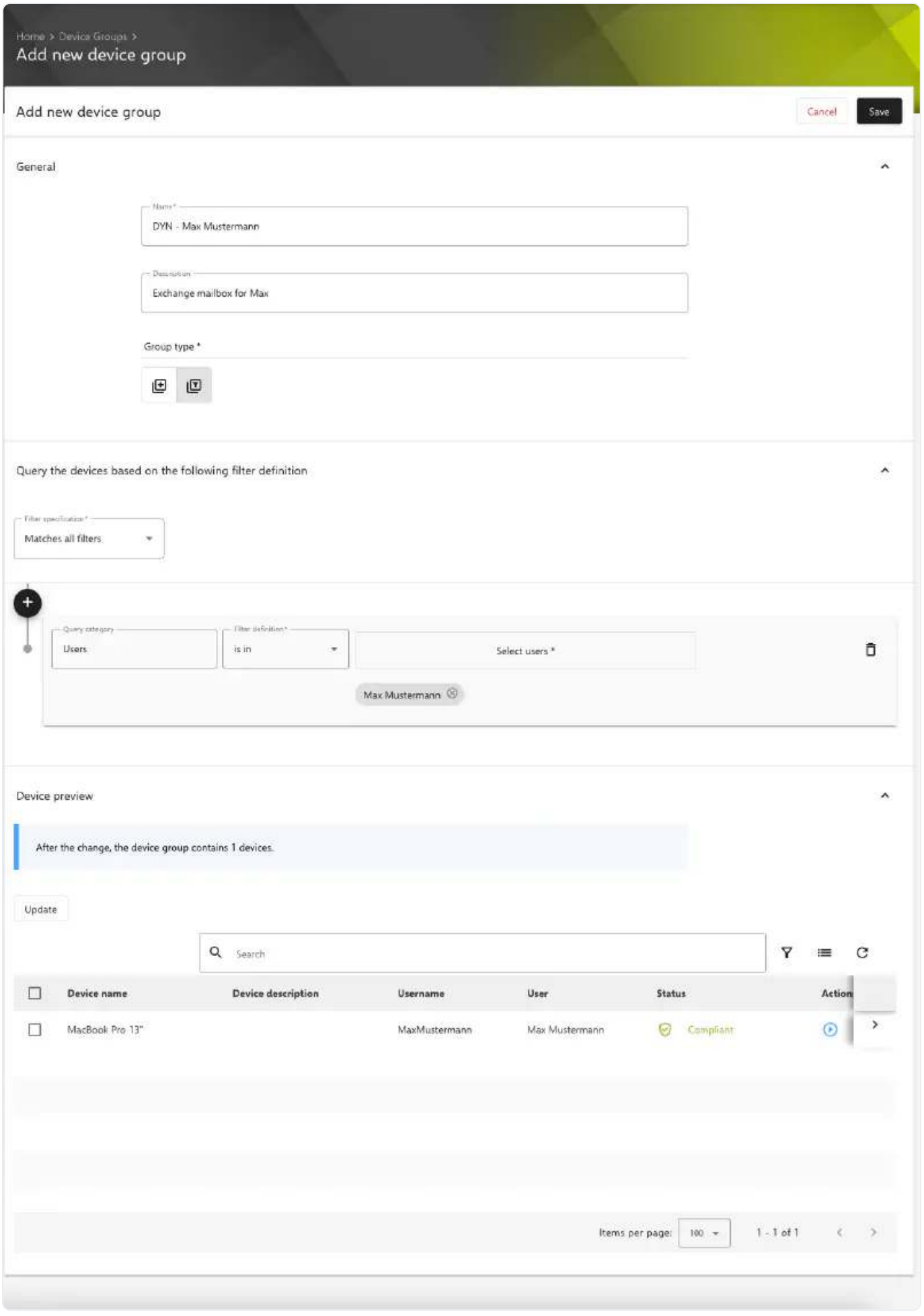
Use Cases

Scenario	Query category	Description
Individual user receives a special policy	Users	e.g. developer needs relaxed restrictions, private Exchange profile
Department receives a standardized configuration	Groups	e.g. all teachers receive a shared Exchange profile
BYOD scenario	Groups	Work profile policies only for registered BYOD users

For an Individual User

1. Navigate to `Devices` → `Device Groups`.
2. Click Add.
3. Enter a meaningful name, e.g. `DYN – John Smith`.
4. Under Group type, select Dynamic (default). The options are shown as icons; the label appears when hovering over them.
5. In the Query the devices based on the following filter definition section, set the following values in the existing filter row:
    - Query category: `Users`
    - Filter definition: `is in`
    - Click Select users and select the desired user in the selection dialog (multiple selection possible).
6. Save the device group.

For version 26.4.0


Home > Device Groups >
Add new device group
Add new device group
Cancel
Save
General
Name *
DYN - Max Mustermann
Description
Exchange mailbox for Max
Group type *
Query the devices based on the following filter definition
Filter specification *
Matches all filters
Query category
Users
Filter definition *
is in
Select users *
Max Mustermann
Device preview
After the change, the device group contains 1 devices.
Update
Search
Device name
Device description
Username
User
Status
Action
MacBook Pro 13"
MaxMustermann
Max Mustermann
Compliant
Items per page:
100
1 - 1 of 1

If several devices are assigned to the user, all of these devices are added to the group.

For a User Group

1. Navigate to `Devices` → `Device Groups`.
2. Click Add.
3. Enter a meaningful name, e.g. `DYN – Teachers`.
4. Under Group type, select Dynamic (default).
5. In the Query the devices based on the following filter definition section, set the following values in the existing filter row:
   - Query category: `Groups`
   - Filter definition: `is in`
   - Click Select user groups and select the desired user group (multiple selection possible).
6. Save the device group.

The filter also includes the members of nested subgroups of the selected user group.

User groups can be synchronized via LDAP/AD. Changes to group membership are automatically transferred to Relution. It can take up to one hour by default until dynamic device groups with a filter on user groups are re-evaluated (in addition to the LDAP synchronization interval). Only sign-ins and sign-outs on Relution Shared Devices are evaluated promptly.

For version 26.4.0

Further Filter Options

Besides `is in`, the filter definitions `not in`, `is empty` and `is not empty` are available for the Users and Groups categories. With `is empty`, a group for all devices without a device user can be created, for example.

Further filters can be added via + → Add filter, e.g. a filter with the Ownership category for the BYOD scenario. The Filter specification determines whether a device must match all filters (Matches all filters) or at least one filter (Matches at least one filter). After clicking Update, the Device preview shows which devices currently meet the filters. Details on all filters can be found in the Device groups → article.

Assign Policies to the Dynamic Device Group

After the dynamic device group has been created, the desired policies are assigned to it:

1. Open the newly created device group.
2. Switch to the Policies tab.
3. Click Add.
4. In the Add policies dialog, select one or more policies and click Confirm.

The policies are now linked to the dynamic device group and will be applied automatically as soon as a device meets the filter condition.

Recommendations and Best Practices

- Naming Convention: A consistent prefix for dynamic device groups, e.g. `DYN –`, makes them easy to distinguish from static groups.
- Policy Priority: Possible conflicts should be considered if a device is a member of multiple dynamic groups at the same time.
- Testing: New dynamic groups should first be tested with a single test device and test user before being deployed in production.
- LDAP Synchronization: When LDAP groups are used, it should be checked whether the synchronization intervals fit the intended use case.

Related Articles

- Policies explained →
- Device groups →
- User Management →
- Network-based policies (BYOD) →
- LDAP Configuration →

For version 26.4.0

Device group actions

With Relution 5.22, it is possible to trigger not only policies but also actions and CRON jobs through membership of device groups. This function fully replaced rule sets with Relution 26.0. Existing rule sets were not migrated to the new functionality.

> Device groups are platform-independent. For this reason, it may not be possible to apply individual actions to certain devices.

The basic functionality of device groups is explained here: Device groups →

Creating actions

Actions always belong to a device group. They are created under `Devices` → `Device Groups` in the detail view of the group, on the Actions tab, via Add. This requires the permission to create or edit device group actions.

The Add action form consists of two sections:

- General: Name, optionally Description, and Trigger. The Trigger field offers the options Event-based and CRON-scheduled.
- Action: The Action type field defines what is executed on the devices (see the Main action types section).

In the list of actions, each action can be switched on and off with the Enabled toggle. Disabled actions are not executed.

For version 26.4.0

Event-based

Event-based actions react to changes in group membership:

1. Trigger of execution defines when the action is executed: No trigger, When a device enters the group, When a device leaves the group or Both.
2. Delay of execution offers Immediately and Delayed. With Delayed, the delay is specified in Days, Hours and Minutes; the default is 90 minutes. If a device that entered the group is no longer a member when the delay expires, or a device that left the group is a member again, the action is not executed. This avoids executions for devices that belong to the group only briefly.

Event-based actions only apply to future entries and exits. Devices that are already members of the group when the action is created do not trigger the action.

CRON-scheduled

1. Actions can be triggered on a schedule defined by a CRON expression WIKI CRON →. At each scheduled time, the action is executed for all devices that are members of the group at that moment.
2. All fields are required. Commas are used to separate individual values, and ranges and step values are accepted. Days of month and Days of week cannot both contain specific values; one of them is set to `*` or `?`.
3. The default is a daily execution at 06:00 and 21:00 (Minutes `0`, Hours `6,21`, Days of month `*`, Months `*`, Days of week `?`). The times refer to the time zone of the Relution server.

Field	Description	Allowed Values
Minutes	Point in time within an hour	0 to 59
Hours	Point in time within a day	0 to 23
Days of month	Specific calendar day	1 to 31
Months	Month of the year	1 to 12 (or JAN-DEC)
Days of week	Day of the week	0 to 6 (0 = Sunday to 6 = Saturday, or SUN-SAT)

For version 26.4.

Common Operators

Values are entered without spaces; otherwise the portal rejects the input as invalid.

- Asterisk (`*`): Represents “every” (e.g., every minute, every day).
- Question mark (`?`): Only for Days of month and Days of week; represents “no specific value”.
- Comma (`,`): Used to separate individual values (e.g., `1,15,30` for the 1st, 15th and 30th minute).
- Hyphen (`-`): Defines a range (e.g., `1-5` for Monday through Friday).
- Slash (`/`): Defines intervals (e.g., `*/5` for every 5 units).

Crontab Guru →

These configurations are directly valid and are applied after saving.

Main action types

The Action type field offers the following types:

1. Delete device
2. Device action
3. Notification action
4. Change device name
5. Refresh device policy
6. Webhook

Delete device

Description:

- This action removes the device from Relution management. What happens on the device depends on the enrollment type:
  - Fully managed Android Enterprise devices are reset to factory settings.
  - On Android Enterprise devices with a work profile or with a personal profile, only the work profile is removed; personal apps and data are preserved.
  - On all other platforms, management is removed (e.g. the MDM profile on Apple devices or the enrollment on Windows), but the device is not reset.
- Important: This action cannot be undone.
- For devices enrolled via KME (Knox Mobile Enrollment), it must be ensured that no profile is assigned in the Samsung Knox Enrollment Portal, as the device will otherwise be re-enrolled automatically after deletion (Android only).

Options:

- Android:
  - Keep the Relution Client App: yes/no
- Managed device (Android Enterprise, fully managed):
  - Keep factory reset protection (FRP) enabled: yes/no
  - Also wipe the device's external storage (such as SD cards): yes/no
  - Message: Text displayed to users of personal devices with a work profile before the work profile is removed. It has no effect on company-owned devices.

For version 26.4.0

Device action

Description:

- Enables various individual actions on the devices.

After selection, the Details section shows the platforms on which the action is available.

Subactions:

1. Enable lost mode
    - Locks the device and enables it to be located. Can be used when a device has been lost.
    - Fields: Message, phone number, footnote, email, address, organisation name
2. Disable lost mode
    - Cancels the Lost Mode.
3. Reboot device
    - Restarts the device.
    - Field: Reason for rebooting (only Android devices without Android Enterprise and interactive whiteboards)
    - Options: Power off (only Android devices without Android Enterprise and interactive whiteboards), Notify user to reboot the device (no forced reboot), macOS 11 or later only
4. Refresh device info
    - Updates the device information stored in Relution.
5. Alert
    - Sounds an alarm on the device.
    - Field: Duration (in seconds)
6. Enable or disable Bluetooth
    - Enables or disables Bluetooth.
    - Option: Enable Bluetooth
7. Scan Device
    - Starts a Microsoft Defender antivirus scan on Windows devices.
    - Field: Scan Type (Quick Scan or Full Scan)
8. Delete local users
    - Deletes all local user accounts and data.
    - Option: Force account deletion
9. Enable or disable personal hotspot
    - Enables or disables the personal hotspot.
    - Option: Enable personal hotspot
10. eSIM Cellular Plan
    - Configures an eSIM mobile plan.
    - Field: Server URL
11. Remove Shortcut
    - Removes a shortcut from the device.
    - Fields: Label, URL
12. Request mirroring
    - Starts AirPlay playback on an Apple TV or other AirPlay-enabled device.
    - Fields: Name, MAC address, scan time (seconds), password
13. Return to Service
    - Resets the device to factory settings. Afterwards, the device tries to re-enroll in Relution automatically; this requires Activation Lock to be disabled. Available for iOS 17 or later and tvOS 18 or later.
    - Field: Wi-Fi configuration (required; selected from the enabled Wi-Fi configurations of published policies)
    - Option: Keep existing data plan (iOS only)
14. Send file to device
    - Sends a file to the device.
    - Fields: Select file, directory, do not decompress ZIP archives
15. Wipe device
    - Resets the device to factory settings.
    - Options: Keep factory reset protection (FRP) enabled, Also wipe the device’s external storage, Message, PIN, Keep existing data plan, Disable Proximity Setup
16. Install Prowise update
    - Installs a Prowise update.
    - Field: Update on
17. Lock device
    - Locks the device with the current password.
    - Fields: Message, phone number, PIN

For version 26.4.0

18. Add Shortcut
    - Adds a shortcut to the device.
    - Fields: Label, URL, Open in full screen, Icon
19. Reset lock passcode
    - Resets the device password.
    - Field: New password
    - Options: Lock immediately, Require input before next reset, Do not ask at boot
20. Reset password (Windows)
    - Resets the password of a Windows user account.
    - Fields: User name, Password, Repeat password
    - Action: Generate example password
21. Shutdown device
    - Shuts down the device.
22. Stop mirroring
    - Stops AirPlay playback.
23. Locate device
    - Triggers location of the device.
24. Clear restrictions password
    - Removes the Screen Time code.
25. Enable or disable data roaming
    - Enables or disables data roaming on iOS devices. The user can change the setting again on the device.
    - Option: Enable data roaming
26. Continue in device Setup Assistant
    - Continues the device in Setup Assistant.
27. Install Media
    - Installs media on the device.
    - Field: Token selection
28. Remove Media
    - Removes media from the device.
    - Field: Token selection
29. Execute PowerShell script
    - Runs a PowerShell script on Windows devices.
30. Log out the user
    - Logs off the current user.
31. Execute shell script
    - Runs a shell script on macOS and Linux devices. The subaction is only available if the macOS companion is enabled (`Settings` → `Relution Client Apps`, switch Enable macOS companion).
32. Request device info
    - Requests specific device information (Android Enterprise, work profile on a personally owned device, Android 13 or later). The user is asked to approve the disclosure of the information.
    - Field: Type (eSIM identifier (EID))
33. Enterprise wipe
    - Removes the work profile and all policies, relinquishing the device for personal use. Apps and data of the personal profile are preserved (Android Enterprise, company-owned device with personal profile, Android 8 or later).
34. Set default apps
    - Sets the default apps for calling, messaging and web browsing on iOS devices.
    - Fields: Default Calling App and Default Messaging App (iOS 26 or later), Default Browser App (iOS 18.2 or later)
35. Enable Remote Desktop
    - Enables remote management via Apple Remote Desktop on Macs: Remote Desktop with All Users access, the ability to receive remote events, and the Observe, Control and Show being Observed options. All other options remain unchanged (macOS 10.14.4 or later).
36. Disable Remote Desktop
    - Disables remote management via Apple Remote Desktop on Macs (macOS 10.14.4 or later).

For version 26.4.0

Notification Action

Description:

- Sends notifications to device users or other people.

Recipients:

- Notify device user
- Notify other users: selection of users and user groups
- Additional email recipients: further email addresses

Message:

- Notify via e-Mail: Sends an email based on a template. Reset to template restores the default text.
- Notify via push message: The recipients receive the push message on all enrolled devices assigned to them.

Placeholders can be used in the texts; the available placeholders are shown in the form: Advanced placeholders →

Change device name

Description:

- Changes the name of the device.

Field: Device name. Placeholders such as `${device.serialnumber}` are resolved for each device. If the result is an empty name, the previous device name is kept.

For version 26.4.0

Refresh device policy

Description:

- Updates the policies applied to the device.

Webhook

Description:

- Sends a request to an external service (e.g. another system).

Fields: URL, Method (GET, POST or PUT; POST is preselected), Headers (request headers as a list), Body

Under Test webhook parameters, Check connectivity makes the server send an OPTIONS request to the specified URL and displays the response. This shows whether the target host can be reached from the Relution server.

Geo-zones

This article describes how to automatically assign policies based on device location.
These geofences must be created in advance and then assigned using dynamic device groups.

Restrictions and notes

> The geofence function requires a permanent internet connection, a GPS module on the device and the installed Relution Agent. Supported platforms are iOS (iPhone and iPad with cellular module, e.g. Cellular iPad →), Android and Android Enterprise.

- On Android devices, detection may be delayed depending on the device state, in exceptional cases by up to 30 minutes.
- In the portal, the radius of a geofence is fixed at 100 meters around the set location.

If the geo-zone is changed without an internet connection and GPS, a manual sync of the location data must be triggered on the device in the Relution Agent.

Preparation

For version 26.4.0

For geofences to work, the Relution Agent must be installed on the device and must have been opened at least once. In addition, the permissions for push notifications and location services must be granted to the Relution Agent; users must not revoke them. This applies to iOS and Android devices. On Android, the Relution Agent requires the location permission permanently, i.e. also in the background.

On iOS devices, the location permission cannot be granted automatically via the MDM interface. Therefore, users must configure this parameter themselves.

> To do this, the value Allow access to location must be set to Always under `Settings` → `Apps` → `Relution Agent` → `Location` on the iOS device.

If this is not the case, the Relution Agent cannot transmit the current location to the server and an automatic assignment of the policies is not possible.

If zones or iBeacons are configured in the organization, Relution creates a compliance notice (Location permission or Location services) for devices whose Relution Agent lacks the location permission or whose location services are turned off. The device remains compliant.

Setting up a geofence

Geofences are managed under `Settings` → `Dynamic policy assignment` → `Zones`. A new geofence is created via Add.
In the General section, a Name is entered (required). In the Address section, the location is set: via the map search bar (address or coordinates in the format latitude, longitude, e.g. `48.7968, 9.2211`), by right-clicking or long-pressing on the map, or directly via the Latitude and Longitude fields. Center map centers the map on the set marker.
Save creates the geofence; the button is only enabled once the name and coordinates are set. Relution determines the displayed address automatically from the coordinates when saving.
An entry should now have been added to the geofence overview.

When a geofence is created, changed or deleted, Relution automatically sends the Reload zones action to all iOS, Android and Android Enterprise devices so that the Relution Agent loads the current zones. The action appears in the device's action history and cannot be triggered manually.

Viewing, creating, editing and deleting geofences requires the permissions for Zones in the Dynamic policy assignment area of the role: Permissions →

What the Relution Agent shows the user about zones and iBeacons in range is controlled by the setting Display of information about iBeacons and zones within range under `Settings` → `Device Management` in the Relution Agent section: Hide (default), Full Information or Obscured representation.

Configuring the device group

For version 26.4.0

To be able to apply the geofence to a dynamic device group, it must be configured with a filter.
Under `Devices` → `Device groups`, a new dynamic device group is created or an existing one is edited.
Entered zones is selected as the Query category and, for example, is in as the Filter definition; the required geofences are chosen via Select zones. Devices that are inside at least one of these zones then automatically become members of the group. The required policy is then assigned to the group.

Further filter definitions: with all of, the device must be inside all selected zones, with not in, inside none of them; is not empty and is empty include devices inside any zone or no zone at all and do not require a zone selection.

Device groups →

The zones a device is currently inside are shown in the device list by the Entered geofence zones column and filter, and in the device details on the Device location card under Entered zones.

Besides the geographic location, policies can also be assigned based on radio signals in a room: iBeacons →

iBeacons

Besides geo zones →, policies in Relution can also be assigned based on iBeacons. An iBeacon is a Bluetooth transmitter whose signal is received by nearby devices. When a device is in range of a registered beacon, it can automatically receive a different policy through a dynamic device group.

In the portal, both approaches belong to the `Settings` → `Dynamic policy assignment` area: Zones work with the geographic location, iBeacons with radio signals in a room. iBeacons are therefore also suitable where GPS is not reliably available — inside buildings, for example.

Limitations and notes

The following requirements must be met to use the feature:

- The Relution Agent app must be installed and must have been opened at least once.
- The permissions for push notifications, location services and Bluetooth must be enabled for the Relution Agent app and must not be disabled by users.
- On Android devices, detection may be delayed depending on the device state. In exceptional cases this takes up to 30 minutes.

For version 26.4.0

iOS, Android and Android Enterprise devices are supported. Relution does not evaluate iBeacons on macOS and Windows, even if a Relution Agent is installed there.

If iBeacons or zones are configured in the organization, Relution creates a compliance notice (Location permission or Location services) for devices whose Relution Agent lacks the location permission or whose location services are turned off. The device remains compliant.

The beacons themselves are third-party hardware and not part of Relution. Relution only manages their identifiers and evaluates which of them a device receives.

Registering an iBeacon

Under `Settings` → `Dynamic policy assignment` → `iBeacons`, a new entry is created via Add. An iBeacon is identified by three values that are determined by the hardware in use:

- Unique identifier (UUID) — a UUID specific to the app and deployment use case.
- Major ID — further specifies a specific iBeacon and use case, for example a sub-region within the region defined by the UUID.
- Minor ID — allows further subdivision of the region or use case.

In addition, a name serves as the human-readable label under which the beacon later appears in the filters.

Name and Unique identifier (UUID) are required. Major ID and Minor ID are optional and accept values from 1 to 65535.

> The combination of UUID, Major ID and Minor ID must be unique. If an entry with the same three values already exists, creation is rejected with a notice.

A typical breakdown uses one shared UUID per site, the Major ID per building or floor and the Minor ID per room. Filters can then be built at whichever granularity is required.

Existing entries can be changed via Edit and removed via Delete in the list. Viewing, creating, editing and deleting requires the permissions for iBeacons in the Dynamic policy assignment area of the role: Permissions →

When an iBeacon is created, changed or deleted, Relution automatically sends the Reload iBeacons action to all iOS, Android and Android Enterprise devices so that the Relution Agent loads the current iBeacon definitions. The action appears in the device's action history and cannot be triggered manually.

Tracking iBeacons on the device

Which beacons a device currently receives is visible in two places:

- In the inventory overview via the iBeacons in range column. The filter of the same name narrows the list down to individual beacons, the filter value No iBeacons to devices without reception.
- In the device details on the Device location card, likewise under iBeacons in range. It shows the beacons that are close enough for the device to be able to receive their signal. The card only appears if the device receives beacons, has entered a zone or reports the status of the location service.

What the Relution Agent shows the user about iBeacons and zones in range is controlled by the setting Display of information about iBeacons and zones within range under `Settings` → `Device Management` in the Relution Agent section: Hide (default), Full Information or Obscured representation.

For version 26.4.0

Configuring the device group

For a beacon to trigger a policy, it is set as a filter in a dynamic device group.

Under `Devices` → `Device groups`, a new dynamic device group is created or an existing one is edited. iBeacons in range is selected as the Query category and is in as the Filter definition; the required beacons are chosen via Select iBeacons. Devices that receive at least one of these signals then automatically become members of the group and receive the policy assigned there.

Further filter definitions: with all of, all selected beacons must be in range at the same time, with not in, none of them; is not empty and is empty include devices with any beacon or no beacon in range and do not require a beacon selection.

Device groups →

Related topics

- Geo-zones → — assign policies based on the geographic location.
- Device groups → — dynamic groups and their filters.

Network-based policies (BYOD)

In BYOD scenarios, devices are used both inside and outside of school.
A purely time-based policy assignment is often inflexible and comes with a high administrative overhead.

A proven alternative is network-based policy assignment, where policies are automatically applied as soon as a device is connected to the school network.
Detection is based on the public IP address of the network.

This approach is particularly well suited for BYOD environments, as devices are not unnecessarily restricted outside of school while administrative effort is reduced.

Basic principle

The location of a BYOD device is determined indirectly via its public IP address.

The setup consists of:

- One policy that should only apply within the school network
- One dynamic device group that collects devices based on their public IP address

When a device contacts Relution from the school Wi-Fi, Relution detects the public IP address of the school network. The device is then automatically assigned to the dynamic device group and receives the corresponding policy.

For version 26.4.0

> The device must remain connected to the school Wi-Fi for the configuration to be applied and maintained.

Recommended BYOD base group

Regardless of the dynamic group for the school network, BYOD devices should always be assigned to a base device group.

This group contains configurations that apply permanently, such as:

- School Wi-Fi profiles
- Required apps
- Basic restrictions that also apply outside of school

This ensures that devices remain functional at all times.

Configuring the dynamic device group

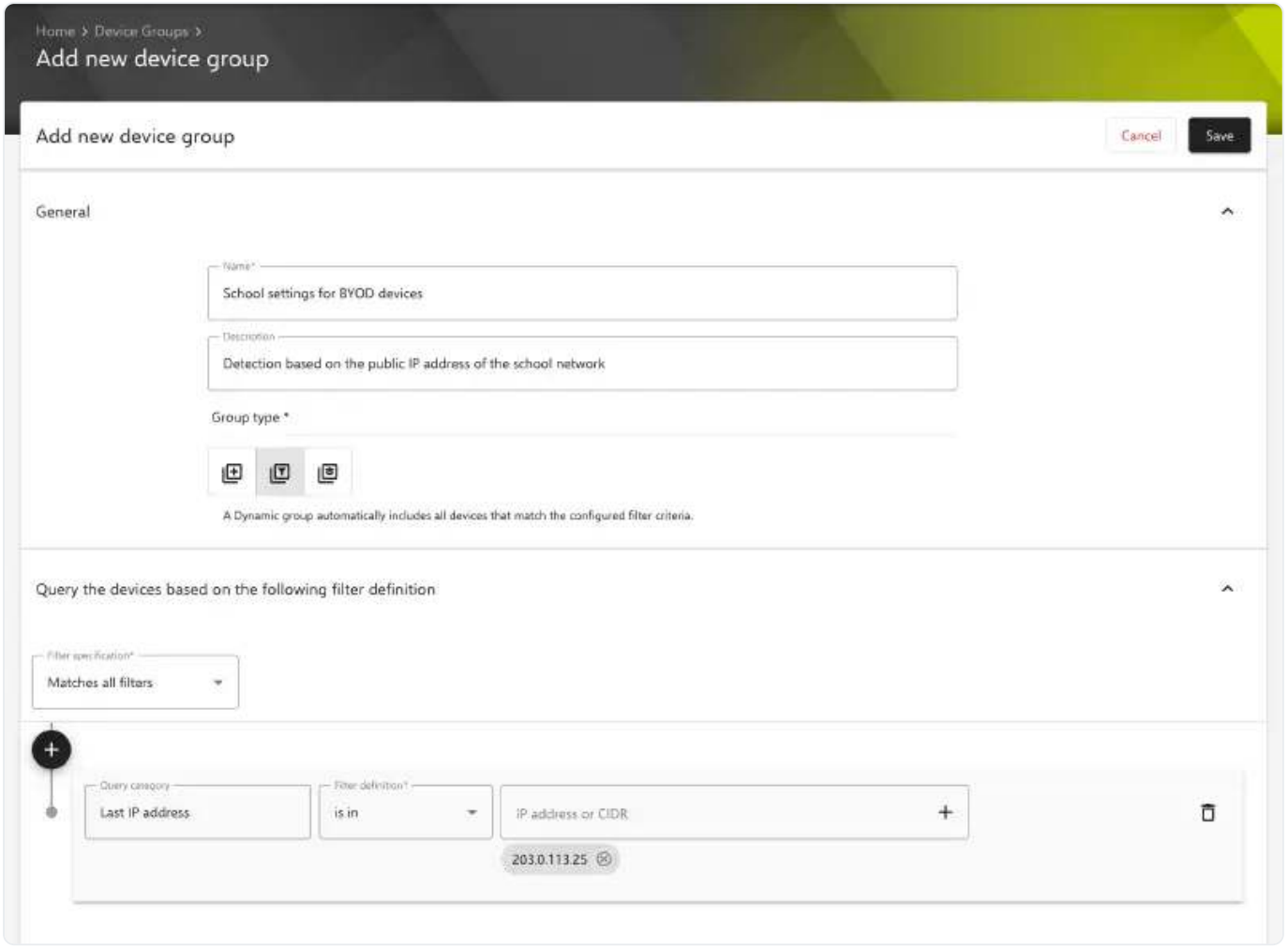
A new dynamic device group is created. Last IP address is selected as the Query category and is in as the Filter definition. The public IPv4 address or IPv4 range of the school network is entered in the IP address or CIDR field (e.g. `203.0.113.25` or `203.0.113.0/24`); multiple entries are possible.

The filter must cover the public IP range of the school network.
All devices whose most recently detected IP address lies within this range are automatically added to the group.

The filter evaluates IPv4 addresses only. If a device reaches the Relution server via IPv6, its last IP address is stored as an IPv6 address and the device is not included in the group.

The IP address Relution most recently detected for a device is shown in the device details on the Network card under Last IP address, and in the column of the same name in the device list. This helps to determine the matching public range.

Device groups →



Updating the IP address

Relution takes the public IP address from the connection whenever the device contacts the server. This can be triggered specifically with the Refresh device info action.

An update takes place in particular in the following cases:

- When policies are executed
- During the periodic availability-check ping, if Check device availability is enabled (once per day by default, configurable via Ping interval in minutes under `Settings` → `Device Management`; not for Android Enterprise)
- Via a device group action with the CRON-scheduled trigger
- When an administrator runs the Refresh device info action for the device in the portal
- When the user triggers a refresh in the Self-Service Portal (at the earliest 5 minutes after the last refresh)
- When the user manually triggers the action in the Relution Agent via the Settings tab

Recommendation: CRON-scheduled action in the base group

In most BYOD environments, a device group action of the action type Device action with Refresh device info and the CRON-scheduled trigger is recommended. The action is created in the BYOD base group, in which the device permanently resides, and not in the dynamic IP group. A CRON action is only executed for devices that are currently members of the group. In the dynamic group, it would never reach devices outside the school network, so these would not be added to the group automatically. Using the base group ensures that devices regularly update their IP address without requiring user interaction.

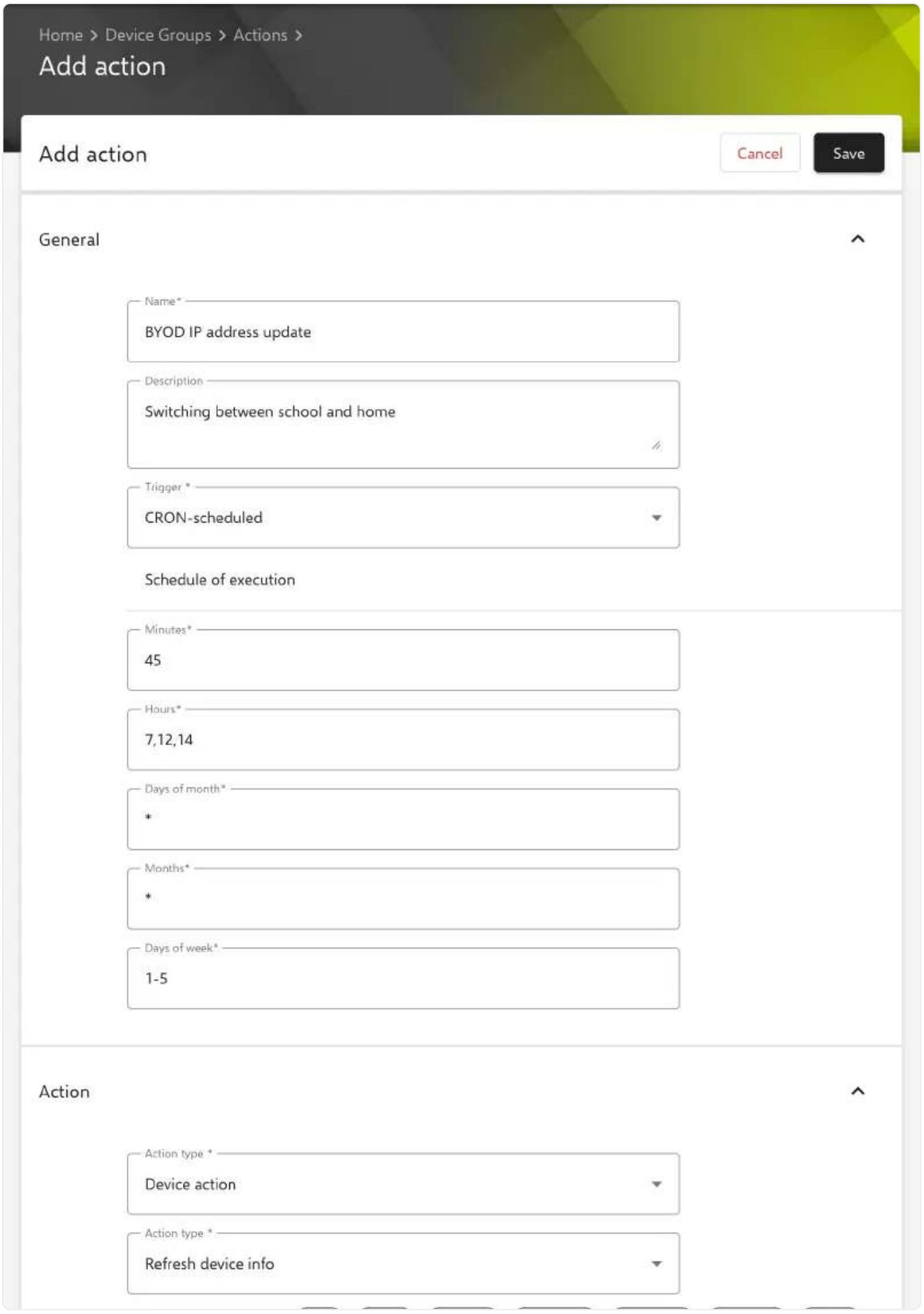
For version 26.4.0

Notes on using CRON actions

- Do not use very short intervals
- Avoid high execution frequencies

For example, running Refresh device info every hour for a large number of devices can lead to significant performance issues.

A moderate interval is sufficient and ensures stable operation.
In the following example configuration, the action is executed on all weekdays at 7:45, 12:45, and 14:45.


Home > Device Groups > Actions >
Add action
Add action
Cancel
Save
General
Name*
BYOD IP address update
Description
Switching between school and home
Trigger *
CRON-scheduled
Schedule of execution
Minutes*
45
Hours*
7,12,14
Days of month*
*
Months*
*
Days of week*
1-5
Action
Action type *
Device action
Action type *
Refresh device info

Advantages of network-based assignment (BYOD)

- No complex schedules required
- Policies only apply within the school network
- Fewer policies compared to time-based approaches
- Ideal for privately owned devices

Limitations and notes

- Devices must be connected to the school network
- The method depends on stable public IP ranges
- Only IPv4 is supported; devices that reach Relution via IPv6 are not detected
- Changes may only take effect after the next device info refresh
- If a reverse proxy sits in front of Relution, it must pass on the client IP in the `X-Forwarded-For` header and be classified as a trusted proxy (Relution evaluates forwarded headers via `server.forward-headers-strategy=native`); otherwise Relution only sees the address of the proxy, see Trust the reverse proxy's IP address →

Summary

Network-based policy assignment using the public IP address is a low-maintenance and reliable solution for BYOD environments.

It allows school-specific policies to be applied only when devices are actually connected to the school network, while remaining unrestricted outside of it.

For version 26.4.0

Inventory overview

The inventory overview in Relution offers a wealth of information and customization options. The following is an overview of the available functions. The device inventory provides all the relevant information and functions necessary for managing devices.

For version 26.4.0

Available columns

- Device name
- Description
- Organization (only visible with read permissions for devices of other organizations)
- User
- Username
- E-mail address
- Status
- Actions (number of open actions)
- Available Updates (Windows)
- Connection state
- Policy state
- Platform
- Enrollment type
- Phone
- Manufacturer
- Model
- Ownership
- Last connected
- Last companion connection date
- Enrolled
- Created on
- Device Groups
- Policies to be installed
- Active Policies
- Auto Enrollment Type
- Serial Number
- OS Version
- OS Edition
- OS Update Status
- Wi-Fi MAC
- Ethernet MAC
- Lost mode status
- Supervised
- Bootstrap Token
- Shared iPad
- Battery level
- IMEI
- ICCID(s)
- Roaming
- Last IP address
- Last known location (country determined from the last IP address)
- iBeacons in range
- Entered geofence zones
- Identity certificate expiration date (in the column selection: Identity certificate expired)
- Trust expired identity certificates
- FDE
- Security patch level
- Disabled policies
- Loan to (only with the lending system enabled, see Lending →)
- Loan until (only with the lending system enabled)

In addition, there are five custom columns that can be activated and named in the settings, see Custom Device Properties →.

For version 26.4.0

The order and visibility of all columns can be individually configured by the user. In the column selection, columns are sorted by drag and drop. Adjusted column widths are saved.

Search and filter options

Columns can be sorted in ascending or descending order. By default, the list is sorted by Last connected in descending order. It is also possible to narrow down the list and make it clearer by using search terms.

The following filter options are available:

- Organization (only with read permissions for devices of other organizations)
- Platform
- Enrollment type
- OS Version
- Security patch level
- Has pending OS Update (yes/no)
- Device models
- Status
- Lost mode status
- OS Edition
- Device group
- Ownership
- Policies to be installed
- Active Policies
- Connection state
- Roaming (yes/no)
- Last known location (selection of country)
- Manufacturer
- Identity certificate expired (yes/no)
- Trust expired identity certificates (yes/no)
- Actions (number of open actions)
- Shared iPad (yes/no)
- Supervised (yes/no)
- Bootstrap Token (yes/no)
- Disabled policies (yes/no)
- Auto Enrollment Type
- iBeacons (only with read permission for iBeacons)
- Entered geofence zones (only with read permission for geofence zones)
- KSP reason policy name and KSP reason message (only with Android Enterprise available and read permission for device policies)
- one filter per activated custom column (named after the column)

By default, the Status filter is set to Compliant, Inactive and Noncompliant. Devices with the status Enrollment pending… are therefore only shown once this status is selected in the filter.

Paging

The lists can contain 50, 100, 250 or 500 entries per page. By default, 100 entries are shown per page.

For version 26.4.0

Additional functions

Devices can be selected from the inventory and actions can be assigned to them directly. For selected devices, options such as Delete, Apply action, Move to (another organization), Re-apply policies, Claim serial number to lifetime license, Add to device groups and Remove from device groups are available.

Individual columns can also be updated with Update via CSV: devices are matched by serial number, and the device name, user (email address) and activated custom fields can be changed.

Export view as CSV exports a CSV file with all columns displayed. For more than 500 entries, a dialog offers the choice between Export current page (only the page displayed) and Export all data.

Deleted devices are first moved to the trash (`Devices` → `Trash`). There, the additional columns Deleted on and Deleted by are available.

For version 26.4.0

Move device to organization

Enrolled devices can be moved from a source organization to a target organization. During that process the user and organization specific device data will be adapted or removed.

Prerequisites

- At least Relution version `5.23.0`
- The functionality is only available in the store organization
- The executing user must have the permission to update devices
- The target organization has a valid device license that is not exceeded. Devices whose serial number is claimed to a lifetime license → are exempt.
- Apple devices: The target organization uses the same APNs certificate the device is enrolled with. This can also be a certificate inherited from the parent organization.
- Supported platforms
  - Android Legacy
  - Apple (iOS, iPadOS, macOS, tvOS)
  - Interactive Whiteboards
  - Windows

If a prerequisite is not met for a device, this device is not moved, while the other selected devices are.

For version 26.4.0

Adaption of device data

User and organization specific data cannot be moved to another organization. Therefore, the corresponding data is either removed from the device or it is adapted for the target organization.

Unfinished actions of the device are canceled before the device is moved.

The following data is always removed:

- All actions of the device
- All assigned rulesets
- The assigned user
- All issued education certificates

The following data is removed if it belongs to the source organization:

- Issued device certificates
- Information for the device lending functionality
- Assigned zones
- Assigned iBeacons

The corresponding data of the store organization is retained. If a device is moved out of the store organization, this data is therefore retained completely.

Further adaptions for the device are described in the following sections.

Adaptions for all platforms

Device groups

- The device is removed from static and dynamic local device groups of the source organization.
  - If a device leaves a device group the applied policies are removed.
- The device will be automatically added to the matching dynamic local device groups of the target organization.
  - If a device enters a device group the corresponding policies are applied.
- The device is not removed from public device groups.

Device history

- The history of the device is completely removed.
- Additionally a new device history is created for the successful moving into the target organization.

Enrollment

- Single enrollments are moved to the target organization.
- For Multi enrollments, there will be a new unusable single enrollment created in the target organization.
- Additionally the referenced user, rulesets, policies and notifications are removed from the device.
- An assignment to an automatic enrollment, e.g. via Automated Device Enrollment (ADE, DEP in the portal), is only retained if it originates from the store organization.

Adaptions for Windows

- The history of local scripts of the source organization is removed from the device. The history of public scripts and of scripts from the meta organization is retained.

For version 26.4.0

Adaptions for Apple

- Apps and Books (VPP in the portal) licenses that belong to a VPP token of the source organization (local VPP token) are removed from the device.
- Licenses that belong to a VPP token of the store organization are moved into the target organization.
- Licenses that belong to a VPP token of a meta organization → are moved into the target organization if the source and target organization belong to the same meta organization. Otherwise, they are removed from the device.
- Managed Media is not removed from the device and will be visible in the target organization.
  - Except when the Managed Media has been applied by a configuration and the device leaves the corresponding device group.
  - Managed Media from the source organization can be removed from the device in the target organization.
- The supervision certificate cannot be moved to the target organization. The certificate can only be downloaded from the moved device if the permission to read devices exists both in the target organization and in the organization the certificate belongs to (usually the source organization).

Process

In the device inventory of the store organization one or more devices can be moved into a target organization. First the devices must be selected. After that the 3-dot-menu entry Move to can be clicked. For a single device, the entry is also available in the 3-dot menu of the respective device row. The entry is not available if the selection contains deleted devices, devices with the status `WITHDRAWN` or devices of an unsupported platform.

In the dialog the target organization must be selected. In general, devices can be moved to all organizations except the store organization, the system organization, meta organizations and the source organization. Meta organizations are shown for selection, but moving devices there is rejected and the devices remain in their previous organization. If only devices from one source organization are selected, this organization is not shown in the dialog. If devices from several organizations have been selected, all those organizations can be chosen as target organization. But selected devices that belong already to the target organization will not be considered.

The second step of the dialog contains an information box with hints for the possible consequences and a link to the documentation.

After confirmation the selected devices will be moved to the target organization. Each device is moved individually. If a device cannot be moved, it remains in its previous organization, e.g. if the target organization has no free device license or, for Apple devices, the APNs certificate of the target organization does not match that of the source organization. The portal does not display an error message in this case. The result should therefore be checked in the Organization column of the device inventory.

For version 26.4.0

Lending

The Relution lending system supports schools in the efficient management of loan devices. The system enables administrators to define lending conditions, track lending periods, and monitor device status.

The goal is a transparent, secure, and smooth process for device handover and return.

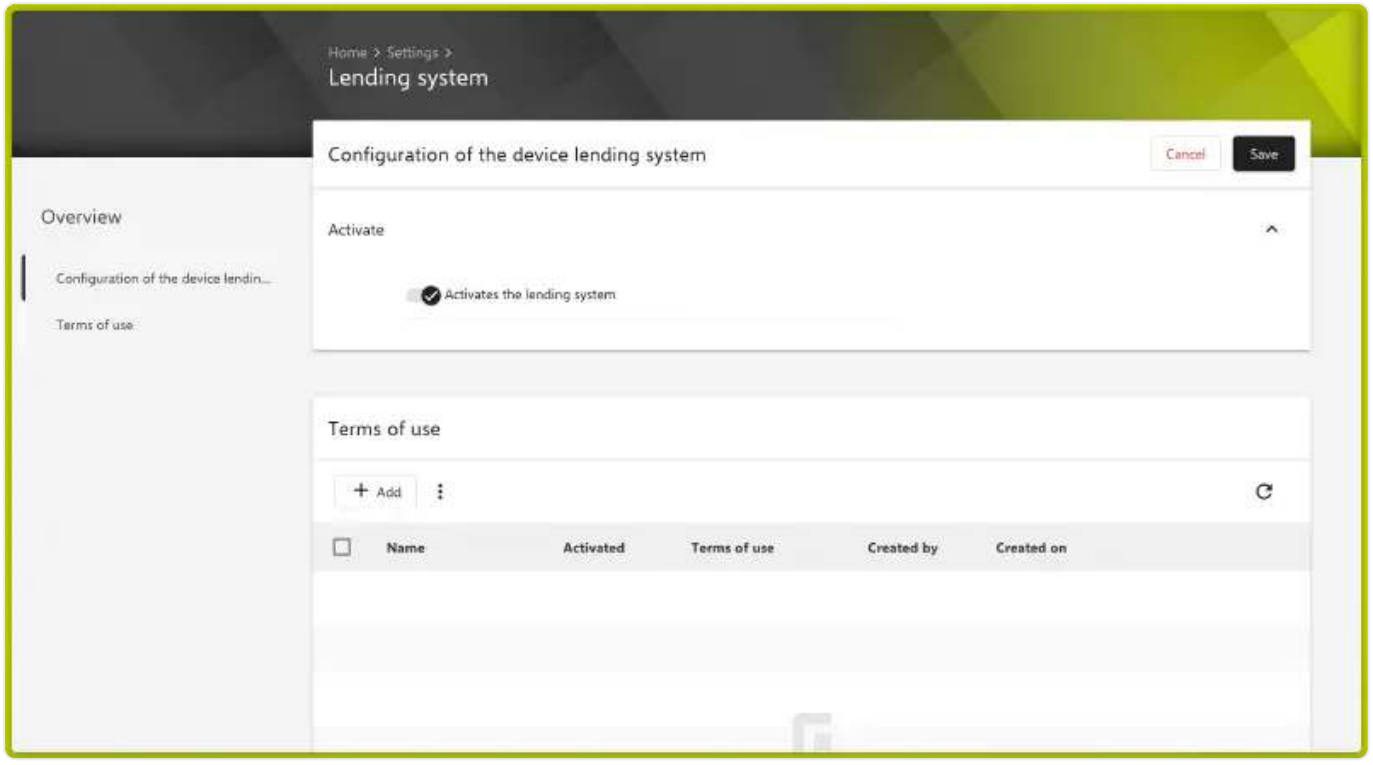
A newly added feature is the option to process device returns with the Relution Assets App, see Assets →.

Activate Lending System

The lending system can be activated in Relution in the desired tenant under the following path:

`Settings` → `Lending system`

The lending system is not available in the global organization.



Terms of Use

Before devices are issued to students or teachers, clear terms of use should be defined.

These include, among others:

- general framework conditions
- regulations for issuing and returning loan devices
- liability in the event of damage or loss
- initial setup and configuration of devices
- compliance with data protection and youth protection regulations

These conditions can be stored in Relution under `Settings` → `Lending system` (section Terms of use, button Add terms of use) and formatted with Markdown for better readability.

It is possible to save multiple usage variants that can be selected during lending.

The documented terms of use are available throughout the lending process and can be selected for each lending transaction. This ensures that it is always traceable under which conditions a device was issued.

Only terms of use enabled with the Activated switch are available for selection. The text of a terms of use entry cannot be changed after it has been created; when editing, only the name and the activation can be changed. For a new version, a new terms of use entry is created and the old one is deactivated.

Additionally, a signed document, e.g. a physical loan agreement, can be uploaded in the Signature field when lending a device.

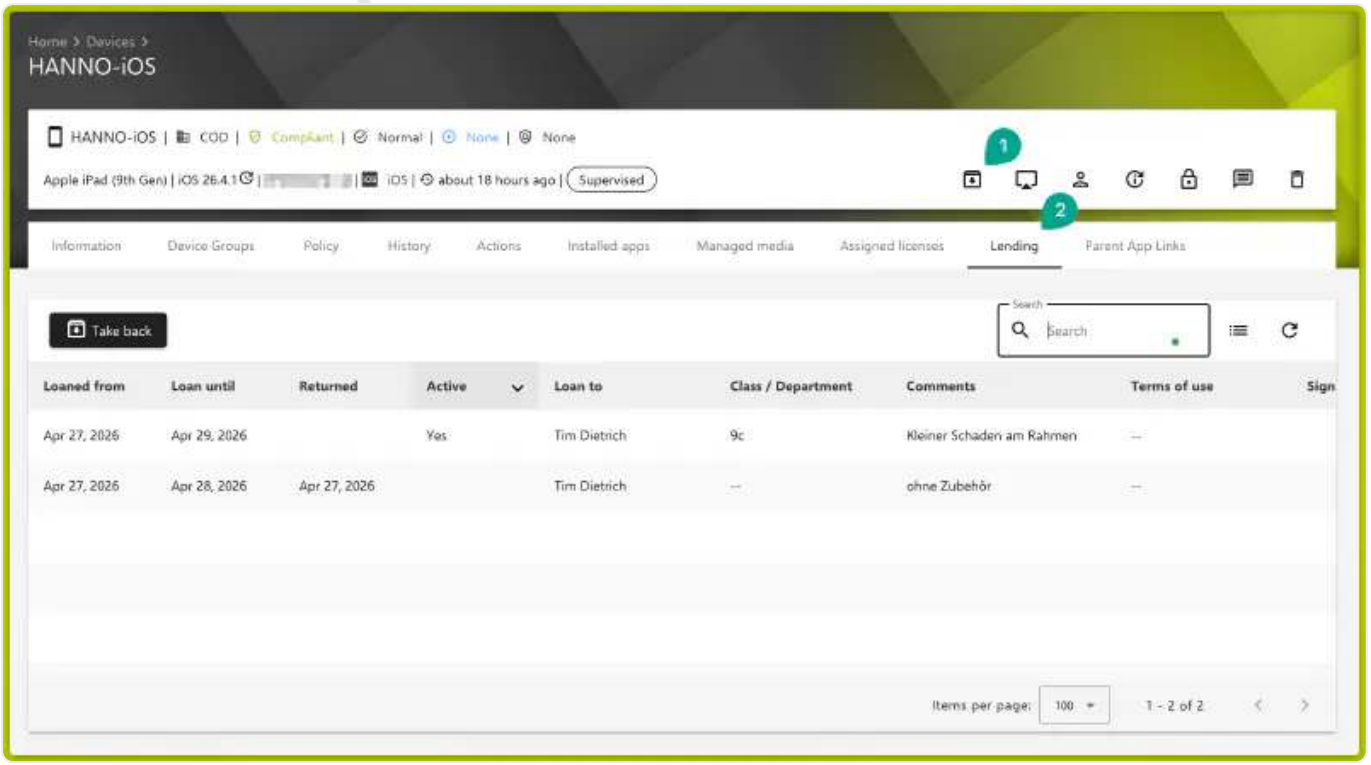
Lending Devices

To systematically map lending in Relution, devices can be lent out in the Inventory.

For version 26.4.0

Two entry points are available in the device details:

- Quick access Lend device in the info box (1)
- Lending tab with the Lend button (2)



In the following dialog, the lending period is defined using the required fields Loaned from (prefilled with the current date) and Loan until. The lending period lasts until the end of the day selected under Loan until.

The device is assigned to a student or teacher. In the required field Loan to, the name of the borrower is entered.

A suggestion function allows previously entered names as well as existing Relution users to be selected.

Optionally, the class or department of the borrower can be entered in the Class / Department field. Previously used entries are suggested here as well.

Additional Information During Lending

The Comments field can be used for notes, for example:

- purpose of the lending
- project or measure
- notes on the device condition

If accessories such as a power supply, case, or pen are issued, this can be documented and checked upon return.

In addition, it is possible to:

- select stored terms of use in the Terms of use field
- upload a signed document (e.g. the loan agreement) as PDF, JPG or PNG in the optional Signature field

In the Lending tab of the device details, an ongoing lending is marked in the Active column. The device is not available until it is returned and can only be lent out again afterwards. The tab also shows the complete lending history of the device with the recorded details, e.g. Loan to, Class / Department, Terms of use, Signature (for download) and Loan by.

In the inventory overview, lent devices can be identified by the columns Loan to and Loan until. These are hidden by default and can be shown via the column selection.

For version 26.4.0

Returning Devices

The return is also processed via the device details page:

- Quick access Take back device in the info box
- Lending tab with the Take back button

In the following dialog, the lending details are locked; only the Comments field can still be changed. The return is confirmed with Return, and the current time is saved as the return date.

After a successful return, the lending is no longer marked as active in the Lending tab; the Returned column shows the return date.

The device is then available again as a loan device and can be lent out again.

Exceeded Lending Period

If the lending period is exceeded and the device is not returned on time, the Loan until date is highlighted in red in the inventory overview and in the Lending tab. In addition, a bell icon with the tooltip Lending period exceeded next to the device name in the inventory list indicates the exceeded period.

Once the lending period has expired, the device automatically receives the compliance violation Lending period exceeded and is considered non-compliant. Relution checks this regularly (hourly by default) and whenever a lending is saved. When the device is taken back, the violation is removed again.

Rules for Exceeded Lending Periods

Further automatic reactions are set up using a dynamic device group with actions: the group filters on Compliance violations with the value Lending period exceeded (alternatively on Loan until), and the group actions are executed for the devices in this group, e.g. as soon as a device is added to the group. See Device groups → and Device group actions →.

The following reactions can be linked to this status via group actions:

- Using a Notification action with the option Notify other users, administrators can be informed automatically.
- Using a Device action, loan devices can be locked or reset to factory settings.

This ensures safe and controlled use of loan devices.

For version 26.4.0

Record Accessories

Relution offers the option to define up to five additional fields individually under Custom Device Properties →.

Examples:

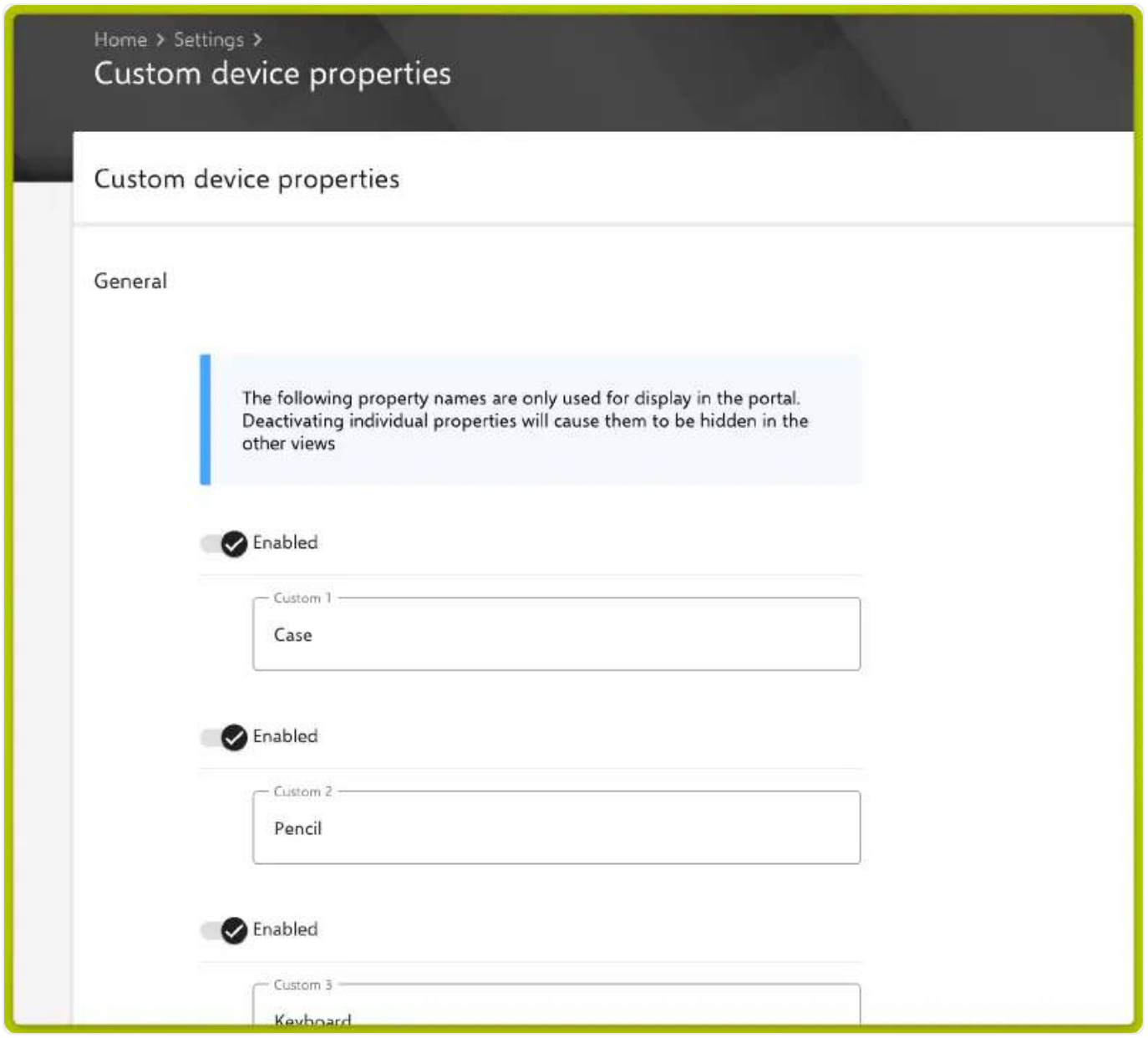
- power supplies
- bags
- pens
- adapters
- additional accessories

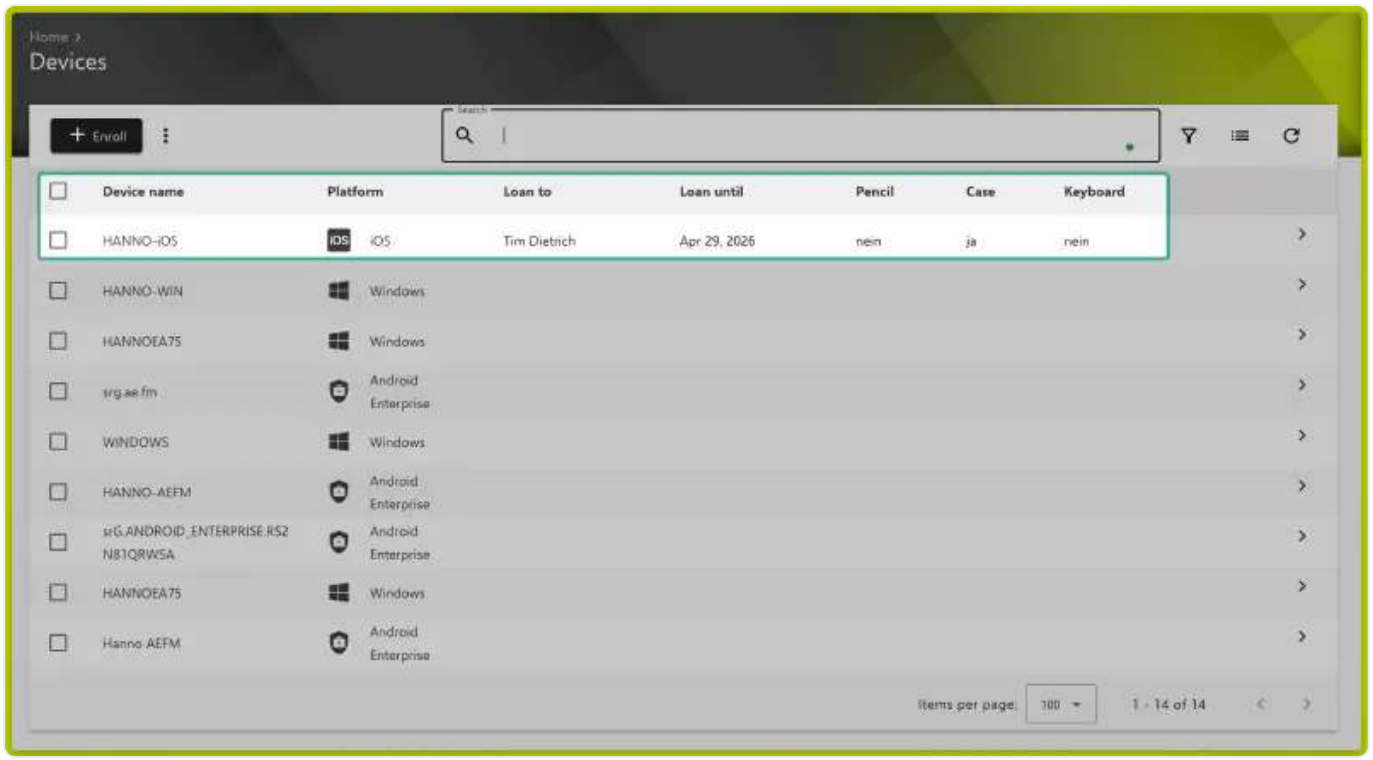
These defined properties can be configured in the device details and specifically checked upon return.

Once custom device properties are activated, they are displayed in the device details under Information at the bottom of the page.

Activated custom device properties can also be shown in the inventory overview in the Relution portal.

This makes it easy to record which accessories belong to a device. Upon return, it can be quickly checked whether all issued items have been returned in full.


Home > Settings >
Custom device properties
Custom device properties
General
The following property names are only used for display in the portal. Deactivating individual properties will cause them to be hidden in the other views
Enabled
Custom 1
Case
Enabled
Custom 2
Pencil
Enabled
Custom 3
Keyboard



For version 26.4.0

Custom Device Properties

Under `Settings` → `Custom device properties`, five freely nameable free-text fields (`Custom 1` – `5`) are available, allowing devices to be enriched with additional information – for example a cost center, location, or included accessories.

Enabling and Naming Fields

Each of the five fields has its own on/off toggle and an editable label. The label can only be entered once the field is enabled. If an enabled field is saved without a label, it appears everywhere with its default name (e.g. Custom 1). The label is only used for display in the portal; disabling a field hides it again in all views. The values stored on the devices are retained.

> There are no field types (number, date, dropdown, etc.) – all five fields are plain free-text fields.

Usage

Enabled fields are available in the following places:

- Device detail view: a dedicated Custom properties card, with values directly editable via the pencil icon (with permission to edit devices).
- Enrollments and auto enrollments: one input field per enabled field in the form and an optional column in the list; the stored values are transferred to the device during enrollment.
- Inventory list: as optional columns that can be shown and as filters with multiple selection from the existing values, see Inventory overview →.
- CSV: export from the device list and the auto enrollment list (columns `custom1` – `custom5`); existing devices and auto enrollments are updated with Update via CSV (matched by serial number, column header = configured label or `custom1` – `custom5`, empty cells change nothing).
- Dynamic device groups: as a filter criterion, using the label configured here as the display name.
- Placeholders: `${device.custom1}` to `${device.custom5}`, e.g. in device names, see Advanced placeholders →.

For a practical example, see Lending: Record Accessories →.

For version 26.4.0

Download Device Logs

Debug logs for individual devices can be enabled and downloaded directly via the Relution portal.

Debug logs for specific devices can be downloaded from the server directly via the Relution portal. This makes troubleshooting considerably easier, as direct access to the server's file system is no longer required.

Prerequisites

- Organization: The feature is only available in the global organization.
- Permissions: System administrator or a user whose role includes the Logging permission in the Devices section (only selectable for the global organization).

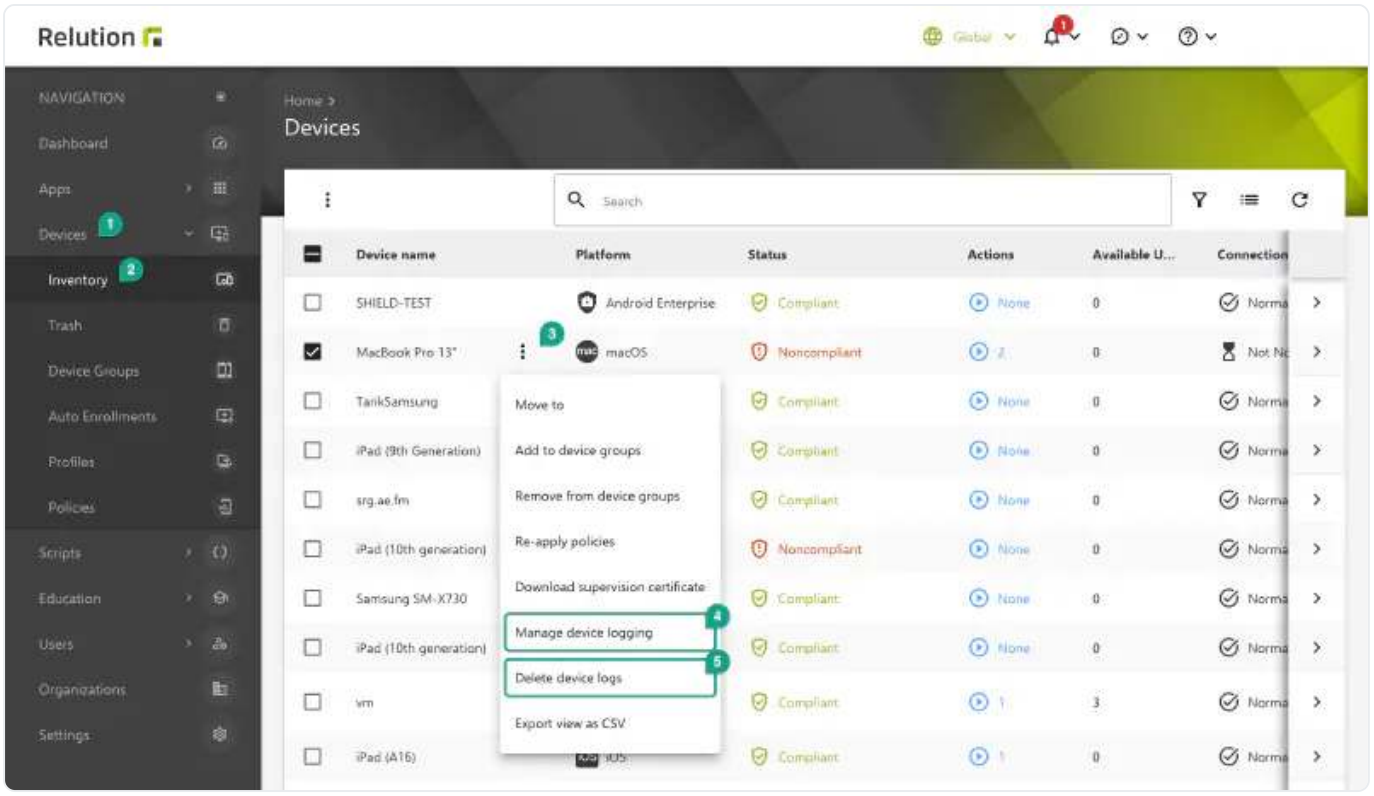
Instructions

The following steps enable logging or download existing logs:

1. Login: Logging in to the Relution portal requires an administrator account of the global organization.
2. Navigate to Device: The device is selected under `Devices` → `Inventory`.
3. Context Menu: The device's context menu opens via the three dots icon (Actions) in the device row.
4. Manage Device Logging: The Manage device logging entry opens the corresponding dialog.
    - Activate logging: The Activate device based logging toggle enables logging and shows the Duration (in minutes) field, which defines how long detailed logging remains active (default: 60 minutes, minimum: 1). Confirm applies the setting. While logging is active, the dialog shows the Start time and End time. To end logging early, the toggle is turned off and the change is applied with Confirm.
    - Download Logs: The Device logs section provides a Download button for the log archive (ZIP file) that the server has collected for this device. In a clustered environment, the archive only contains the logs of all instances if Spring Boot Admin is enabled; otherwise, only the logs of a single instance are downloaded.
5. Delete Device Logs: The Delete device logs entry in the context menu removes the collected logs of the selected devices from the server.

The menu entries are also available in the device list of a device group.

For version 26.4.0



Notes on Storage

- The logs are only held in the server's memory and are lost when the server is restarted.
- A limited number of log events is stored per device (10,000 by default). With a long logging duration or very active devices, older messages are discarded.
- One day after logging has ended, the system deletes the logs automatically.

Test version 26.4.0

Configure DEP

Apple Automated Device Enrollment (ADE, DEP in the portal; formerly `Device Enrollment Program`) provides organizations with the ability to enroll and provision their own Apple devices. ADE streamlines the process of large-scale device provisioning and management by allowing devices to be pre-configured before they are distributed. Users receive their devices fully configured and ready to use out of the box, while data remains private and the system is secure. All pre-configured settings are controlled by administrators via remote management, and compliance is maintained wirelessly, never requiring on-site manual intervention.

ADE-compatible devices

All iPhones, iPads, Mac computers or Apple TVs purchased on or after March 1, 2011, either directly from Apple or from a participating Apple Authorized Reseller, are eligible for ADE. iPhones and iPads must be running iOS/ iPadOS 7 or later, Mac computers must be running OS X 10.9 or later, and Apple TVs must be running tvOS 10.2 or later. Apple Vision Pro (visionOS) can also be enrolled in Relution via ADE. Apple devices can be added to ADE using `Apple Configurator`, regardless of where the devices were purchased. When an Apple device that was manually registered is set up, it behaves like any other registered device with mandatory supervision and mobile device management (MDM) enrollment. For Apple devices that were not purchased directly, users have a 30-day transition period to remove the device from MDM enrollment and supervision.

For version 26.4.0

Advantages of ADE

The biggest advantage of ADE is the simplicity of the auto-enrollment process. This process ensures that all Apple devices are configured according to the organization's requirements, and it also guarantees that all users have the same apps, settings, restrictions and permissions on their devices before they are even issued to them.

Other benefits

- Installation of MDM profiles that users cannot remove, so that the devices remain under remote management. To achieve this, the option User may remove MDM Enrollment is disabled in the DEP profile (enabled by default).
- Ability to enable supervision wirelessly.
- Pre-configuration of an initial setup, avoiding time-consuming issues for end users.
- Silent app installation and push capabilities.
- More control for the IT department.
- Fewer security issues.

Supervised iOS devices, DEP and MDM →

Migration of devices via Apple Configurator

`Apple Configurator` is a solution for small organizations that only have a few Apple devices to manage or only need a basic configuration for their devices. Because `Apple Configurator` does not provide wireless capabilities, devices managed with `Apple Configurator` must be physically connected to a Mac computer in order to make changes. This can be beneficial for organizations that need a hands-on approach.

Migrating from `Apple Configurator` to ADE with Relution is the solution for organizations of any size that want a user-friendly system for managing any number of Apple mobile devices. The migration provides a user-friendly and wireless solution with advanced features that can be customized to meet the needs of organizations of any size.

Add DEP devices with Apple Configurator 2 →

Restrictions on adding devices to ADE

Apple devices purchased on or after March 1, 2011 can be enrolled in ADE after a factory reset. The only other restriction is that the device must be enrolled in ADE within three years of the purchase date.

Remove devices from ADE

Devices can be removed from ADE at any time. Damaged, lost or stolen devices can and should be removed from ADE as soon as possible. Once a device has been removed from ADE, it can no longer be assigned automatically via the reseller; it can only be added again manually using `Apple Configurator`.

Adding devices from authorized dealers to ADE

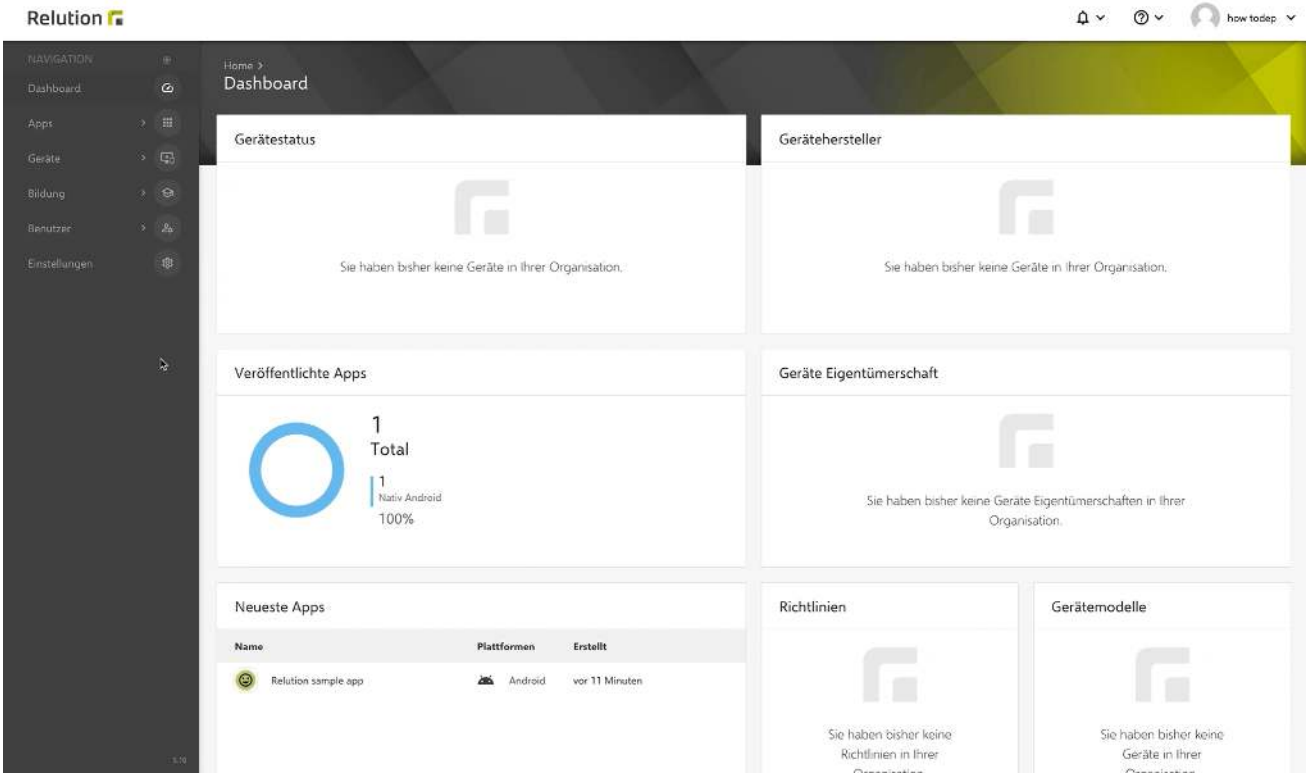
ADE works with Apple devices that support ADE when purchased from authorized resellers and carriers. Checking with the dealer before purchasing an Apple device is recommended. To register for ADE with Apple, an Apple customer number or a DEP reseller ID must be entered. If a reseller does not have this number, ADE cannot be accessed.

For version 26.4.0

How To

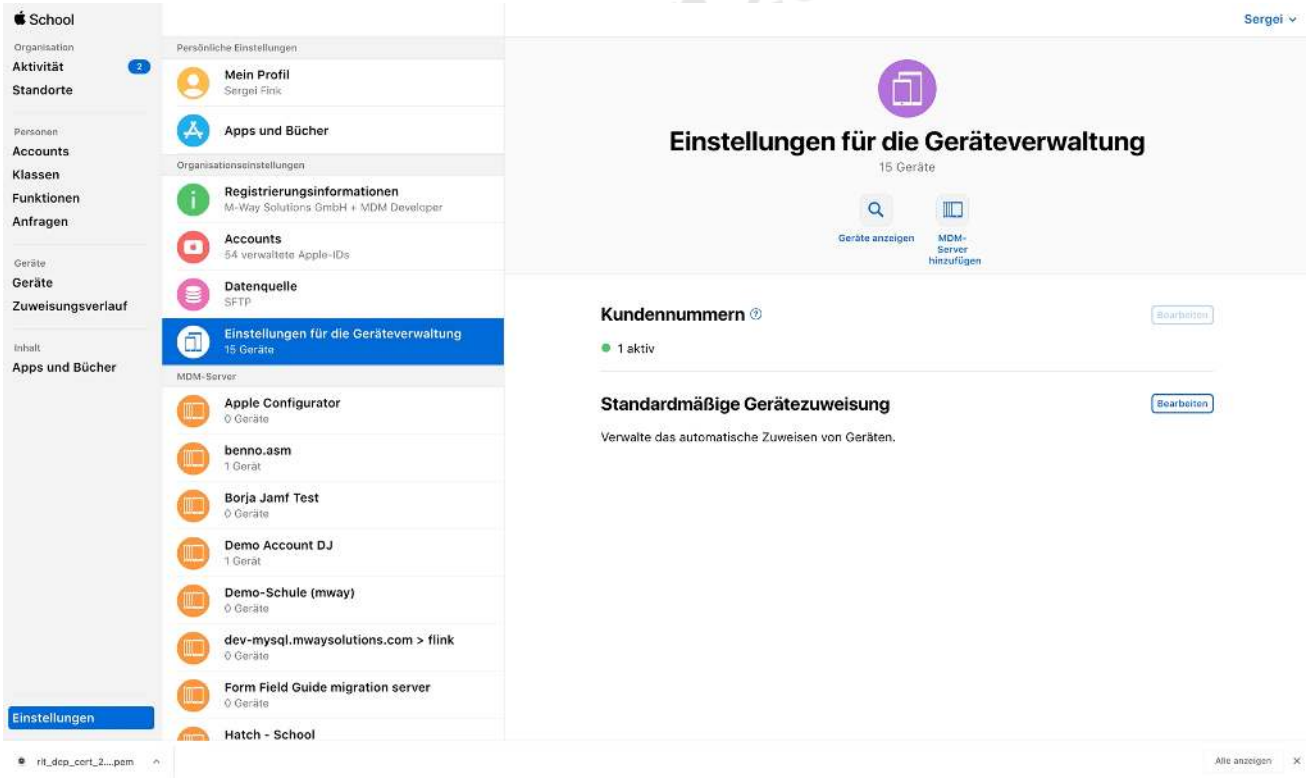
The DEP account is set up in Relution under `Settings` → `Apple Automated Device Enrollment` (Device platform specific section).

1. The server certificate is downloaded in Relution via Download certificate.

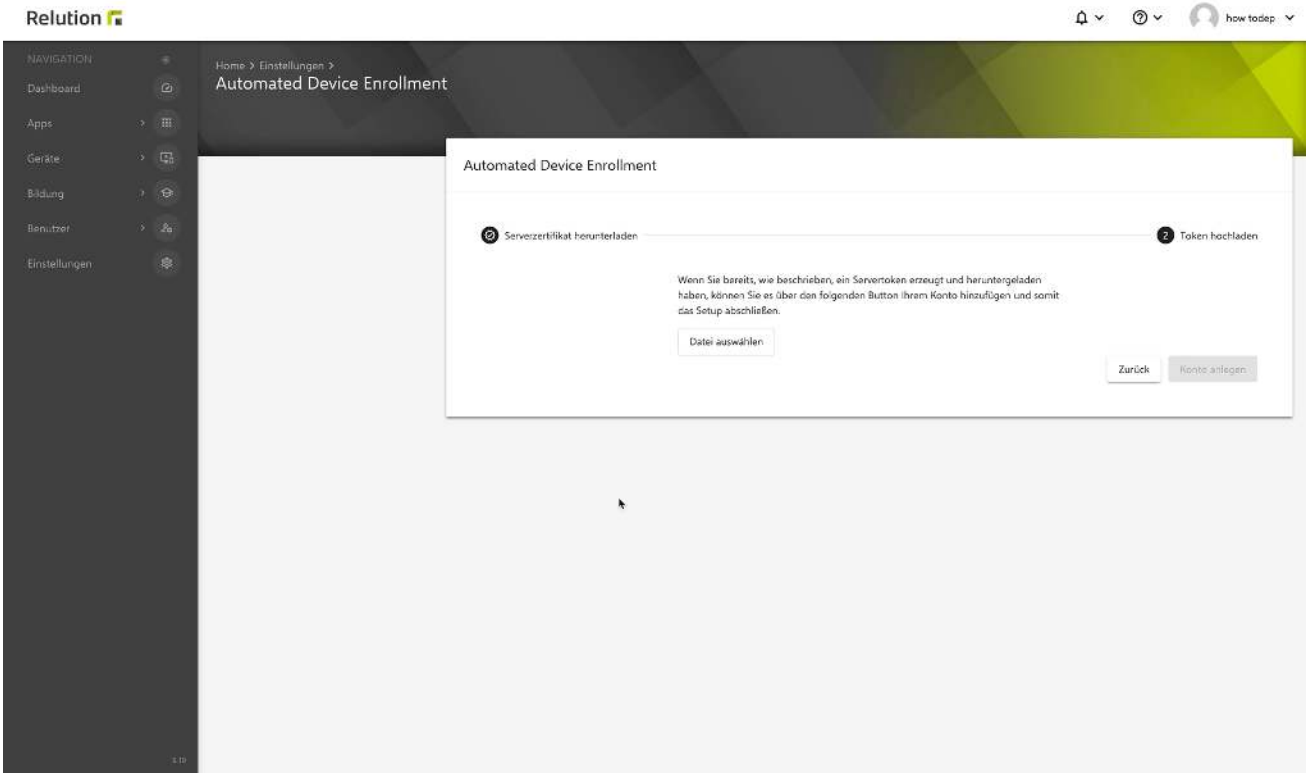


2. An MDM server is created in Apple School/ Business Manager.

3. The certificate is uploaded and the token is downloaded.



4. The token is uploaded to Relution via Upload token, and its validity is checked.



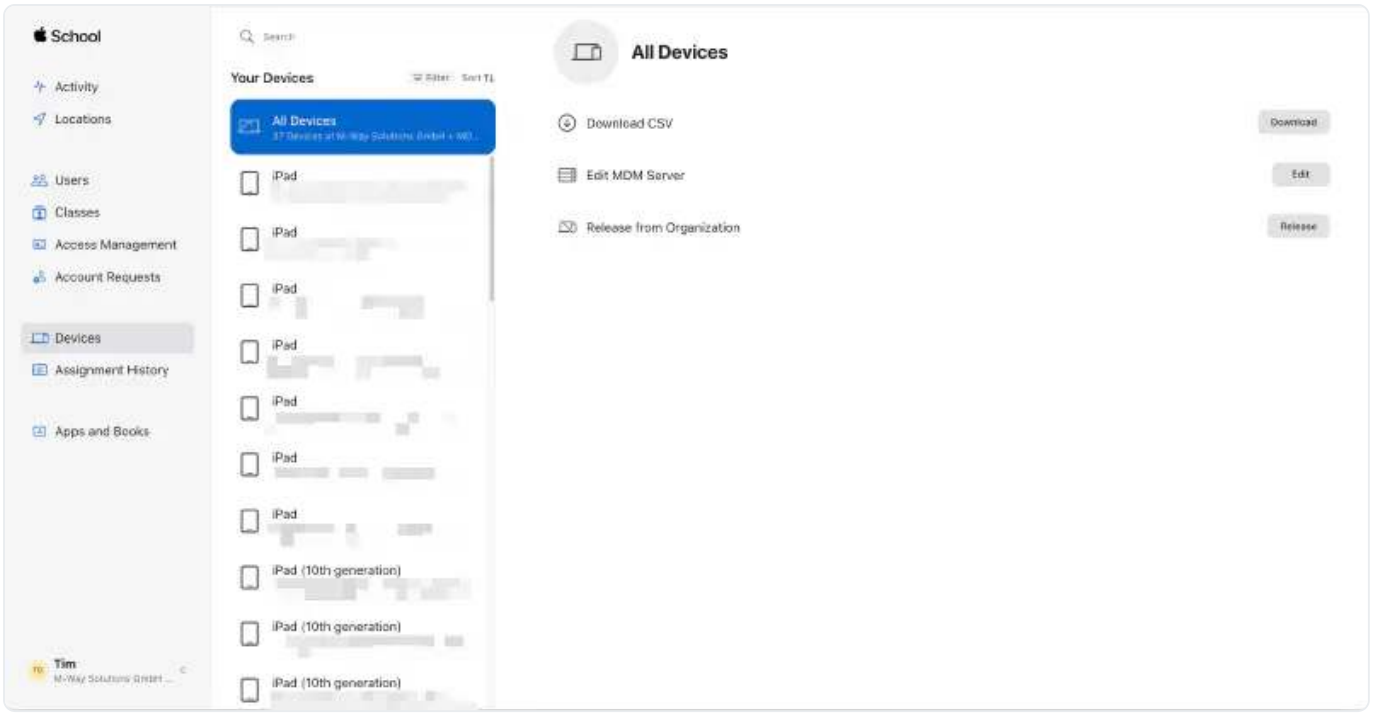
Common errors during token upload, an overview of the file extensions and reasons for premature token invalidation are described under Important Notes & Troubleshooting →.

The DEP token is valid for one year and must be renewed afterwards. The procedure is described under Renewing DEP Tokens (Server Tokens) →.

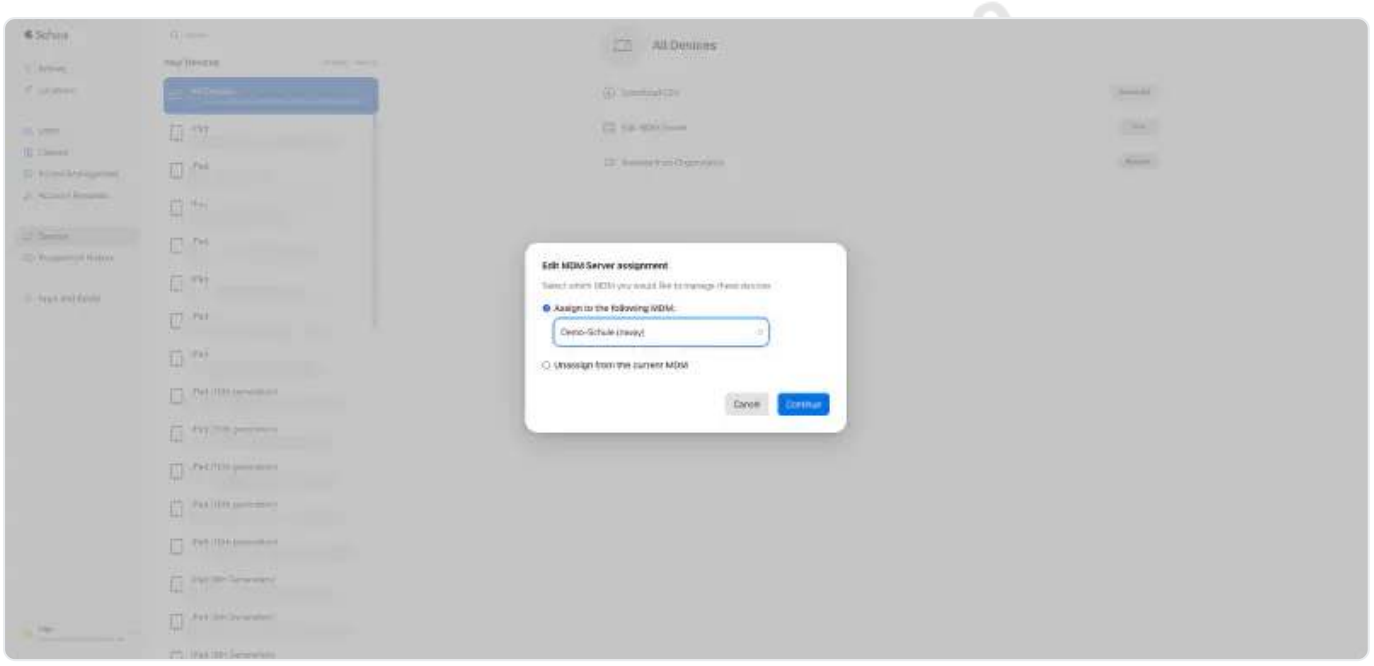
For version 26.4.0

Assigning devices to the MDM server

Assigning Apple devices to the MDM server in Apple School/Business Manager requires access with appropriate permissions. In Apple School/ Business Manager, the Devices section is opened.



The desired devices are selected and assigned to the appropriate server.



Synchronizing the devices

After that, the Apple devices become visible in Relution under `Devices` → `Auto Enrollments`. By default, Relution synchronizes the devices automatically once a day (at night, around 3:00 a.m. server time). The Sync devices button triggers the synchronization immediately; it synchronizes all configured auto enrollment services.

If a DEP profile was previously created and marked with Use as default profile, it is automatically assigned to the new devices during synchronization. Otherwise, the DEP profile is assigned manually via Set profile — a DEP profile is mandatory. DEP profiles are created under `Devices` → `Profiles`, see Profile for ADE →.

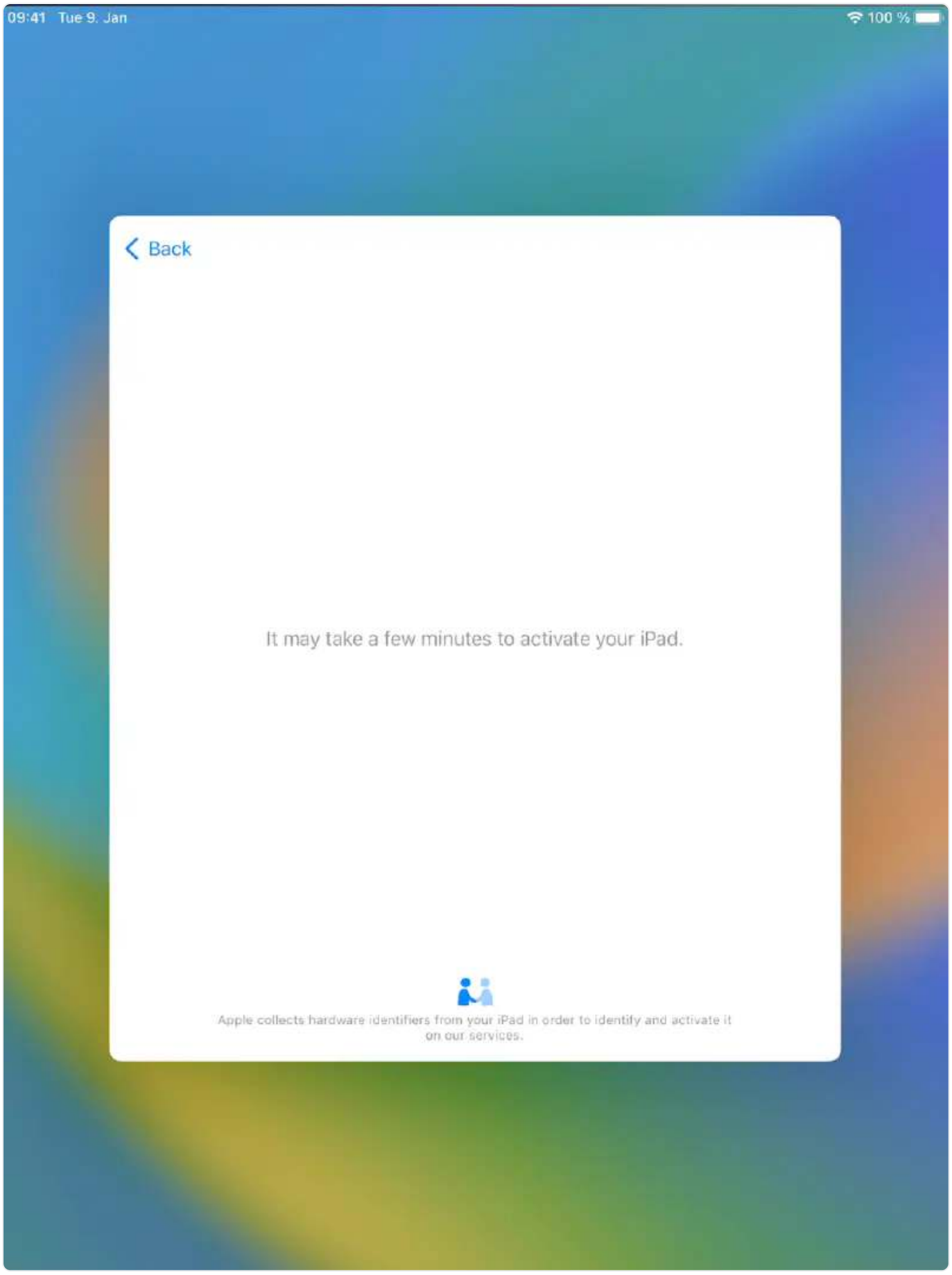
The following actions are also available for selected devices in the auto enrollments:

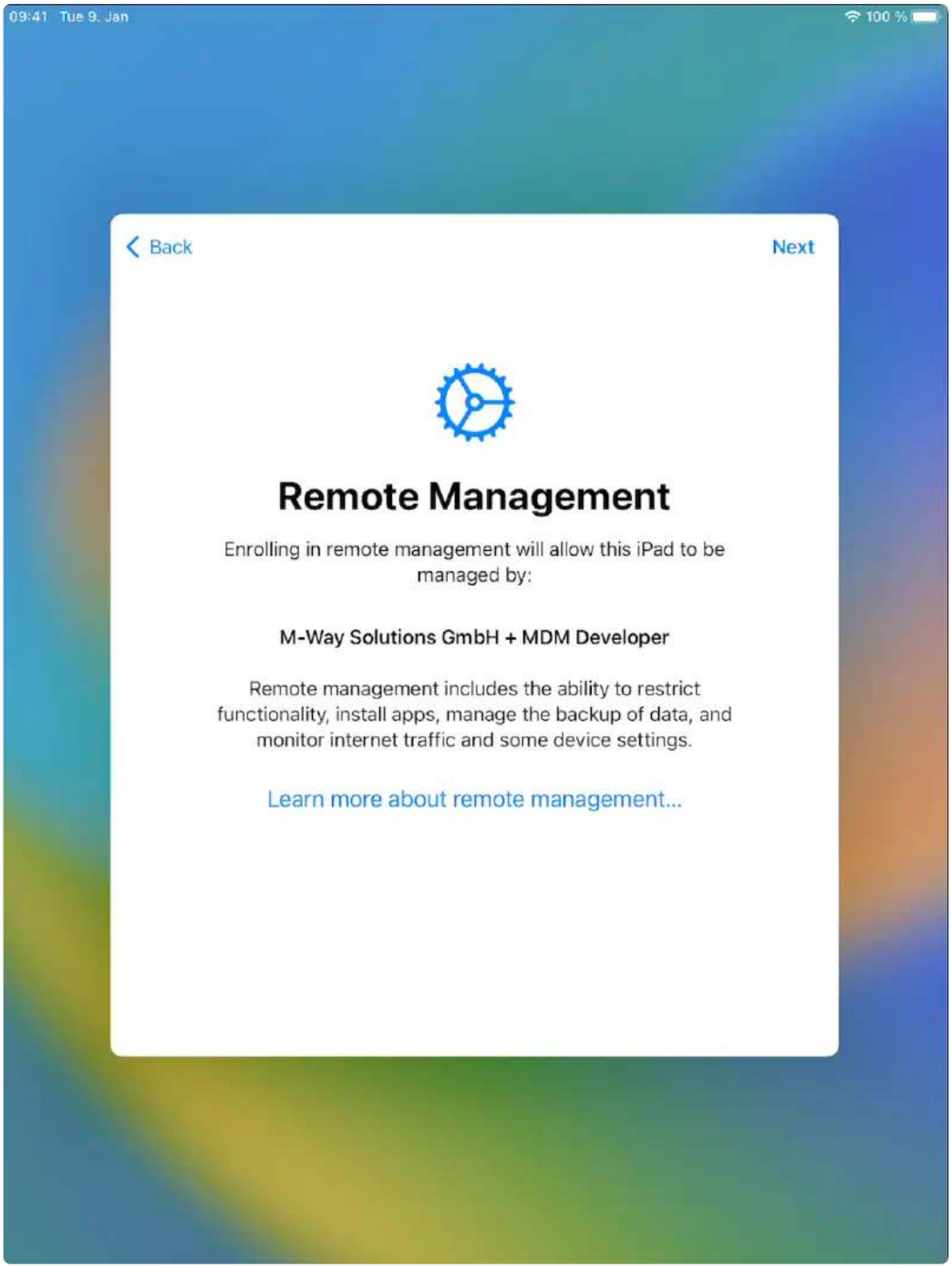
- Assign user and Unassign user: Assigns a user to the devices or removes the assignment.
- Use user name as device name: Uses the name of the assigned user as the device name.
- Add to device groups and Remove from device groups: Assigns the devices to static device groups. The policies of these groups are applied automatically on enrollment.

Commissioning the DEP devices

When one of the devices is started up, or a factory reset is performed if it's already up and running, the device logs into Apple and downloads the DEP profile, provided an Internet connection is available. Following the on-screen instructions is all that is required: at the end of the wizard, the Apple device is enrolled and the `Relution Agent` should be installed.

For version 26.4.0


09:41 Tue 9. Jan
100 %
Back
It may take a few minutes to activate your iPad.
Apple collects hardware identifiers from your iPad in order to identify and activate it on our services.


09:41 Tue 9. Jan
100 %
Back
Next
Remote Management
Enrolling in remote management will allow this iPad to be managed by:
M-Way Solutions GmbH + MDM Developer
Remote management includes the ability to restrict functionality, install apps, manage the backup of data, and monitor internet traffic and some device settings.
Learn more about remote management...

If the error message `Profile could not be loaded` is displayed, it is checked whether enough free device licenses are left and whether a DEP profile is associated with the device.

For version 26.4.0

Profile for ADE

If Apple devices are to be enrolled via Automated Device Enrollment (ADE, DEP in the portal), a profile (formerly DEP profile) is used. This profile is transferred from Relution to the Apple server and is applied to the devices before the actual enrollment.

> Only one profile can be applied per device at a time. In addition, the profile is only transmitted to the devices once during enrollment. If changes are to be transmitted later, the devices must be reset to factory defaults to receive the updated profile.

A profile can only be created if ADE (formerly DEP) is set up in the Relution organization and a valid DEP token is on file.

Configure DEP →

New profiles are created under `Devices` → `Profiles` via Create. If other types of auto enrollment are set up as well, the profile type is requested first; DEP is selected there. This area also provides an overview of existing profiles.

Use as default profile makes a profile the default profile. It is automatically assigned to new auto enrollments that do not have another profile assigned yet. For devices with an active MDM migration, this only happens if Await configuration and Preserve all installed apps are enabled in the default profile. It is recommended to define a default profile. The name of the profile should be meaningful so that it can be easily identified.

Agreements allows selecting agreements that were created under `Settings` → `General` → `Agreements`. Relution provides their texts to the device during enrollment. The selection is only shown to users with read permission for agreements.

The Default device name (up to 255 characters) is applied to the devices in the Auto Enrollments during enrollment. Placeholders can also be used and combined here, see Advanced placeholders →. The fields Support phone number, Support email address, Department name (up to 125 characters) and Authentication prompt (up to 255 characters) contain information that is displayed during enrollment.

For version 26.4.0

Force MDM enrollment

This option makes it mandatory for devices to be enrolled during startup. There is no option to skip or cancel the enrollment process. For example, if devices are stolen, they cannot be put into service without MDM enrollment.

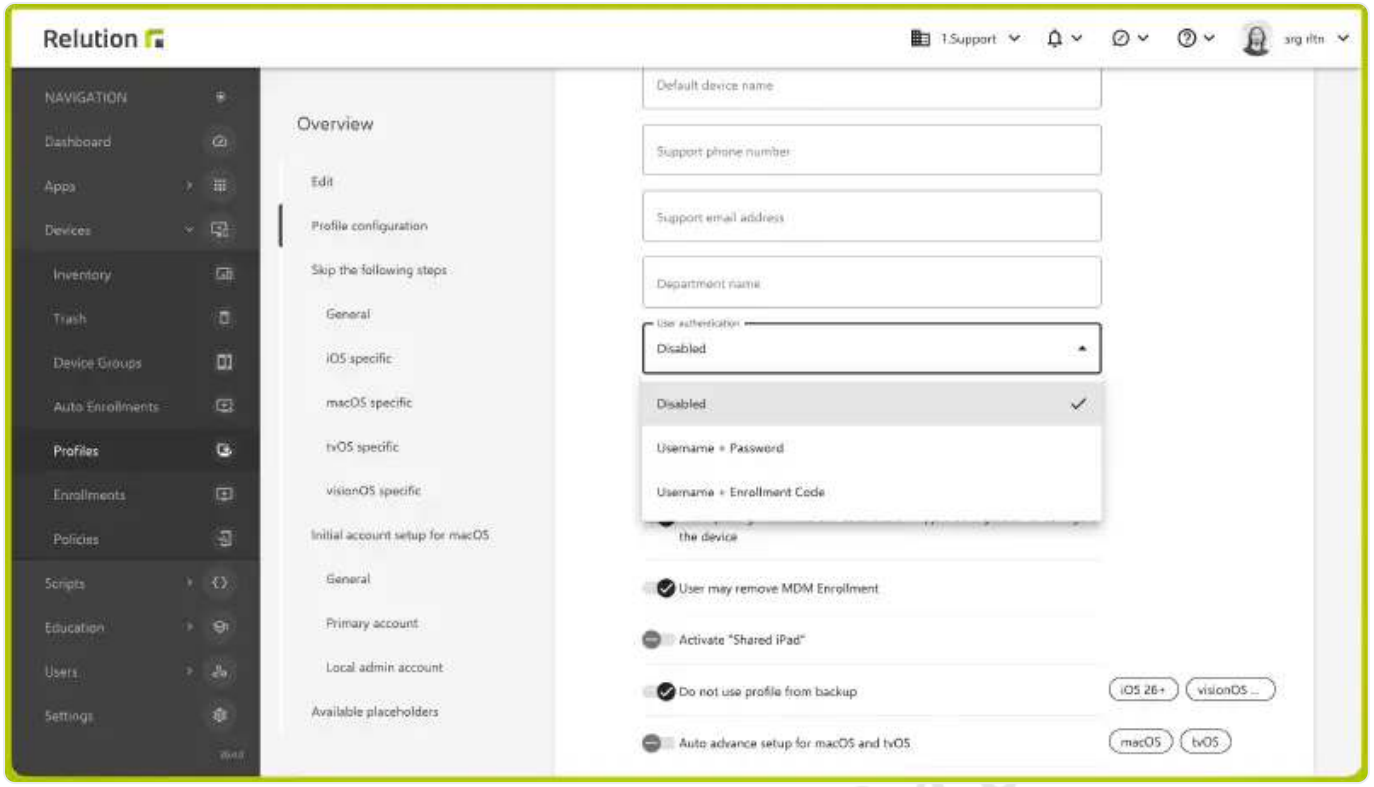
User authentication during enrollment

New in 26.4

The User authentication field determines whether and how users must authenticate during enrollment. Three options are available:

- Disabled: No user authentication takes place.
- Username + Password: Enrollment must be authenticated with a Relution user account. An Apple Account is not necessary for this and is not supported here.
- Username + Enrollment Code (as of version 26.4): Instead of a password, a one-time enrollment code generated by Relution is requested.

If devices are assigned to individual users in the Auto Enrollments list, only they will be able to authenticate and put the corresponding devices into operation.



> Username + Enrollment Code requires the device's auto enrollment to be assigned to a user account with an email address on file. The code is generated during enrollment and sent exclusively by email to that address. For this to work, mail dispatch must be set up and working on the server. Set up mail dispatch →

With Username + Enrollment Code, the email address of the assigned user is also accepted instead of the username. The eight-character code can only be used once and becomes invalid after more than five failed attempts. If the sign-in page is opened again, Relution generates a new code and sends it.

Allow pairing with Macs or PCs and allow Apple Configurator to configure the device

This option is enabled by default; if it is disabled, the portal displays a warning. If this option is deactivated, it will not be possible to connect to a PC or Mac later, e.g. to copy photos or create a backup of the devices. It is recommended to enable this option and to prohibit the connection with computers in the restrictions, if this is desired. The advantage is that restrictions in the policies can be changed at any time. The profile, on the other hand, cannot. In this case, the devices would have to be mandatorily reset to change the option.

User may remove MDM enrollment

If the option is enabled, users on devices can remove the MDM profile and thus the manageability by Relution.

This option is enabled by default for new profiles. To prevent users from removing the MDM profile, the option must be disabled before the devices are enrolled; changing it later requires a factory reset of the devices.

Enable Shared iPad

The Activate “Shared iPad” option is the only way to enable Apple’s multi-user mode Shared iPad. If this option is enabled, all the checkmarks set below for the setup steps to be skipped become redundant, as they will be skipped automatically.

Do not use profile from backup

This option applies to devices running iOS/iPadOS 26 or visionOS 26 and later. If it is enabled, the device does not use the profile contained in the backup when it restores a backup. Details on moving devices via backup: Backup →

Auto advance setup for macOS and tvOS

If this option is enabled, the Setup Assistant on macOS and tvOS devices automatically advances through its screens. The device needs an Ethernet connection for this. As long as the option is enabled, the setup steps to be skipped cannot be selected.

For version 26.4.0

Await configuration

If Await configuration is enabled, the device remains in Setup Assistant until all apps and configurations have been installed. The device action Continue in device Setup Assistant informs the device that the pre-configuration is completed and it can proceed in the Setup Assistant.

The Preserve all installed apps option is only available together with Await configuration and is enabled by default. It is required to preserve managed apps and their data when migrating managed devices between MDM servers.

Minimum OS version

New in 26.5

The Minimum OS version option requires devices to first update to a specific OS version during the Setup Assistant before they can be enrolled. A minimum version can be set independently for each platform:

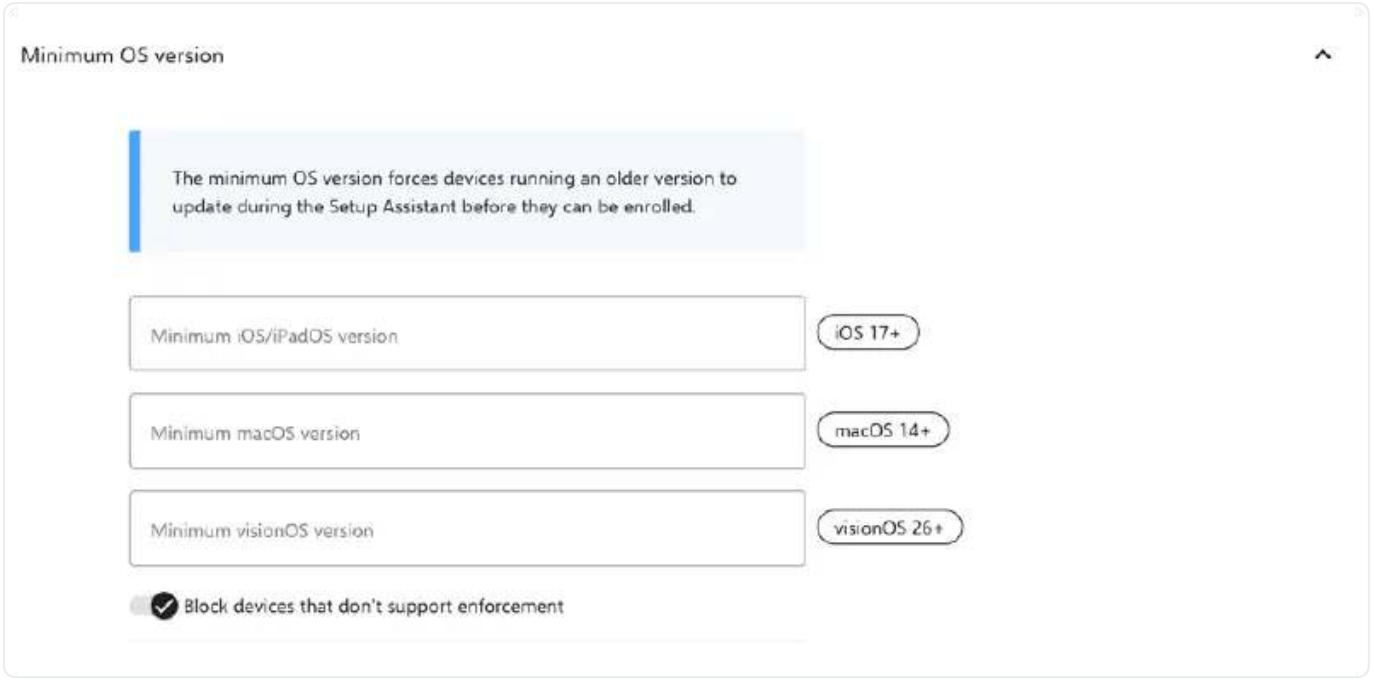
- Minimum iOS/iPadOS version
- Minimum macOS version
- Minimum visionOS version

If a field is left blank, no minimum version is enforced for that platform. tvOS is not supported by this feature.

If a device already meets the configured minimum, enrollment is unaffected. If a device reports a version below the configured minimum during enrollment, it is first asked to update within the Setup Assistant. Enrollment continues only once the update has completed and the Setup Assistant has run again. Relution automatically requests the lowest version currently offered by Apple that satisfies the minimum requirement — not necessarily the latest available version. This enforcement also requires the device to be able to be asked to update in the first place, which Apple supports from iOS/iPadOS 17, macOS 14, and visionOS 26 onward.

> If Apple does not currently offer a version that satisfies the configured minimum, the device's enrollment is rejected instead of pointing it to an unavailable version. This prevents devices from getting stuck in the Setup Assistant.

The Block devices that don't support enforcement option (enabled by default) determines how devices are handled that cannot be asked to update during enrollment, for example because they run too old an OS version. If enabled, such devices are prevented from enrolling. If disabled, such devices are enrolled without applying the minimum OS version.



Skip the following setup steps

Any options that are enabled, will be skipped during initial device setup.

Setup steps that are shown again after the initial setup, e.g. after a software update, are not covered by this. They can be hidden via the configuration Setup Assistant in a policy, see Setup Assistant (iOS) → and Setup Assistant (macOS) →.

If Location Services is not enabled, the step is shown during setup. There, device location can be allowed so that devices automatically set the correct time zone. The option only affects the Setup Assistant and has no influence on later device location tracking.

Initial account setup for macOS

In this section, user and administrator accounts can be added to macOS devices, which are automatically created at startup. Placeholders are also available here, see Advanced placeholders →.

For version 26.4.0

Add devices to DEP

Originally, only Apple devices purchased directly from Apple or from trusted resellers could be added to Apple School/Business Manager. If devices were purchased from other sources, they could not be automatically enrolled in Relution via Automated Device Enrollment (ADE, DEP in the portal).

iOS / tvOS devices via Apple Configurator 2

Apple now allows iOS and tvOS devices to be added manually to Apple School/Business Manager using the Apple Configurator. This provides all the benefits of automatic enrollment via ADE, regardless of where the devices were purchased. Add Apple devices to DEP at a later date →

macOS devices via Apple Configurator (mobile)

With the Apple Configurator for mobile devices (iOS/iPadOS), Apple has provided an easy way to add macOS devices to the Apple School/ Business Manager. Apple Configurator Manual →
Apple Configurator App →

For version 26.4.0

Instructions

1. Apple Configurator is installed on an iOS/iPadOS device with at least iOS 16.
2. On this device, Apple Configurator is signed in with a valid Apple School/Business Manager account.
3. The macOS device is started, and the Setup Assistant is paused as soon as the Country or Region screen is displayed.
4. The iOS/iPadOS device is held close to the Mac; on the Mac, Manually Pair is clicked in the bottom left of the Setup Assistant.
5. The 6-digit number combination is entered on the iOS/iPadOS device.
6. Once the macOS device is finished with the process, it will offer a restart or shutdown.
7. In Apple School/Business Manager, the device is assigned to a location.
8. In Relution, under `Devices` → `Auto Enrollments`, the synchronization is triggered via Sync devices (without a manual trigger, it runs automatically once a day). If a DEP profile is marked with Use as default profile, it is automatically assigned to devices without a profile during synchronization; otherwise, the device is selected and a DEP profile is assigned via Set profile.
9. The usual Apple welcome setup is completed on the device.

DEP profiles are created under `Devices` → `Profiles`, see Profile for ADE →.

Note on the Status in Auto Enrollments

- Blue - Profile assigned - A DEP profile has been assigned to the device but has not been applied yet.
  - This can occur when the profile is changed for already enrolled devices or for devices that have not yet completed the setup.
- Green - Profile pushed - The profile has been applied and reported back as executed by the device.
- Red - Profile removed - The profile has been removed from the device.
- Grey - No Profile - No DEP profile is assigned to the device or an assigned profile has been deleted.
- Grey - Unknown Profile - Apple has reported a profile status that Relution cannot map.

Remove devices

Often there are devices that are owned by end users and were added to ADE for educational purposes, for example, but are later to be returned to private use. In this case, the devices must be properly removed from the MDM and from ADE to ensure problem-free continued use.

The following order must be observed:

1. The data is backed up.
2. In Apple School/Business Manager, the device is released from the organization or unassigned from the Relution MDM server.
3. Only then is the device reset, either by the user or in Relution via the Wipe device action.

> If the device is reset before step 2, the ADE assignment remains in place and the device enrolls in Relution again in the Setup Assistant.

Backing up the data

The easiest way to back up user data between reset and new setup is to use Apple iCloud with a private Apple Account. To do this, it must be ensured that the option Allow Account modification is enabled in the Restrictions configuration in Relution and has been applied to the device. The option is enabled by default; action is only required if an assigned restriction disables it. This allows the user to log in to the device with a private Apple Account and perform the desired data backup.

For version 26.4.0

Removal from the Apple School / Business Manager

The release or unassignment can easily be carried out in the Apple ASM/ABM portal without having any immediate effect on the device. Only at the next complete reset to factory settings does the device receive the current assignment from Apple and is no longer enrolled automatically. In Relution, the auto enrollment is removed during the next synchronization once Apple reports the device as removed. The synchronization runs automatically once a day or immediately via Sync devices under `Devices` → `Auto Enrollments`.

Removal from the MDM

In Relution, the option Enable ‘Erase All Content and Settings’ should be enabled in the Restrictions configuration (enabled by default). This way the user can reset the device after the backup. Reporting back to the Relution administrator is advisable, as a previously disconnected Wi-Fi network on the device may prevent communication with the MDM, in which case no information about the status of the device is available. Alternatively, the Wipe device action can be triggered in Relution, which will move the device to the trash and update the device information accordingly.

> Changes to the ADE assignment and the DEP profile only take effect after a factory reset.

Configure VPP

When acquiring and distributing apps to users, the administrator of an MDM system faces certain challenges. When users obtain an app from the Apple App Store, whether from a school/corporate or personal device, the app must be downloaded individually using a personal Apple ID. The app license then does not belong to the school or company, but is assigned to the private Apple ID.

This is especially a problem with paid apps when the procured app license is reimbursed to the users in the form of cost reimbursement or purchased coupons, as users always remain the owner of the app license via the personal Apple ID. If the school is changed or the company is left, the app license is irrevocably lost with the students or employees. If an app is to be distributed to a large number of devices, the use of personal Apple IDs quickly creates a confusing and difficult-to-control situation for the administrator.

What is Apps and Books (VPP) for?

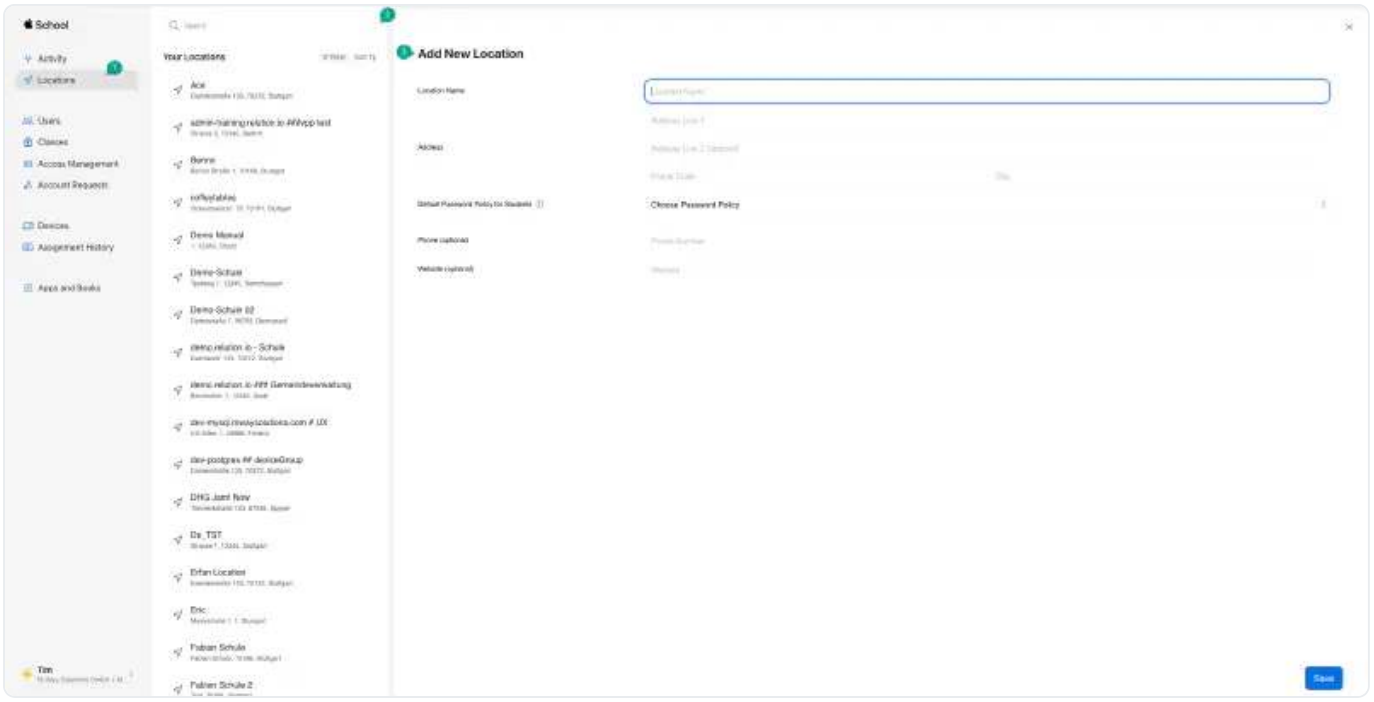
To solve the challenges described above and to be able to distribute apps from the Apple App Store via Relution without requiring an Apple ID on the mobile device, there is Apple's Apps and Books program (VPP in the portal), formerly the Apple Volume Purchase Program. This allows apps to be purchased centrally in large quantities and distributed independently of the user without requiring an Apple ID on the devices. App licenses from Apps and Books, called VPP licenses in the portal, are thus centrally managed without ever changing ownership and can be withdrawn at any time by the administrator.

Apps and Books is mapped and configured via the Apple Business Manager or Apple School Manager. This is also where app licenses are procured centrally using a school or company Apple ID. This applies to both free and paid apps.

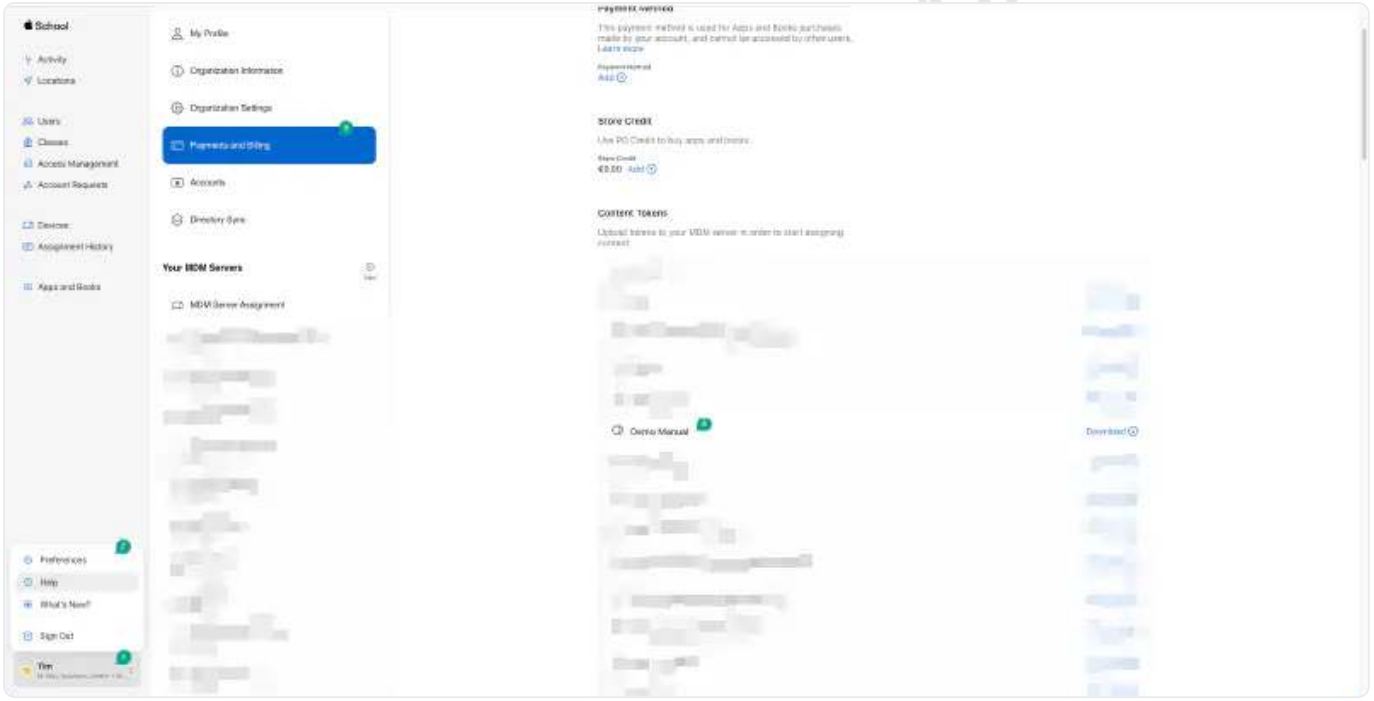
For version 26.4.0

How is VPP linked to Relution?

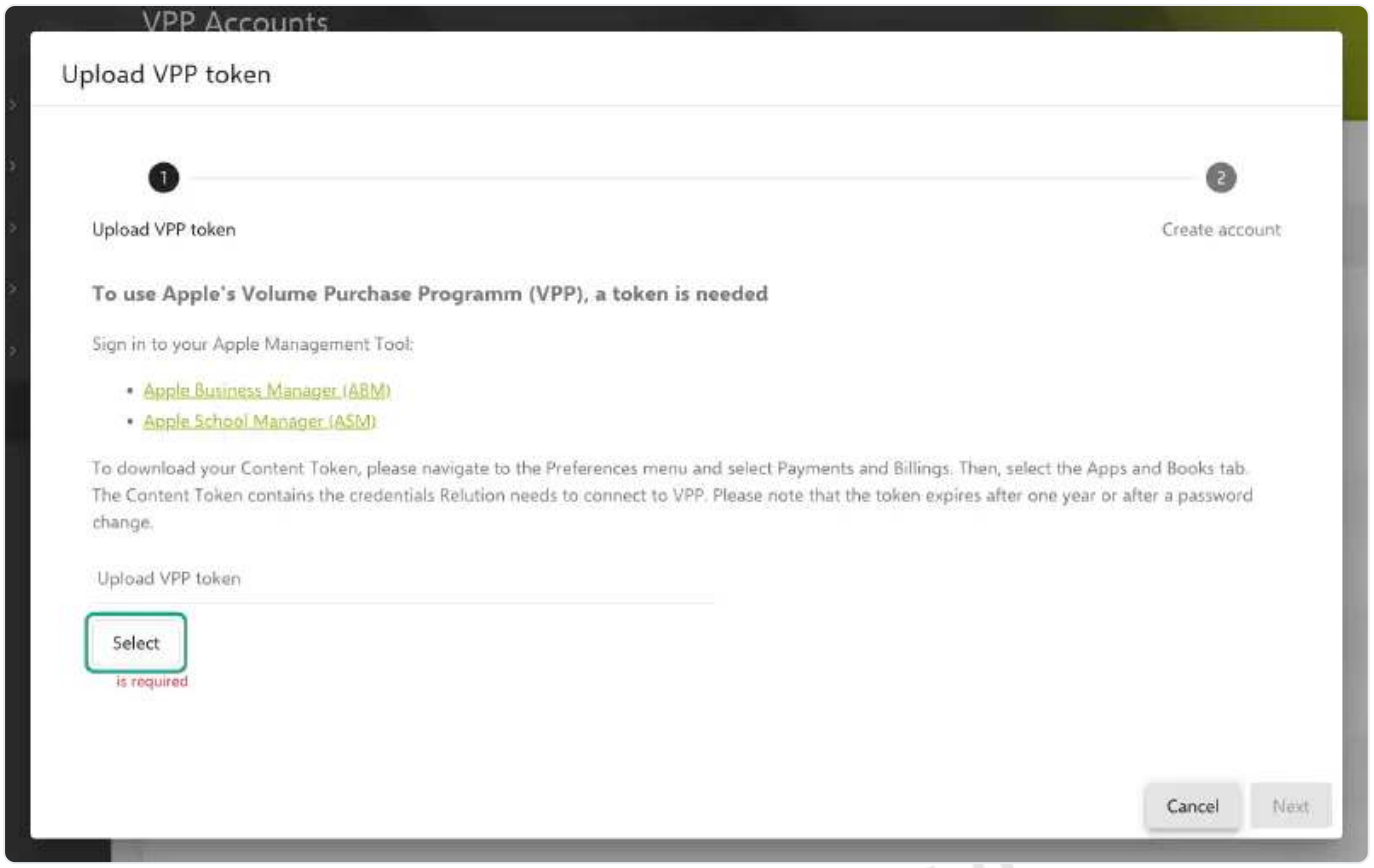
In order to distribute procured VPP licenses via Relution, the two systems must be linked. In Apple Business Manager or Apple School Manager, a new location is first created under Locations.

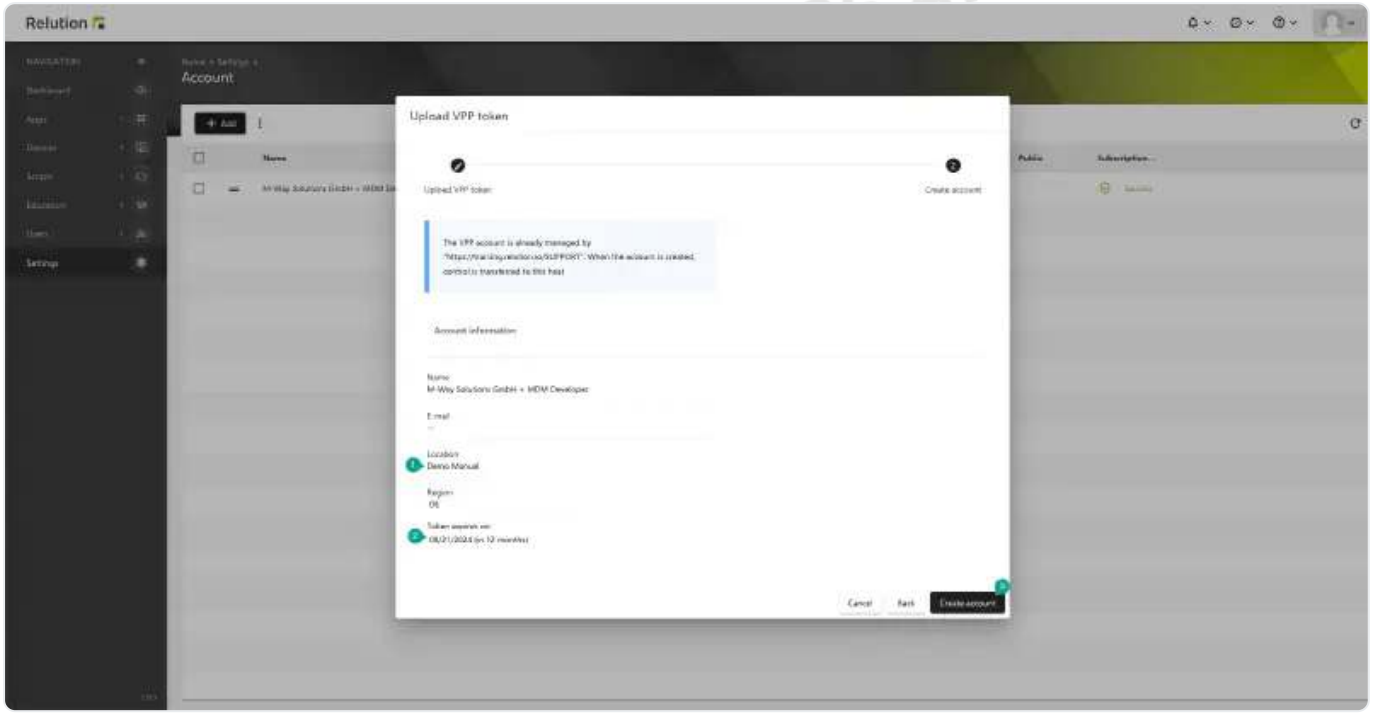


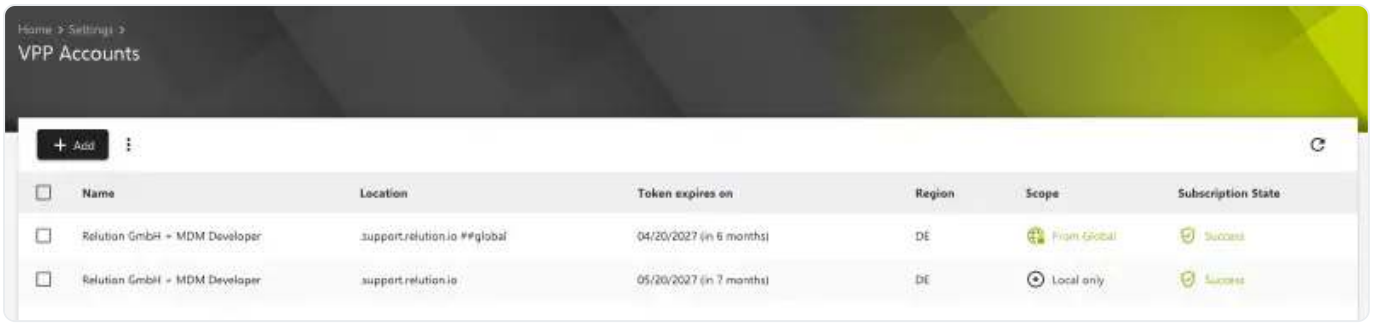
To connect this location to an MDM server, a VPP token must be generated for the respective location under `Settings` → `Apps and Books`.



Once the VPP token is uploaded to Relution under `Settings` → `Volume Purchase Program (VPP)` → `Account`, the two systems are linked.


VPP Accounts
Upload VPP token
1
2
Upload VPP token
Create account
To use Apple's Volume Purchase Programm (VPP), a token is needed
Sign in to your Apple Management Tool:
Apple Business Manager (ABM)
Apple School Manager (ASM)
To download your Content Token, please navigate to the Preferences menu and select Payments and Billings. Then, select the Apps and Books tab. The Content Token contains the credentials Relution needs to connect to VPP. Please note that the token expires after one year or after a password change.
Upload VPP token
Select
is required
Cancel
Next


Relution
Account
Upload VPP token



If the token is already managed by another MDM server, the dialog points this out when the account is created. When the account is created, Relution takes over the management of the token. The Subscription State column in the account list shows whether Relution is registered for notifications from Apple for this account. This requires the Relution server to be reachable for the Apple servers.

> Each VPP token is valid for one year and must then be downloaded again in Apple Business Manager or Apple School Manager for that location. The new token is uploaded to the existing account in Relution via the three-dot menu → Update token (see Renewing VPP Tokens (Content Tokens) →). Deleting the account removes all VPP data, and a second account for the same location cannot be created in the same organization. Relution Notification Center will send a timely alert if a VPP token expires.

Email notifications for expiring and expired VPP and DEP tokens are enabled by default and can be adjusted under `Settings` → `Notifications` via VPP token will expire soon, VPP token is expired, DEP token will expire soon and DEP token is expired. The first reminder is sent 30 days before expiration, then daily from 15 days before expiration. The emails go to the users who are permitted to manage the VPP or DEP settings.

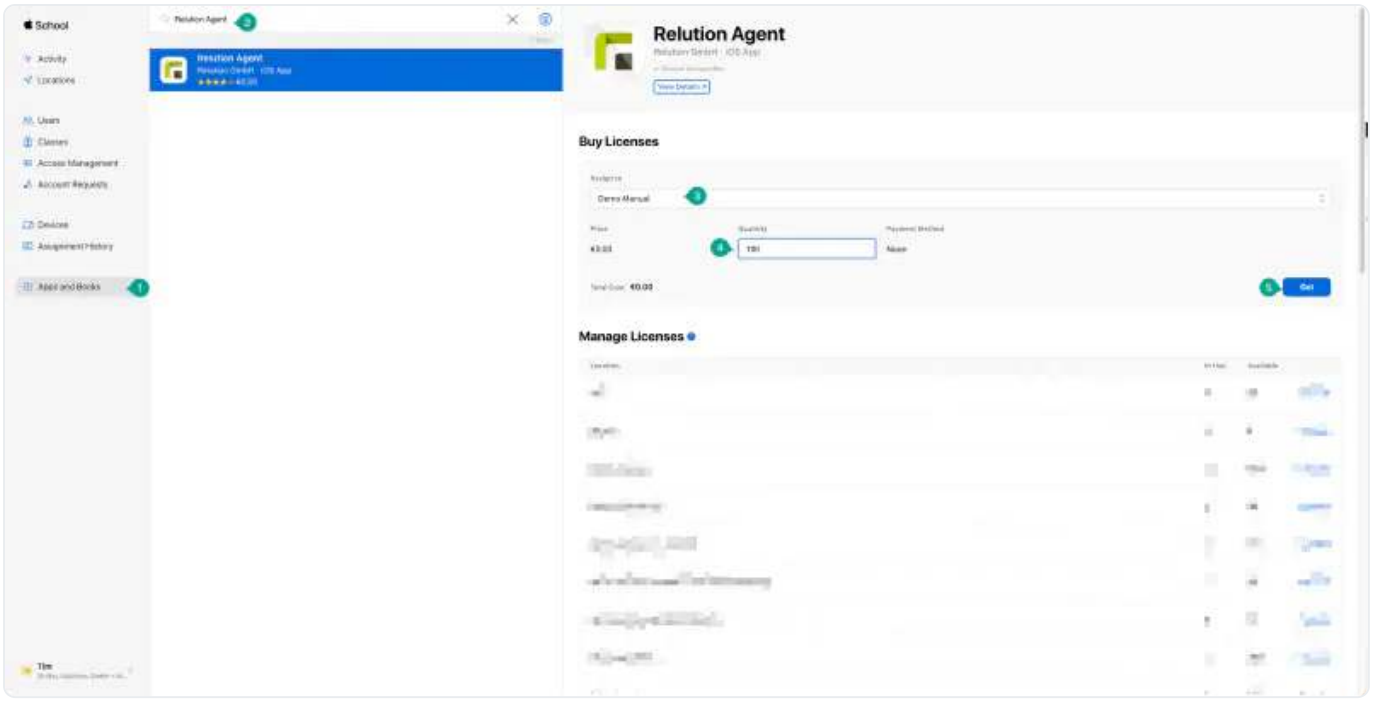
The use of multiple VPP tokens in a Relution organization is described in a separate section.

After pairing, the menu items Purchased Apps and Media appear in Relution under Apps. Purchased Apps lists all apps procured via Apps and Books and the corresponding VPP licenses (number), Media contains the procured books. The VPP licenses are automatically synchronized at regular intervals. In addition, the VPP licenses for the organization can also be updated manually via Synchronize. The history of synchronizations, including failed runs, is shown under `Settings` → `Volume Purchase Program (VPP)` → `Synchronization History`.

How are app licenses obtained in VPP?

In Apple Business Manager or Apple School Manager, app licenses can be obtained under Apps and Books and assigned to a configured location.

For version 26.4.0



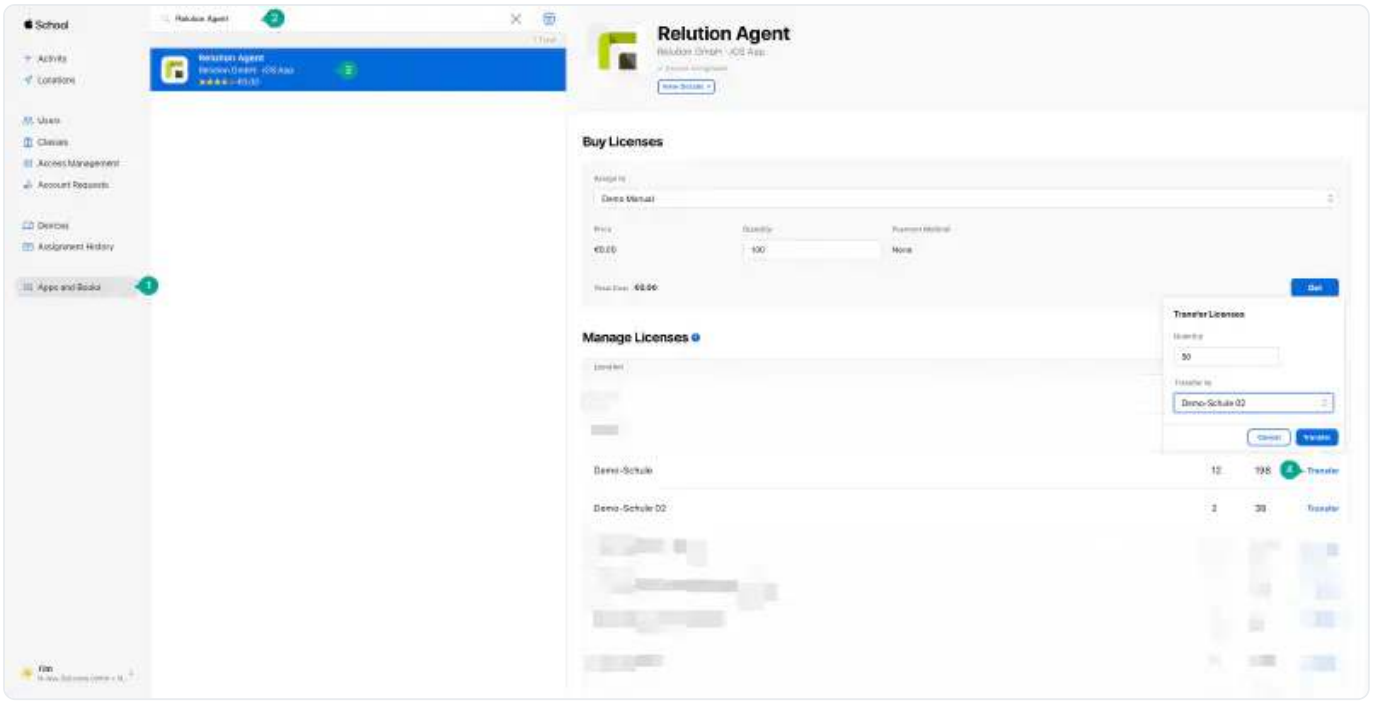
Once loaded, they are available in Apple Business Manager or Apple School Manager. In addition, the app licenses can be distributed to devices in the appropriate organization in Relution associated with the selected location via a VPP token.

Can VPP also be used to manage app licenses for different organizations or locations?

For version 26.4.0

If multiple organizations are managed in Relution via the multi-client capability, as is the case, for example, with a school board with multiple schools, then app licenses can be procured centrally with an Apple ID of the school board and distributed to the respective schools. To do this, a location must be created in Apple School Manager for each school and the VPP token must be stored in the corresponding Relution organization of each school. This applies analogously to Apple Business Manager in the corporate context.

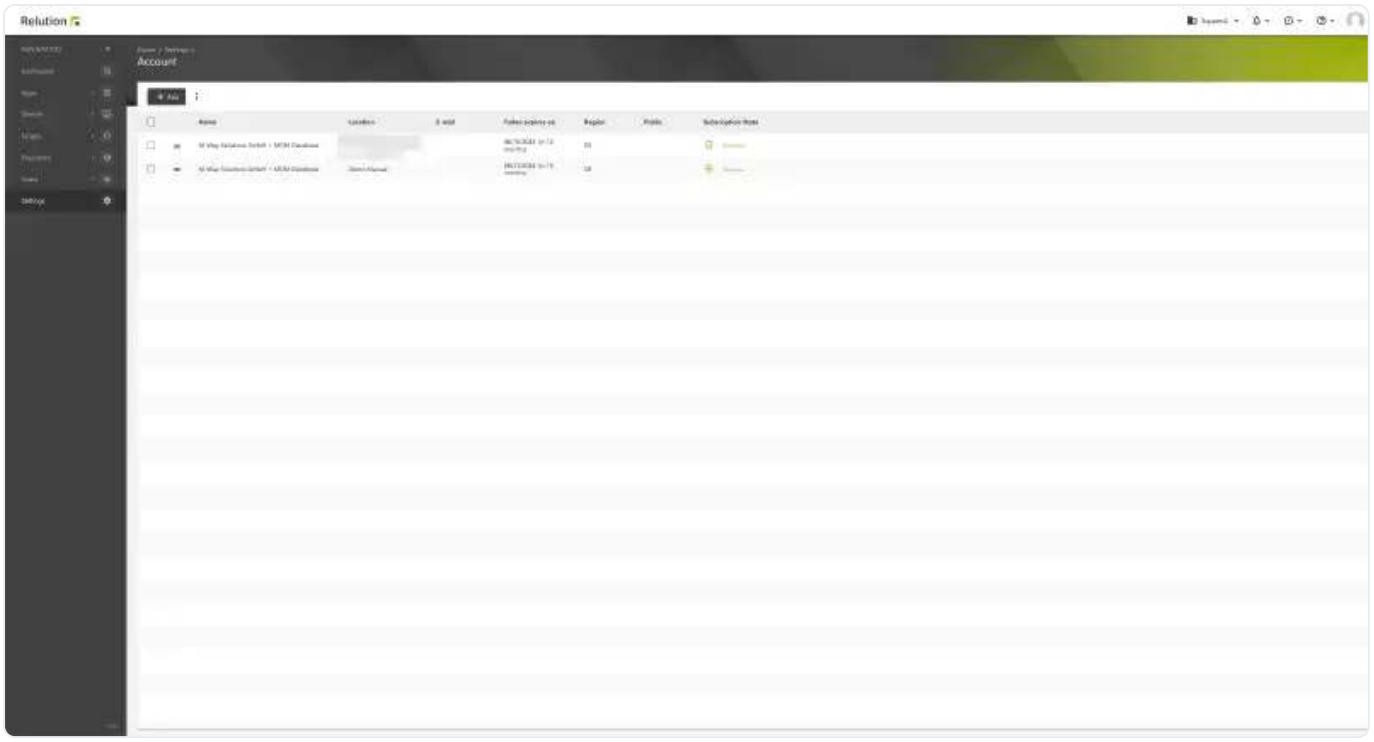
Purchased VPP licenses can be managed in Apple Business Manager or Apple School Manager and transferred to other locations. This makes it possible to procure app licenses centrally once for a leading site and then distribute them to other sites in packages.



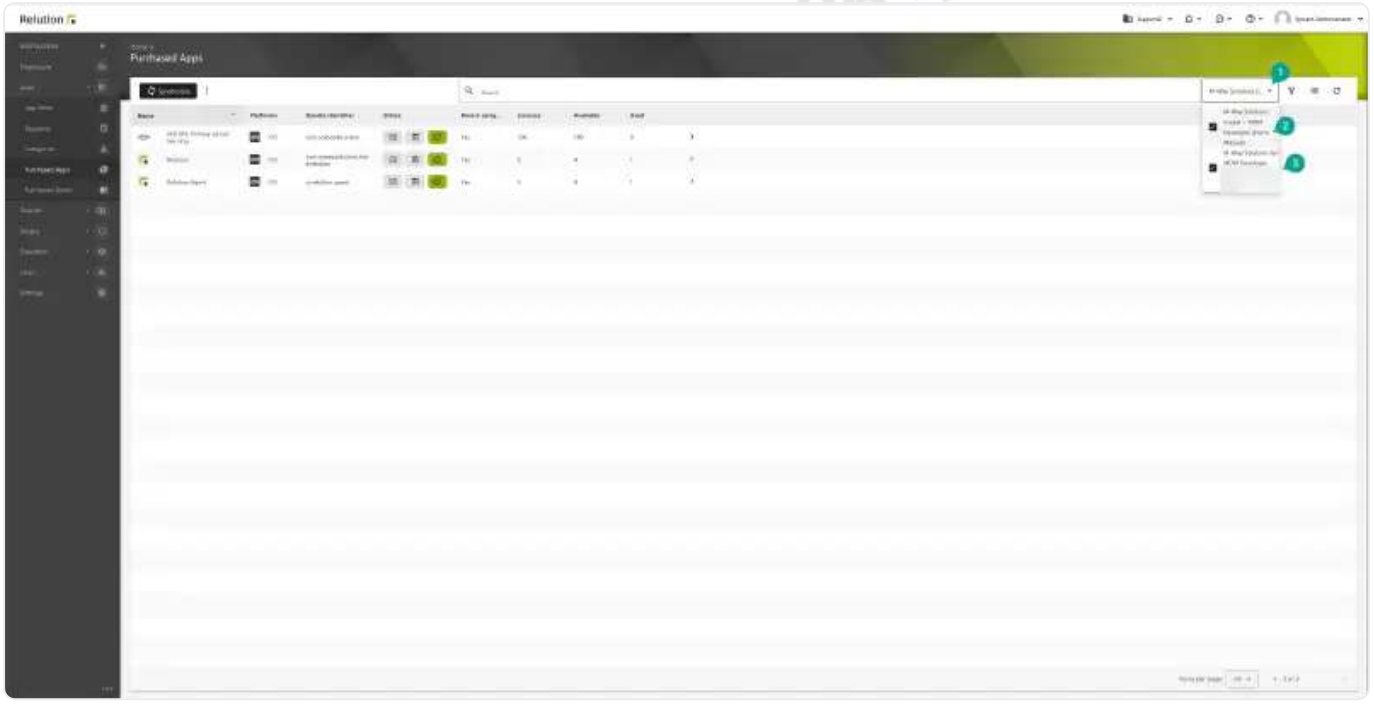
Is it possible to use multiple VPP tokens within a Relution organization?

Within Relution, it is possible to store multiple VPP tokens under `Settings` → `Volume Purchase Program (VPP)` → `Account`. The purpose of this is to link different Apple School Manager accounts, e.g. if a school is equipped with VPP apps by a school board, but at the same time also owns and uses its own VPP licenses. Analogously, this also works with Apple Business Manager.

For version 26.4.0



The sum of all app licenses from multiple VPP tokens for an organization is displayed aggregated in the Purchased Apps view. A drop-down list can be used to filter VPP licenses by location from Apple School Manager.



VPP licenses are assigned under `Apps` → `Purchased Apps`: after selecting an app, Associate license opens a dialog for selecting devices, users or groups. If the app license exists in more than one stored VPP token, the token to use for the app license is selected first. Revoke license removes an assignment again.

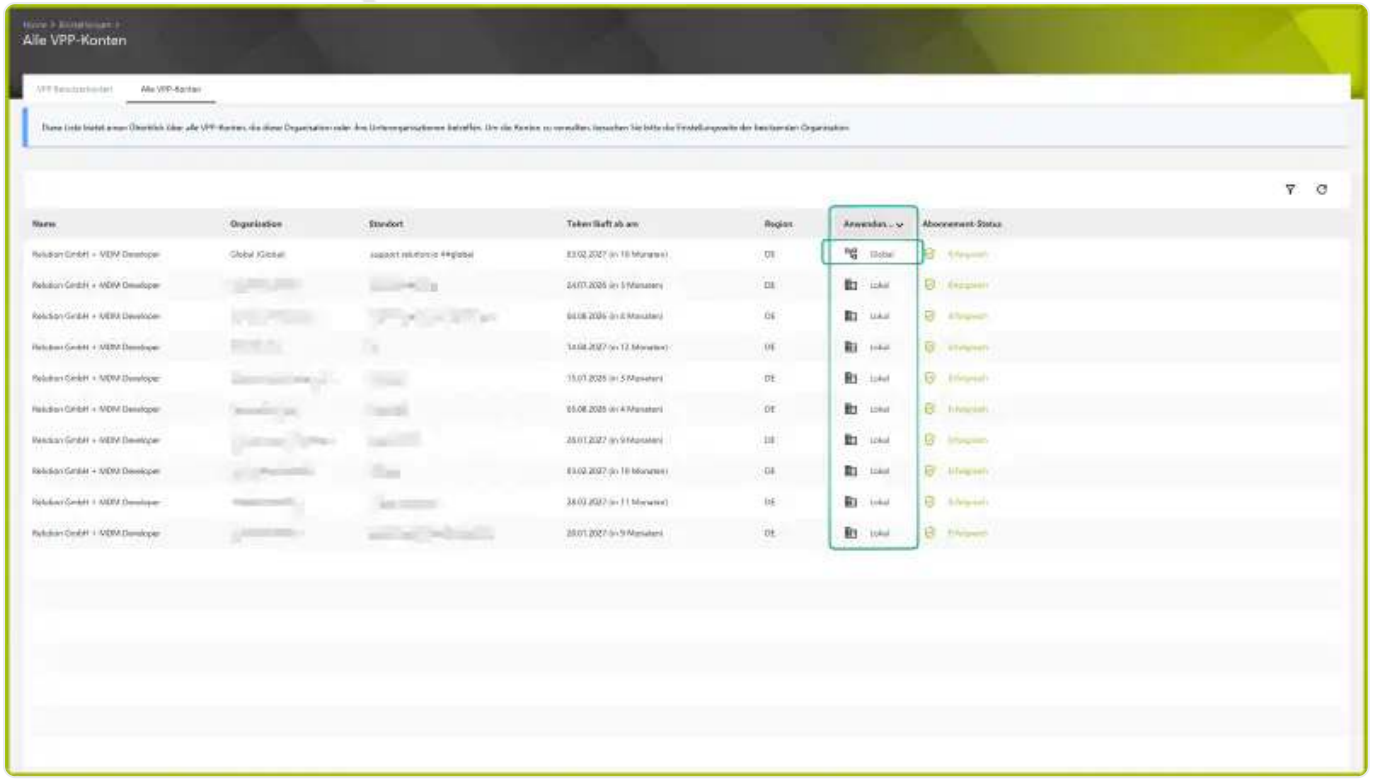


Global VPP

With Relution, it is possible to integrate VPP tokens into the global organization. This allows centrally purchased apps to be distributed down to tenants.

A VPP token in the global organization is automatically available in all organizations, a VPP token in a meta organization in its sub-organizations. Apps from VPP accounts of the global organization automatically replace existing apps in the other organizations; this cannot be undone. In the subordinate organization, the inherited token cannot be edited (including the app update settings); only its order can be changed. In Purchased Apps and Media, the assignments shown refer to the current organization, while the total number of licenses applies across all organizations.

This eliminates the need for multiple setups in the Apple School Manager / Apple Business Manager as well as the repeated updating of multiple tokens. In the best case, only a single token needs to be renewed once per year.



For version 26.4.0

Important note on licensing

It is essential that sufficient VPP licenses are purchased for all devices and tenants.

Example:

- Organization 1: 250 devices
- Organization 2: 100 devices
- Organization 3: 1000 devices

In this case, at least 1350 VPP licenses should be purchased globally.

Tenant-specific VPP tokens

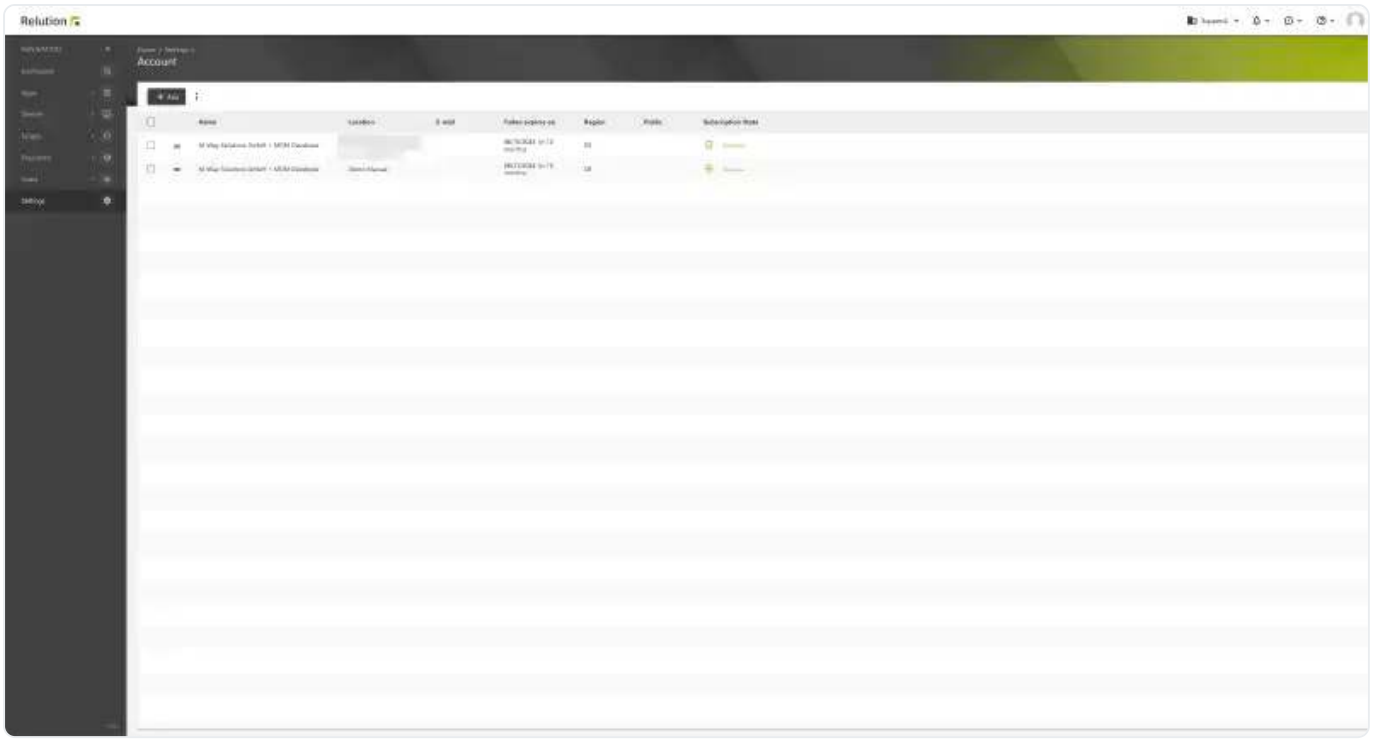
If a site requires paid apps or an additional separate VPP token with its own apps, this can be integrated directly into the respective tenant.

This allows a clear separation of costs and licensing between global and local management.

Can VPP licenses in Relution also be automatically assigned to devices?

For version 26.4.0

If apps are automatically installed on devices via auto-deployments or a policy (app compliance), Relution checks if a VPP license is stored for this app. If so, the VPP license is automatically assigned to the device. For App Store apps that support only macOS or only tvOS, VPP licenses are a prerequisite for an auto-deployment: without available VPP licenses in the organization, no auto-deployment can be configured for these apps. For iOS apps, the VPP license is optional. If multiple VPP tokens are stored for the organization and the app license is present in all of them, the VPP license from the first VPP token in the list is used. Under `Settings` → `Volume Purchase Program (VPP)` → `Account` the order of the VPP tokens can be changed to determine from which token the VPP license should be used in case of automatic assignment via auto-deployments.



Whether Relution installs available updates of apps from Apps and Books on the devices is defined under `Settings` → `Volume Purchase Program (VPP)` → `App updates` with Perform app updates: Never, Immediately, after an app update was detected or Scheduled. For a schedule, the weekdays are specified under Repeats on together with the Start time.

Common errors when uploading tokens, an overview of file extensions and reasons for premature token invalidation are described under Important Notes & Troubleshooting →.

For version 26.4.0

Renew DEP / VPP Tokens

Tokens for Apple Automated Device Enrollment (ADE, DEP in the portal) and for Apps and Books (VPP in the portal) have a maximum validity of 1 year and must be renewed regularly to ensure uninterrupted device management and app assignment. This guide explains how to easily renew these tokens.

The ADE and Apps and Books tokens are independent of each other: each token expires one year after its own creation. Therefore, only the token whose expiration is approaching is renewed. Relution sends email reminders about expiring and expired tokens, first 30 days before expiration and then daily from 15 days before expiration (see Configure VPP →). In the list of DEP accounts, the Token expires on column marks a token with a warning icon from 60 days before expiration and an expired token with a red icon.

> In April 2026, Apple renamed Apple Business Manager (ABM) to Apple Business.

Additionally, as of version 5.33, Relution provides a centralized overview of all connected DEP and VPP tokens. Administrators of the `Global` organization or a meta organization can see at a glance:

- Which DEP and VPP tokens are valid or expired
- When the respective tokens expire

Token Overview in the Relution Portal

For version 26.4.0

The two token types are managed in different places in the portal.

Accessing DEP Accounts

The central overview of DEP accounts can be reached as follows:

1. The login takes place in the `Global` organization or a meta organization.
2. Settings is opened in the left sidebar.
3. The Device platform specific section is opened.
4. Apple Automated Device Enrollment is selected.
5. The All DEP accounts tab is opened (available from version 5.33.0).

Accessing VPP Accounts

The overview of VPP accounts can be reached as follows:

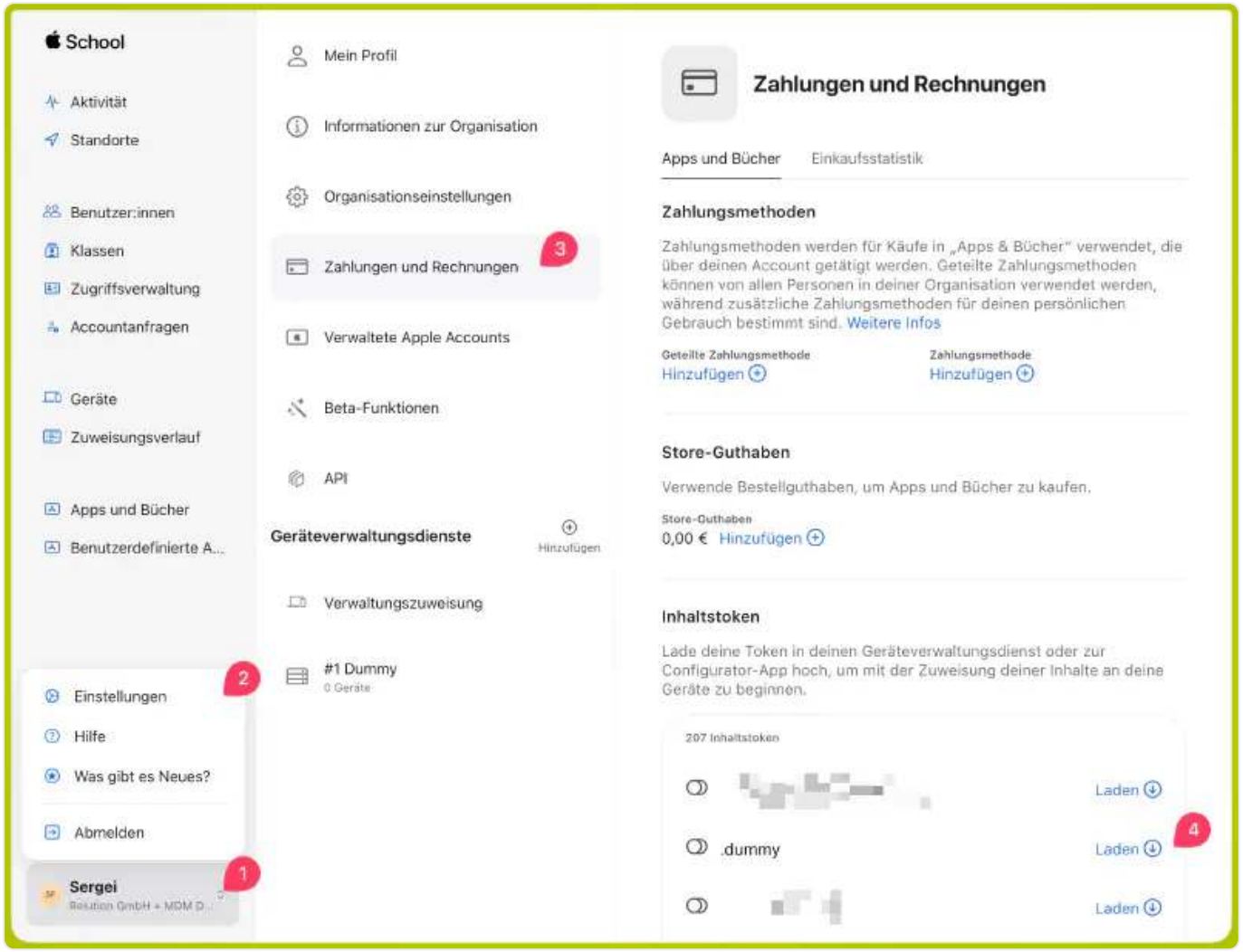
1. The login takes place in the `Global` organization or a meta organization.
2. Settings is opened in the left sidebar.
3. The Volume Purchase Program (VPP) section is opened.
4. Account is selected.
5. The All VPP Accounts tab is opened (available from version 5.33.0).

Renewing VPP Tokens (Content Tokens)

The VPP token is first downloaded from Apple and then uploaded to Relution.

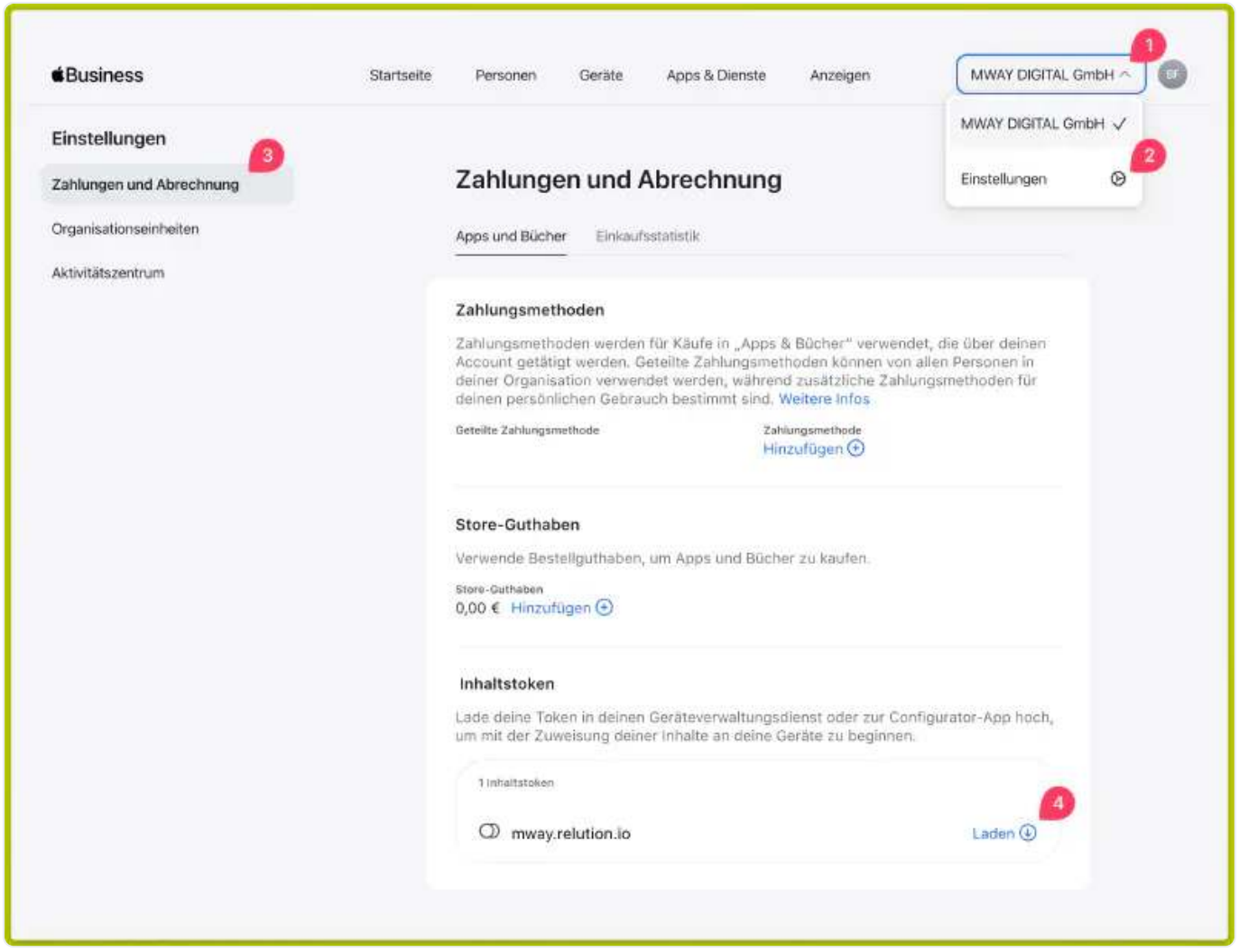
Download from Apple School Manager (ASM)

1. The login takes place in Apple School Manager →.
2. The logged-in user name in the bottom left corner is clicked.
3. Settings is opened.
4. Payments & Billing is selected.
5. Under Content Tokens, the desired token is downloaded.
    - *File format:* `sToken_for_[Location].vpptoken`



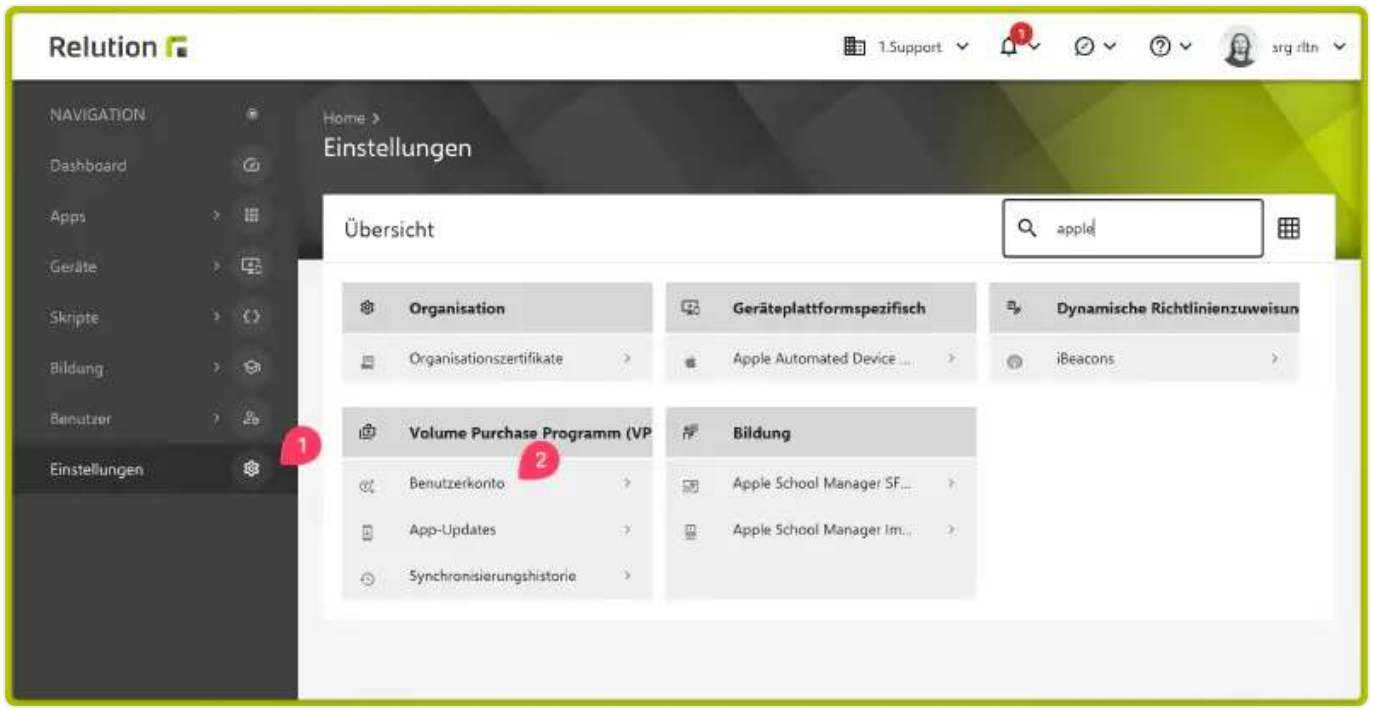
Download from Apple Business (formerly ABM)

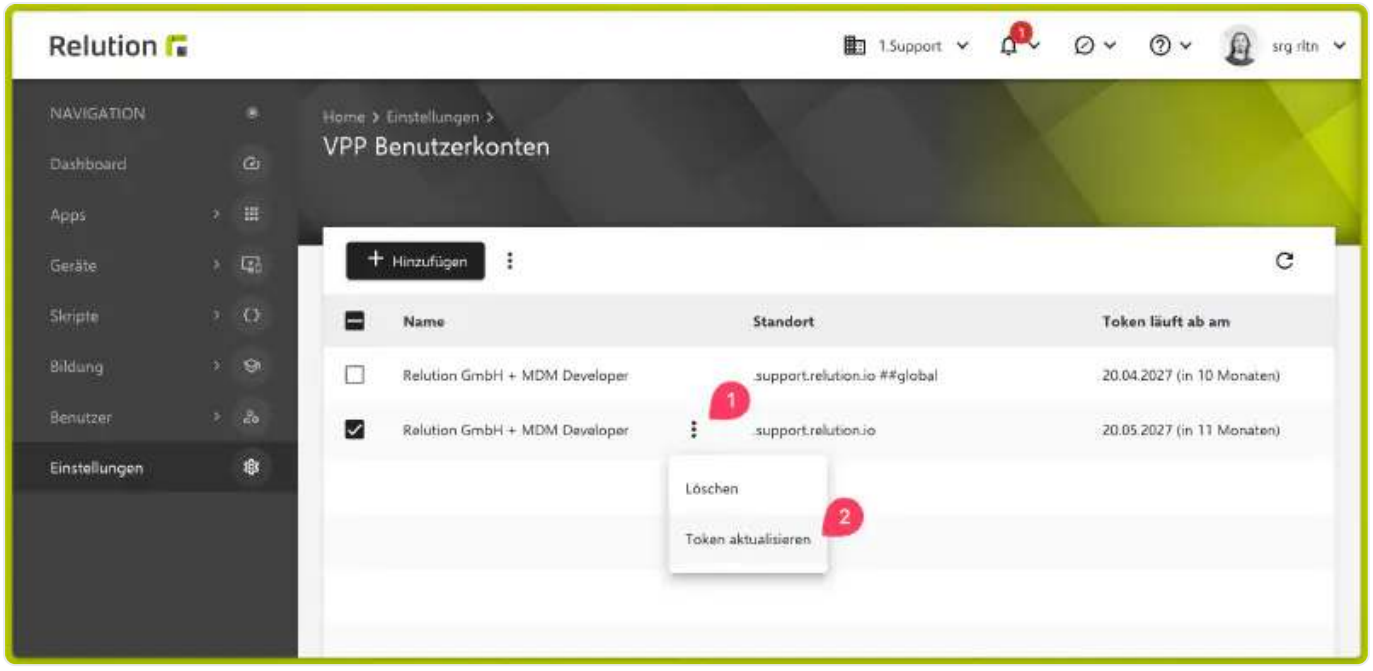
1. The login takes place in Apple Business →.
2. The organization name in the top right corner is clicked.
3. Settings is opened.
4. Payments & Billing is selected.
5. Under Content Tokens, Download is clicked for the desired token.
    - *File format:* `sToken_for_[Location].vpptoken`



Uploading to Relution

1. The login takes place in the Relution portal, followed by a switch to the corresponding organization.
2. Settings is opened.
3. Volume Purchase Program (VPP) → Account is opened.
4. The token to be renewed is selected via the three-dot menu.
5. Update token is clicked.
6. The previously downloaded file (`*.vpptoken`) is uploaded.
7. The process is completed by clicking Update token.





In the `Global` organization, the dialog points out that apps from global VPP accounts replace existing apps in other organizations. If the account is already managed by another MDM server, a notice appears as well; with the update, Relution takes over the management.

Renewing DEP Tokens (Server Tokens)

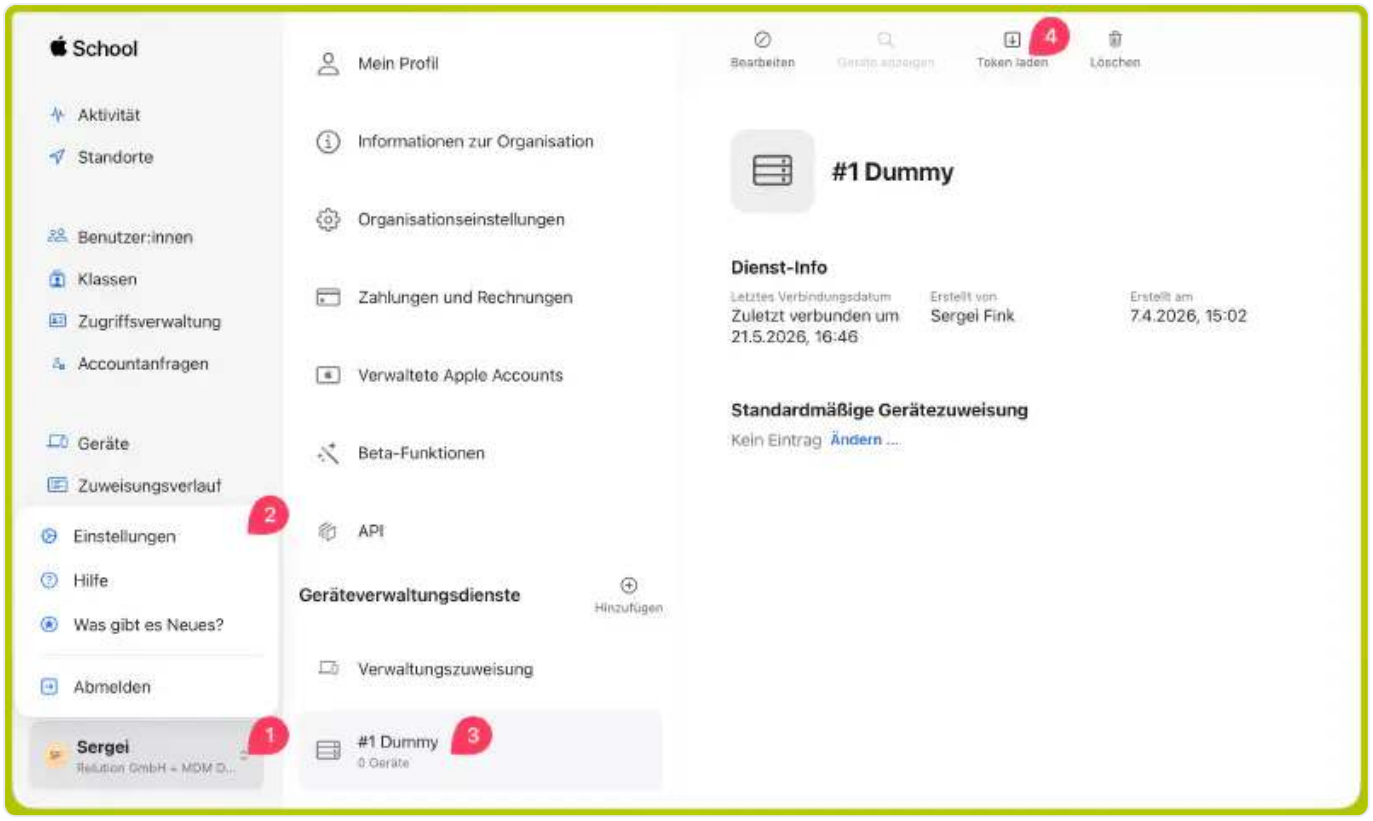
Apple encrypts the new token with the public key that was stored in ABM/ASM during the initial setup. Relution keeps the corresponding certificate for each DEP account, so the public key does not have to be uploaded again when renewing. If the certificate is needed anyway, it can be saved in the Upload token dialog (opened via Update token) using Download certificate.

Download from Apple School Manager (ASM)

1. The login takes place in Apple School Manager →.
2. The logged-in user name in the bottom left corner is clicked.
3. Settings is opened.
4. In the list of device management services, the device management service connected to Relution is selected.
5. The new token is downloaded via the corresponding button of the device management service.

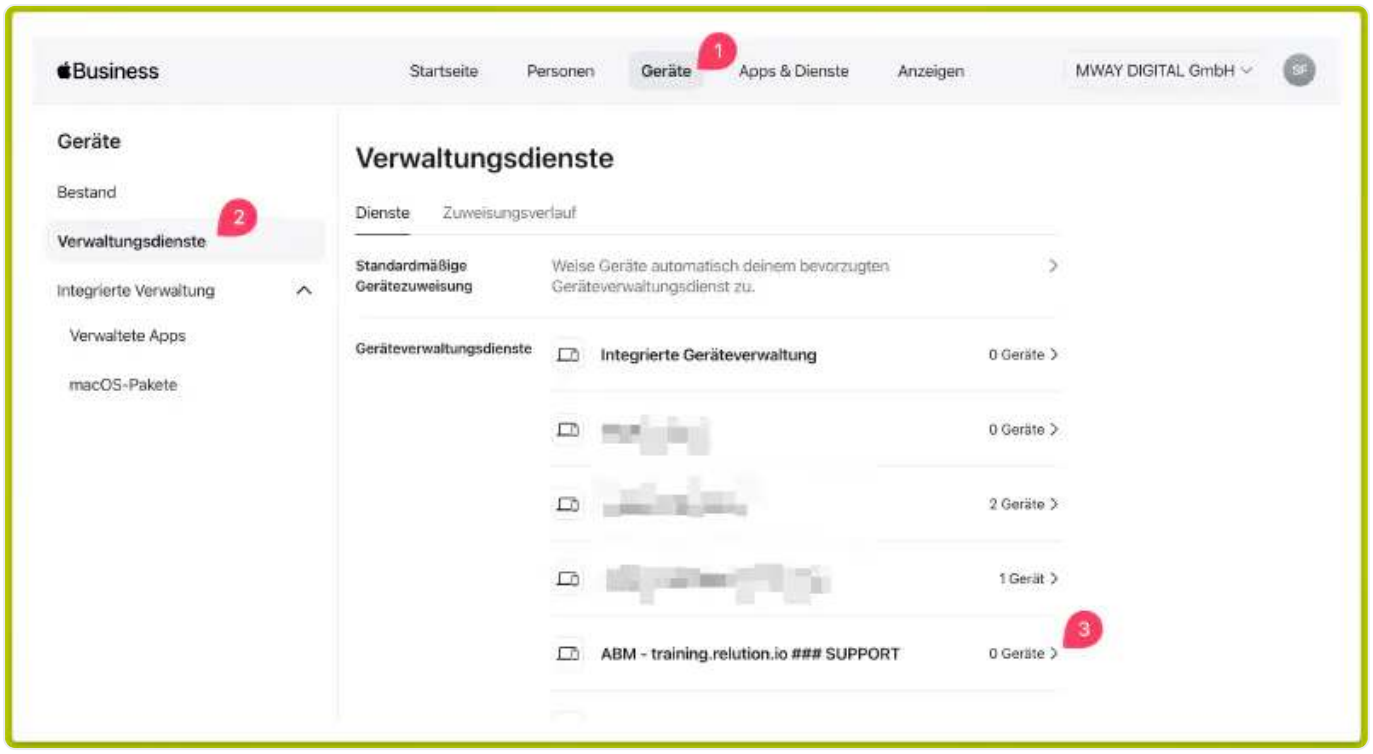
> Downloading a new token resets the existing token.

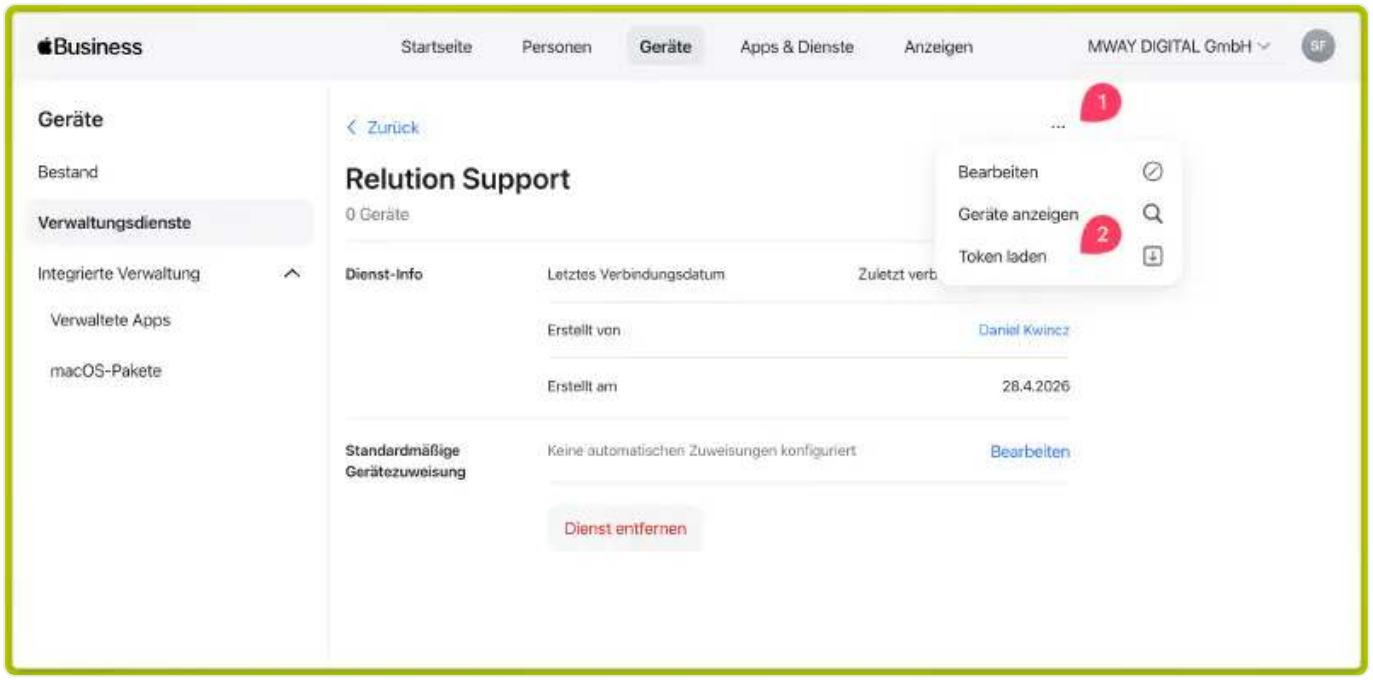
   - *File format:* `*_smime.p7m`



Download from Apple Business (formerly ABM)

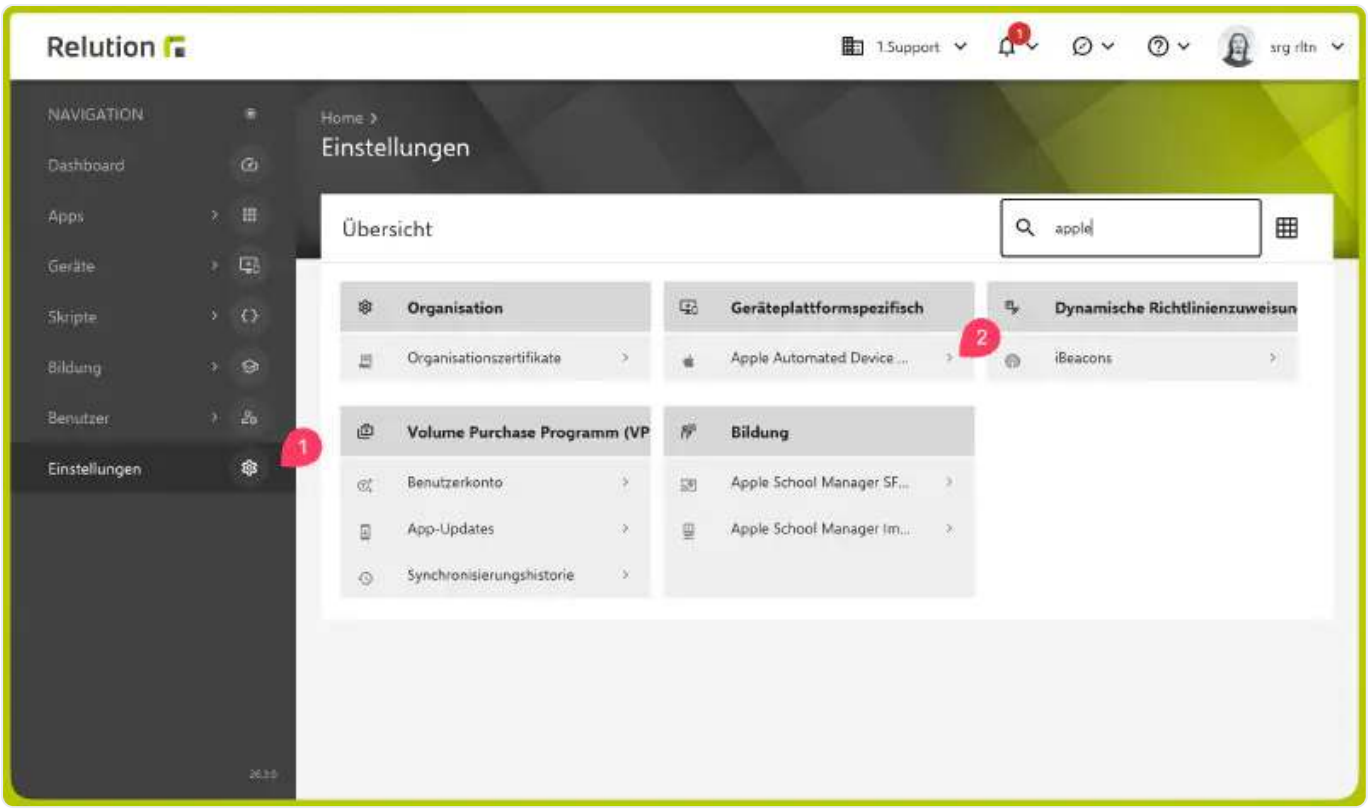
1. The login takes place in Apple Business →.
2. Devices in the top center is clicked.
3. In the left navigation, Management Services is selected.
4. In the list of device management services, the desired service is selected.
5. At the top right, the three-dot menu (⋯) is opened and the new token is downloaded from there.
   - *File format:* `*_smime.p7m`

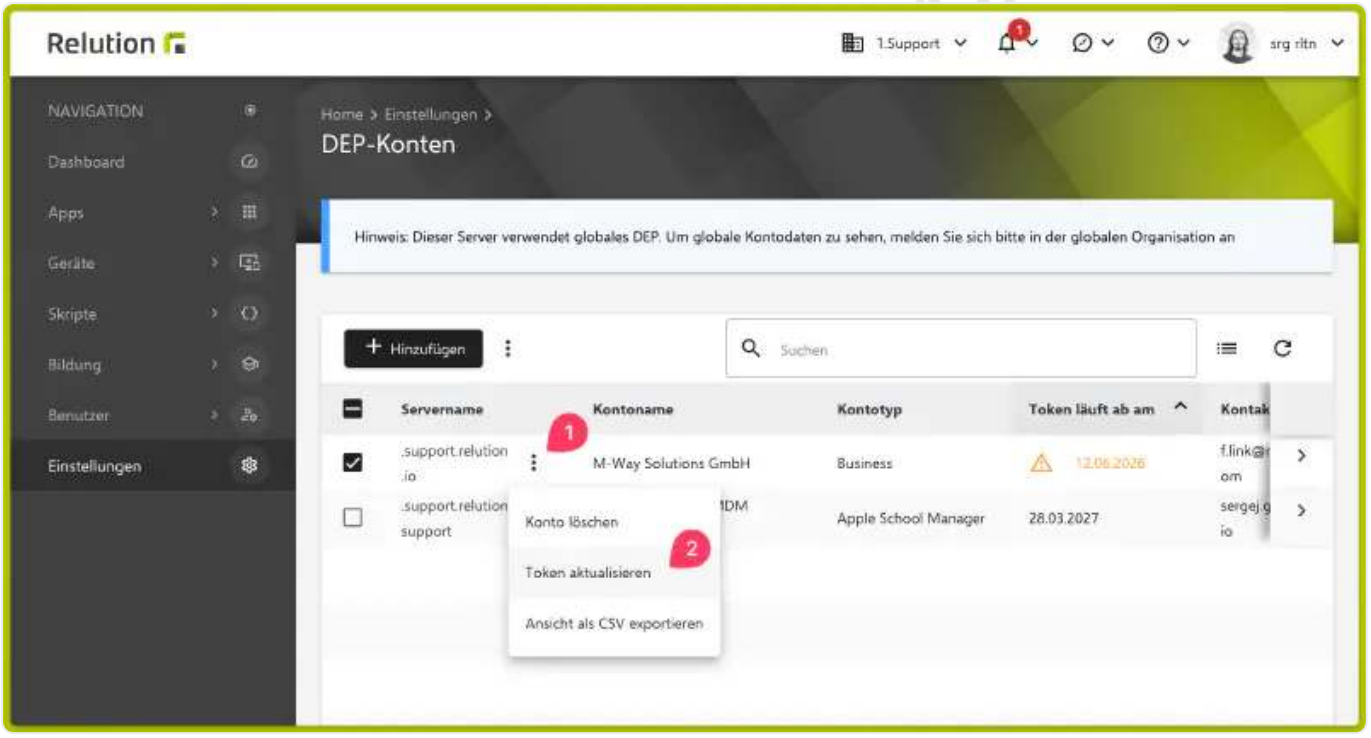




Uploading to Relution

1. The login takes place in the Relution portal, followed by a switch to the corresponding organization.
2. Settings is opened.
3. Device platform specific → Apple Automated Device Enrollment is opened.
4. The desired token is selected via the three-dot menu.
5. Update token is clicked.
6. The `*_smime.p7m` file is uploaded via Select.
7. The process is completed by clicking Save.





Important Notes & Troubleshooting

The following points are the most common causes of failed token renewals.

Common Errors

In practice, VPP tokens (`.vpptoken`) and DEP tokens (`.p7m`) are frequently mixed up and uploaded into the wrong menus. In the DEP menu, Relution rejects a `.vpptoken` file with the message Invalid data provided. In the VPP menu, a `.p7m` file is not accepted: the file is discarded without a message and the upload field remains empty. If a `.p7m` file is not a valid DEP token, Resource is not supported or the resource is corrupt appears.

If a DEP token belongs to a different device management service than the one linked to the DEP account, Relution rejects it with The uploaded token does not belong to the MDM server linked to this DEP account. In this case, the token is downloaded from the correct device management service in ABM/ASM.

If the error message Unknown error or The token is invalid. Please update the token in the settings appears when uploading the DEP token, Apple has rejected the request. One possible cause is a server time that is out of sync; it is checked and corrected first. If the error persists, the token is invalid (for example because a new token for the MDM server has since been generated in Apple Business Manager or Apple School Manager). In this case, a new token is downloaded and uploaded.

File Extensions Overview

Token Type	Purpose	File Extension
DEP Token	Automated Device Enrollment (ADE)	`*_smime.p7m`
VPP Token →	App and book licenses (Volume Purchase Program)	`*.vpptoken`
Public Key	Encryption certificate from Relution for ABM/ASM	`*.pem` *(Only required during initial setup)*

Premature Token Invalidation

A token can become invalid before its regular 1-year expiration date. Common causes include:

- Password Changes: The password of the underlying Managed Apple Account (Managed Apple ID in the portal) in ABM/ASM was changed.
- Account Status Changes: The administrator account used to generate the token was deleted, deactivated, or downgraded in permissions.
- New Apple Terms & Conditions: Apple has published updated terms of service in the ABM/ASM portal. Token communication is temporarily blocked until a main administrator accepts the new terms within the Apple portal.

Add to DEP retroactively

This guide describes how to retroactively add iOS, iPadOS, and tvOS devices to the Apple Business Manager (ABM) or Apple School Manager (ASM) using Apple Configurator 2 so they can be managed via the Device Enrollment Program (DEP) with Relution.

What is Apple Configurator 2 used for?

Apple Configurator 2 is a free Mac app used for the manual configuration of Apple devices via USB. It enables:

- Creating and deploying configuration profiles.
- Retroactively adding devices to DEP that were not already assigned by an authorized reseller.

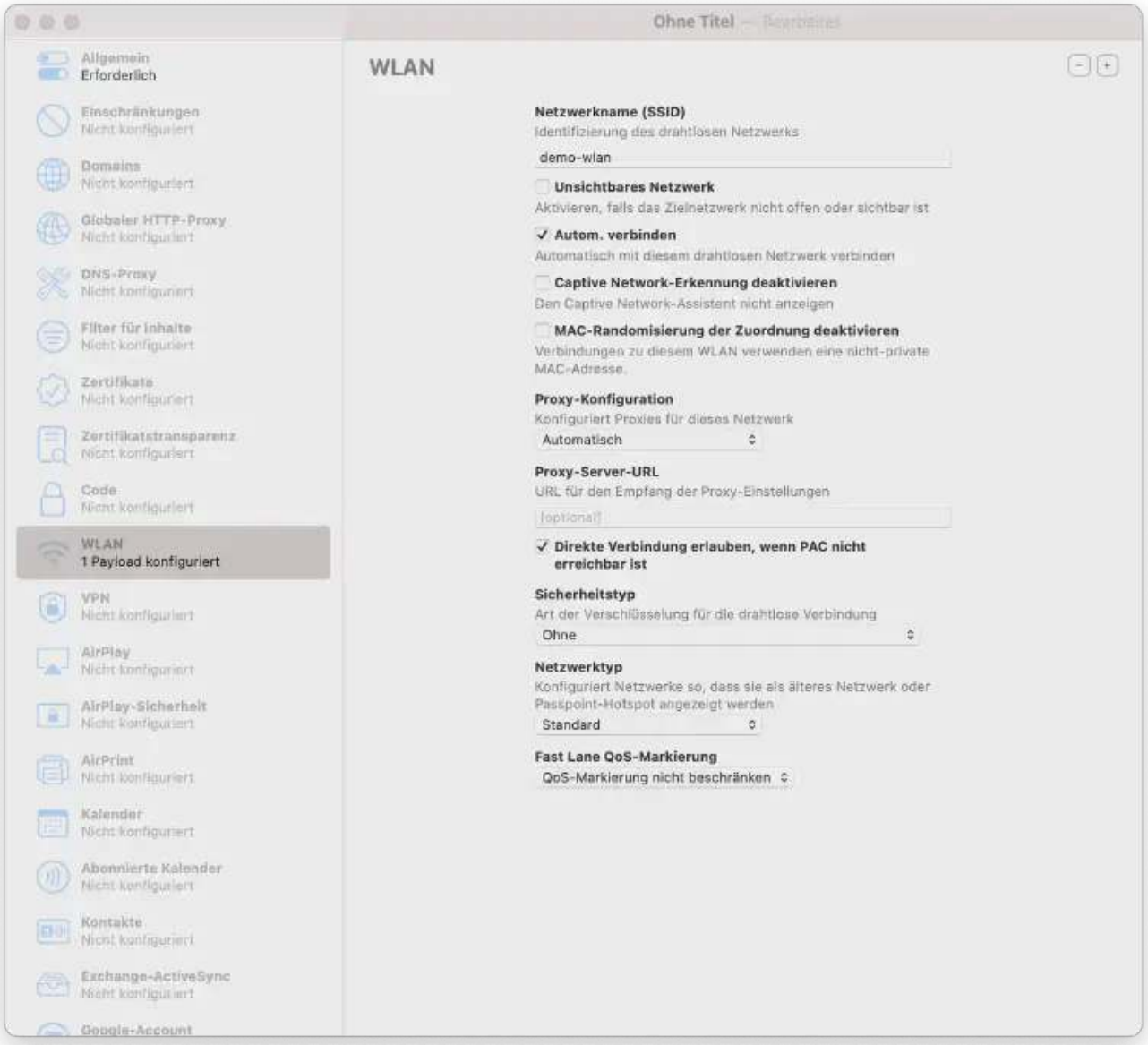
Preparations

To ensure smooth automatic registration, create a Wi-Fi profile in advance:

1. In Apple Configurator: Go to `File` → `New Profile` → `Wi-Fi`.
2. Enter the network credentials.
3. Save the profile as a file on the Mac.

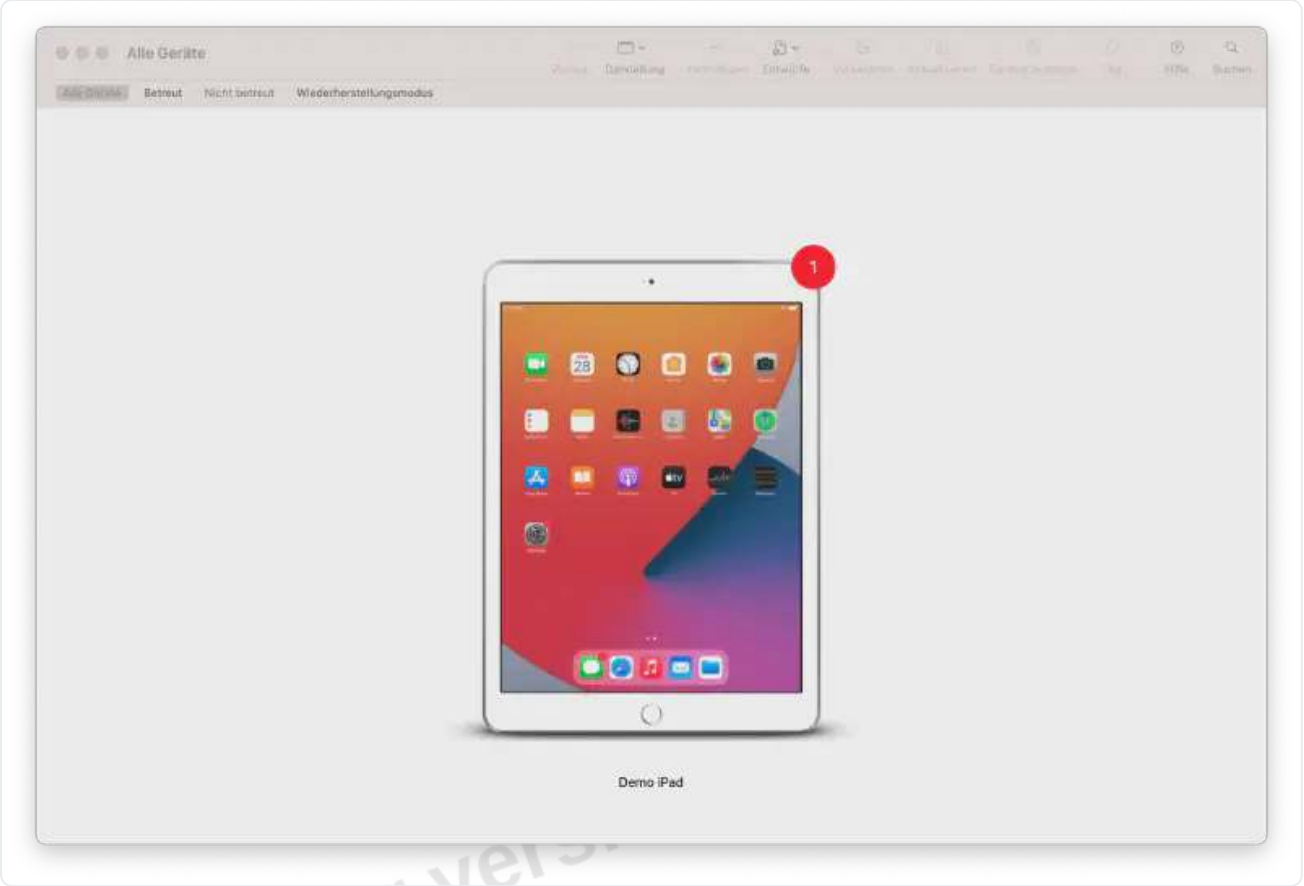
Ensure that the entered credentials are correct and functional.

For 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

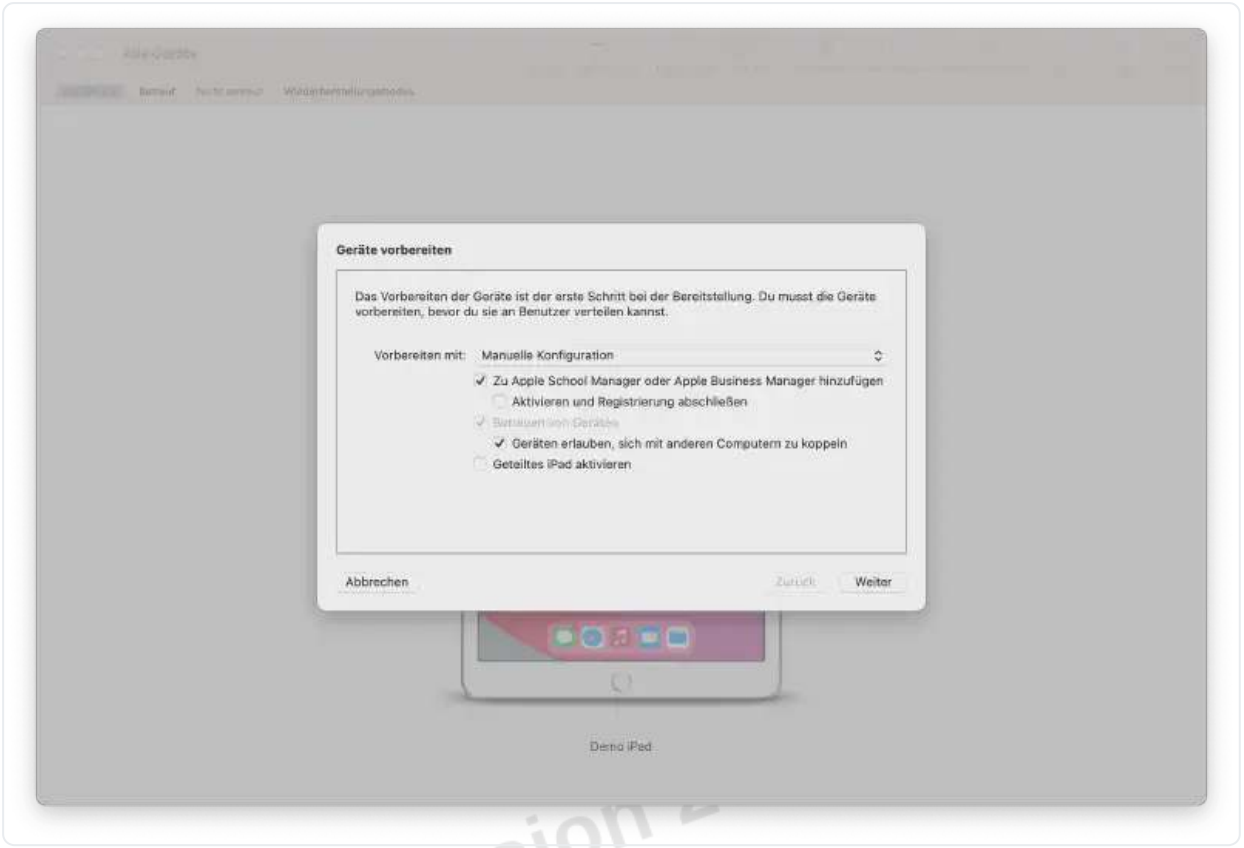
Execution: Adding Devices to DEP

1. Connect Device: Connect the Apple device to the Mac via USB and launch Apple Configurator 2.



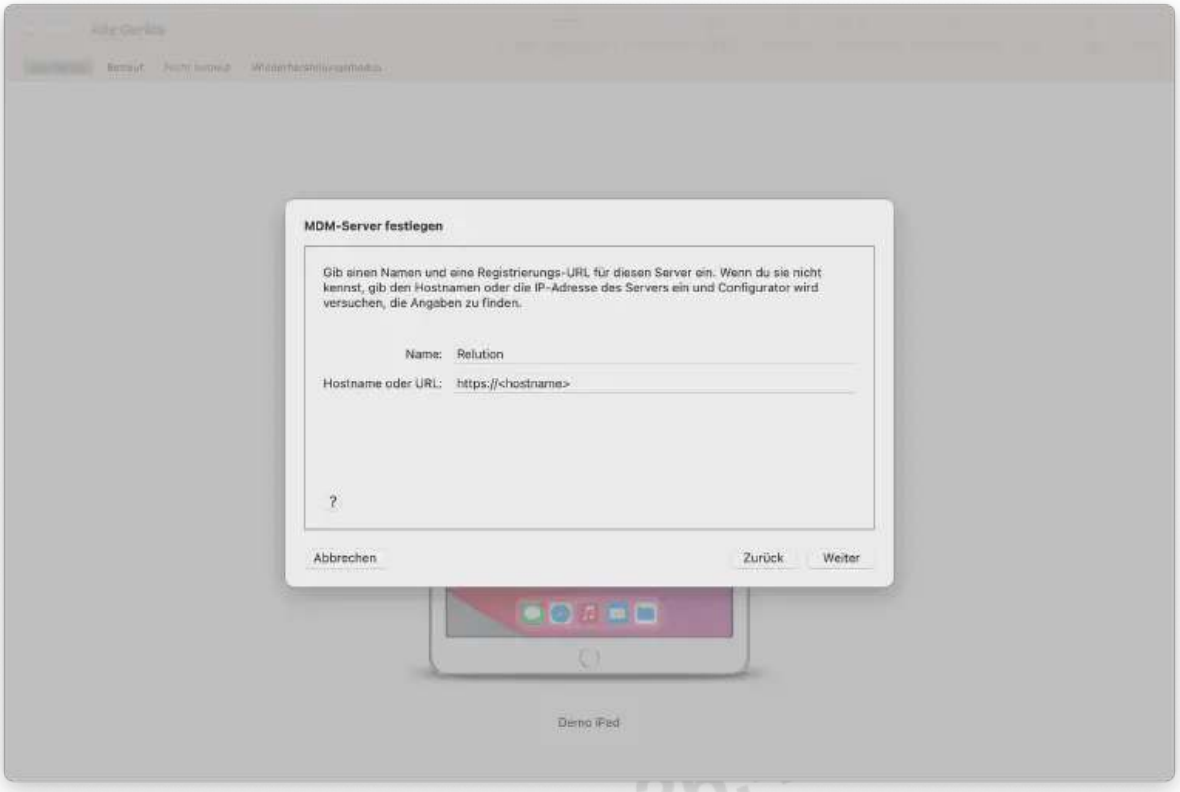
2. Factory Reset: Right-click the device and select `Advanced` → `Erase All Content and Settings`.
3. Prepare: Right-click the device and select Prepare….

4. Select Options:
    - Add to Apple Business Manager or Apple School Manager.
    - Allow devices to pair with other computers (enable).
    - Important: The option Activate and complete enrollment must NOT be selected.



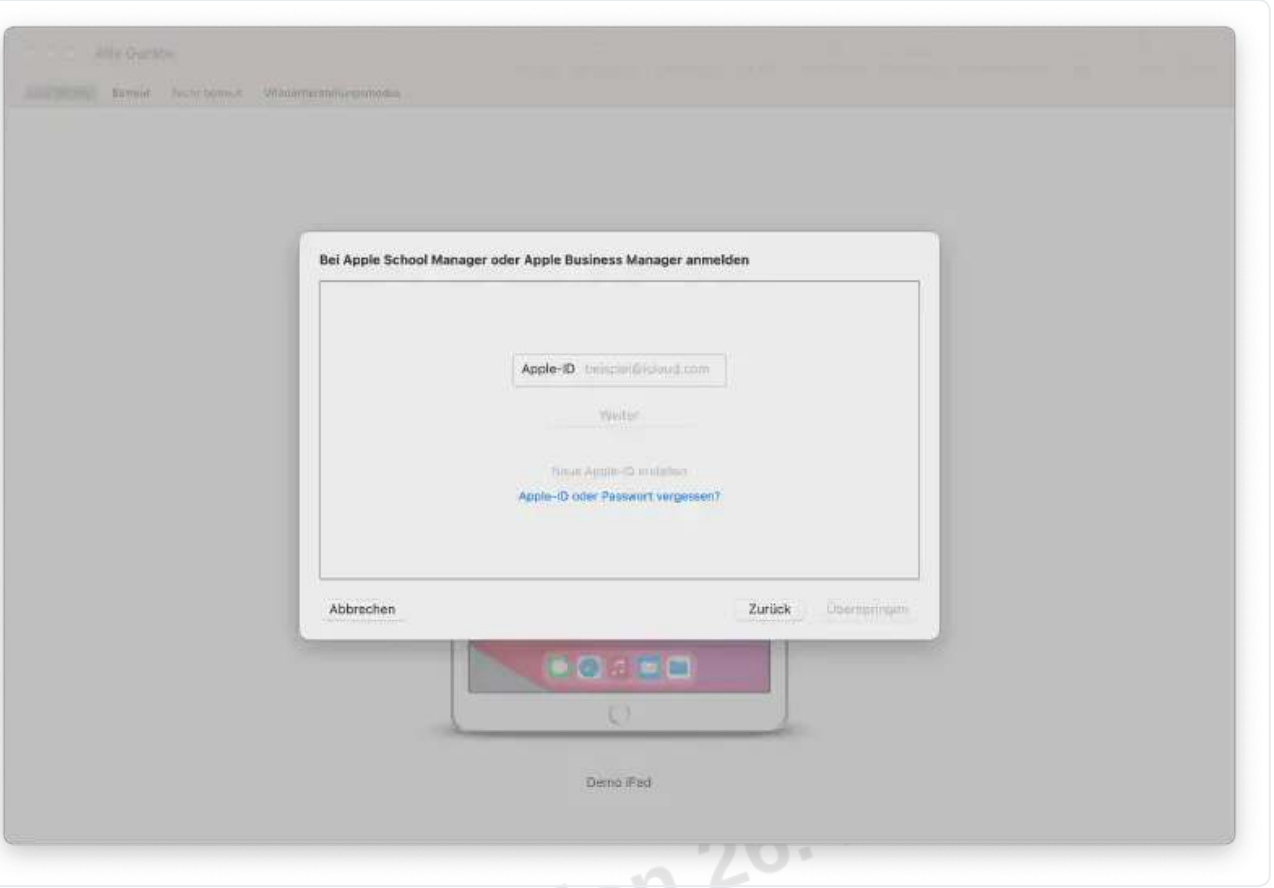
For version 2

5. Server Configuration: Select New Server and enter the Relution URL:
    - Standard (iOS/iPadOS): `https://live.relution.io/`
    - For tvOS: `https://live.relution.io/api/enrollment/v1/appleMdm/depenroll`



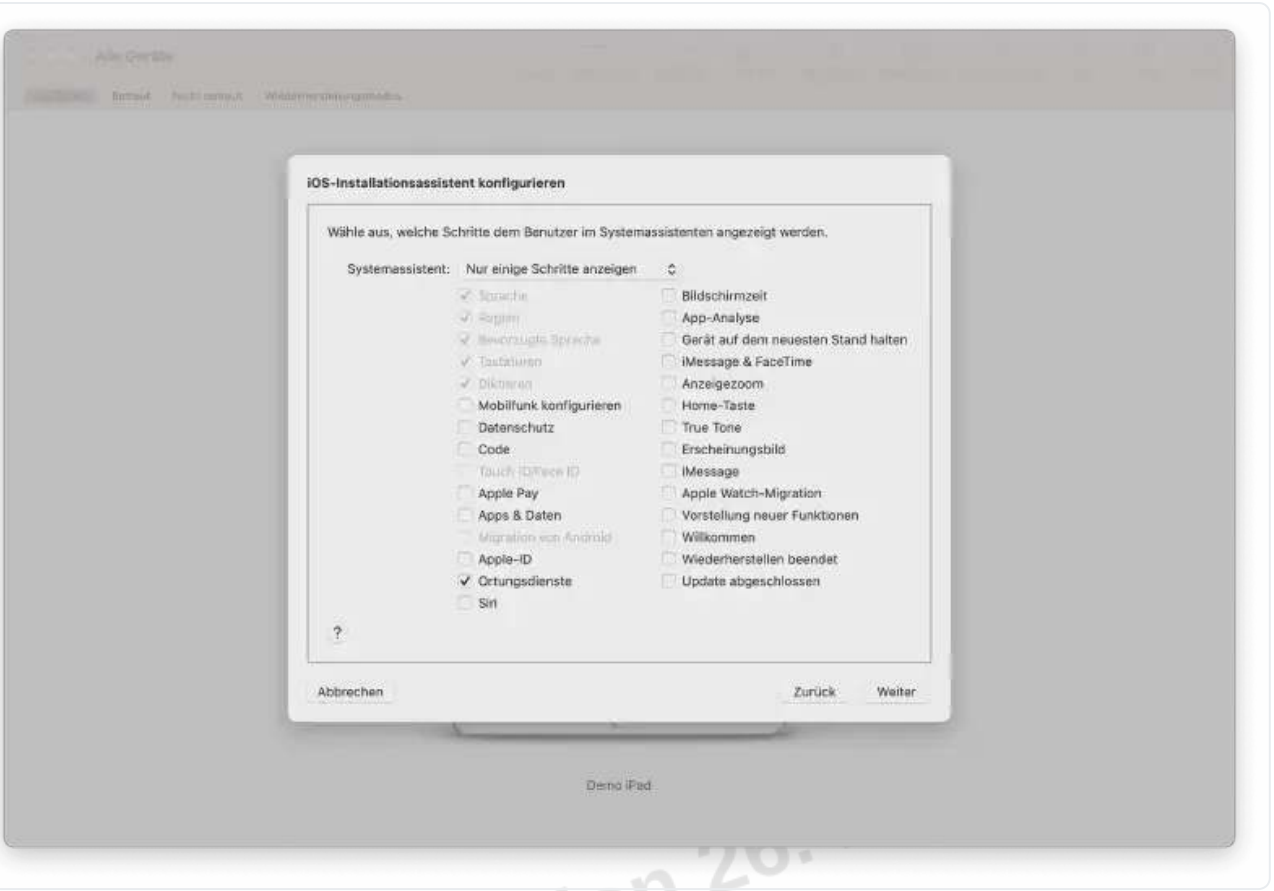
For version 26.

6. Organization: Select New Organization and sign in with the Apple ID of the ABM/ASM account (2-factor authentication required).



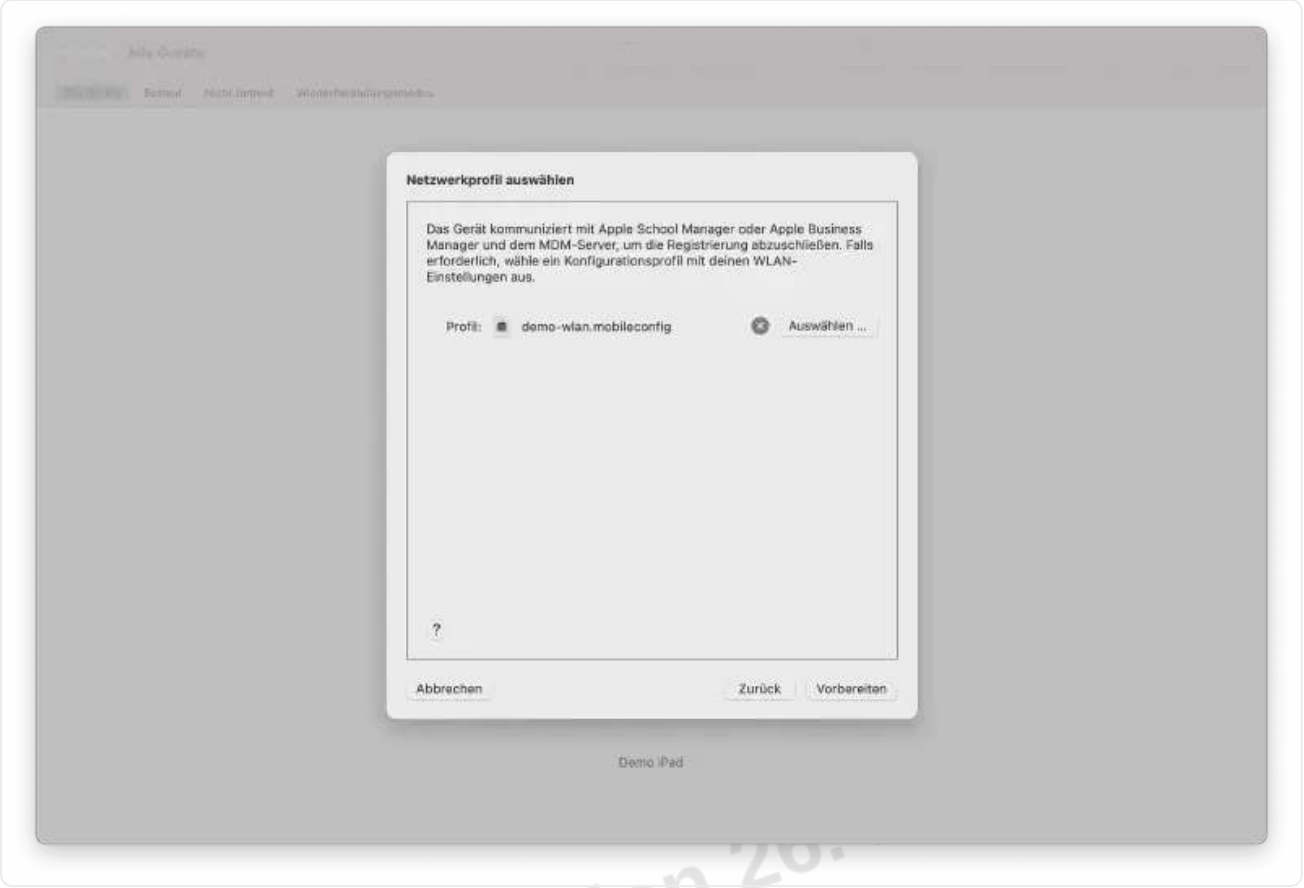
For version 26.

7. Setup Steps: Choose the steps that should not be skipped on the device (Recommendation: Location Services for correct time zone assignment).



For version 26.

8. Network Assignment: Select the previously created
   Wi-Fi configuration profile. This allows the device to transmit the DEP registration to Apple's servers after the restart.



9. Completion: Click Prepare. The device will restart and be registered in ABM/ASM.

For version 26.

Completing Enrollment

1. Assignment in Portal: Log in to the Apple Business/School Manager. Assign the new devices to the Relution MDM server.
2. Synchronization: In Relution, go to `Devices` → `Auto-Enrollments` and refresh the list.
3. Profile Assignment: Ensure that a DEP profile is assigned and synchronized to the devices in Relution.
4. Activation: Restart the device and follow the Setup Assistant until the automatic configuration is applied.

> Note on Grace Period: For devices added retroactively to DEP, there is a 30-day provisional period. During this time, the MDM management can be manually removed by the user in the settings. The management becomes permanent only after this period expires.

Troubleshooting: Unexpected Error 33007

If the error message `Provisional Enrollment failed. Network communication error [MCCloudConfigErrorDomain – 0x80EF (33007)]` appears during the process, it is usually due to one of the following reasons:

---

1. The device is still managed by another MDM

A device cannot be added to a new DEP system (ABM/ASM) as long as it is still registered or locked in another MDM instance.

- Solution: Completely remove the device from the previous MDM system and, if necessary, reset it to factory settings before restarting the process in Apple Configurator.

2. Missing internet connection during preparation

The device strictly requires access to Apple’s servers during the “Provisional Enrollment” phase.

- Solution: Ensure that a Wi-Fi profile is assigned to the device during the preparation step so it can go online immediately after the restart. Without an active internet connection, communication with the Cloud Config Domain will fail.

For version 26.4.0

Enrollment types

In order to manage iOS devices in Relution, they must first be enrolled. This enrollment process can be done in three different ways. The enrollment types differ and have a lasting effect on the later functions.

Manual enrollment

This enrollment is performed by manually downloading and installing an MDM profile on the devices. This requires either scanning a QR code on the devices or manually accessing the corresponding URL. Subsequently, the MDM profile must be installed on the devices.

Advantages

- This enrollment can be performed without having to reset the devices to factory settings.

Disadvantages

- The Enrollment can be removed at any time in the settings on the devices (MDM profile).
- Only partially suitable for BYOD devices, as administrators can see which apps are installed.
- Not all actions and policy configurations are possible.
- Devices are often not supervised (supervised mode).

For version 26.4.0

For manual enrollment →
Supervision →

Automatically via Apple DEP.

The iOS devices connect to the Apple server at startup and, if they are devices that have been enrolled in the DEP, are automatically redirected to the MDM server and enrolled. This process can be forced so that users cannot skip it. Similarly, the Apple shared iPad feature can be enabled and the MDM profile on the devices can be protected from deletion. This requires access with appropriate permissions for Apple School/Business Manager.

Advantages

- Enrollment is largely automatic.
- Devices are protected against theft.
- Enrollment (MDM profile on the device) cannot be removed.
- Devices are in supervised mode.
- Apple shared iPad (Shared iPad) can be enabled.

Disadvantages

- Devices must be reset to factory settings beforehand.

For automatic enrollment →
Profile for ADE →

Enrollment via Apple User Enrollment.

This is the typical enrollment for Bring Your Own Device (BYOD) devices. Users can enroll themselves and iOS devices do not need to be reset to factory defaults.

Benefits

- Administrators cannot view privately installed apps.
- Devices remain under user control.

Disadvantages

- Not all actions and policy configurations are possible.
- Managed Apple IDs are required.

Go to Apple User Enrollment for iOS →

For version 26.4.0

User Enrollment

With user enrollment, private iOS and macOS devices can be enrolled without the owner having to give up all control over the devices. Based on the `Bring Your Own Device` approach (BYOD), private devices of students or employees can be integrated and used in the school or company context while maintaining the protection of private data.

> Devices must not be in Monitored Mode/Supervised Mode for Apple user enrollment.

Two variantes of enrollment are available: account-based and profile-based (conventional manual enrollment)

> Profile-based User Enrollment is no longer supported starting with iOS 18

Benefits

- Administrators cannot view privately installed apps.
- Devices remain under control of users.

For version 26.4.0

Disadvantages

- Not all actions and policy configurations are possible.
- Managed Apple IDs are required.

Prepare enrollment in Relution

Starting in the Relution organization, a manual enrollment for iOS or macOS devices can be created classically and the enrollment link can be sent to the desired students or employees.

The basic prerequisite for the creation of a user enrollment is the assignment of users. For these, either a ‘Managed Apple ID’ or ‘Email address’ must be stored in the user details. Afterwards the corresponding users can be added and the enrollment can be completed. Users assigned to devices can no longer be changed or removed from enrolled devices via user enrollment.

User-based user enrollment (only up to iOS 17)

The received enrollment link will perform the device enrollment on the iOS or macOS device using the users’ Managed Apple IDs and the device will automatically appear in the device inventory of the corresponding Relution organization.

Account-based user enrollment

Relution supports account-based user enrollment of iOS and macOS devices that are not in Supervised Mode.

Account-based user enrollment requires the following:

- Service Discovery Well-Known Hosts

A service discovery must be configured so that Apple can transfer the devices to the correct MDM server. To do this, a http well-known resource file must be stored at the domain that users will use to log in. Apple must be able to retrieve this file via an HTTP GET at the following URL:

```
https://yourdomain.com/.well-known/com.apple.remotemanagement
```

Enter the domain also used for the Apple ID's under `yourdomain.com`.

The created file must be stored on a domain that can handle HTTP GET requests. Create the file in JSON format with content type application/json.

To enter the correct information in the file, copy the required information directly from the Relution Portal. To do this, open:

1. Settings
2. Device Management / Device Management
3. Account-based Apple user registration
4. Set the slider for on
5. copy the text in the curly brackets and insert it into the file.

For version 26.4.0

> Important: for the file to work properly, it must not have any file extension.

Example: maxmustermann@musterhausen.de

In this example, the domain of the ID would be `musterhausen.de`, so the service discovery would need to be stored there.

Option 2 makes it much easier to register personal devices in Relution. As soon as Relution users register on private devices via the option `Log in to work or school account...` in `VPN & Device Management` of the general settings, user enrollments are automatically generated in Relution. Using the Managed Apple ID of the respective users, the enrollment URL of the respective MDM solution is automatically identified. After logging in with the users login credentials from Relution, the devices automatically show up in the device inventory of the corresponding Relution organization after successful authentication.

Related Topics

- Apple DEP & VPP Overview → — Overview of Apple deployment programs.
- Add devices to Apple DEP retroactively → — Instructions for adding unsupervised devices.

Manual enrollment

Enrollment is performed by manually downloading and installing an MDM profile on the iOS devices. This requires either scanning a QR code on the devices or manually accessing the corresponding URL. Subsequently, the MDM profile must be installed on the devices.

Advantages

- Enrollment can be performed without having to reset the devices to factory settings.

Disadvantages

- Enrollment can be removed at any time in the settings on the devices (MDM profile).
- Only partially suitable for BYOD devices, as administrators can see which apps are installed.
- Not all actions and policy configurations are possible.
- Devices are often not supervised (supervised mode).

For version 26.4.0

To perform a manual enrollment, it must first be created in Relution. To do this, switch to `Devices` → `Enrollments` in the menu and then click `Add`.

Enrollments depend on the operating system. Therefore, select either `iOS, macOS or tvOS` as `Platform` and the `Device enrollment` as `Type`. The `ownership` can be chosen accordingly.

To associate a `User` with the device to be enrolled, select it. Note that users should have the Device User role for this.

Each enrollment can only be used once, unless the switch for `Multiple enrollment` is activated. If this is the case, new devices can be enrolled via the enrollment link until either the validity date has been exceeded or no more device licenses are available in Relution.

Under `Policies` and `Rules` the same can be linked to the enrollment. If the device is enrolled, these are applied directly.

After saving the enrollment, the created QR code can be scanned on the iOS device, or the URL can be entered manually in the browser. The MDM profile is downloaded via the `Enrollment` button and must be installed on the device in the next step in the `Settings` under `VPN and Device Management`.

Step by step instructions

1. Start the enrollment by pressing `Enrollment` button.
2. Then press `Allow`.
3. `Close` the next window.
4. Switch to the `Settings`.
5. There in the section `General`.
6. Press `VPN and Device Management` at the very bottom.
7. Select the loaded MDM profile.
8. Check the MDM profile and press `Install` and confirm the dialog again by pressing `Install`.
9. A security message is displayed. Press `Install` again.
10. Trust the remote administration.
11. by pressing `Done` the MDM profile is installed.

This completes the enrollment.
Now the Relution Agent is installed on the device and a new entry should appear in the device inventory of the Relution portal.

For version 26.4.0

Migrate Apple devices

With the release of iOS 26, Apple now offers the ability to migrate managed Apple devices from a mobile device management (MDM) solution such as Jamf or iServ to Relution. The goal is to fully transfer devices without resetting them, without manual re-enrollment, and without losing existing configurations, apps, or Managed Apple IDs.

Device requirements

- An iPhone, iPad, or Mac that is managed (active MDM profile) via DEP through Apple Business Manager (ABM) or Apple School Manager (ASM).
- Device must be in Supervised mode.
- Operating system version iOS/iPadOS 26+ or macOS 26+.
- The iPad must not be operated in Shared iPad mode – migration is not available for Shared iPads; these devices must be reset and re-enrolled.
- The device must not be in Single App Mode (Kiosk mode) – it must be disabled before the migration, otherwise the migration cannot be performed.

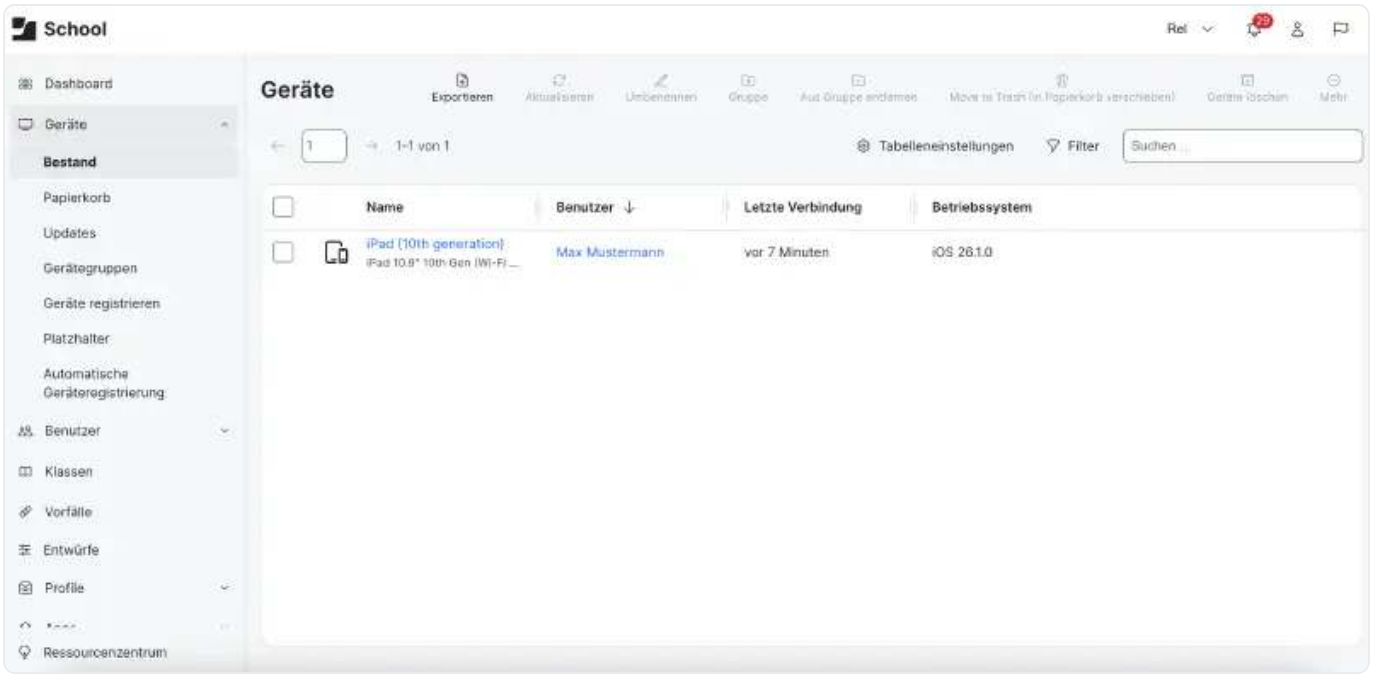
MDM requirements

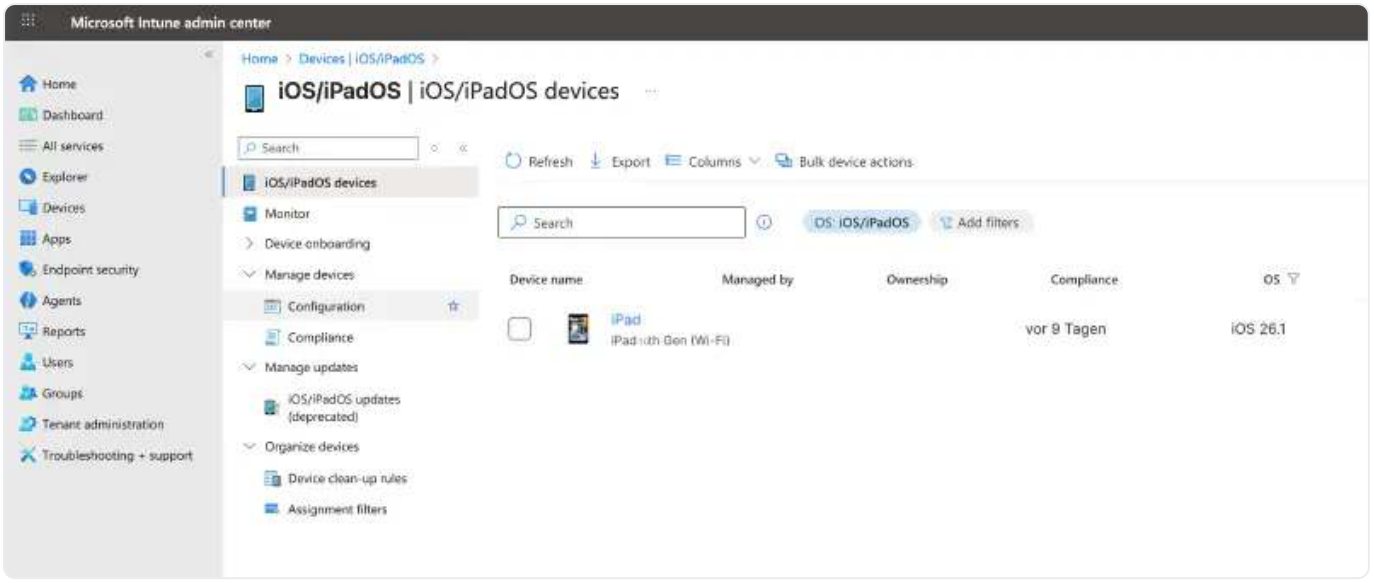
For version 26.4.0

- The existing third-party MDM system must allow device assignment or transfer via ABM/ASM. This feature has been supported in Relution since version `5.34`.
- Relution is registered as an MDM server in ABM/ASM and is fully operational.

Verify devices in the third-party MDM

- Devices that should be migrated to Relution must be visible in the third-party MDM, as shown in the following examples.
- No further configuration within the old MDM is required for the migration to Relution.



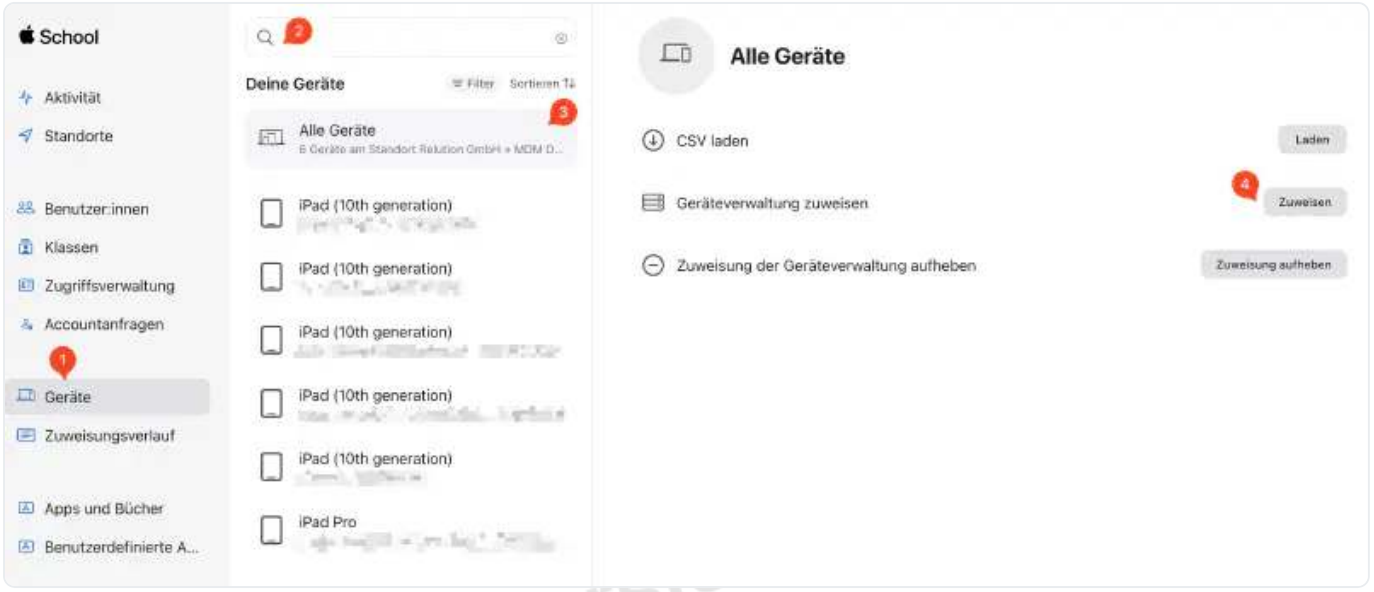


Preparation in Relution

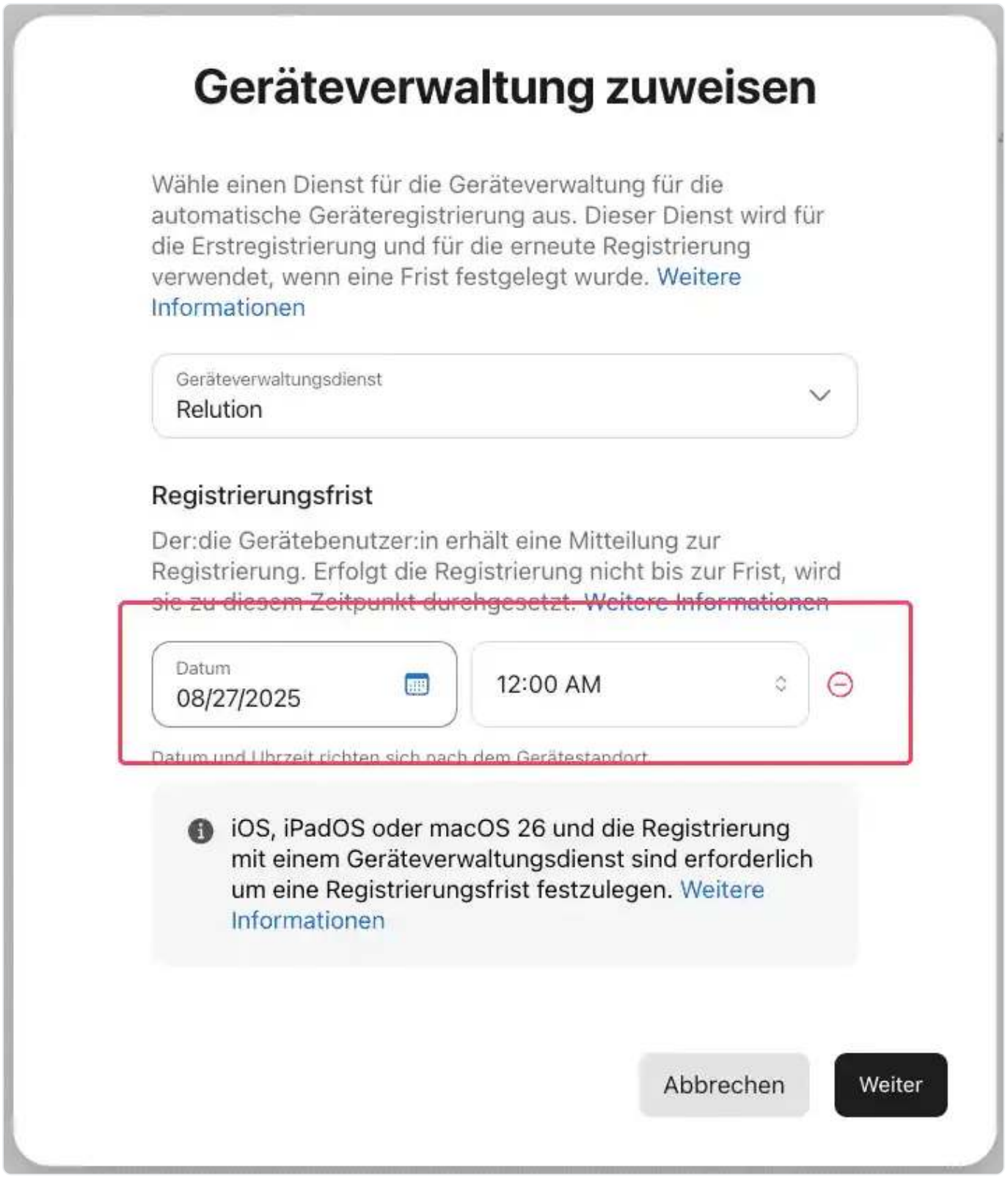
- In Relution, verify that the DEP → and VPP → tokens are available and valid.
- Create or identify a device group that will contain the devices to be migrated.
- Set up all required configurations (profiles, certificates, apps) in Relution.
- To avoid misconfigurations, it is recommended to perform the migration with test devices first.
- Adjust the DEP profile setting Install and configure apps before continuing with the Setup Assistant. Otherwise, no configuration profile will be automatically assigned during enrollment.

Assignment in ABM/ASM

- Log in to Apple Business Manager or Apple School Manager.
- Navigate to `Devices` → `All Devices`, then filter by the serial numbers of the devices to be migrated.
- Select the devices → Assign Device Management.
- In the dialog, choose Relution as the new server.
- A migration deadline should be set; this gives users time to complete the migration before the deadline. After the deadline, migration must be completed in order to continue using the device.
- Confirm the assignment—Apple now marks the devices for Relution.

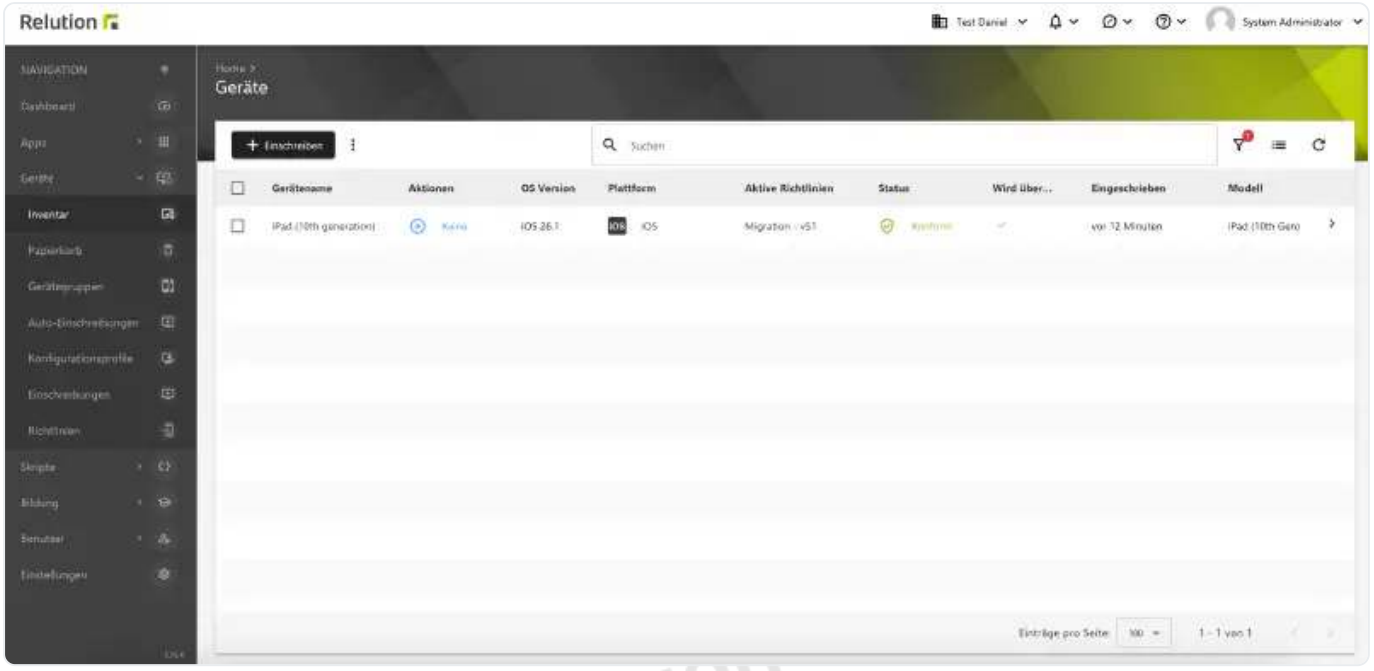


For versi

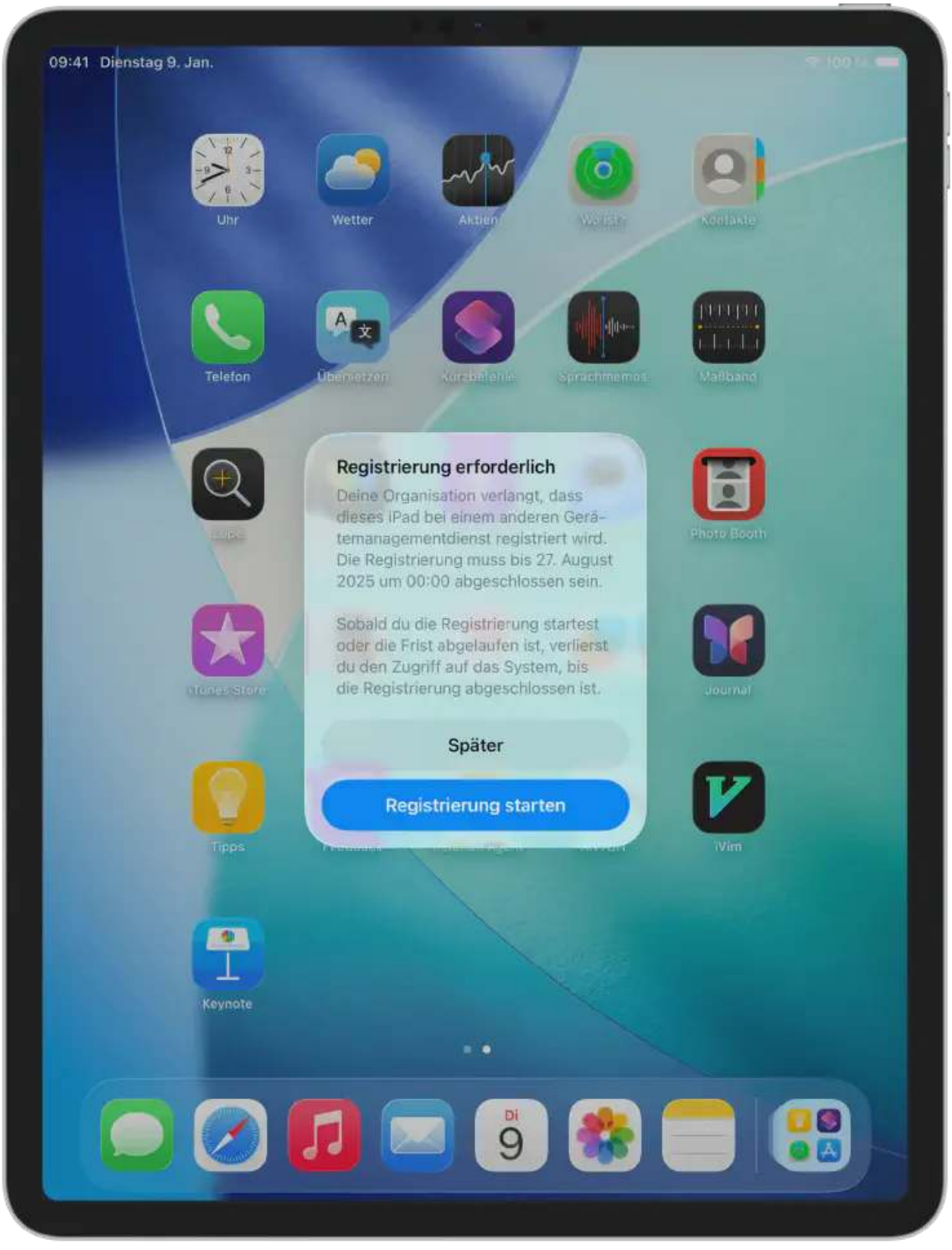

Geräteverwaltung zuweisen
Wähle einen Dienst für die Geräteverwaltung für die automatische Geräteregistrierung aus. Dieser Dienst wird für die Erstregistrierung und für die erneute Registrierung verwendet, wenn eine Frist festgelegt wurde. Weitere Informationen
Geräteverwaltungsdienst
Relution
Registrierungsfrist
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

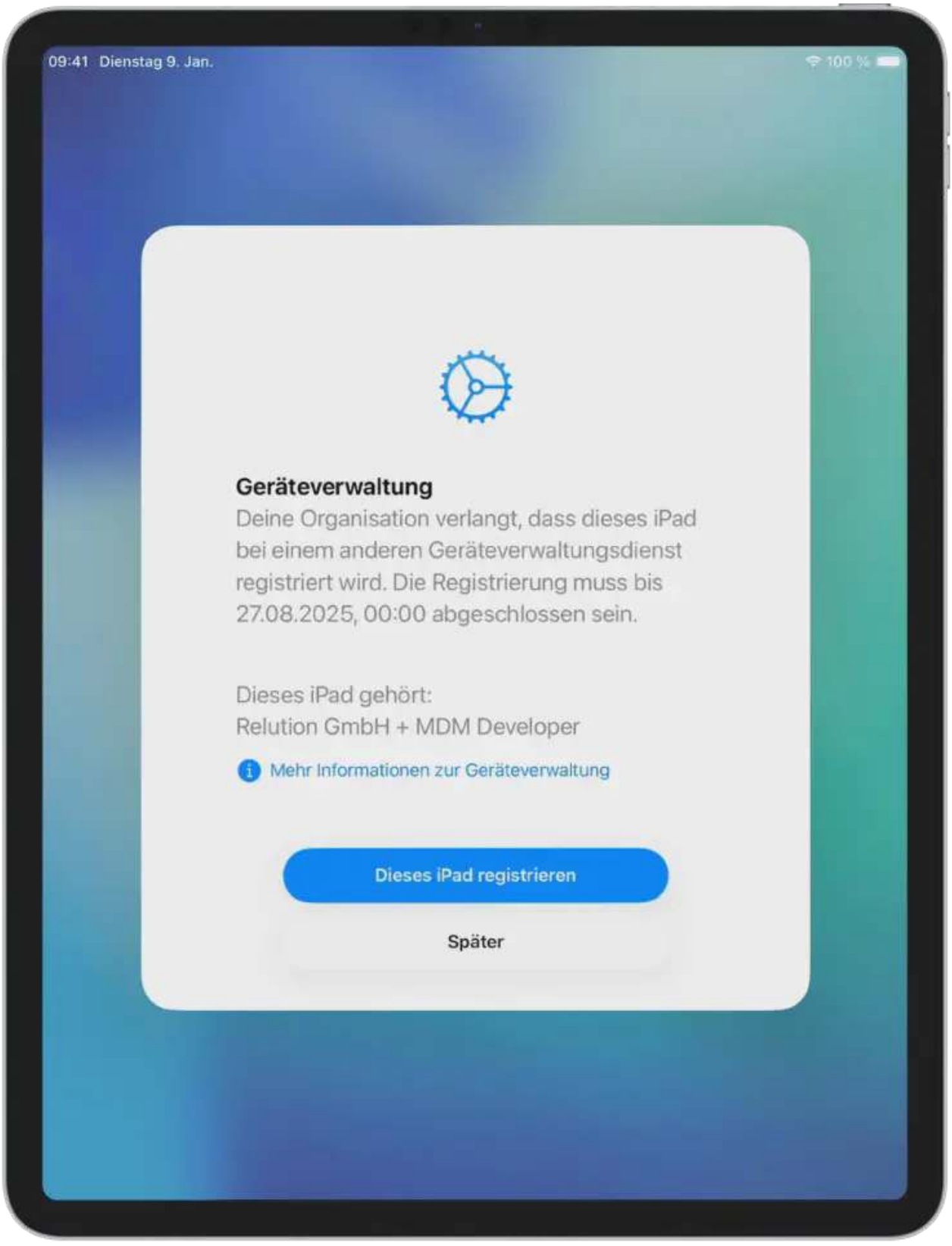
Migration on the device

- To begin migration directly on the device, go to `Settings` → `General` → `VPN & Device Management` and tap Start Enrollment.
- Once initiated, the device will be removed from the old MDM and added to Relution, without a factory reset.
- After completion, the device appears in Relution as managed.



For version


09:41 Dienstag 9. Jan.
Uhr
Wetter
Aktien
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

Limitations & Notes

- Devices that are not supervised and not assigned via DEP in ABM/ASM must be re-enrolled manually.
- To enable migration in iOS 26, a migration deadline must be set in ASM/ABM. If the option is greyed out, migration is not available.
- The migration option in ASM/ABM may take up to two days to appear after the update to iOS 26.

For version 26.4.0

Enrolling an unmanaged device as supervised

An unsupervised iOS device can retroactively be registered in Apple DEP without users losing their data and content. According to Apple documentation, restoring a backup on the same device restores the device management status from the backup — an unsupervised device cannot be converted into a supervised DEP state directly from its own backup. The following workaround routes the backup through a second temporary device: because restoring to a different device applies device management from Apple School or Business Manager instead.

Apple describes this behavior as follows:

- Restoring from a backup to the same iPhone or iPad restores device management status from the backup.
- Restoring from a backup to a different iPhone or iPad obtains device management status from Apple School / Business Manager.

Example

If a device is configured to be supervised and automatically enrolled in MDM, but is restored from a backup created when that same device was unsupervised, the device becomes unsupervised. An unsupervised device cannot be directly restored from its own backup if supervised mode and Apple DEP registration are desired — which is why routing through a second device is required.

For version 26.4.0

Preparing the DEP Recovery Profile

Create a dedicated temporary DEP profile in Relution for this workaround with the following settings:

- Enable `Allow pairing with Macs or PCs and configuration via Apple Configurator`.
- Do not skip the setup step `Allow Device Location`.
- Do not skip the setup step `Restore from Backup`.
- Do not skip the setup step `Sign in with Apple ID`.

Learn more about configuring a DEP profile in Relution: Profile for ADE →

Workflow

Device-01 and Device-02 must run the identical operating system version. Also make sure `Find My iPhone` is disabled on both devices, since an active device search can prevent a backup from being created or restored.

1. Backup

Create a backup of the unsupervised Device-01 via iCloud or locally on a Mac or PC. Restore this backup onto a second device, Device-02. Then create a new backup of Device-02 via iCloud or locally — this second backup will later be restored onto Device-01 and will be treated as a backup from “another device”.

2. Preparation

Reset Device-01 to factory settings. Add Device-01 to Apple School / Business Manager using Apple Configurator 2. Learn more in Adding Apple devices to DEP retroactively →. Assign the temporary DEP recovery profile to Device-01.

3. Integration in Relution

Assign Device-01 via Apple School / Business Manager to the corresponding Relution server with the prepared DEP recovery profile. Set up the device by following the setup assistant on the device.

4. Restore Backup

On Device-01 in the setup assistant, select `Restore Apps & Data` and choose the backup created from Device-02. For iCloud backups, use the same Apple ID used during backup creation.

Because the backup originates from Device-02, the restore counts as a restore on a different device: management settings are not taken from the backup, but from the DEP profile configured in Relution — making Device-01 supervised and DEP-enrolled.

After successful restore, switch back to the default DEP profile. The setup step for restoring backups on the device will no longer be displayed.

For version 26.4.0

Unenroll devices

Unenrollment ends the management of a device by Relution. A device is unenrolled by deleting it: the Delete action is available in the device inventory and on the device details page. After the deletion is confirmed, the MDM profile — including all configurations, certificates, and managed apps distributed through Relution — is removed from the device and the device is deleted from the inventory. The device itself is not erased; personal data remains on the device.

The unenrollment is recorded in the audit log, and the device can be enrolled again at any time. This applies to devices enrolled via Manual enrollment → as well as via User Enrollment →.

Devices enrolled via Automated Device Enrollment (DEP)

Deleting a device in Relution does not remove it from the Apple School Manager or Apple Business Manager. If a device is to leave the organization permanently — for example, to be returned to private use — it must additionally be removed from the Apple DEP. See Remove devices → for the complete procedure.

Trash

Deleted devices are first moved to the Trash of the device inventory. Only deleting a device again from the trash removes it permanently from Relution.

Supervised Mode / Supervision

`Supervised Mode`, also called `Supervision`, is a deployment strategy introduced by Apple for organizations to manage iOS, macOS and tvOS devices. Since its introduction with iOS 5, `Supervision` has been available to organizations as an effective method for managing Apple devices. Supervision means that an organization owns and has complete control over the devices. End users can access and use supervised devices, but the organization has full administrative control. Thus, the owner can decide which features may be used on the devices by enforcing advanced restrictions or adjusting device settings via MDM system.

Relution supports enrollment type via Apple DEP to put devices in `monitored mode`.

Automatic Enrollment →

Put devices in supervised mode / Supervised Mode

In order to access all functions of Apple devices via an MDM system, they must be monitored or supervised. This state is achieved by enrolling the devices in the Apple `Device Enrollment Program` (DEP). For this purpose, it is necessary to add the devices to the Apple School/Business Manager. If devices are already enrolled, proceed to the following section.

Automatic Enrollment →

For version 26.4.0

Add iOS and tvOS devices to Apple School / Business Manager

> A Mac and Apple Configurator 2 software are required.

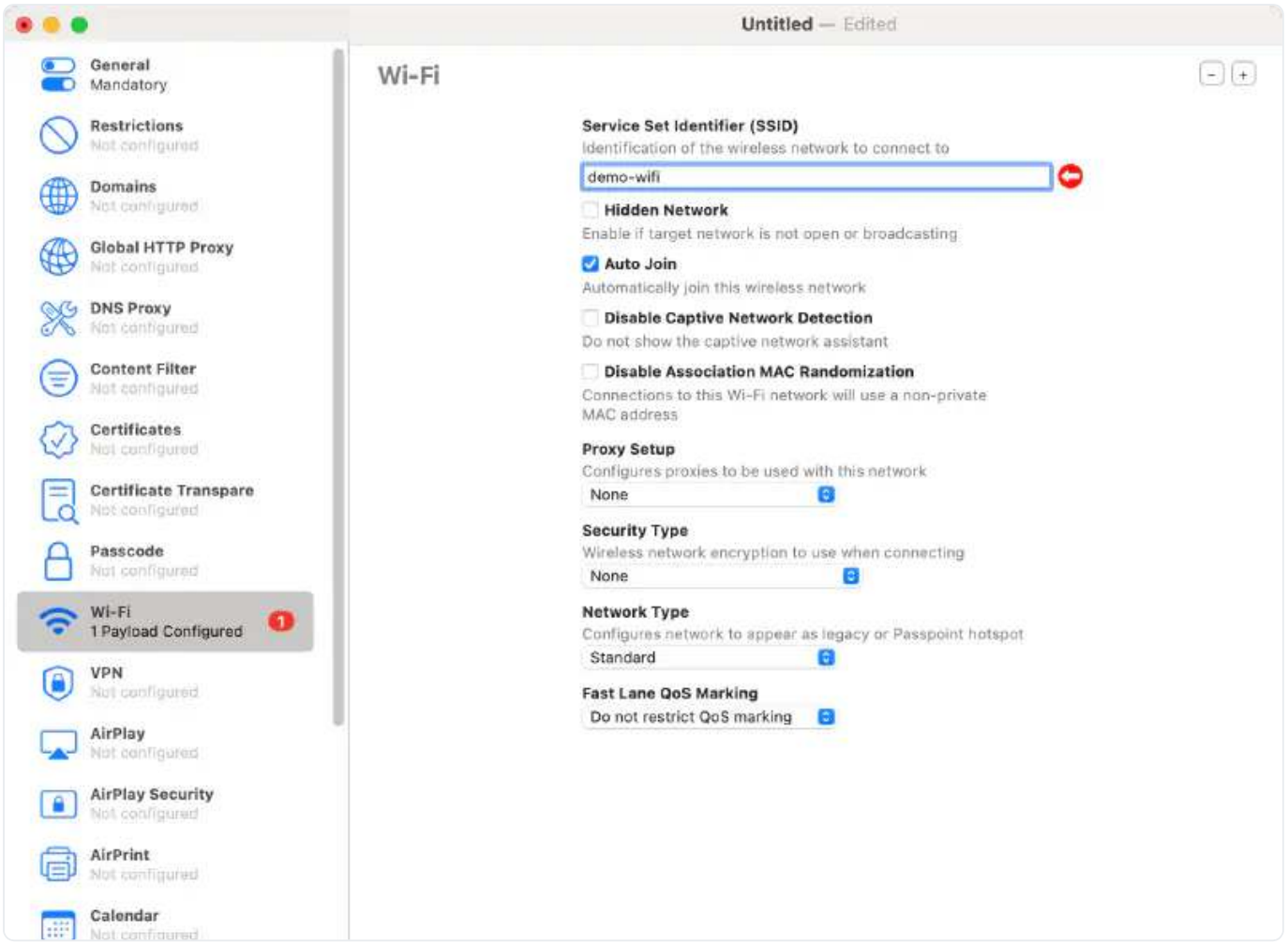
`Apple Configurator 2` is a free app available from the Mac App Store. The application can be used to manually configure Apple devices connected via USB to a Mac computer before the devices are handed out to users. For this purpose, so-called profiles can be created and applied to the devices. In addition, `Apple Configurator 2` allows Apple devices that have not already been added to the DEP by an authorized reseller to be subsequently added to the DEP. This option is only available for iPhones, iPads and Apple TVs. macOS devices must be purchased from an authorized reseller to take advantage of automatic enrollment through Apple DEP. Overall, it is recommended to purchase DEP devices directly, as adding them after the fact involves manual effort.

Apple devices that are subsequently enrolled via `Apple Configurator 2` in Apple School/Business Manager will not function for the first 30 days after provisioning as devices enrolled directly in DEP when purchased through an authorized reseller. Even if manual removal of MDM management on devices has been blocked via the associated DEP profile in the MDM system, users can remove MDM management under `Preferences` > General > `Profiles`.

With the expiration of the 30-day period from registration, user will be prevented from removing MDM management on devices.

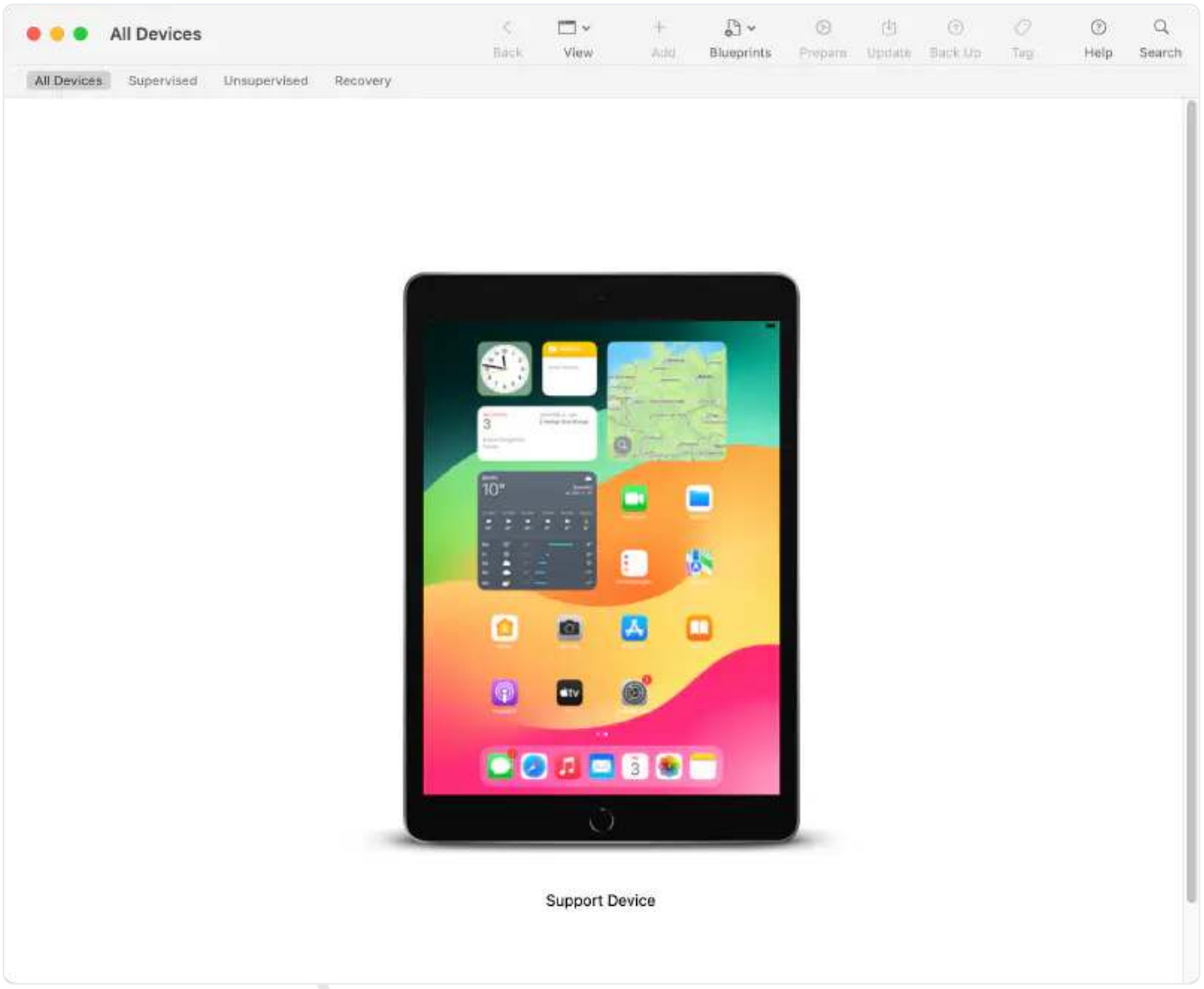
Preparation

In order for Apple devices to automatically connect to the Internet and for the subsequent registration to DEP to be as convenient as possible, it is recommended to create a `WiFi profile` in advance. This can be created on a Mac via the menu item `File` → `New Profile` → `WiFi` and then saved as a file.



Add devices to DEP

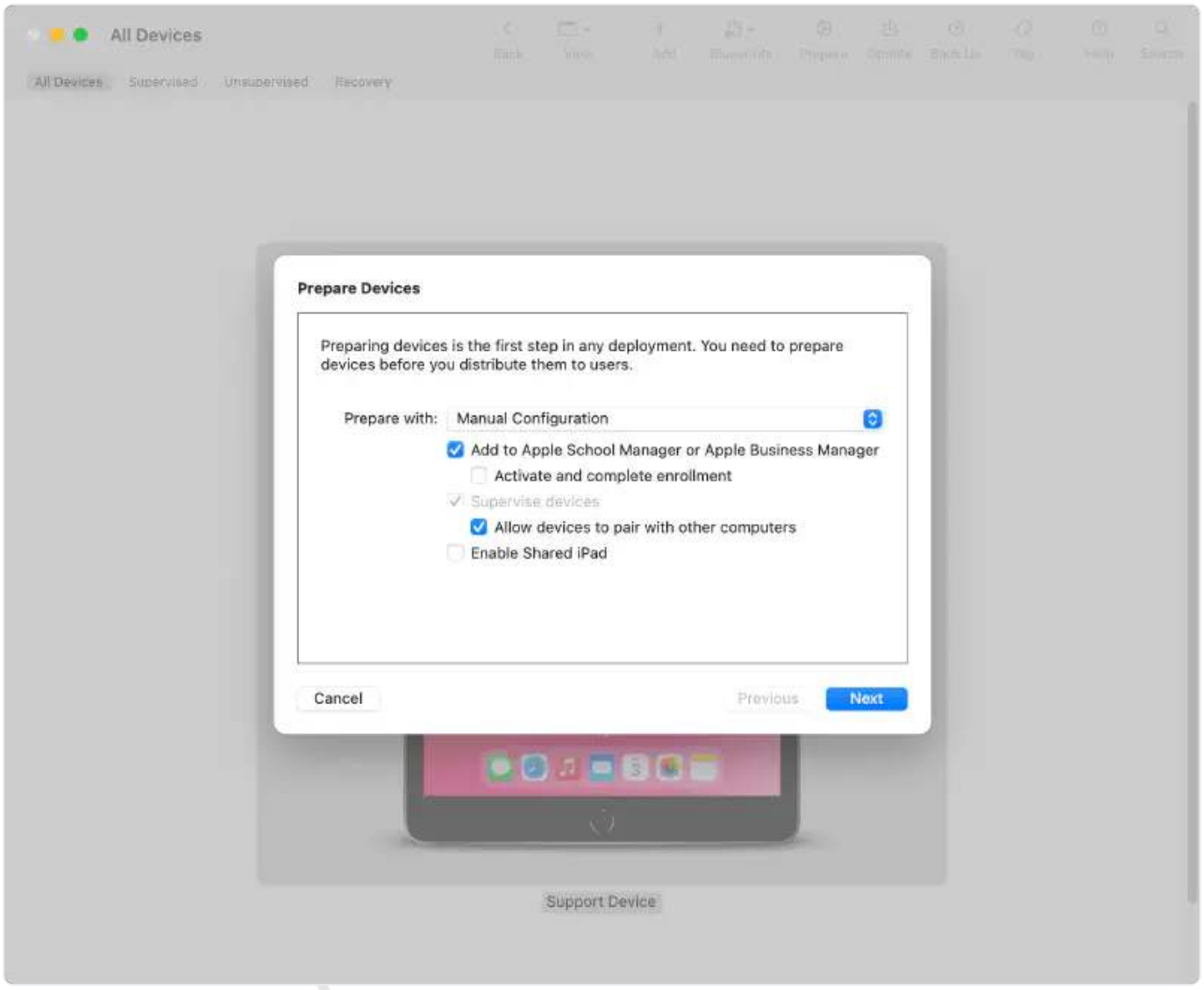
The Apple devices have to be connected with a USB cable to a Mac computer, on which the `Apple Configurator 2` is started afterwards. The following dialog appears:



Select the displayed device with the right mouse button and click `Prepare...`. In the next step, the following options must be selected:

- Add to Apple School Manager or Apple Business Manager (educational/corporate).
- Allow devices to pair with other computers.

> The activate and complete enrollment option must not be selected, otherwise the device will directly try to enroll. However, this requires further configuration in Apple School/Business Manager and Relution after adding to DEP.

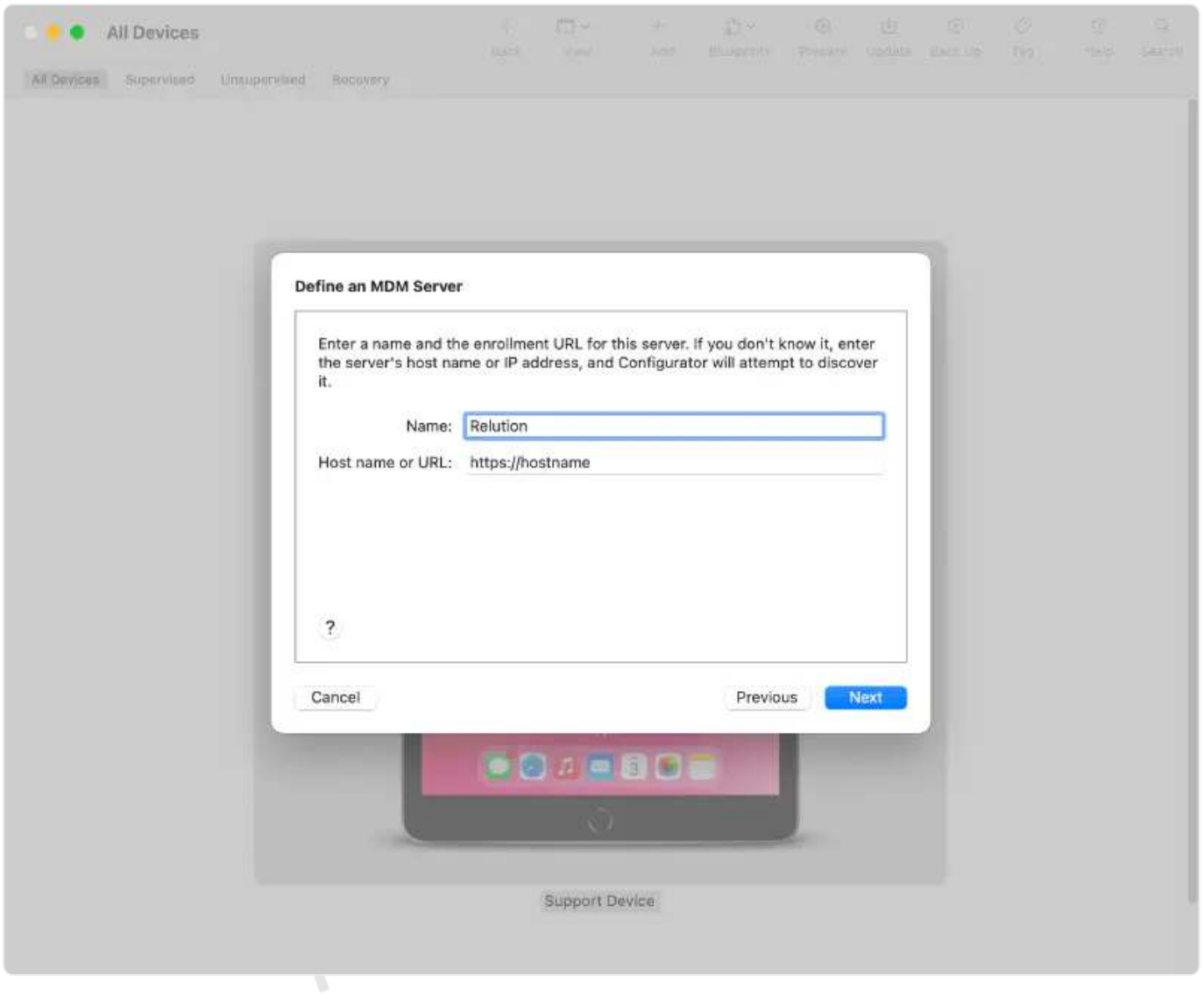


In the next step select `New Server...` and click `Next`.

Now specify the name and URL of the corresponding Relution Server. The name can be chosen arbitrarily. The URL starts with `https://` and is for example for the Relution live system:

- For iOS devices `https://live.relution.io/`
- For tvOS devices `https://live.relution.io/api/enrollment/v1/appleMdm/depenroll`.

This only works if the devices are to be managed on the Relution test system.

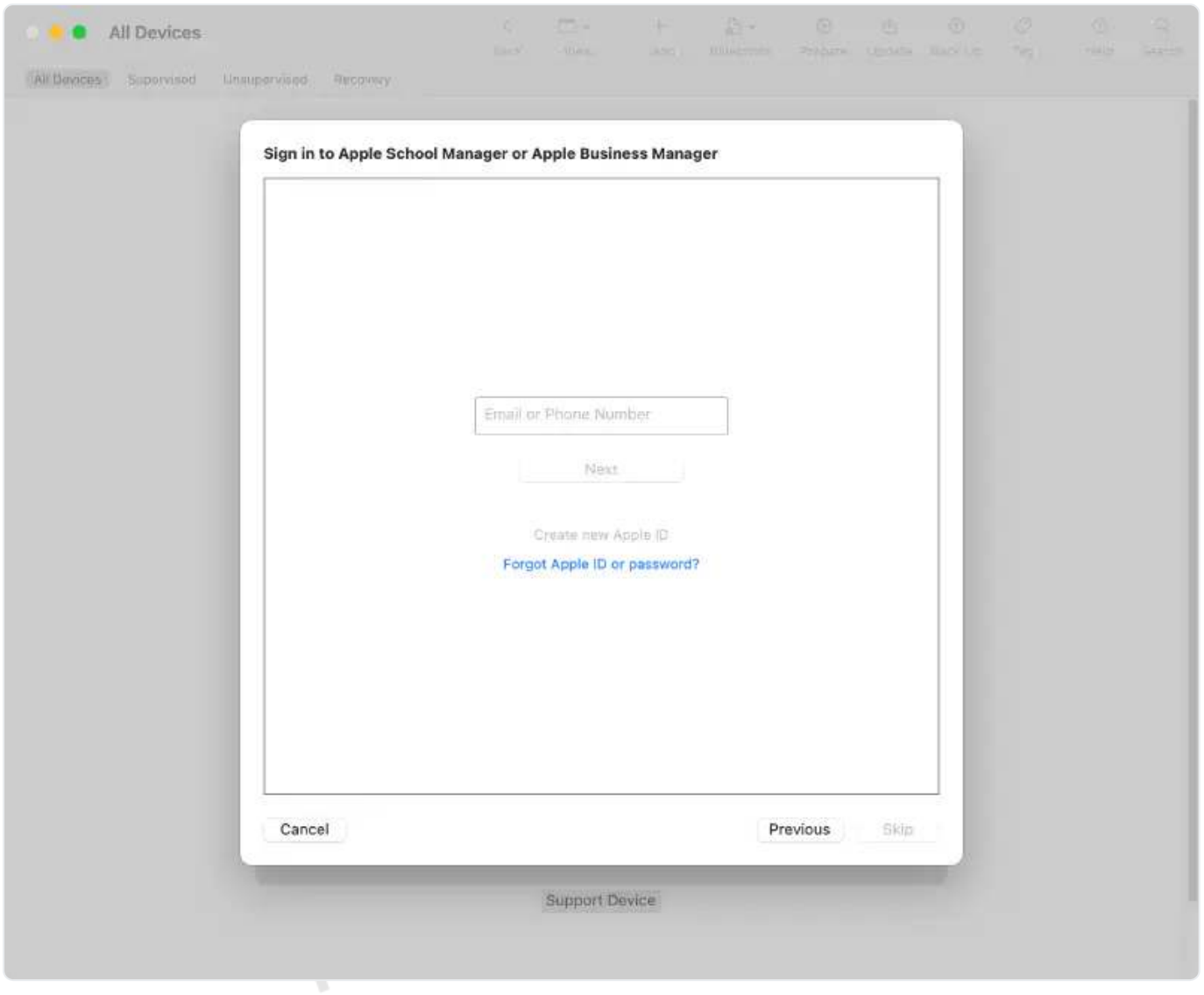


Then, the next step is to select the displayed certificate. If there are several certificates, the first one is selected.

With this the server, is defined and stored in the `Apple Configurator 2`. The information is available again for adding further devices to the `Device Enrollment Program` at a later time.

Now, in the following dialogue `New Organization...` is selected and confirmed with `Next`.

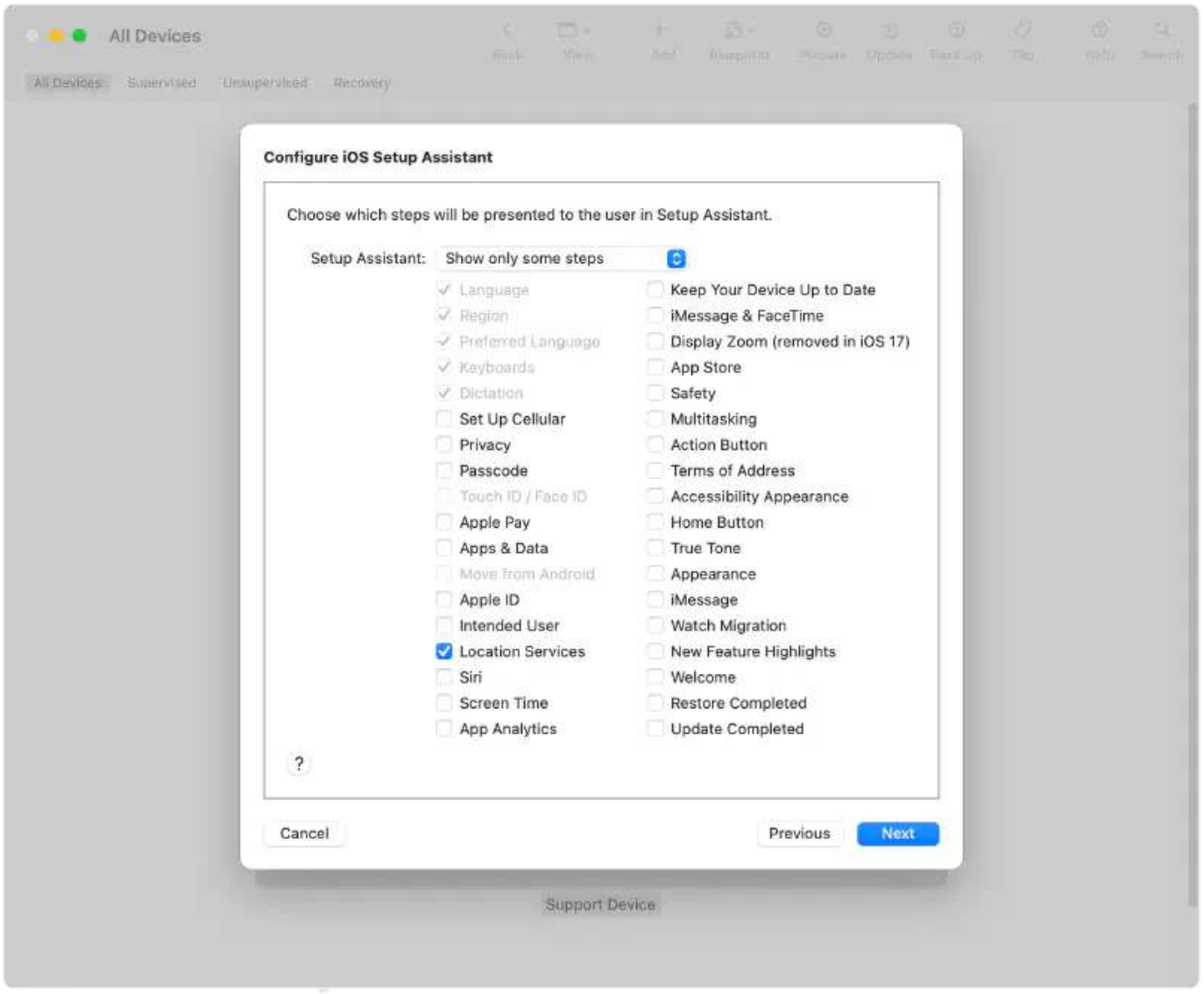
The next step is to connect to the Apple DEP server. For this purpose, the Apple ID and password of the respective Apple School / Business Manager account are entered.



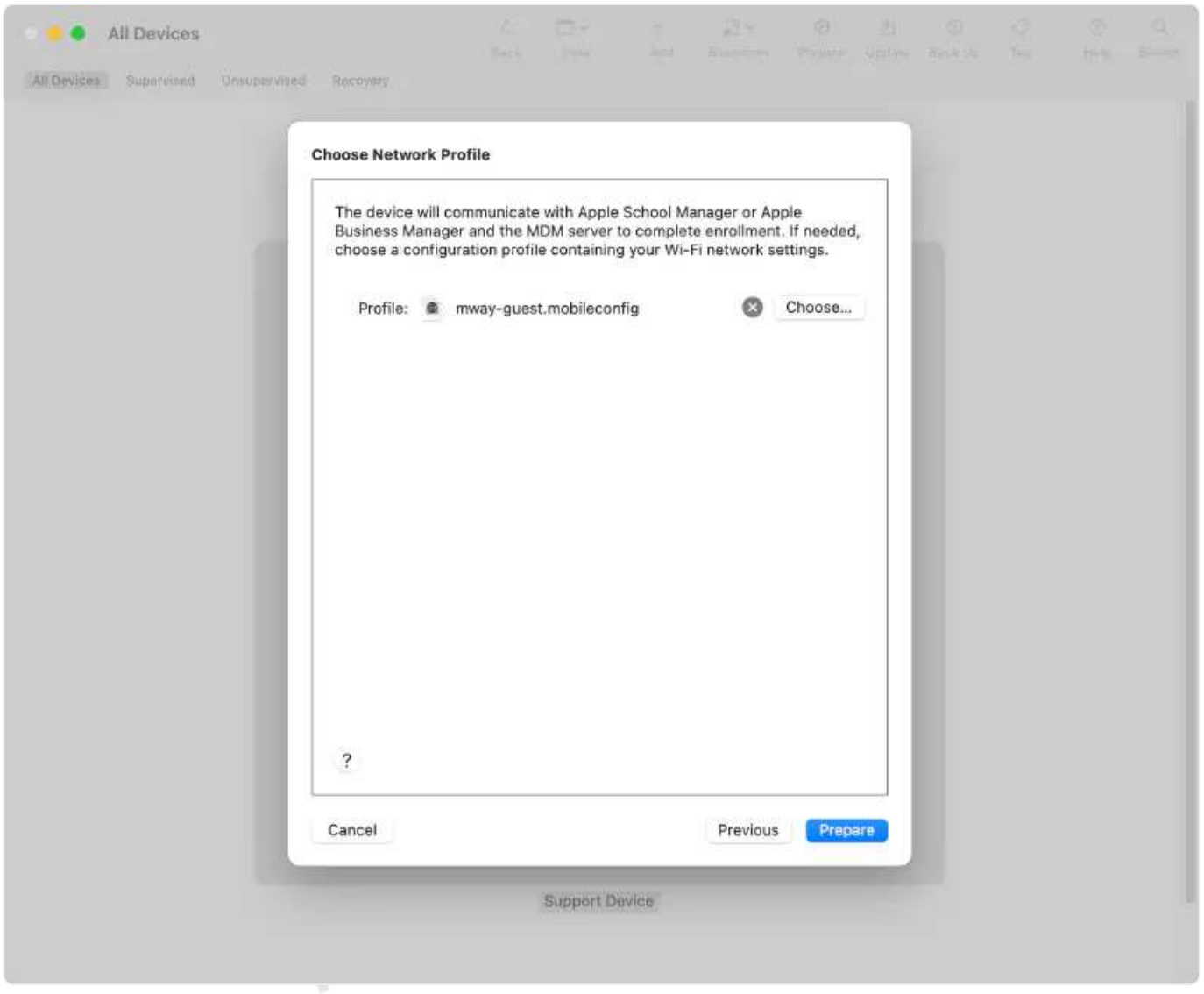
If necessary, this login has to be confirmed via two-factor authentication (entering a four-digit code sent via SMS).

Now select `Create new caregiver identity` and confirm with `Next`. The organization data is also saved by `Apple Configurator 2`, so that it can be reused later and no new organization needs to be created.

Afterwards, the setup steps that should not be skipped when setting up the devices are selected in the next dialog. The option `Location Services` should be selected, otherwise the Apple device will not be assigned to the correct time zone.

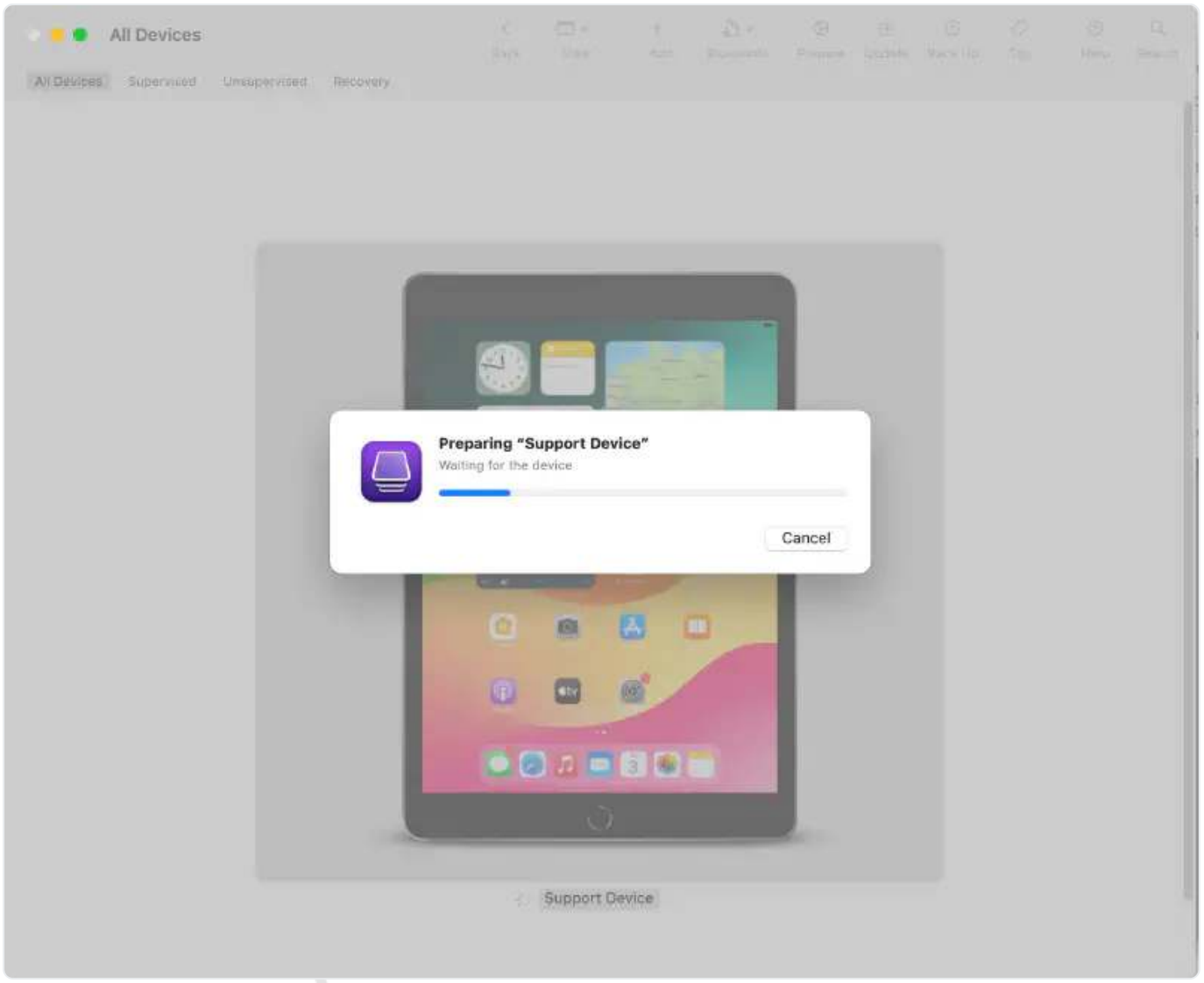


Next, select a WiFi configuration profile that was previously created in `Apple Configurator 2` via `File` → `New Profile`. This profile will be automatically adopted by the device after reboot and will directly establish an Internet connection.



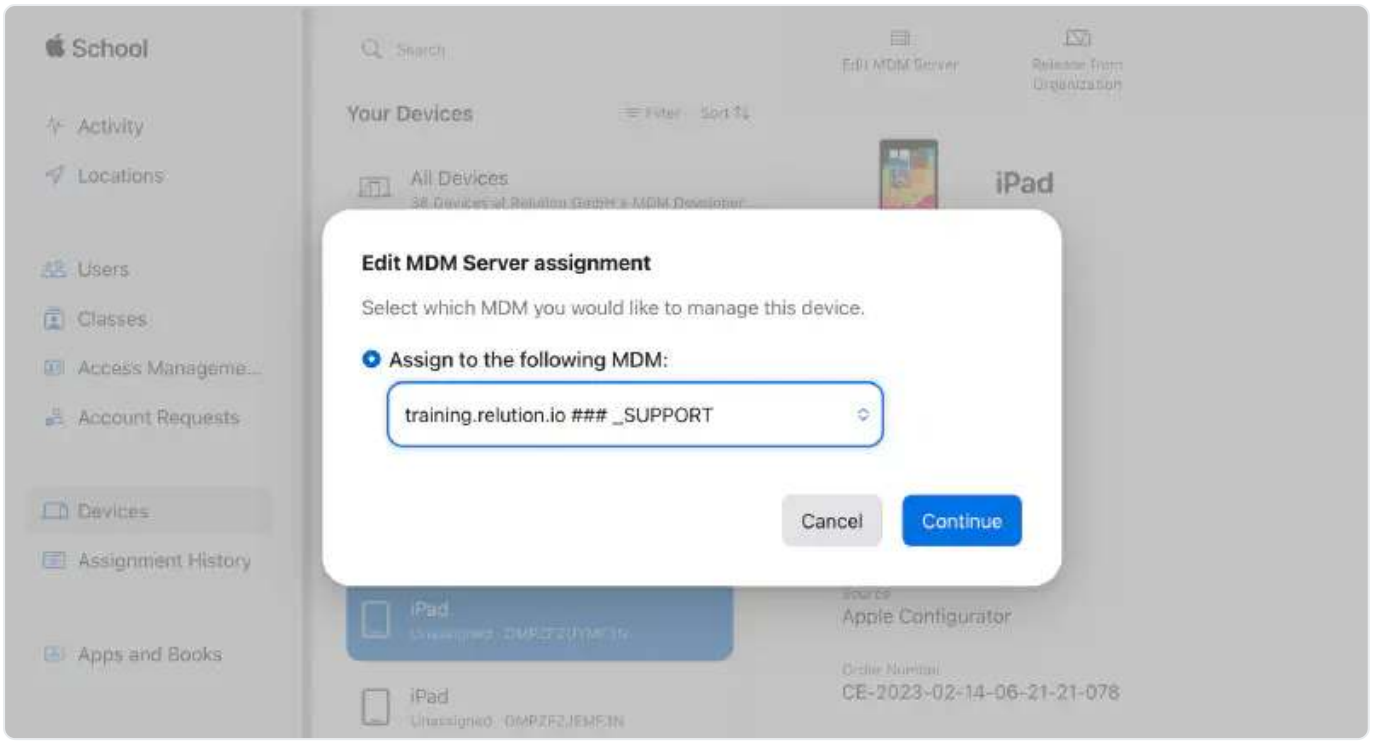
This allows the Apple device to transfer the subsequent registration for DEP to the Apple servers. As an alternative to the WiFi profile, the Internet connection from the Mac computer can also be shared with the connected device via the USB connection. If no profile is selected, the WiFi settings are entered manually when the devices are restarted. Click on `Prepare` to reboot the device. It is automatically enrolled into the DEP and then manually assigned to the appropriate Relution MDM server in Apple School/Business Manager.

By default, devices are assigned to Apple Configurator 2 via this path.



Settings in Apple School and Business Manager

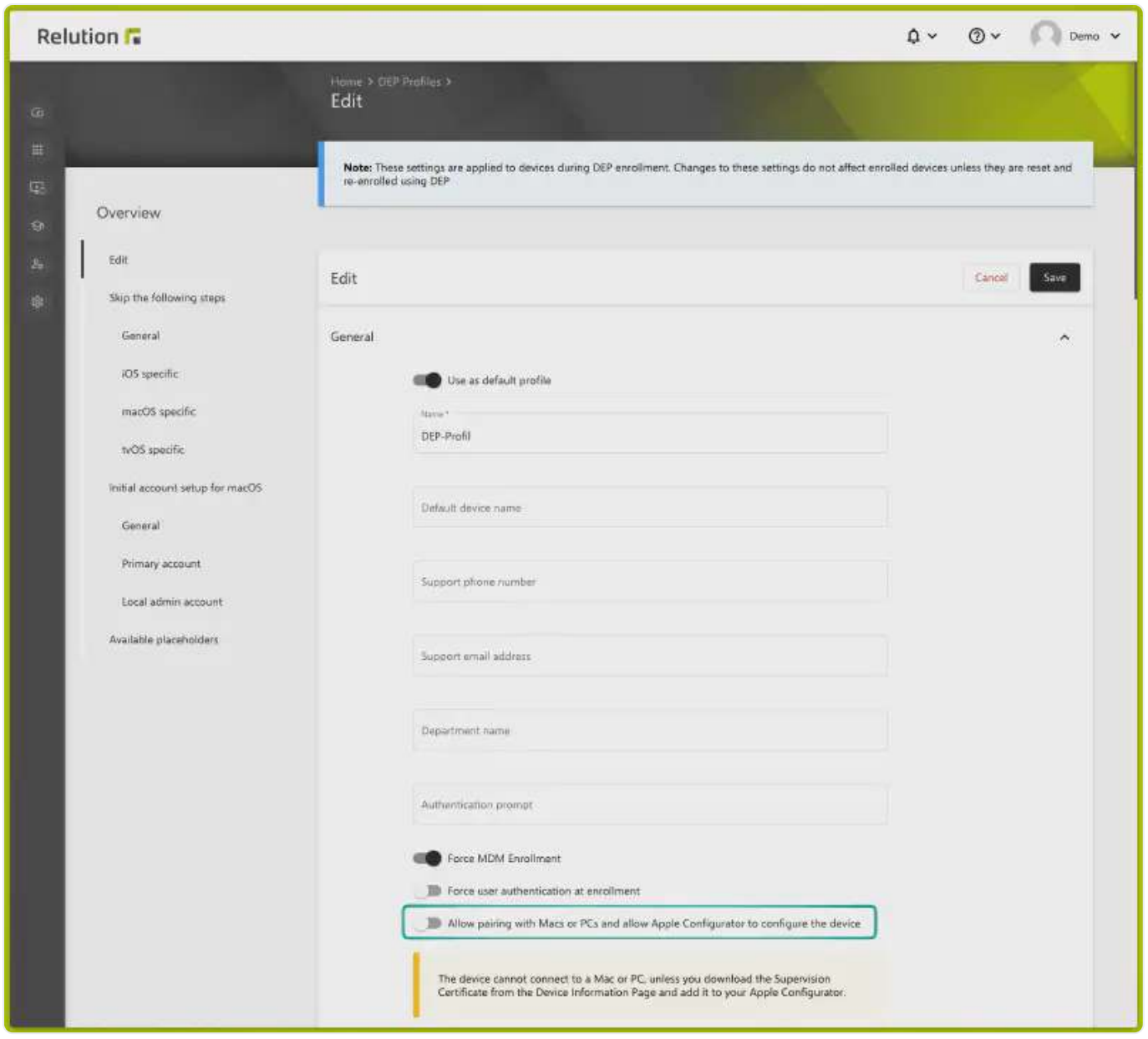
After manually adding Apple devices in DEP, they must be assigned to the desired MDM server in Apple School / Business Manager. Alternatively, a setting can be configured in Apple School / Business Manager, whereby new devices are automatically assigned to a defined MDM server. All configuration options are described in Apple's online documentation.



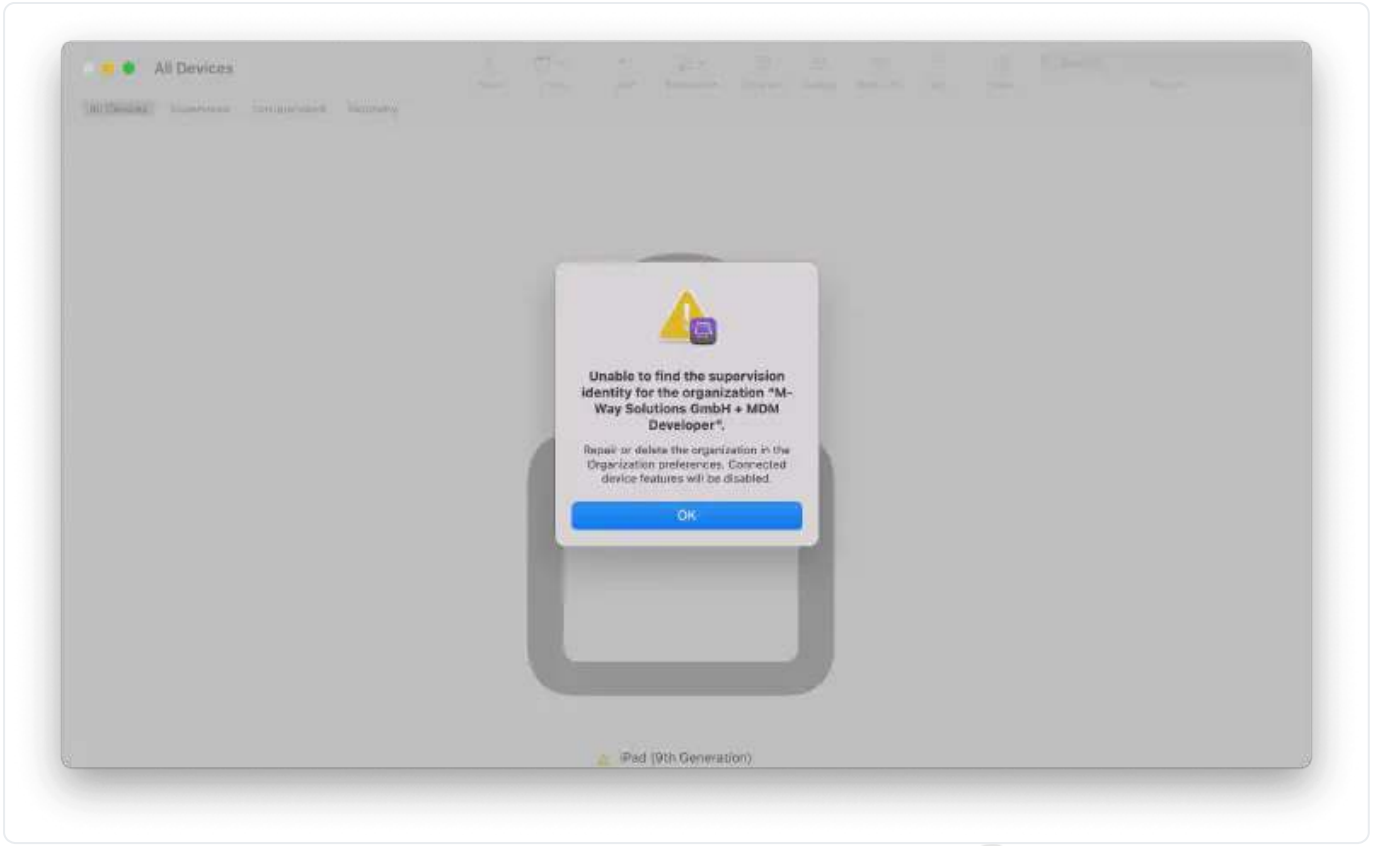
Supervision Certificate

For version 26.4.0

To protect DEP devices and prevent unauthorized access, Relution allows the setting “Allow connecting to Macs or PCs and configuring with Apple Configurator” to be disabled in the DEP profile. This prevents the Apple device from connecting to a Mac or PC and subsequently configuring the device using Apple Configurator. For example, this prevents users from removing the MDM profile. This configuration cannot be changed without resetting the device.



What should be considered when using this setting? In some cases, blocking access via a Mac or PC can prevent the administrator from manually resetting a device from a computer. This can occur, for example, if the Wi-Fi settings are incorrectly configured or the MDM server malfunctions. The device is then no longer accessible via Relution and cannot be managed or reset. This is also known as a lock-in effect.



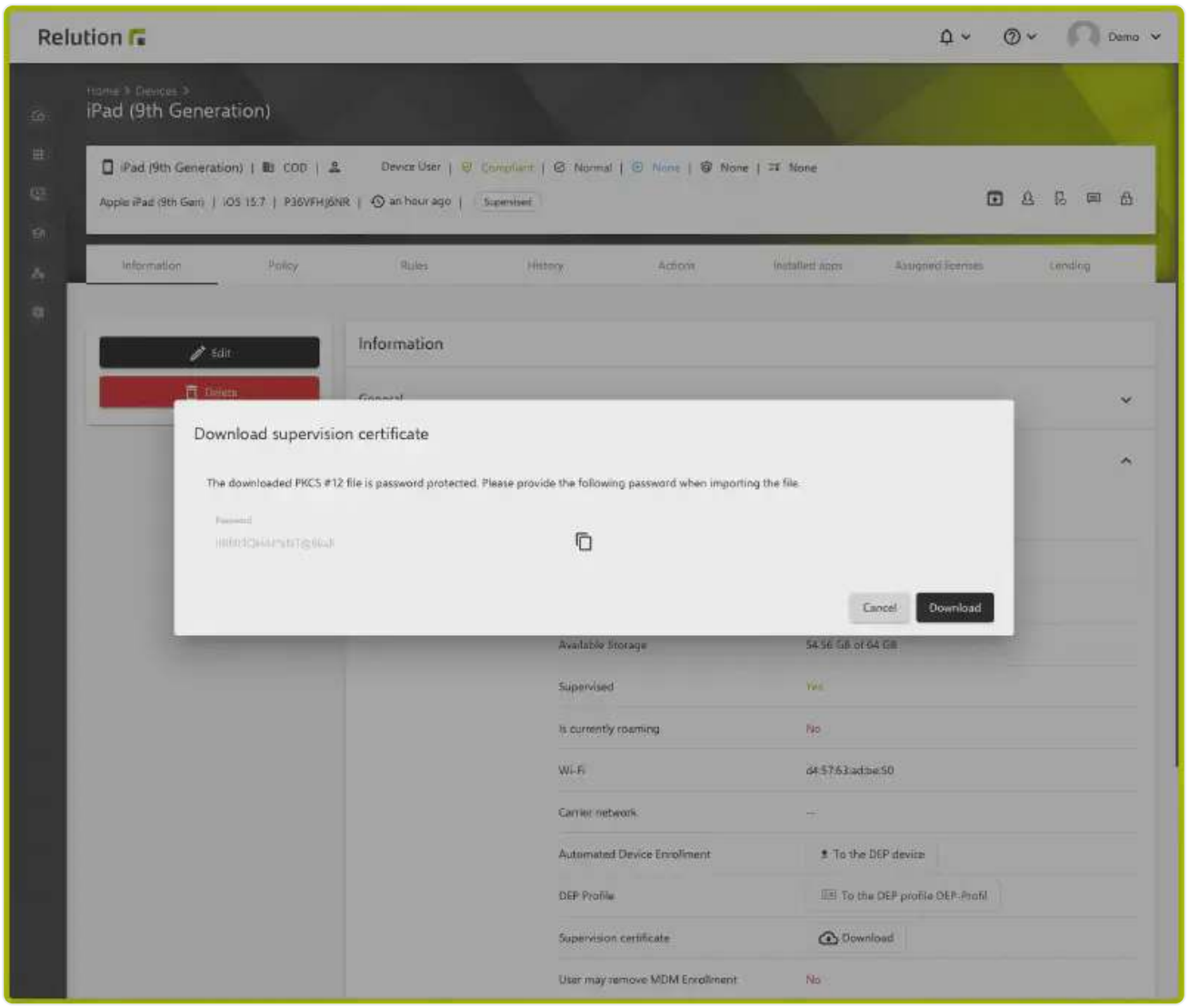
For version 26.4.0

How can authorized access be ensured with Relution? With server version 5.13, Relution allows connections to Macs or PCs, even if this is prohibited by the DEP profile. When enrolling DEP devices in Relution, a supervision certificate is automatically generated. Using this certificate, the administrator can connect the device to a Mac or PC despite the restriction. To do this, the certificate is downloaded from Relution and initially specified once when connecting via Apple Configurator. The certificate is then available for download in the device details. Afterward, the device can be accessed again.

With Relution, the device can be accessed again. What needs to be considered when unlocking the device?

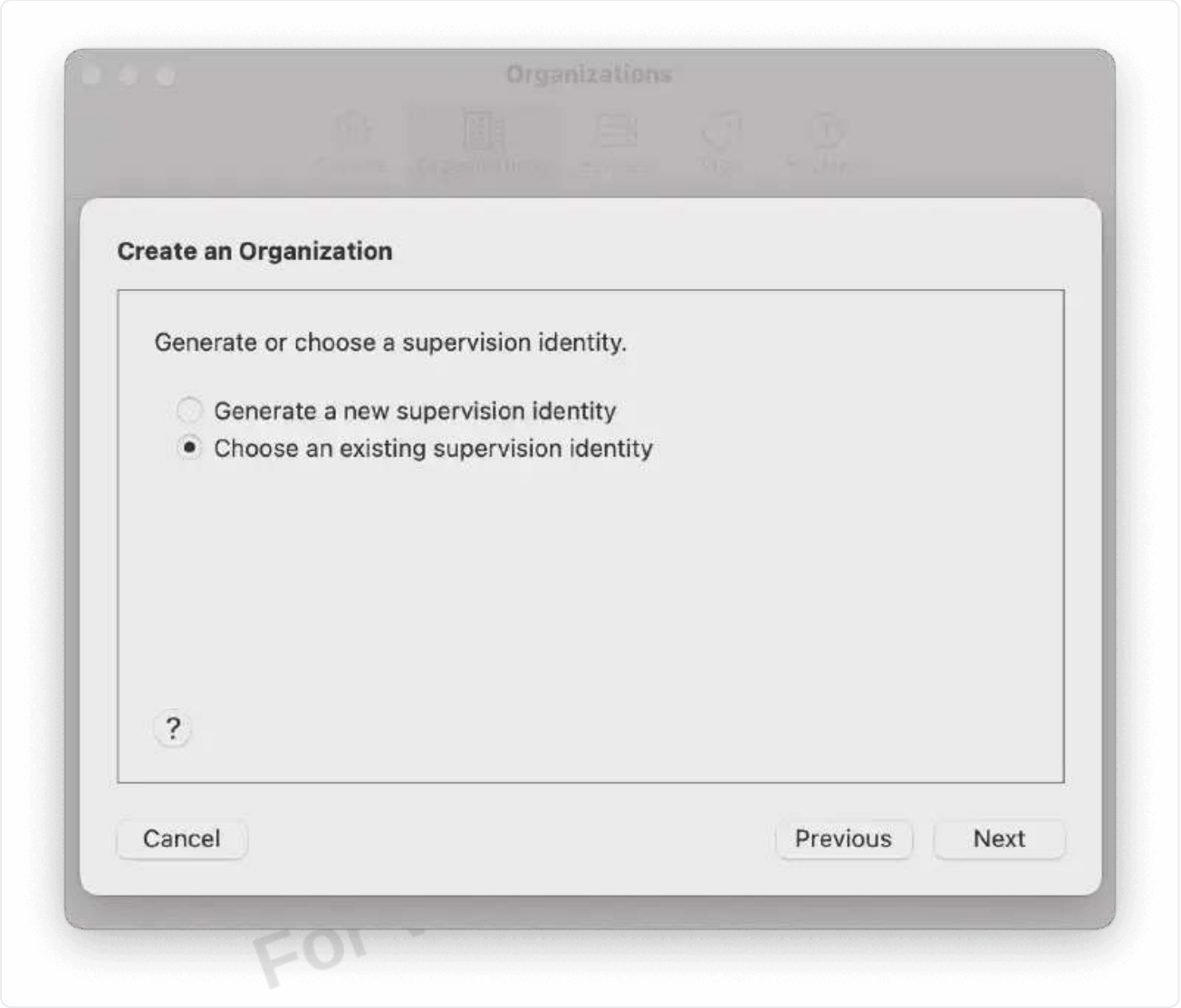
The following describes the unlocking process using Apple Configurator:

1. Download the supervision certificate and copy the password.



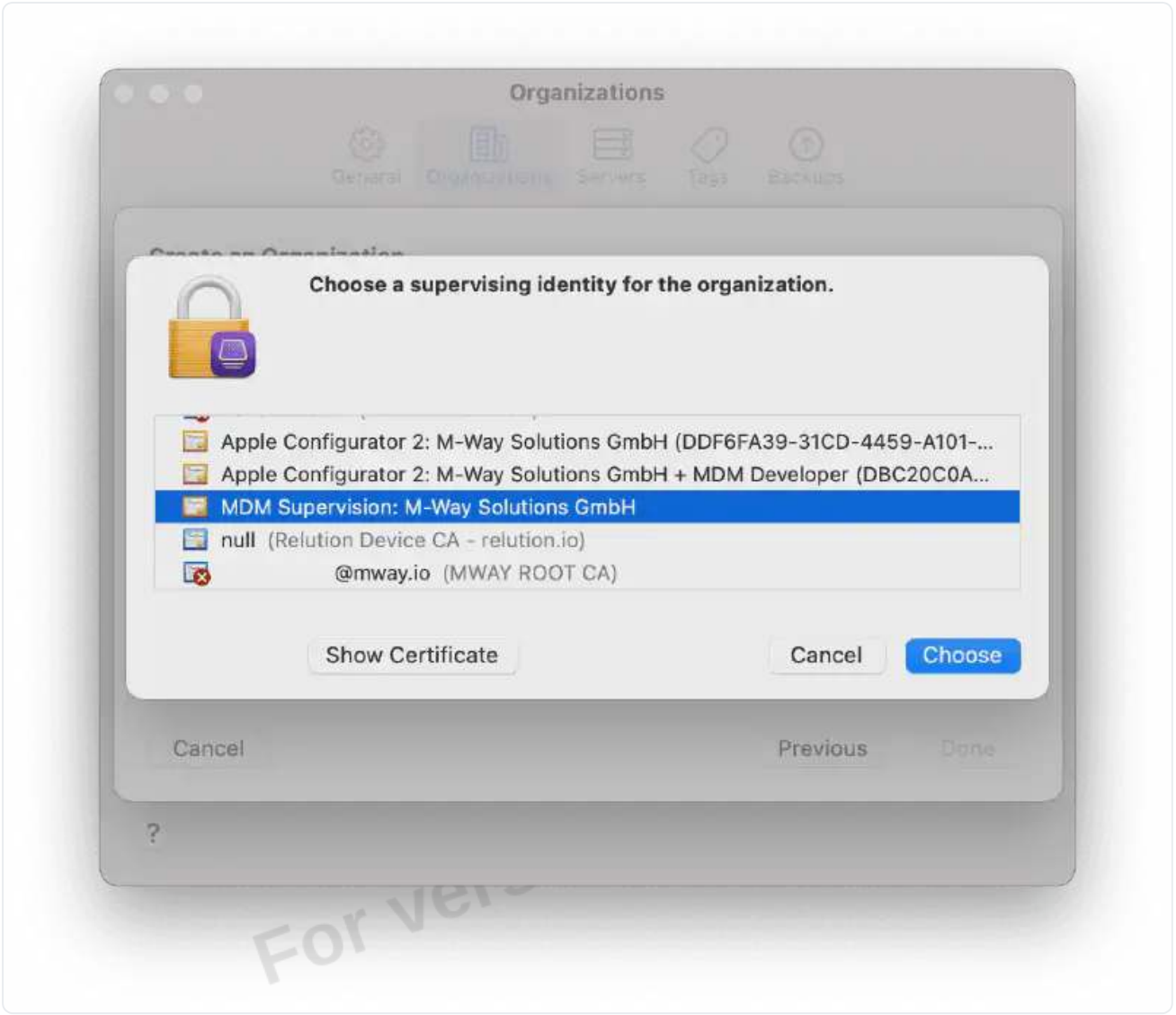
2. Create a new organization in Apple Configurator settings and enter the Apple ID and verification code.

3. Select the existing supervisor identity and click Next.

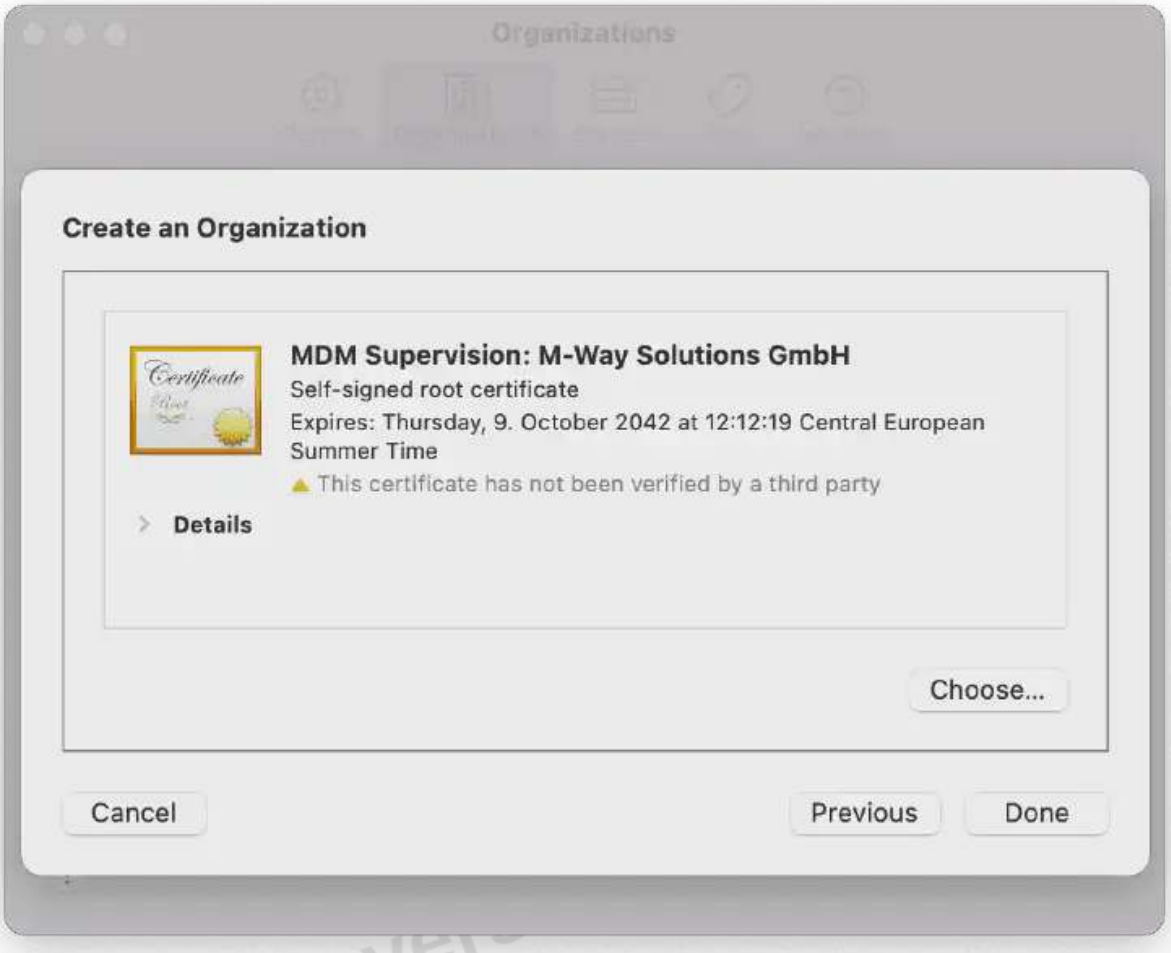


4. Then, open the downloaded supervision certificate on the computer using the password from Relution. The Keychain containing the certificate opens.

5. The certificate then appears in the Apple Configurator dialog under Supervisor Identities for selection.

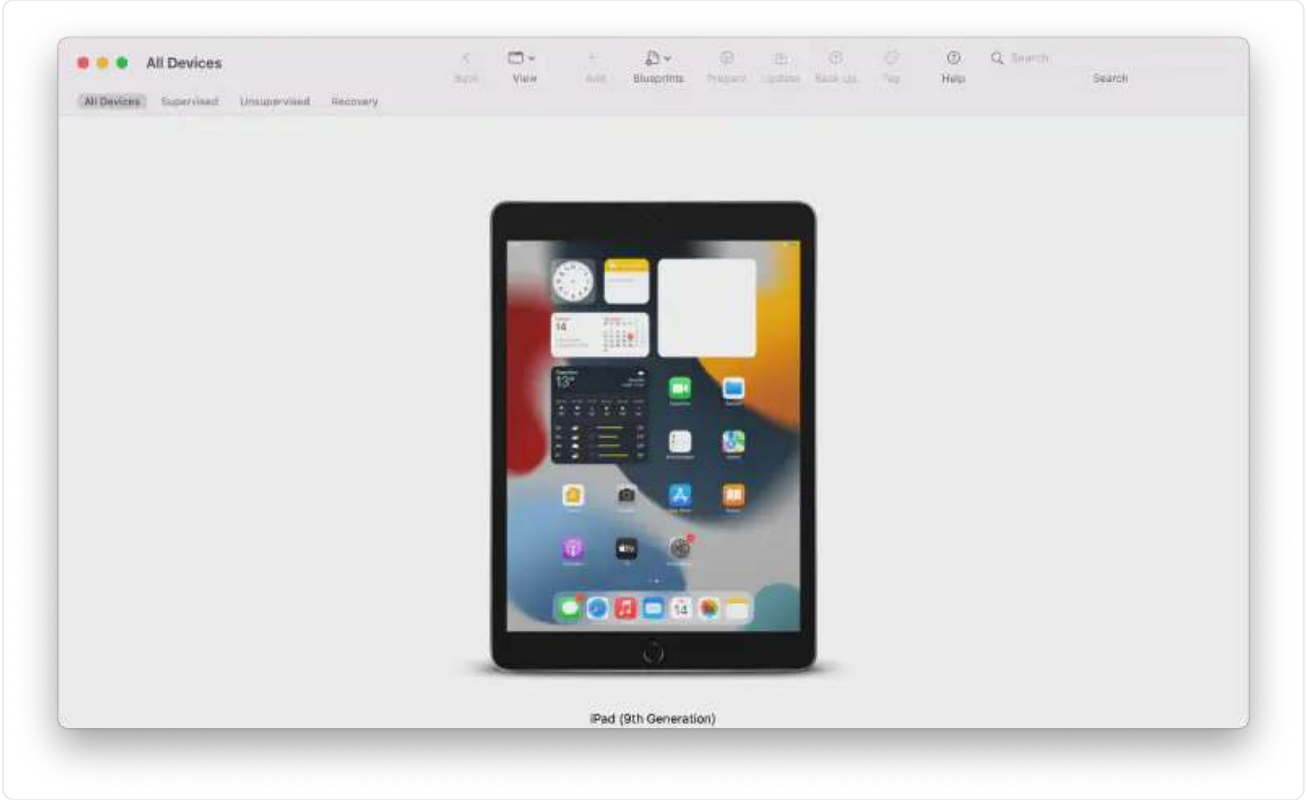


6. Create an organization.



For ver

7. The device is now unlocked and can be managed via Apple Configurator.



What should be considered when using the supervision certificate? The certificate is only generated when DEP devices are newly enrolled. During DEP enrollment, the certificate is automatically created and installed on the device. This functionality does not apply to already enrolled devices, and no certificate is generated for existing devices.

For version 26.4.0

Remove Supervised Mode

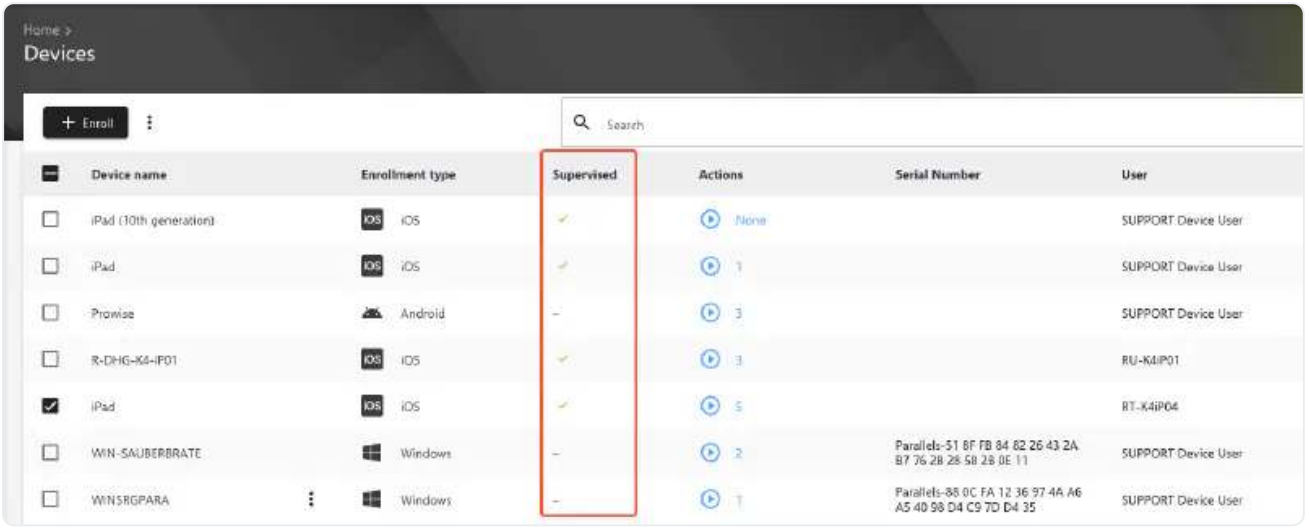
Every now and then, it may be necessary to revoke this mode from Apple devices that are running in `Supervised Mode`.

> For iOS and tvOS devices, this state can be reversed. macOS devices, on the other hand, can only be operated in `Supervised Mode` as of version 11.

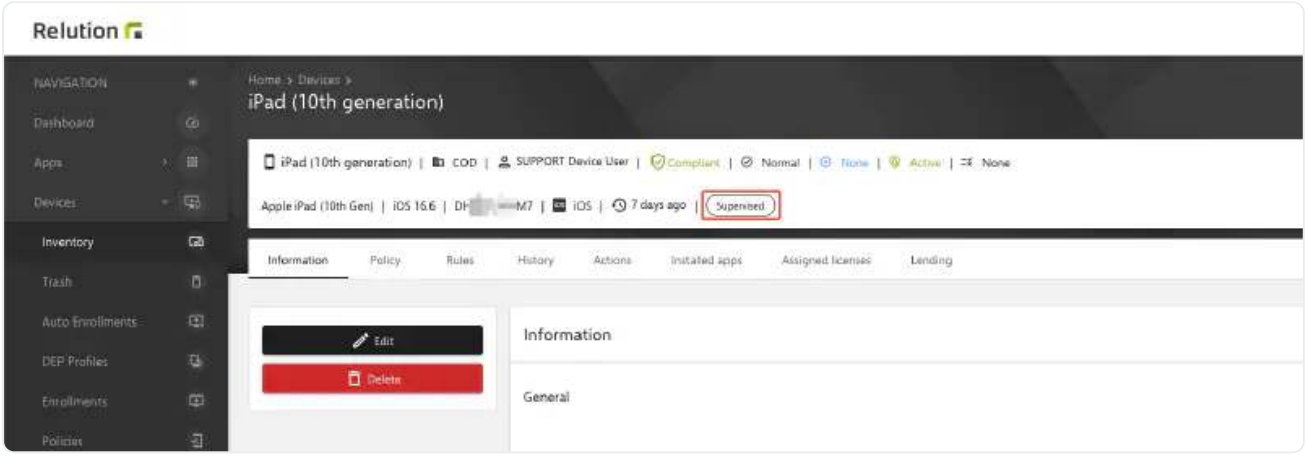
Identify monitored devices

Monitored devices can be located as follows:

1. Show the column `Will be monitored` in the inventory. The corresponding devices are marked with a check mark.



2. In the device details, the status can be seen by the corresponding badge `Will be supervised` in the infobox.



Devices enrolled via Apple Configurator

> This operation will also remove the MDM profile from the devices and they cannot be managed afterwards without re-enrolling them. In addition, all apps and data will be removed from the devices.

Reset the devices using one of the following options:

1. Send a “factory reset device” action to the devices.
2. Go to device settings under `General` → `Transfer/Reset iPad` → `Erase All Content & Settings`.
3. Connect devices to Mac computer and open `Apple Configurator 2` application. Right click on devices and select `Advanced` and there select `Erase All Content & Settings`.

It is possible that end users are not allowed to perform a `Factory Reset` on the devices as it has been prohibited in the restrictions.

DEP devices enrolled through Apple School/ Business Manager via authorized reseller

If devices have been added to the MDM system via Apple School / Business Manager, the link must be undone there, otherwise the devices will always automatically report back to the MDM system after a `Factory Reset` and get `Supervised Mode`.

1. Log in to Apple School / Business Manager and click on `Devices`.
2. Select the appropriate device and click on `Edit Device Assignment` on the right hand side.
3. Click on `Unassign`.
4. Reset the device to factory settings.

For version 26.4.0

DEP devices added later via Apple Configurator

Removing `Supervised Mode` from devices added to Apple School / Business Manager via `Apple Configurator` works in the same way as enrolled DEP devices via an authorized reseller.

However, end users can manually remove the MDM profile on the devices within the first 30 days of adding the devices to DEP. This will result in the loss of MDM enrollment as well as Monitored Mode.

Overview

Optimize the management of your iOS devices with Relution's versatile actions.

Relution offers a variety of actions that can be performed on iOS devices to optimize device management. These actions enable efficient device control, enhance security, and improve workflows. The following overview describes the available actions and provides examples to illustrate their benefits.

For version 26.4.0

The following actions can be performed on iOS devices

Action	Description
Add shortcut →	Adds a shortcut to a website.
Alert	Sounds an audible alert on the device, even in silent mode.
Clear restrictions password	Clear the restrictions password and the restrictions.
Continue in device setup assistent	Informs the device that the pre-configuration is completed and it can proceed the Setup Assistent.
Delete local users	Removes local user accounts.
Deploy an app from the Apple App Store →	Installs apps directly from the Apple App Store.
Deploy Relution Store App →	Install an app from the Relution App Store.
Enable Lost Mode →	Enables Lost Mode with lock screen and location.
Disable Lost Mode	Unlocks the device.
Enable or disable Bluetooth	Enables or disables the Bluetooth function.
Enable or disable personal hotspot	Activates the hotspot on the device.
eSIM Cellular plan	Updates the eSIM's Cellular plan.
Install Media →	Installs media on the device.
Install update	Installs an OS update if available.
Locate device	Fetches the current location of the device.
Lock device	Locks the device with the current password.
Log out user	Forces the current user to log out.
Reboot device	Reboots the iOS device.
Refresh device info	Synchronises the device information with Relution.
Remove app	Uninstalls a selected app from the device.
Remove Media →	Removes deployed media (PDF, ePub).
Remove Shortcut →	Removes a shortcut from the device home screen.
Request mirroring	Enables wireless screen transmission to compatible display devices.

Action	Description
Reset lock code	Reset the user's password.
Return to Service →	The device is reset to factory settings and then automatically put back into operation without user intervention.
Send Message	Displays a text message on the device.
Set default apps	Set default apps for calling, messaging and web browsing.
Shutdown device	The device will shutdown.
Stop mirroring	Stops the current AirPlay transmission.
Update MDM Profile	Updates the MDM profile on the device.
Wipe Device	Deletes all data and resets the device.
Conditional Access →	Requires setting up conditional access on the device via the Relution Agent to be able to use protected resources.
Data Roaming →	Enables or disables data roaming.

For version 26.4.0

App Installation

Relution offers several ways to install apps on devices, depending on the managed platform.

1. Installation via `action`.
2. Installation via policy configuration.
3. Installation via `auto-deployments`.

Each of these ways has features that can be useful in certain use cases.

Installation by action

On devices managed in Relution, apps can be installed via `Action`. To do this, switch to the `Actions` tab in the device details and click on the `Apply Action` button there. Here, depending on the operating system, select the options `Install app from Play Store` (`Android Enterprise`) or `Install app` (all other platforms).

Then select the app to install and click on `Next`.

A new `Action` will be created in the action overview and the installation will be started as soon as it has been delivered to the corresponding device.

For version 26.4.0

Installation via policy configuration

Installing apps via policy configuration is a more sensible approach for a larger number of apps and devices than doing this via actions individually.

Please refer to the individual chapters of the platform policies to learn how this works.

App compliance iOS →
App compliance tvOS →
Manage apps Android Enterprise →

Installation via auto-deployment

`Auto-Deployments` are user-specific app installations that are dependent with the user accounts and groups associated with the devices. This allows certain apps to be installed on devices as soon as the corresponding user log in to them.

> Auto-deployments can conflict with an app conformance. If an app conformance prohibits the use of a particular app, but it is stored in a user or group level auto-deployment, it will not be available to the corresponding user.

The settings for `Auto Deployments` can each be found in the following places in the Relution portal:

User or group details

At the bottom of a detail page of a user or a group, corresponding apps can be deployed user- or group-specific.

App details

At the bottom of an app detail page, corresponding user or groups can be deposited.

Data Roaming

Control data roaming on iOS devices directly through Relution.

With Relution 26.2, administrators have the ability to enable or disable data roaming on iOS devices.
This feature can also be executed as a direct action on the device.

> This setting can be disabled by the user on the device.

For version 26.4.0

Return to Service

With iOS 17+ and Relution Server version 5.20 it is possible to trigger a `Return to Service` action on iOS devices. This action resets the device to factory settings. The device will try to log in again automatically after the reset. This eliminates the otherwise repetitive steps such as WLAN entry and setup steps that are enabled as not skipped in the DEP profile.

> The user must disable all activation locks for this feature to work correctly.

Prerequisite

1. the target device must be an iOS 17+ device enrolled in Relution with a DEP profile.
2. the Relution server must be at least version 5.20+.
3. a policy with a WLAN configuration must be specified.

Execute action Return to Service

To do this, the menu item ‘Apply Action’ must be selected for the desired device in the inventory.

The action can be found and selected via the search.

In the next step the policy with the WLAN configuration is selected. For eSIM there is the option ‘Keep existing data tariff’.

Finally there is a last feedback to execute the action.

For version 26.4.0

Lost Mode and Device Tracking

Lost Mode can be used to lock an iPhone or iPad to ensure that no one can access personal data. The mode makes it possible to configure a message for the device stating that the device has been lost, along with contact details for getting in touch. In addition, the device's current location can be displayed on a map. This provides an additional option for retrieving the device if it is lost.

> The Lost Mode and location tracking require an internet connection on the device.

One-time application

To lock or locate a device, it must be selected in the `Device inventory` in Relution. In the `Actions` tab, select the option `Lost Mode`. Information about the contact that will be displayed on the lock screen can be entered here.

In addition, the device can be located. To do this, another action must be triggered `Locate device`. After the action has been performed, the Relution web page must be reloaded by pressing the keyboard shortcut `CTRL+R` (Windows) or `CMD+R` (Mac). This will display the `Location` tab next to the `Actions` and show the location on a map.

For version 26.4.0

Permanent application

It is also possible to permanently activate Lost Mode for DEP devices, especially if the device is stolen. The advantage of this is that devices that are reset and put into operation are automatically placed in Lost Mode as soon as they are connected to the Internet. This can be activated permanently for the device via the Relution portal under `Devices` > `Auto-Enrollments` > `Affected Device` > `Activate Lost Mode` > `Save`.

Hint

- To limit potential misuse, Relution from version 5.31.0 onwards offers the ability to adjust a location permission.

Lock MDM profile

Apple DEP automatic device enrollment enables organizations to automatically enroll Apple devices in an MDM solution. The configuration profile associated with devices during DEP enrollment allows configurations to be deployed directly at startup. Continuous device management is therefore only possible as long as the MDM profile remains locked on the devices. If users manually remove the MDM profile from devices, administrators can no longer manage those devices. Therefore, the MDM profile can be locked on the devices so that end users cannot remove it from the devices.

Lock MDM profile

Edit or create DEP profile in Relution portal under `Home` → `Devices` → `DEP profiles` > `Create / edit`.

Here, the option `Users may remove MDM enrollment` can be disabled.

Set DEP profile as default

DEP profiles can be set as default for all future devices. New enrollments will then automatically assign the selected DEP profile.

Assign a DEP profile to already enrolled devices

A DEP profile can be subsequently assigned and synchronized for already existing devices.

> Changes to the DEP profile do not automatically affect devices that have already been enrolled. For this, the affected devices must be reset and re-enrolled.

For version 26.4.0

SFTP Upload

Relution can be used to create Managed Apple IDs in large numbers.
This is possible via the Relution Portal in the settings and makes it easier for schools and school authorities to automatically configure these IDs so that they can be made available to students and teachers.
This process also automatically migrates classes created in Relution to classes in Apple School Manager.

Requirements

- Allow port 22 outbound to the Apple servers, especially for the URL: `upload.appleschoolcontent.com`
- An Apple School Manager
- An Education license in Relution
- At least one verified domain in Apple School Manager (reserve addresses from Apple are not possible)
- A class in Relution with at least one teacher and one student user
- The teachers must be part of the `Teacher` system group, and the students must be part of the `Student` system group

Configuration

For Version 26.4.0

- Open the Relution portal and Apple School Manager.
- Navigate to the following point in Relution: `Settings` → `Education` → `Apple School Manager SFTP Upload`
- Continue in the setup wizard until the server URL, user, and password can be entered.
- In School Manager, navigate to the following point: in the bottom left corner, click the `User` menu → `Settings` → `Managed Apple Accounts` → `Start the first steps of linking directory synchronization`.
- Click `Create new accounts`
- Click `Use CSV file in Apple format`
- At step 1, `Set up SFTP`
- Copy the values and enter them into the fields in Relution, then click `Next`.
- Enter the verified domain from Apple School Manager and continue navigating.
- Click `Synchronize data`
- Click `Next` in Apple School Manager and wait for the import.

The IDs will now be displayed and can be checked for errors here. In the next step, the structure of the Apple IDs can be specified.

e.g.:

- Students: `(First Name + Last Name)@relution.io`
- Teachers: `(First Letter of First Name + Last Name)@relution.io`

Location

The SFTP upload creates a new location in Apple School Manager for each Relution organization that uses SFTP upload. The name of this location is the same as the unique name of the respective Relution organization.

For example:

- Organization Name: `User-Import-Test`
- Unique Name of the Organization: `UIT`
- New Location in ASM: `UIT`

If the location in Apple School Manager used for purchasing apps and already exists has the same name, this can cause problems.
Please discuss this with the server operator or partner beforehand.

Disconnecting

Never disconnect the SFTP upload connection if the IDs are still actively in use and additional IDs are to be created in the future. If disconnected, all IDs created via SFTP upload will be changed to the source Manually from SFTP.
Reconnecting afterward may result in duplicate Apple IDs. Since Relution version 5.26 also introduced user import, this can create a vicious cycle.

For version 26.4.0

Overview

A policy is a collection of one or more configurations. Each policy can be applied to one or more devices at the same time. In addition, one or more policies can be associated with each device.

For version 26.4.0

Available configurations

Configuration	Description
Managed Domains →	Define managed email or web domains
AirPlay	Management of wireless content streaming to AirPlay-enabled receiver devices
AirPrint →	Management of AirPrint printer settings
App Compliance →	Management of app-specific restrictions
App to VPN Mapping →	Configuration of the VPN used by individual apps
Apple Configurator 2 Configuration →	Apply a configuration profile (mobileconfig) created using Apple Configurator 2 to devices.
Audio Accessory Settings →	Centrally configure and manage temporary pairing of audio accessories
Notifications →	Configure notification settings for apps
DNS Proxy	DNS Proxy configuration
DNS Encryption Settings	Configure DNS encryption settings
Email	Add email configurations for multiple users
Apple Watch Enrollment →	Enables enrollment of a paired Apple Watch through a managed iPhone
Shared iPad Settings	Configure settings for shared iPad devices
Single App Mode →	Limit devices to a single app
Extensible Single Sign-On →	Configure an app extension that performs Single Sign-On
Exchange →	Management of Exchange accounts
External Intelligence Settings →	Control external, cloud-based AI integrations via Siri and Apple Intelligence
Content Filter →	Allow or block specified URLs
Device Lock Time →	Set up a time-limited device lock
Device Settings	Configure general device settings
Device Name →	Configure the device name
Global HTTP Proxy	Configure global proxy settings
Google Account	Management of Google accounts
Wallpaper →	Manage wallpaper

Configuration	Description
Homescreen Layout →	Group apps on the homescreen by category
Intelligence Settings →	Centrally control Apple Intelligence features such as Genmoji, Image Playground, and Writing Tools
Relution Decon →	Configuration for the Relution Decon app
Calendar	Management of CalDAV calendars
Calendar Subscriptions	Manage calendar subscriptions
Contact	Management of CardDAV accounts
Managed App →	Push app configurations for managed apps
Managed Media →	Push self-created PDF or ePUB files to the device
Mathematical Settings →	Centrally configure functions and modes of the Apple Calculator app
Cellular Network	Configures settings for the cellular network
Message on Lock Screen	Configure custom text on the lock screen
Password →	Password policy for Apple devices
Relution File Shares →	Configuration of file shares for the Relution client app
Relution Shared Device →	Put devices into Shared Device mode
Restrictions →	Management of device restrictions
Safari Settings →	Centrally control the Safari browser's behavior (cookies, JavaScript, start page, etc.)
Safari Extensions →	Allow individual Safari extensions and restrict them to specific domains
SCEP	Management of SCEP settings
Fonts →	Add fonts to the device
Setup Assistant →	Hide setup steps shown after the initial setup (supervised devices only)
Siri Settings →	Centrally control Siri's behavior, including the profanity filter and access while locked
System Updates →	Manage updates of Apple devices (iOS/tvOS)
Managed Software Updates →	Enforce operating system updates, targeting a specific version by a deadline (successor to System Updates)
Keyboard Settings →	Centrally control keyboard features such as autocorrection, dictation, and spell check
VPN	Management of VPN settings
Weblink →	Add a weblink to devices

Configuration	Description
WLAN	Management of WLAN settings
Time Zone	Configuration of the time zone
Certificate	Select a certificate to be installed on the device by default

For version 26.4.0

Passcode

The Apple passcode policy defines security requirements for device passcodes on iOS devices. When a user registers a device with iOS, a system-level restriction applies: if a passcode policy is configured, iOS automatically enforces a complex passcode with at least six characters – regardless of other settings. As a result, certain configuration values may be ignored.

Still, the policy offers a wide range of options to further adapt passcode security. These include requirements for complexity, length, validity period, and the number of allowed failed attempts.

Configuration Options

- ☐ Allow simple passcodes
- ☐ Require alphanumeric passcodes
- Minimum passcode length
- Required number of special characters
- Maximum passcode age (in days)
- Inactivity timeout (in minutes): Maximum selectable value for the end user
- Passcode history
- Maximum auto-lock time (in minutes)
    - Immediately
    - 1 minute
    - 5 minutes
    - 15 minutes
    - 60 minutes
    - 4 hours
- Maximum number of failed attempts

    If the limit is exceeded, a wipe action is triggered.

For version 26.4.0

Shared iPad: Operating Modes and Passcode Behavior

Apple offers two operating modes for the Shared iPad:

Using Managed Apple IDs In this mode, the device is configured with user accounts based on Managed Apple IDs. Passcodes are assigned and managed centrally through these accounts. As of now, users cannot individually adjust the auto-lock duration in this configuration.

Using Guest Mode In this mode, users log in as a Guest without a personal account or passcode. This option is particularly suitable for environments with frequently changing users and no need for personalized data.

Please note: For a flexible setup without passcodes, Guest Mode is usually the recommended option.

Device Name

Relution allows setting the device name for iOS, iPadOS, and macOS. A policy with the `Device Name` configuration can be created and distributed to device groups.

The device name can be assigned statically, e.g. `Case iPad`, so all devices in the group receive the same name.

However, for multiple devices in a group, using placeholders might be more practical.

For example, the device name could be composed as follows: `Case ${device.model} ${user.name}` This would result in a display like: `Case iPad12,1 Max.Mustermann` making it easier to manage the inventory.

For version 26.4.0

App Conformance

The policy configuration `App Conformance` defines, which app should be available on an iOS device and which should not. In Relution, it is possible to configure `App Conformance` in two different ways.

All apps in the following list are not allowed

This is a classic `blocklist`. All apps on this list will be hidden on iOS devices and users will not be able to access them. The apps are not uninstalled. For example, individual system apps or apps from the public App Store that are not allowed to be used on the devices can be stored here.

> This list type is not compatible with Relution Shared Device. Always use the positive list (Allowlist) in combination with Relution Shared Device.

Allow all apps in the following list

This is the classic `Positive list (Allowlist)`. All apps, that are stored here can be installed on iOS devices, are subsequently visible to users and can be used.

There are three more options that can be configured:

For version 26.4.0

Add all required apps

All apps that are stored on the `Required apps` list are automatically added to the `Positive list`. This saves effort and avoids errors.

Add all auto-deploys

All apps that are stored in the `Auto Deployments` for corresponding user accounts or groups are automatically added to the `Positive List`. This saves effort and avoids errors.

Web links

- Block weblinks
  All web links are blocked - regardless of whether they were brought to the iOS devices via a policy or an action.
- Allow full screen web links.
  Only web links configured for full screen mode will be displayed.
- Allow all web links.
  All web links will be allowed. The Safari Browser is automatically enabled here.

Required Apps

All apps on this list are automatically installed and users cannot remove them from iOS devices. If an app on this list has not been installed, the corresponding device will be displayed as `non-compliant` in the device inventory. The `Relution Agent` cannot be added to this list. It is automatically installed on devices upon enrollment.

In addition, system apps should also not be included on the required apps list. They do not need to be installed as they are already on the devices. It is enough to add them to the positive list.

For version 26.4.0

Configuring SSO Login for iOS

Single Sign-On (SSO) technology enables users to log in once and seamlessly access various applications. Especially for iOS devices, the integration of Microsoft SSO offers an efficient solution for combining user-friendliness and security. It not only simplifies everyday work through simplified logins, but also reduces security risks and IT effort. This guide serves as the basis for an SSO configuration with iOS and Microsoft SSO.

Requirements

Two configurations and one app are required for this in Relution.

- `App Compliance`
- `Extensible Single Sign-On`
- `VPP App Microsoft Authenticator`

App Compliance Configuration

The Microsoft Authenticator app → must be added to the list of required apps. This includes the extension `com.microsoft.azureauthenticator.ssoextension` required for Microsoft SSO.

For Version 26.4.0

Extensible Single Sign-On Configuration

The following configuration points can be used as a minimally functional template for Microsoft SSO. Points not mentioned can be left as default. The final configuration must be adapted to the specific environment.

- Extension Identifier
  - `com.microsoft.azureauthenticator.ssoextension`
- Type
  - `Redirect`
- 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`

User Interaction

Once configured and assigned to the devices, users can now log in to a Microsoft service in the browser, such as Outlook, or a Microsoft app, such as Teams, and will be automatically logged in to all other compatible apps.

App to VPN assignment

When setting up a cross-device VPN, all device data is routed through the private network. Sometimes, a company may want to set up a VPN only for their enterprise applications. Apple allows VPN connections to be set up for iPhones, iPads and MacBooks on an app-by-app basis. Here, administrators can control exactly what data flows through the VPN. The policy configuration of an app-to-VPN mapping helps organizations keep app-level traffic apart, allowing for the separation of personal and corporate data.

Prerequisite

An app-to-VPN association can be set up directly through Relution. This only works for apps that are installed and managed by the MDM on the devices. In addition, administrators can also configure VPN connections to automatically establish VPN connections for specific domains when a corresponding app requests a network connection.

Relution supports the following connection types for establishing a VPN connection on iOS and macOS devices:

- IPSec
- JuniperSSL
- SonicWALL
- AnyConnect Legacy
- AnyConnect
- IKEv2
- Custom SSL.

For version 26.4.0

How to configure app-to-VPN for iOS and macOS devices.

1. Two policy configurations are required to set up used VPN for individual apps:
    - VPN
    - App-to-VPN mapping.
2. Within the VPN configuration, the option `VPN connection for apps and accounts` has to be activated and depending on the VPN type, all necessary fields have to be filled in.
3. Within the configuration ‘app-to-VPN-association’ apps can be defined for stored VPN connection.
4. Additional domain and email settings are possible in the VPN configuration under `Per-Account-VPN`.

Fonts

With Relution it is possible to distribute fonts to iOS and macOS devices via a policy.
This font is then available in supported apps such as Keynote.
The font cannot be set as a system font and is only selectable in apps.

Requirements

- A font in the format `otf` or `ttf` (other formats such as `ttc` or `woff` are not supported)
- A policy with the font configuration
- Apps that allow the selection of an installed font, e.g. `Keynote`

Managing Fonts

Fonts are managed centrally under `Settings` → `Fonts` before they can be assigned to a policy.

Uploading a Font

Use Add to upload a new font. A name (max. 255 characters) and the font file in `otf` or `ttf` format are required.

For version 26.4.0

Visibility (Scope)

A font's visibility is determined automatically by the organization it was created in — it cannot be selected manually:

- Global: Created in the global organization → available in all organizations.
- Local: Created in a regular organization → only available there.

The overview list also shows the scope, creation/modification date, and who made the change, and can be exported to CSV.

> Only fonts belonging to the organization can be downloaded — fonts inherited from other organizations via global scope cannot be downloaded.

Deleting

Fonts can be deleted individually or via multi-select; editing an existing font is not possible.

> Deletion does not check whether the font is still in use by a policy. Deleting a font that is still in use causes a compliance violation on affected devices the next time the configuration is transferred.

Usage

The desired font can be uploaded in Relution under `Home` → `Settings` → `Fonts` → `Add`.
In addition, a name must be given to the font.
Afterwards, it must be added to an iOS or macOS policy in the `Font` configuration.

For version 26.4.0

Homescreen Layout

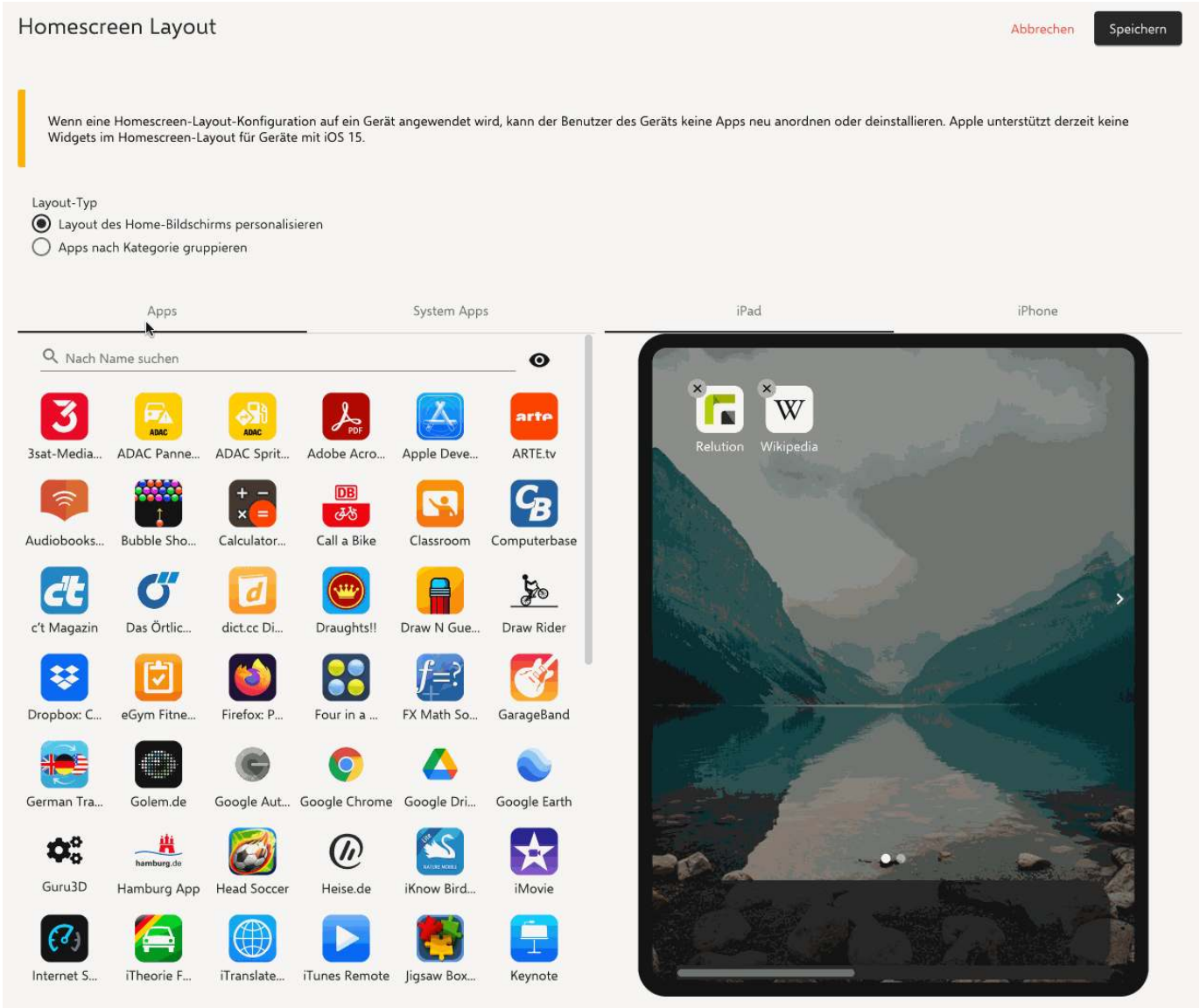
With the Homescreen Layout, the arrangement of apps and folders on iOS and iPadOS devices can be controlled by administrators. There are two layout types for this:

1. Personalize the Homescreen Layout.
2. Group apps by category.

> When a Homescreen Layout configuration is applied to devices, users cannot manually rearrange or uninstall apps on the devices. Apple does not currently support Homescreen Layout widgets for devices running iOS 15.

Personalize home screen

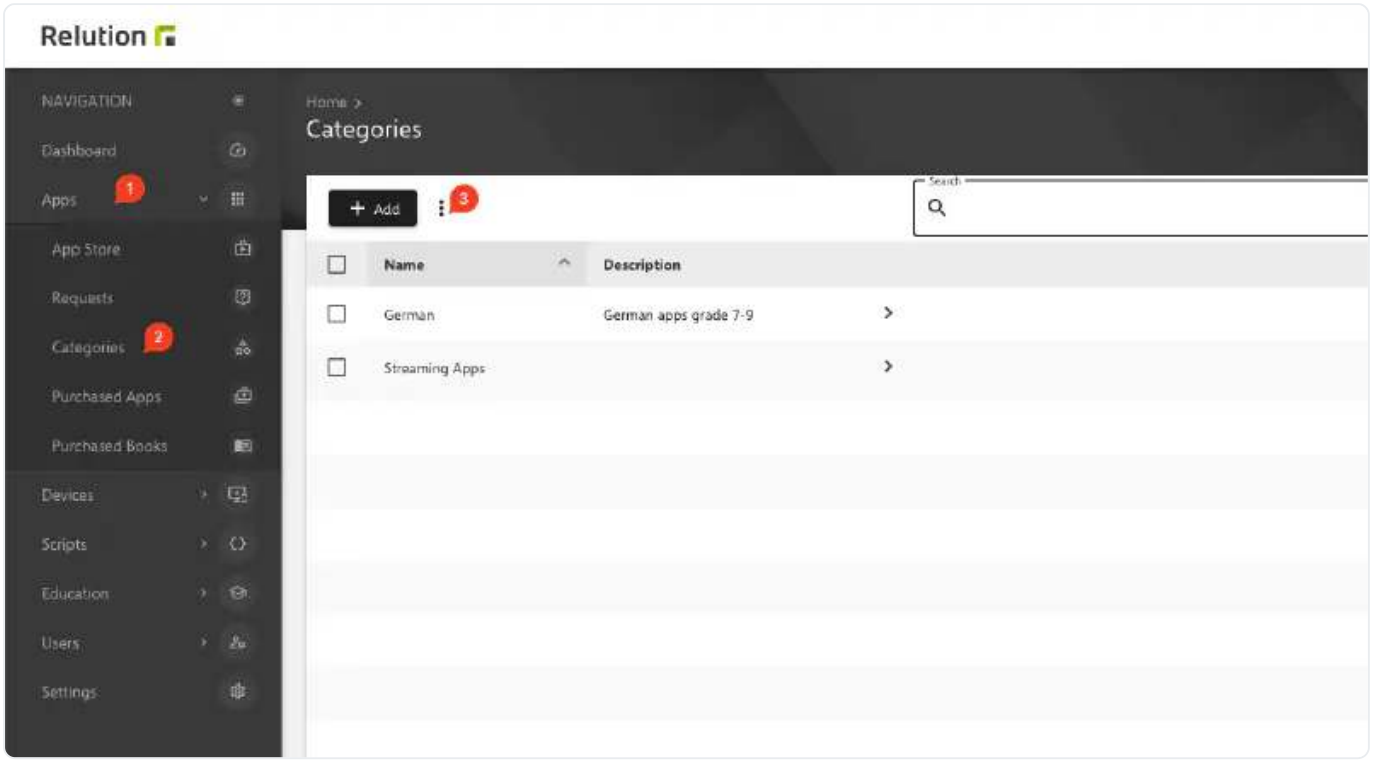
The layout can be personalized by arranging apps individually. Folders can be created for categorization of apps.



Holding the mouse still while dragging and dropping on another app will automatically create a folder. Homescreen Layout is limited to 20 apps per page.

Group apps by category

This layout groups installed apps according to the categories created in the Relution portal. System apps are grouped automatically.



Relution Decon (content filter)

Starting with version 5.27, Relution for iOS enables the setup of a DNS-based content filter. Relution Decon is also available for Android Enterprise devices starting with version 26.2.0. This feature ensures a secure and focused internet experience by restricting access to selected websites and apps. With AI-powered content categorization, Relution Decon also provides a comprehensive parental control filter with advanced configuration options.

What is Relution Decon?

Relution Decon is an AI-powered add-on for iOS, iPadOS and Android Enterprise that filters content in real-time, creating a safe digital environment. Using DNS-based content control, Decon blocks unwanted websites and apps, allowing users to work and learn in a protected, distraction-free space.

Relution Decon uses a DNS proxy to forward all requests to the Decon server. Websites are classified and either allowed or blocked according to policy rules. All data transfers are SSL-encrypted, ensuring user activities remain secure.

Decon App

The Decon app is automatically deployed on devices when the policy is installed. It monitors device DNS requests and ensures that only approved content is accessible.

For version 26.4.0

App features:

- Activates a system-wide DNS proxy, which cannot be disabled by the user
- Displays the current status of Relution Decon
- Provides insight into blocked websites and applied filter categories

iOS & iPadOS

> Recommendation: Ensure sufficient VPP licenses for the app before deployment.

VPP setup in Relution →
Relution Decon on the Apple App Store →

Decon Policy

In the device policy, click `Add` → `Relution Decon`. This policy automatically installs the Decon app on associated and supported devices and acts as a proxy for all DNS requests.

Policy configuration is completed upon publishing.

Policy configuration hierarchy (highest to lowest priority)

1. Allow Apps
2. Block Apps
3. Allow Websites
4. Block Websites
5. Blocked Categories

Decon in Relution Teacher

Decon can be selected and managed in class profiles with Relution Server 5.32.0 and Relution Agent 5.19.0. Student devices must have a Decon policy assigned.

More about Relution Teacher →

Category Classification

Relution Decon automatically assigns each website to a category. Administrators can define which categories are blocked:

For version 26.4.0

Category	Description	Examples
Not suitable for minors	Sites inappropriate for youth	Pornography, Violence, Weapons, Drugs, Gambling, Adult Entertainment, Adult Shopping, Dating, Google Safe Search
Advertising	Advertising websites	Ad providers
Communication	Communication services	Email, Messenger, (Video) Calling
Social Media	Social media content	Facebook, Instagram, TikTok, etc.
Entertainment	Entertainment websites like streaming or games	Movies, Games, Videos
Music	Music streaming services	Spotify, Tidal, etc.
News	News and magazines	News, Weather
Shopping	Online shops (excluding adult content)	Amazon, eBay, etc.
Work	Work-related websites	Office, File Sharing, Intranet
Education	Learning websites	Wikipedia, Google Scholar
Generative AI	AI-specific websites	ChatGPT, Perplexity.ai, etc.
Phishing	Potential phishing websites	Potential scams, Data theft
Other	Everything else	Remaining sites

Allow and Block Lists

- Allow / Block Websites: Specific domains can be allowed or blocked independently of categories. Only the domain should be specified, not the path.
- Allow / Block Apps: Apps can have internet access controlled; base functionality remains unless internet connection is required.

Advanced DNS Configuration

Device DNS Servers: Alternative DNS servers can be configured if the Relution Decon DNS is unavailable. Fallback: Cloudflare Families DNS (1.1.1.3).

Relution Decon Server DNS: An alternative DNS server can replace the standard Cloudflare Families DNS on the Decon server

For version 26.4.0

Relution Shared Device

Relution comes with its own multi-user mode for iOS devices. For this, users log in to the devices via the `Relution Agent` with an existing Relution user (account). A (managed) Apple ID is not necessary. With Relution, it is also possible to log in with an LDAP user account. Unlike Apple's multi-user mode, `Shared iPad`, `Relution Shared Device` mode can be conveniently enabled and disabled via the appropriate policy configuration.

> Prerequisite for using this configuration is that the target devices are in Supervised Mode.

Notes

The `Relution Shared Device` mode installs all required apps at user login and uninstalls them automatically at user logout. This automatically deletes all content temporarily created in the apps from the devices. In this way, Relution ensures privacy-compliant use of devices when used across users via `Relution Shared Device` mode.

Make sure that system apps, such as the Safari browser or the Photos app, cannot be uninstalled on the Apple side. This means, that no temporarily created data can be deleted for these apps. Here, it is recommended to switch to alternative apps such as the Firefox browser or the Relution photo function.

The reinstallation of apps can cause significant load peaks in the network. Therefore, the `App Conformance` configuration should be kept as lean as possible. In this case, the `positive list (Allowlist)` should contain only very few and small apps as required apps. Users can easily install apps from the Relution App Store via the Relution Agent, or have them installed in the school context by a teacher using the Relution Teacher App and a teaching profile.

For version 26.4.0

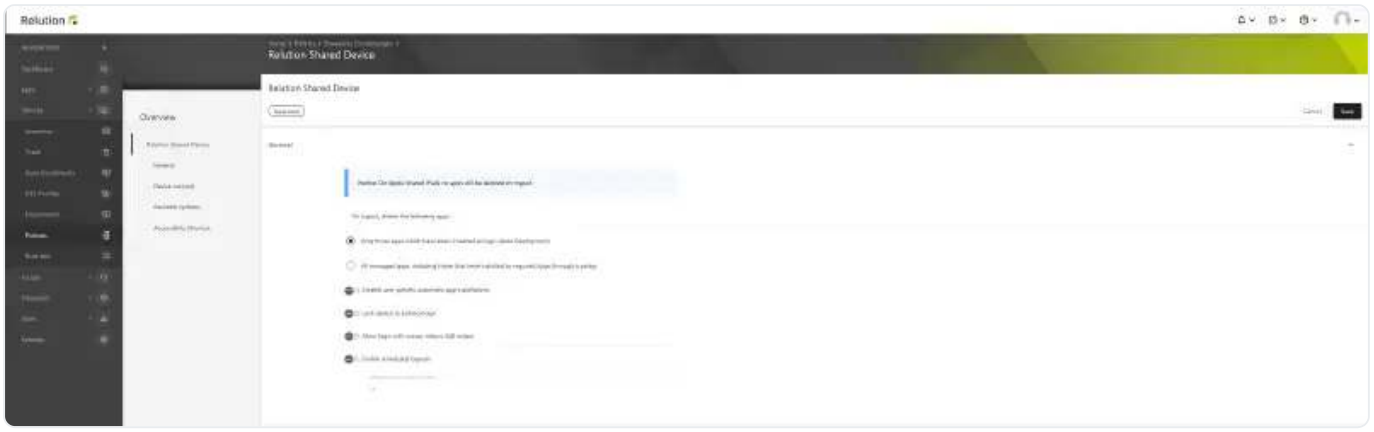
In terms of network data volume, it is not advisable to have every app installed on a Relution Shared Device at all times.

If `Relution Shared Device` mode is used in combination with Apple `Shared iPad` functionality, no uninstallation of installed apps takes place. In this use case, data protection-compliant work is only possible if users log in as guests in Apple `Shared iPad` mode. In `Guest` mode, all temporary data on the devices is automatically deleted by the Apple `Shared iPad` functionality after guest logout.

Apple Shared iPad guest mode is not compatible with the Apple Classroom app. In the school context, this means that student iPads in the above setup will not show as online in the teacher's Apple Classroom app.

Note that app compliance only works in the form of a positive list in combination with Relution Shared Device mode. Block lists have no effect.

Relution Shared Device settings



With iOS 17.x, using the restriction configuration allowCloudKeychainSync false leads to a slower login on Apple shared devices

- The first four options of the `Relution Shared Device` configuration are the most important ones. First, decide whether only the user-specific apps installed via `Auto-Deployments` should be deleted when the user logs out, or whether all apps installed via Relution should be deleted. Depending on the configuration, the second configuration ensures that more apps are uninstalled.
- The checkbox for disabling `User specific auto app installment` disables auto deployments.
- The checkbox for option `User specific auto app install` disables existing auto deployments on user or group level.
- The checkbox for option `Lock device and force login` sets the `Relution Agent` to `Single App Mode` before user login. Users must thus first perform a successful user login in order to exit the Relution Agent and then access the device. This option doesn't work on Apple Shared iPads.

For version 26.4.0

It is not recommended to use the last option, because in this mode, there is no access to the device settings and, among other things, no WiFi connection can be set up manually if no network configuration is applied. If the option is disabled, users will be able to open the settings on the device without user login.

Data that needs to be backed up must either be stored on an external server via `Relution Files` or stored on an external system via services like Own- or Nextcloud.

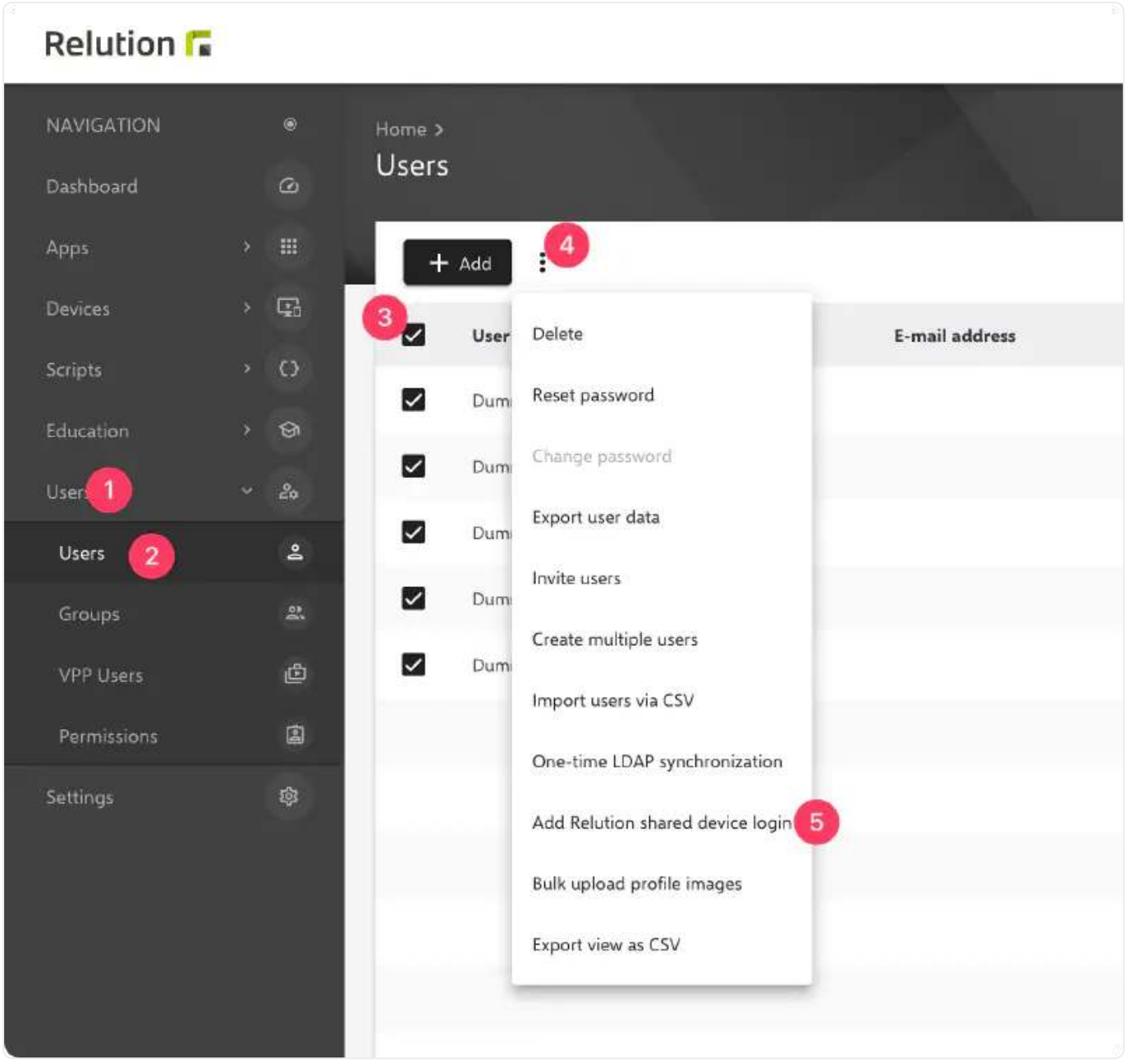
Login via QR code

In addition to username and password, the `Relution Agent` also supports login via QR code. Each QR code contains a personal access token of one user. This makes login easier wherever entering credentials is cumbersome, e.g. for primary school students.

Prerequisite is that the option Allow login with access tokens (QR codes) is enabled in the `Relution Shared Device` configuration. Without this option, the `Relution Agent` does not offer login via QR code.

Creating QR codes for multiple users

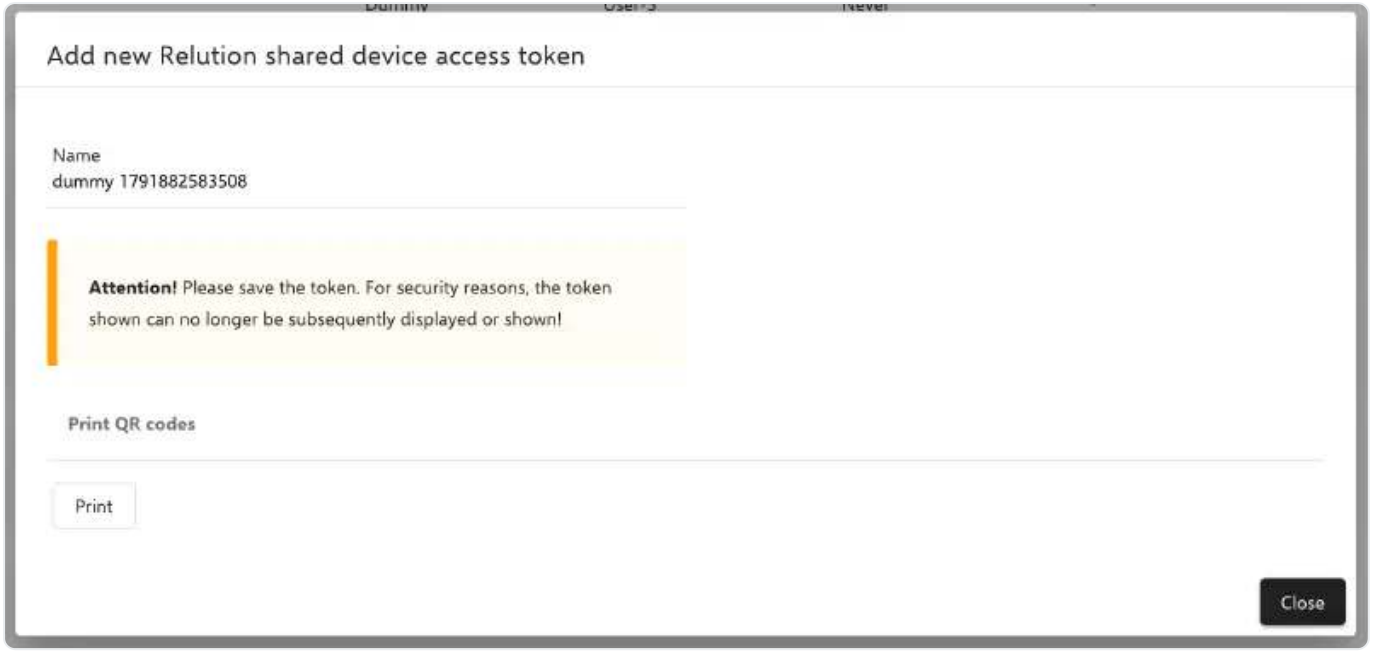
QR codes can be created for any number of users in one step and printed together. To do so, the desired users are selected in the list under `Users` → `Users`. Then Add Relution shared device login is selected from the three-dot menu next to Add.



In the following dialog, a Name is assigned to the access tokens. The Limited time of use switch optionally sets an Expiration Date; without an expiration date, the tokens remain valid indefinitely. Clicking Add creates a separate token with this name for each selected user.



In the Print QR codes section, the Print button opens the browser's print dialog with all created QR codes. Below each QR code, the username and the expiration date (`EXP` followed by the date) or the note `Does not expire` are shown.



> For security reasons, the tokens are only shown in this dialog. After clicking Close, the QR codes cannot be printed again. The QR codes should therefore be printed right away or saved as a PDF via the print dialog. If a QR code is lost, a new token is created for the affected user.

For individual users, a token can also be created in the user profile.

Printing QR codes compactly

The print view outputs each QR code on a separate page. If the QR codes are to be cut out as small cards, several pages can be printed on one sheet via the print dialog:

- Google Chrome and Microsoft Edge: `More settings` → `Pages per sheet`
- macOS print dialog: `Layout` → `Pages per Sheet`

Alternatively, the print output is first saved as a PDF and then printed with several pages per sheet. Up to nine QR codes per A4 sheet usually remain easy to scan. Readability should be checked with a test print on the device before printing all cards.

Further information

For this configuration, please also see our
Decision support for multi-user mode →

For version 26.4.0

Relution Files

For iOS, Relution offers the possibility to integrate local file shares, also called network drives, via SMB and WebDAV. By connecting to e.g. school or corporate server solutions, relevant documents and content can be accessed and data and work results can be stored securely on a central server.

Advantages of Relution Files

Data should not be stored in an unsecured cloud with servers outside the EU if GDPR-compliant work is required. Likewise, it is advisable not to store data directly on devices if devices are used by multiple user. Saving and storing documents on local servers via `Relution Files` ensures data security and data sovereignty for all users.

Configure local network drives for Relution Files

Local file shares can be set up in Relution in two ways:

For the manual setup please check the app documentation itself -> Relution Files →

For version 26.4.0

Automatic configuration of Relution Files via policies

A prepared configuration, which the administrator carries out via the Relution Portal, removes almost every hurdle for the end user when setting up the device. In this way, file sharing can be used seamlessly.

A WebDAV or SMB connection can be prepared for use by configuring `Relution File Sharing` in a policy. To do this, it is necessary to select a protocol and enter the path to the share.

There is also the option to use the Relution user already 'logged in' to the device, which makes an additional login for file sharing when using 'Relution shared device' superfluous.

Alternatively, for 1:1 devices, the user assigned to the device can log in with their user data. In this case, the login process can be simplified by using placeholders such as `${user.fullname}`.

Two extension types are available: `classic` and `modern`. This setting defines the internally used extension type by Relution Files to integrate the shares into the native Apple Files app.

The `classic` type should be used in rare cases where the default `modern` one does not work as expected (e.g. iOS 18+ has a bug for Shared iPads where `modern` extension type does not display files).

Apple Configurator 2

This policy configuration can be used to transfer `.mobileconfig` files to Apple devices. This can contain, for example, a WiFi connection and the corresponding certificate.

Configuration

To be able to transfer a `.mobileconfig` file to devices, the corresponding information must be stored and named directly in the Relution configuration.

```
<?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>
```

It is not possible to use a mobileconfig file in which a large number of configurations are stored.

Managed App Configuration iOS

It is possible to pre-configure some apps with the policy configuration `Managed App (Managed App)`. This configuration is only available for iOS devices from version 7 and macOS devices from version 11+.

Configuration

Specify the bundle ID of the app to be configured and attach a valid app configuration payload. In the payload, the placeholders that appear at the bottom of the page can be used. For example, an email client app can be configured by using the placeholder `${user.email}`. This makes the configuration usable for different users. The placeholders will be filled in when the configuration is pushed to the devices.

> The app to be configured must already be installed on the devices before the app configuration is applied. If the app is installed on the devices in the same policy, add the app configuration to the list of configurations after the app installation step, so it runs afterward.

Basically, the manufacturer of each app is responsible for the configuration options. We have listed some examples here that worked with the apps at the time of writing. We make no guarantee, that this will continue to be the case.

For version 26.4.0

Goodnotes 6

```
com.goodnotesapp.x
```

```
<?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>
```

Additional informations can be found on the Goodnotes webseite. →

Microsoft Outlook for 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 for an 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>
```

For versi

SecurePIM for 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>
```

For version 26.

Configuration incomplete

When an existing configuration is exported from another MDM system as XML and then converted into a `plist` file, a value that was marked as optional and left empty can turn into an empty `<string></string>` value in the `plist`. The key `subscriptionWebServiceEndPointURL` is affected by this, among others.

In this case, SecurePIM shows the persistent message “Configuration incomplete” on app start, even though the key worked without a value in the original system. Entering any non-empty value for the affected key, or removing the key from the `plist` entirely, resolves the issue.

FileBrowser for Education

```
com.stratospherix.filebrowsereducation
```

Configuration of an 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>
```

For versi

IBM Verse client

```
com.ibm.lotus.traveler
```

Show full configuration example

Single App Mode

This configuration restricts a device to running only one specific application. In this mode, users cannot exit the app or access other device functions.

Preparation & Configuration

> Ensure the desired app is pre-installed via an action or an App Management policy. If Single App Mode is activated before the app is present on the device, the device may become blocked by an error message. In this case, the app must be installed manually, and the device must be restarted.

Error message:

```
Guided Access is unavailable. Please contact your administrator.
```

For version 26.4.0

1. App Selection: First, select the application to display in Single App Mode.
2. Restrictions: Then, select the desired options to apply additional restrictions while the app is running.

Device Control

Use these options to restrict physical interaction with the device:

- Disable Touch Input: Blocks all touch interactions on the screen.
- Disable Motion (Screen Rotation): Prevents the screen from switching between portrait and landscape mode.
- Disable Volume Buttons: Locks the physical buttons for volume control.
- Disable Side Switch: Deactivates the mute/silent switch. The behavior depends on the switch's position at the time it was first disabled.
- Disable Sleep/Wake Button: Prevents the device from being turned off or locked using the power button.
- Disable Auto-Lock: Prevents the device from automatically entering sleep mode after a period of inactivity (the screen remains permanently on).

Accessibility

Allow users to adjust specific accessibility features while the mode is active:

- VoiceOver: Allows the use of the screen reading function.
- Zoom: Permits the magnification of screen content.
- Invert Colors: Allows the inversion of display colors.
- AssistiveTouch: Enables the on-screen digital assistance menu.
- Speak Selection: Allows the device to read highlighted text aloud.
- Mono Audio: Switches audio output to mono.

Accessibility Shortcuts

Define which features should be available via the accessibility shortcut (e.g., triple-click of the side button). By default, these options are disabled:

- VoiceOver: Enables the shortcut for the screen reader.
- Zoom: Enables the shortcut for the zoom function.
- Invert Colors: Enables the shortcut for color inversion.
- AssistiveTouch: Enables the shortcut for AssistiveTouch.

Filter for content

This is a parental control filter that can be enabled or disabled on iOS and macOS devices.

> Relution has no control over the filtered content. Apple is responsible for managing the filter. Additionally, it is not possible to determine whether or not content meets a specific age rating.

Configuration

For version 26.4.0

Nevertheless, websites can be added to a `blocked list (Blocked URLs)` or a `positive list (Allowed URLs)`. In the configuration, the filter is basically active if the checkbox `Enable Auto-Filter` is set:

Under certain circumstances, the filter does not always achieve the desired result, since URLs that do not contain content harmful to minors are sometimes filtered.

To filter a certain URL that is not blocked by the automatic filter, put it on the `Blocked URLs` list. To unblock a filtered URL, put it on the `Allowed URLs` list.

Special attention should be paid to the `Determined bookmarks` list. If entries are made here, only these URLs are allowed. Regardless of what has been configured in the `Allowed URLs` list. In addition, these `Determined Bookmarks` are created as bookmarks in Safari.

If the content filter is active, the Delete function can no longer be executed on the devices in the Safari History and Web Page Data settings.

Device lock time

By setting lockout times for iOS devices, active usage can be prevented. If the policy configuration is active, all apps will be hidden and will be available again after the end time has expired.

Notifications

From version 5.25, Relution for iOS allows the settings for notifications to be preconfigured for individual apps. The `Notifications` policy configuration is available for selection for this purpose.

Configuration

To configure notification settings, an app to which the setting is to be applied must be selected. The usual selection options `Relution App Store`, `Apple App Store`, `iOS System Apps` and `Manual entry` are available for this purpose. Once an app has been selected, it can be configured accordingly.

At this point, notifications can be activated on the device for the corresponding app. This includes the display in CarPlay, on the lock screen or in the message centre. The notification type can be set as a temporary or permanent banner.

Critical warning messages can also be activated and sounds can be switched on.

The preview type can also be set. Available options are `Always`, `Unlocked`, and `Never`.

Grouping by app is also possible.

For version 26.4.0

Exchange

With Relution, a Microsoft Exchange configuration for iOS devices can be transferred to the native Mail app. This eliminates the complex setup for the end user. Depending on the selected authentication →, the device only requires the user's password, a sign-in via OAuth or no input at all.

General

- Use Secure Mail Gateway: If this feature is enabled, the URL and domain of the Secure Mail Gateway will be distributed to the devices instead of the Exchange URL and Exchange domain. This allows the devices to communicate with the Exchange server via the Secure Mail Gateway.
- Exchange Host
- Exchange Domain
- Exchange Server uses SSL for authentication

Account Settings

For version 26.4.0

- Account Name
- Use user's email address `${user.email}`
- Email address

Username

- Manual
- Use user's username `${user.name}`
- Use user's email address `${user.email}`

The fields OAuth, Password and Certificate define how the device signs in to the Exchange server. They are described in the section Authentication →.

Enabled Services

- Enable Calendar
  - User can enable and disable the calendar
- Enable Email
  - User can enable and disable emails
- Enable Notes
  - User can enable and disable notes
- Enable Reminders
  - User can enable and disable reminders
- Enable Contacts
  - User can enable and disable contacts

Synchronization Settings

- Allow move
- Prevent mail sending via share sheet
- Synchronize recent email addresses
- Enable S/MIME signing
- S/MIME signing can be overwritten by the user
- Enable S/MIME encryption by default
- Enable per-message encryption option
- S/MIME encryption can be overwritten by the user
- Sync period
  - No limit
  - 1 day
  - 3 days
  - 1 week
  - 2 weeks
  - 1 month

Authentication

Three methods are available for signing in to the Exchange server: a password, OAuth or a certificate. Relution does not know the users' passwords and therefore cannot transfer them per user.

Password

A value entered in the Password field is transferred unchanged to all devices the policy is assigned to. There is no placeholder for the password of the respective user. For personal accounts, the field therefore usually remains empty and the password is entered on the device.

For Version 26.4.0

Whether iOS prompts for the password on its own is controlled by the operating system. Relution cannot trigger a password prompt in the Mail app.

OAuth

If OAuth is enabled, the user signs in via the sign-in page of the identity provider, e.g. Microsoft Entra ID for Exchange Online or Exchange Server with Hybrid Modern Authentication. In this case, the Password field is locked.

Certificate

With a certificate, the device signs in to the Exchange server without a password. The Exchange server must accept certificate-based sign-in. There are two variants:

- Select certificate: A specific certificate or certificate template from the Certificate Management → is used.
- Use user certificate: The certificate of the respective user is used. If a user has several certificates of this type, the Certificate name field selects one of them. If it remains empty, the certificate with the longest validity is used.

For direct certificate-based sign-in to the Exchange server, OAuth remains disabled.

Relution does not prevent OAuth and a certificate from being configured at the same time. In this case, the certificate is still transferred to the device.

Update Mode

If this setting is set to Only on new policy version publication, updates for this configuration will only be sent when the published policy version has changed. Updates triggered for other reasons, such as a changed device user or placeholder, will not be applied to the devices.

This reduces the number of synchronizations for this configuration, which can decrease resource usage on the device, while also carrying the risk of missed updates.

Update Mode

- Default
- Only on new policy version publication

For version 26.4.0

Software Update

With Relution 26.1.0, the new Apple configuration Software Update has been introduced for devices running iOS 18 or later. This configuration can be used alongside the existing System Updates configuration. It replaces, among other things, the Update Deferral restrictions and the update behavior from the legacy System Updates configuration, which is marked as deprecated in Relution.

To ensure updates across the entire device fleet, both Software Update and System Updates can be configured in parallel and deployed to all iOS devices.

> The deprecated System Updates configuration will be phased out by Apple in the medium term.

General

Beta Program Enrollment

- Allowed
- Always Off

Software Update Notifications

- Show all notifications
- Updates shown to the user:
  - All
  - Latest
  - Oldest

For version 26.4.0

Automatic Software Update Actions

Automatically Download Available OS Updates

- User Choice
- Always Off
- Always On

Automatically Install Available OS Updates

- User Choice
- Always Off
- Always On

Automatically Install Available Security Updates

- User Choice
- Always Off
- Always On

Deferral of OS Updates

- Number of days: Number of days to postpone a major or minor operating system update on the device

---

Rapid Response for Security Updates

- Allows the user to install security improvements in the background
- Enables the user to roll back security updates in the background

---

Managed Software Updates

New in 26.4

The Managed Software Updates configuration enforces operating system updates, targeting a specific version by a deadline. It is the successor to the deprecated System Updates configuration and complements the Software Update settings described above: those control the update *behaviour* (automatic download, deferral, notifications), while Managed Software Updates defines bindingly *which* version has to be installed by *when*.

For version 26.4.0

It requires iOS 17 or later in supervised mode. The configuration is also available for tvOS 18.4 and later and visionOS 26 and later.

Target version

- Version to enforce
  - Latest major version — the device is raised to the most recent available major version.
  - Latest minor version — updates happen within the installed major version.
  - Minimum specific version — a concrete version is set as the minimum level.
- Details page URL — optional link that iOS shows to users in the update announcement.

Enforcement

- Enforcement schedule
  - Relative to release date — the deadline results from Days after release and Time of day. The same rule then applies automatically to every future version.
  - Specific date and time — the Deadline is set as a fixed point in time.
- Grace period after enrollment — optional. Postpones the deadline until this many days after a device was enrolled, so that freshly enrolled devices are not forced to update immediately. It applies to both enforcement schedules and only ever extends a deadline, never shortens it. Leaving the field empty disables the function.

If the available operating system versions cannot be loaded in the portal, the configuration reports this when opened. Selecting a minimum specific version is then not possible, while the other two modes remain usable.

Triggering Updates

There are two ways to perform iOS updates:

Policy Configuration The System Updates policy can be used to define the time window for system updates.

Device Action Through actions in the device inventory, devices can be updated immediately to the latest available version.

For iOS devices to successfully perform an update, the following conditions must be met:

- Devices must be sufficiently charged or connected to a power source.
- Devices must be unlocked; otherwise, users must enter their device passcode.
- The installed update will always be the latest publicly available iOS version.
- Supported iOS devices check for updates independently of this policy configuration once per day.
- This configuration overrides any restrictions on deferring updates.
- No users should be signed in on shared devices.

For version 26.4.0

Wallpaper

With the configuration Wallpaper for iOS devices, an image can be stored for the homescreen and/or lockscreen that appears on the devices after the policy has been applied. For example, student devices in a school or devices in a company can be provided with a uniform background image and/or an image on the lock screen.

If the background image is set via the policy, the original background image of the device is discarded and cannot be restored with Relution.

Which views can be configured on the devices?

The wallpaper can be set to display only on the lock screen or home screen after login, or on both views.

Calendar (CalDAV)

The Calendar policy hands a CalDAV account to the native Calendar app of iOS and iPadOS via a configuration profile, which removes the need for manual setup by the end user. On current iOS versions, the calendar paths belonging to the account are discovered automatically according to RFC 6764 through a redirect at `/.well-known/caldav`. A correctly configured server-side `/.well-known/caldav` redirect is therefore mandatory on current iOS versions; specifying a principal URL alone is no longer sufficient there.

Configuration options

The following fields are available for the CalDAV account. They correspond to the keys of the Apple CalDAV payload (`com.apple.caldav.account`).

Account settings

- Account description — display name of the account on the device.
- Host — server address without scheme and without path (e.g. `calendar.example.com`).
- Port — usually `443`.
- Use SSL — mandatory when the server is reachable via HTTPS. Without SSL enabled, an unencrypted connection is attempted on port `443`, which fails.
- User name — entered manually or via the placeholders `${user.name}` or `${user.email}`.
- Password — if left empty, the device prompts for it during profile installation.
- Principal URL *(optional)* — the path to the user principal (e.g. `/remote.php/dav/principals/users/${user.name}/`).

> The principal URL must be given as a plain path, not as a full URL with scheme and host (not `https://host/...`). Host, port and encryption are derived from Host, Port and Use SSL. On current iOS versions, however, a configured principal URL no longer replaces automatic discovery — what counts is a correctly configured `/.well-known/caldav` redirect. The field can therefore be left empty.

Automatic discovery via .well-known

Current iOS versions set up CalDAV accounts according to RFC 6764. The sequence is:

1. A `PROPFIND /.well-known/caldav` request to the server configured under Host.
2. The server responds with a redirect (`301`) to its DAV endpoint (`/remote.php/dav` for ownCloud/Nextcloud).
3. The DAV endpoint is used to determine the `current-user-principal` and, from there, the user's calendar area.

Reliable setup therefore depends entirely on a correct `/.well-known` redirect. On newer iOS versions, automatic discovery can no longer be bypassed by specifying a principal URL — without a working `/.well-known` redirect the setup fails, even if a principal URL is configured.

for version 26.4.0

Newer iOS versions evaluate the redirect more strictly than iOS 17. A faulty redirect (for example to `http://` instead of `https://`) that iOS 17 still tolerated causes discovery to abort on current versions. Accounts already set up under iOS 17 on older devices may continue to work while new setups fail.

Server-side configuration of the redirect

`/.well-known/caldav` and `/.well-known/carddav` must redirect to the server's DAV endpoint with a `301`. The target address must begin with **`https://`** and must not contain an internal port.

For nginx:

```
location = /.well-known/caldav  { return 301 https://$host/remote.php/dav; }
location = /.well-known/carddav { return 301 https://$host/remote.php/dav; }
```

For Apache (in the vHost):

```
Redirect 301 /.well-known/caldav  https://calendar.example.com/remote.php/dav
Redirect 301 /.well-known/carddav https://calendar.example.com/remote.php/dav
```

Operation behind a reverse proxy / TLS termination: if an upstream proxy terminates the TLS connection and forwards internally via HTTP to a different port (e.g. `8080`), the web server often only knows its public address as `http` on the internal port. A redirect generated from this is then incorrect, for example `http://calendar.example.com:8080/remote.php/dav`. Since current iOS versions do not follow a switch from `https` to `http`, discovery fails. In this case the redirect must be set with a full **`https://`** target address — either directly on the TLS-terminating proxy or as an absolute target URL as in the Apache example.

Verification

The redirect can be checked with `curl`:

```
curl -sI https://calendar.example.com/.well-known/caldav
```

The response must contain a redirect with a correct `location` header:

```
HTTP/2 301
location: https://calendar.example.com/remote.php/dav
```

The `location` header must begin with `https://` and must not contain an internal port (e.g. `:8080`).

Troubleshooting

Symptom	Cause	Solution
Setup fails only on newer iOS versions; older devices keep working	The redirect points to `http://` (downgrade); older iOS versions tolerated this	Correct the redirect to `https://`
`301` points to an internal port (e.g. `:8080`)	Reverse proxy/TLS termination, the web server does not know its public address	Set the redirect with the full `https://` address on the proxy or web server
`405 Method Not Allowed` on paths such as `/` or `/principals/`	Automatic discovery does not take effect and falls back to default paths that do not exist on the server	Configure the `/.well-known` redirect correctly (mandatory on newer iOS versions)
The discovered path is obviously wrong	Principal URL configured as a full URL instead of a plain path, or Use SSL not enabled	Enter the principal URL as a plain path and enable Use SSL

Isolating the problem on the device

For isolation, a CalDAV account can be set up directly on the device as a test under `Settings` → `Calendar` → `Accounts`. If the manually configured account connects while the account distributed via profile fails, the cause lies in automatic discovery (`/.well-known`) or in the principal URL distributed through the profile — not in the server itself.

Use on macOS

The CalDAV configuration and the server-side `/.well-known` requirement apply to macOS unchanged:

- Calendar (CalDAV) for macOS →

Managed Domains

The configuration Managed Domains defines which email and web domains iOS treats as company domains. The configuration is available for devices with Device Enrollment, but not for devices with User Enrollment (BYOD).

Email domains

The company domains are entered in the list Email Domains, e.g. `relution.io`. When composing a message, the Mail app marks all recipient addresses in red whose domain is not on the list. This makes it immediately visible when a message leaves the company.

Sending to these addresses is not blocked. The marking is purely informational.

Web domains

iOS treats URLs from the domains in the list Web Domains as managed. Content downloaded from these pages in Safari is therefore considered company data, e.g. a PDF from the intranet.

This list only has a visible effect in combination with the restrictions on opening documents in the configuration Restrictions →:

- Allow opening managed documents in unmanaged apps
- Allow opening unmanaged documents in managed apps

If opening managed documents in unmanaged apps is prohibited, a PDF from the intranet can then only be opened in managed apps. More background on separating managed and unmanaged data is available in the article Data separation →.

For version 26.4.0

Intelligence Settings

With Relution, the Intelligence Settings configuration can be centrally managed to control Apple Intelligence features on managed iOS devices. This policy makes it possible to allow or block individual AI-powered features such as the Apple Intelligence Report, Genmoji, Image Playground, Image Wand, Personalized Handwriting Results, the Visual Intelligence Summary, and Writing Tools. It also allows app-specific Intelligence features in Mail, Notes, and Safari to be controlled, and enforces that dictation and translation are processed exclusively on the device, without any connection to Apple's servers.

This configuration is available for iOS devices running version 26.4 or later and can only be applied through device enrollment, not through user enrollment (BYOD). It is available in the same form for macOS and visionOS 26.4 or later.

Not every option is supported on every platform. The form still shows them for all platforms.

- visionOS: Allow Personalized Handwriting Results, Allow Visual Intelligence Summary, Force On-Device-Only Translation and, in the Notes section, Allow Transcription and Allow Transcription Summary are not supported.
- macOS: Allow Image Wand, Allow Personalized Handwriting Results, Allow Visual Intelligence Summary and Force On-Device-Only Translation are not supported.

Settings

For version 26.4.0

- Allow Apple Intelligence Report
  - When disabled, the Apple Intelligence Report is disabled on the device. Enabled by default.
- Allow Genmoji
  - When disabled, the Genmoji feature is disabled. Enabled by default.
- Allow Image Playground
  - When disabled, Image Playground is disabled. Enabled by default.
- Allow Image Wand
  - When disabled, Image Wand is disabled. Enabled by default.
- Allow Personalized Handwriting Results
  - When disabled, personalized handwriting results are disabled. Enabled by default.
- Allow Visual Intelligence Summary
  - When disabled, the Visual Intelligence Summary is disabled. Enabled by default.
- Allow Writing Tools
  - When disabled, Writing Tools are disabled. Enabled by default.
- Force On-Device-Only Dictation
  - When enabled, dictation is processed exclusively on the device, without any connection to Apple's servers. Disabled by default.
- Force On-Device-Only Translation
  - When enabled, translation is processed exclusively on the device, without any connection to Apple's servers. Disabled by default.

Mail

- Allow Smart Replies
  - When disabled, Smart Replies in Mail are disabled. Enabled by default.
- Allow Summary
  - When disabled, the summary feature in Mail is disabled. Enabled by default.

Notes

- Allow Transcription
  - When disabled, transcription in Notes is disabled. Enabled by default.
- Allow Transcription Summary
  - When disabled, the summary of transcriptions in Notes is disabled. Enabled by default.

Safari

- Allow Summary
  - When disabled, the summary feature in Safari is disabled. Enabled by default.

For version 26.4.0

External Intelligence Settings

The “External Intelligence Settings” configuration provides central control over whether and how external, cloud-based AI services (e.g. ChatGPT) may be used via Siri and Apple Intelligence on iOS devices. The policy is available starting with iOS 26.4 — only for devices with full device enrollment, not in User Enrollment/BYOD mode — and is delivered to the device via Declarative Device Management (DDM). The same configuration is available in identical form for macOS and visionOS devices running the respective 26.4 version.

> This configuration is a separate, DDM-based policy and complements the existing external intelligence integration fields within the iOS restrictions →. Both configuration types can appear side by side in the portal, but cover the same three functions.

External AI Integrations

- Allow External AI Integrations
  - When disabled, external AI integrations are fully blocked. Enabled by default.
- Allow Sign-In for External AI Integrations
  - When disabled, signing in to external AI integrations is not possible. Enabled by default.
- Allowed Workspace ID
  - Sets the workspace ID that the external AI integration is restricted to. Currently limited to a single workspace ID.

Keyboard Settings

Starting with iOS 26.4 and Relution 26.3, the “Keyboard Settings” configuration is available, implemented via Declarative Device Management (DDM). This policy allows keyboard functions to be centrally enabled or disabled, such as auto-correction, dictation, spell check, predictive text, text replacement, slide-to-type, and mathematical keyboard suggestions – useful, for example, for educational institutions or organizations that want to ensure consistent, controlled text input on managed devices.

> This configuration requires iOS 26.4 or later and is only available for devices managed via Device Enrollment. All settings are enabled by default; disabling a setting restricts the corresponding keyboard function.

Keyboard Settings

- Allow Definition Lookup
  - If disabled, looking up word definitions (Look Up) on the keyboard is no longer available.
- Allow Dictation
  - If disabled, the keyboard’s dictation feature can no longer be used.
- Allow Math Keyboard Suggestions
  - If disabled, the keyboard no longer displays automatic solution suggestions for mathematical expressions.
- Allow Auto-Correction
  - If disabled, the keyboard no longer automatically corrects typing mistakes.
- Allow Predictive Text
  - If disabled, predictive word suggestions are no longer shown above the keyboard while typing.
- Allow Slide to Type
  - If disabled, typing by sliding across the keyboard (Slide to Type) is no longer possible.
- Allow Spell Check
  - If disabled, the keyboard no longer underlines misspelled words.
- Allow Text Replacement
  - If disabled, configured text replacements/shortcuts are no longer automatically inserted while typing.

For version 26.4.0

Siri Settings

As of iOS 26.4 and Relution 26.3, the Siri Settings configuration is available, implemented through Declarative Device Management (DDM). This policy provides centralized control over Siri's general availability, the profanity filter, and — on iOS only — the processing of user-generated content and access to Siri while the device is locked.

> This configuration requires iOS 26.4 or later and is only available for devices managed through Device Enrollment; it is not available for devices with User Enrollment (BYOD).

> Comparable Siri toggles already exist within the iOS Restrictions → policy. Siri Settings is a separate, additional configuration and does not replace the restrictions.

Siri settings

- Enable Siri
  - Enables or disables Siri on the device. Enabled by default.
- Force profanity filter
  - Enforces Siri's profanity filter. Disabled by default.
- Allow user-generated content
  - Allows Siri to access user-generated content. Enabled by default.
- Allow Siri while locked
  - Allows the use of Siri while the device is locked. Enabled by default.

For version 26.4.0

Safari Settings

The “Safari Settings” configuration provides centralized control over the behavior of the Safari browser on managed iOS devices. This includes handling of cookies, the fraud warning, JavaScript, and pop-ups, as well as clearing the browsing history, private browsing, content summarization, and the start page shown when opening a new tab. On macOS devices, only the four last-mentioned options are available — cookies, the fraud warning, JavaScript, and pop-ups cannot be configured there.

> This configuration is only available for devices with a Device Enrollment profile (not for User Enrollment/BYOD) and requires at least iOS 26.

Safari Browser Settings

- Allow Cookies
  - Determines how Safari handles cookies.
    - Always – Safari always allows cookies. *(default)*
    - From Visited – Safari only allows cookies from websites the user has already visited.
    - From Current Website – Safari only allows cookies from the currently open website.
    - Never – Safari always blocks cookies.
- Allow Disabling the Fraud Warning
  - When disabled, the system enforces the fraud warning in Safari; users cannot turn it off. Enabled by default.
- Allow JavaScript
  - When disabled, JavaScript is disabled system-wide in Safari. Enabled by default.
- Allow Pop-ups
  - When disabled, pop-up windows are disabled system-wide in Safari. Enabled by default.
- Allow Clearing History
  - When disabled, the browsing history in Safari cannot be cleared. Enabled by default.
- Allow Private Browsing
  - When disabled, private browsing mode is not available in Safari. Enabled by default.
- Allow Content Summarization
  - When disabled, automatic content summarization in Safari is disabled. Enabled by default.
- Start Page *(required field)*
  - Determines which page is displayed when opening a new tab in Safari.
    - Start Page – Safari uses its default start page; the homepage is disabled. *(default)*
    - Extension – Safari uses the Safari extension referenced by the specified identifier as the start page; the homepage is disabled. Requires an extension identifier in the format `Identifier (TeamIdentifier)`, e.g. `com.example.app (ABCD1234)`.
    - Home – Safari uses the specified URL both as the start page for new tabs and as the homepage. Requires a homepage URL that must start with `https://` or `http://`.

For version 26.4.0

Safari Extensions

The Safari Extensions configuration provides centralized control over the behavior of individual Safari extensions on managed iOS devices. For each extension, its unique identifier determines whether it is generally allowed, always enabled, or always disabled, whether it may also be used in private browsing, and which domains it may or may not access. Multiple extensions can be configured per policy.

> This configuration is only available for supervised iOS devices from iOS 18 that were enrolled through Device Enrollment; it cannot be used for devices in User Enrollment (BYOD).

Settings per Safari extension

- Extension identifier
  - The identifier of the Safari extension, or “*” to apply settings to all extensions. To manage the extension, the app it belongs to must be installed on the device. This identifier can be determined via `codesign -dv <path to the extension (in the app's PlugIns directory)>` on a macOS device, if the extension is available on macOS. Otherwise, this information must be provided by the extension’s developer.
- State
  - Controls whether the extension is allowed. Options: Allowed / Always On / Always Off.
- Private Browsing
  - Allow the extension in Private Browsing mode as well. Options: Allowed / Always On / Always Off.
- Allowed Domains
  - Controls the (sub)domains the Safari extension has access to. Domains without a prefix take precedence over those with a prefix; denied domains take precedence over allowed domains. Any domains not configured through either list can be configured by users on the device.
- Denied Domains
  - Controls the (sub)domains the Safari extension does not have access to. Domains without a prefix take precedence over those with a prefix; denied domains take precedence over allowed domains. Any domains not configured through either list can be configured by users on the device.

For version 26.4.0

Audio Accessory Settings

Starting with version 26.1.0 of Relution, the new Audio Accessory Settings configuration has been introduced for devices running iOS 26+.

This feature enables temporary pairing of audio accessories (e.g., headphones or speakers) with managed devices. Audio accessories can be paired for a limited time and then automatically or manually unpaired afterward.

Disable Temporary Pairing of Audio Accessories “On/Off”

This toggle is used to enable or disable temporary pairing of audio accessories.

- Enabled: Temporary pairing is allowed.
- Disabled: Temporary pairing of audio accessories is not possible.

Unpairing Policy

This setting defines how and when a temporarily paired audio accessory will be disconnected:

- No automatic unpairing The device does not automatically remove the pairing.

  > This option should only be used when a device is deleted and re-registered (e.g., *Return to Service*) or when a user change takes place.

- Automatic unpairing at a specific time The device automatically removes the pairing of temporarily connected audio accessories at a defined time.

Unpairing Time

- Set time (e.g., 4:30 PM) Defines the time at which the device automatically removes the pairing of temporarily connected audio accessories.

  At the specified time, only the pairing of previously temporarily connected audio accessories will be removed.

For version 26.4.0

Conditional Access

Complementing the following article Microsoft Conditional Access →, Relution 5.33 introduces a Conditional Access policy for iOS.

There are the following 2 options:

- Device is marked as non-compliant if the user has not yet registered it via the Relution Agent
- Informs the user via push notification to register their device

For version 26.4.0

Mathematical Settings

Starting with version 26.1.0, Relution provides the new Mathematical Settings configuration for devices running iOS 18+.

This policy allows the functions and modes of the Apple Calculator app to be centrally managed and adapted to educational or organizational requirements.

Settings for the Apple Calculator App

Basic Mode

- Add Square Root: Adds a square root button to the basic calculator by replacing the “+/-” button. By default, the square root function is only available in scientific mode. This option makes the square root accessible even if scientific mode is restricted.

Math Notes Mode

- Enable / Disable: Determines whether Math Notes mode can be used within the Calculator app.

Scientific Mode

- Enable / Disable: Specifies whether the scientific mode of the Calculator app is available.

Global Calculator Input Options

- Enable Unit Conversion: Allows the use of the built-in unit conversion feature within the app.

For version 26.4.0

System Behavior

Enable Keyboard Suggestions

- Enable / Disable: Controls whether keyboard suggestions automatically display mathematical solutions.

Enable Math Notes in Other Apps

- Enable / Disable: Determines whether the “Math Notes” feature can also be used in other apps (e.g., Notes).

AirPrint

The AirPrint policy configuration transfers AirPrint-capable printers to iOS and iPadOS devices via a configuration profile. The printers defined there then appear in the device's print dialog without having to be discovered on the local network via Bonjour.

Use case

AirPrint printers are discovered via Bonjour (mDNS) by default. Bonjour announcements, however, do not cross subnet or VLAN boundaries — in school and corporate networks with separate segments for devices and printers, the printers are therefore often not visible in the print dialog. The AirPrint configuration specifies the printer's address directly, so the device can reach it in a targeted way.

The configuration is also available for devices with User Enrollment and is offered in macOS policies as well as in iOS and iPadOS policies (see AirPrint for macOS →).

Prerequisites

- An AirPrint-capable printer or print server (e.g. CUPS) reachable via IPP or IPPS.
- Network connectivity between device and printer on the port used (IPP default: `631`); firewalls between network segments must allow this port.
- Host name or IP address and the resource path of the printer.

For version 26.4.0

Configuration

The configuration is created under `Devices` → `Policies` in an iOS policy via Add Configuration → AirPrint. The General section lists the printers in a table; Add opens the Add printer dialog. A configuration can contain any number of printers; it can only be saved once at least one printer has been entered.

The following fields are available per printer:

Field	Required	Description
Host Name or IP Address	yes	Address of the printer or print server, e.g. `192.168.10.25` or `printer01.example.com`.
Port	no	Port of the IPP service (`0`–`65535`). If left empty, the default port is used.
Resource Path	yes	Resource path of the print queue, e.g. `ipp/print` for many network printers or `printers/<queue>` for CUPS servers.
Use TLS	no	Enforces a TLS-encrypted connection (IPPS) to the printer. Disabled by default.

Printers already entered can be changed via Edit or removed via Delete in the table's context menu; several printers can be deleted at once using multi-selection.

> The printer announces its resource path in the Bonjour TXT record `rp`. On a Mac in the same network as the printer, it can be read with `dns-sd -B _ipp._tcp` (browse for printers) followed by `dns-sd -L "<printer name>" _ipp._tcp`. Alternatively, it is often shown in the printer's web interface.

Related restrictions

In addition to the AirPrint configuration, the Restrictions policy configuration contains further AirPrint-related options in the Restrictions of settings section, including Allow AirPrint, Allow AirPrint credentials storage, Allow iBeacon discovery of AirPrint printers and Require trusted TLS for AirPrint. If Allow AirPrint is disabled, printing is not available on the device even with printers configured.

- Restrictions for iOS →

> If Require trusted TLS for AirPrint is active, the device only accepts printers with a trusted certificate. Printers with self-signed certificates can then no longer be used unless the issuing certificate is additionally installed on the device via policy.

For version 26.4.0

Setup Assistant

The configuration Setup Assistant hides setup steps that iOS shows on a device that has already been set up, e.g. after a software update. The configuration is available from iOS 14 and only takes effect on supervised devices. It is not available for devices with User Enrollment (BYOD).

Difference from the DEP profile

The steps of the Setup Assistant can be skipped in two places that take effect at different times:

	DEP profile	Setup Assistant configuration
Time	Initial setup of the device	After enrollment, e.g. after a software update
Configured in	profile → of Automated Device Enrollment (ADE, DEP in the portal)	Policy with the configuration Setup Assistant

For version 26

The steps selected in the DEP profile only apply to the initial setup. If iOS later shows setup steps again, e.g. for appearance, Siri or Screen Time after an update, these can only be hidden via the configuration Setup Assistant. Without this configuration, such steps appear as intended by Apple.

The configuration is therefore not a prerequisite for enrollment. It is only needed if no additional setup steps should be shown after the initial setup either.

Settings

In the section Skip the following steps, the steps to be hidden are enabled. The selection corresponds to the setup steps in the DEP profile.

The switches in the section General, e.g. Skip accessibility or Skip Siri setup, only apply to macOS and have no effect on iOS devices. See Setup Assistant (macOS) →.

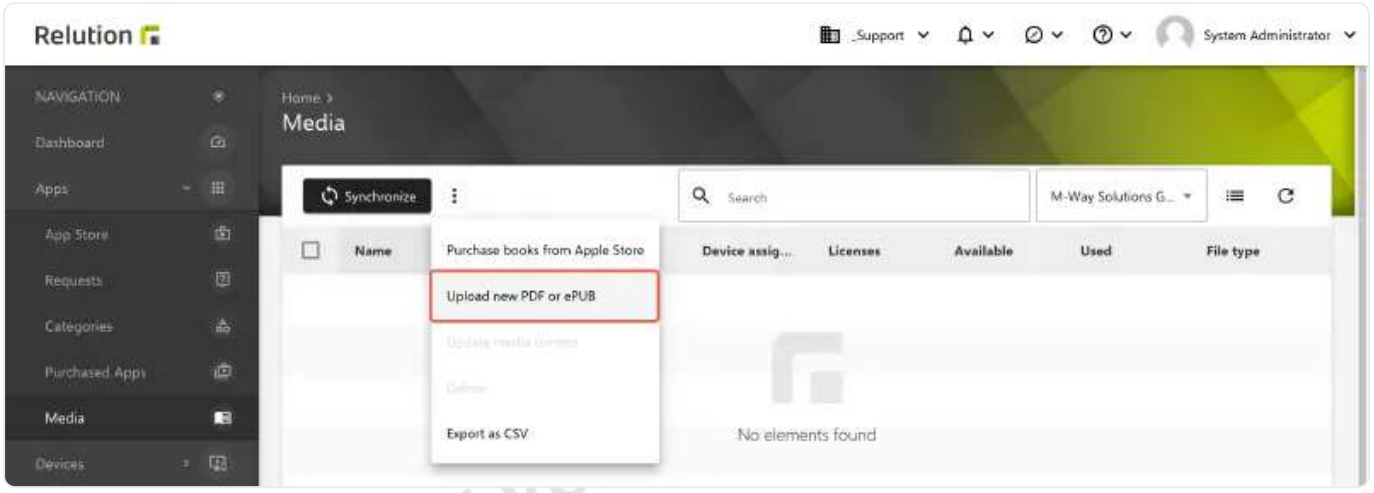
> Apple allows only one Setup Assistant configuration per device. A device should therefore not be assigned several policies with this configuration at the same time.

Managed Media

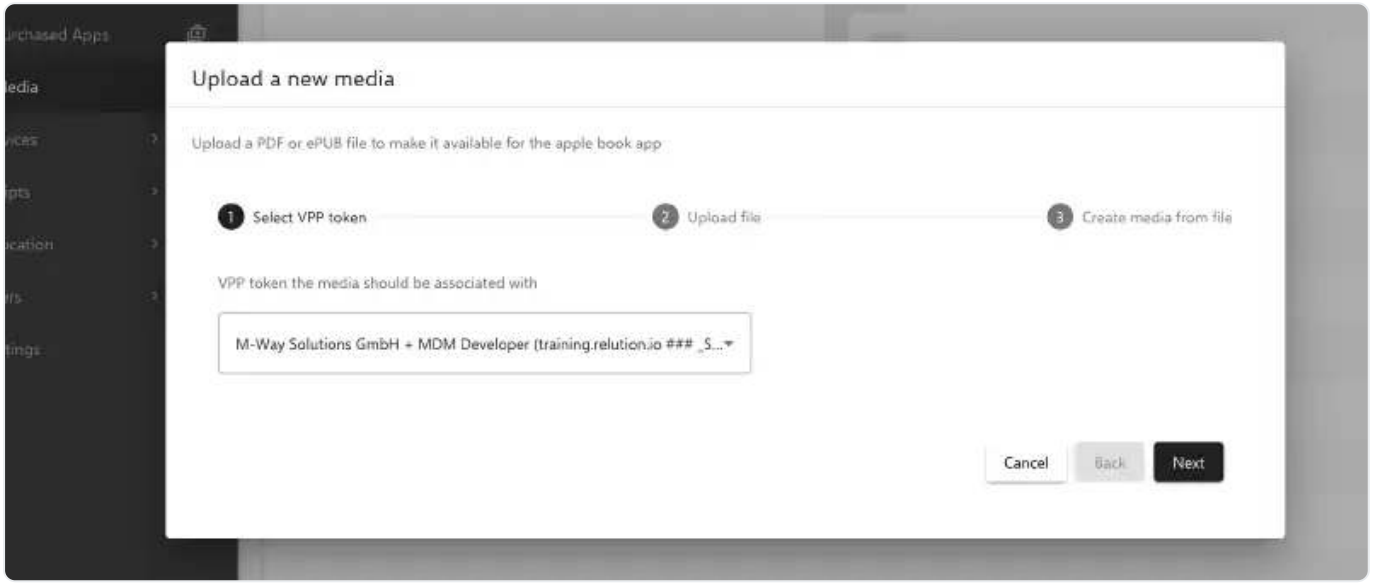
As of Relution 5.20, it is possible to distribute PDF or ePUB files directly to iOS devices via the Managed Media policy configuration and display them in the Books app on the iPad. VPP books can only be linked to VPP users and not to devices.

Preparing and uploading media

In order to be able to distribute PDF and ePUB files, they must first be uploaded to Relution. This is done via the overview of books. To do this, go to the corresponding section in the side menu.

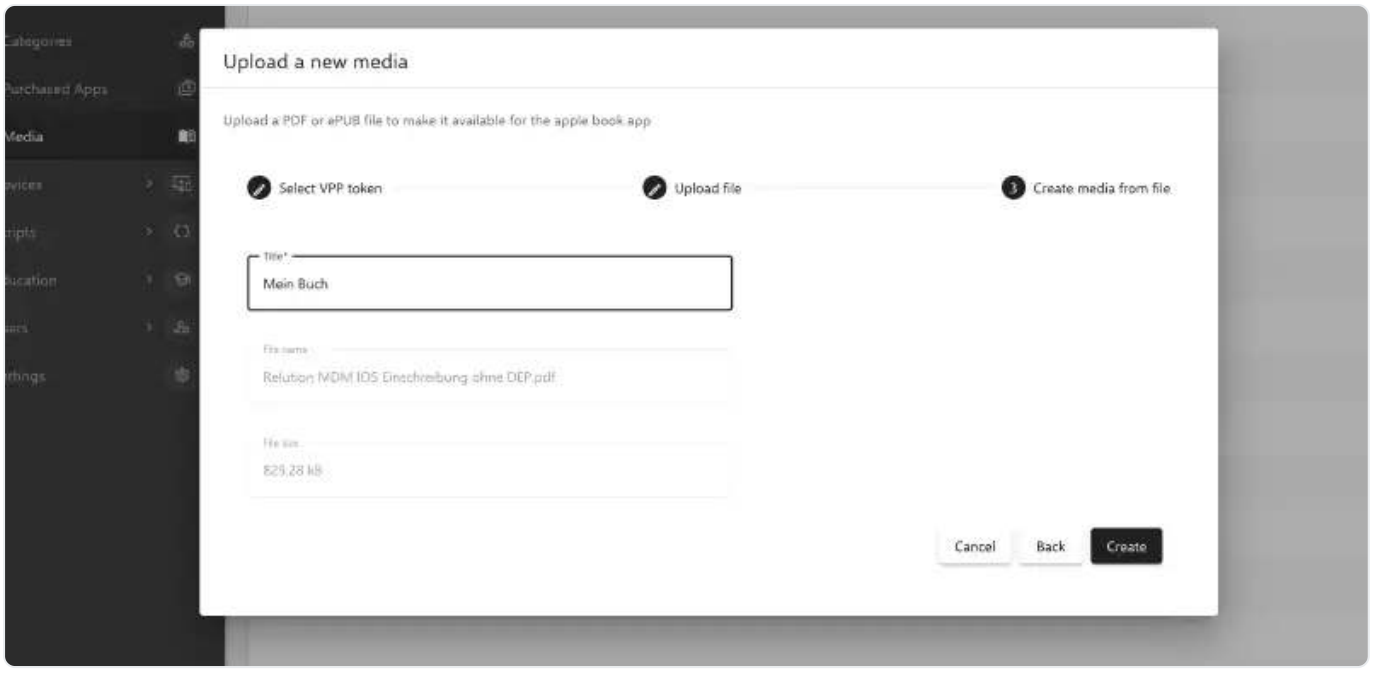


Via the menu behind the three dots, Upload new book can be selected.



In this step, the VPP token to be associated with the media file must be selected.

Then the file (pdf or epub) must be selected and uploaded.



In the last step, the book can be given a title.

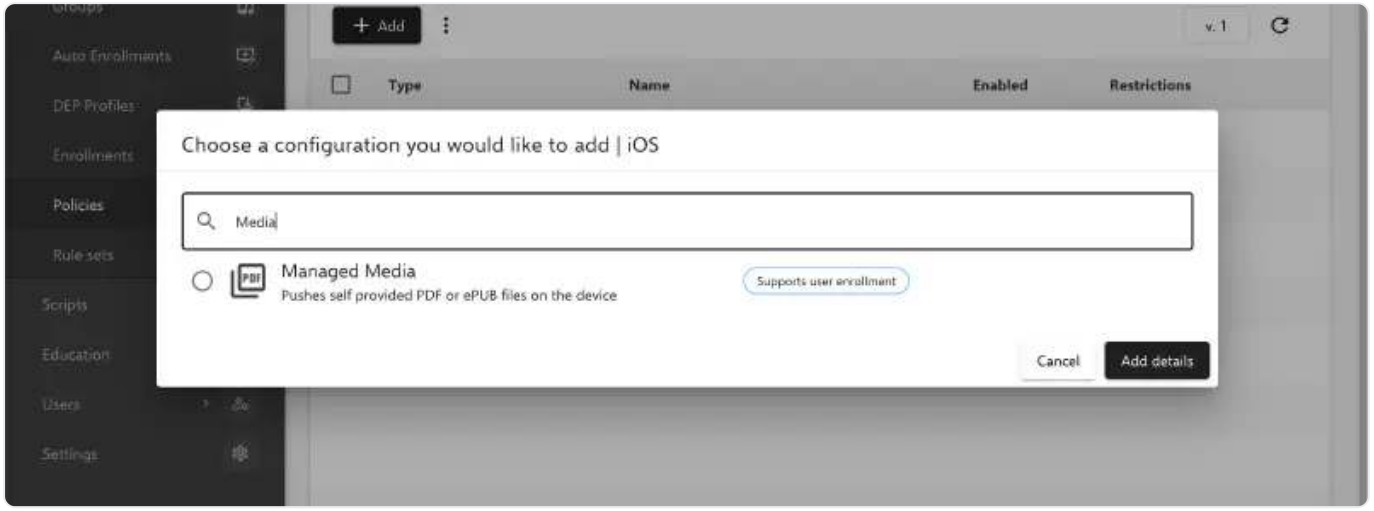
The PDF file is now visible in the overview of books.

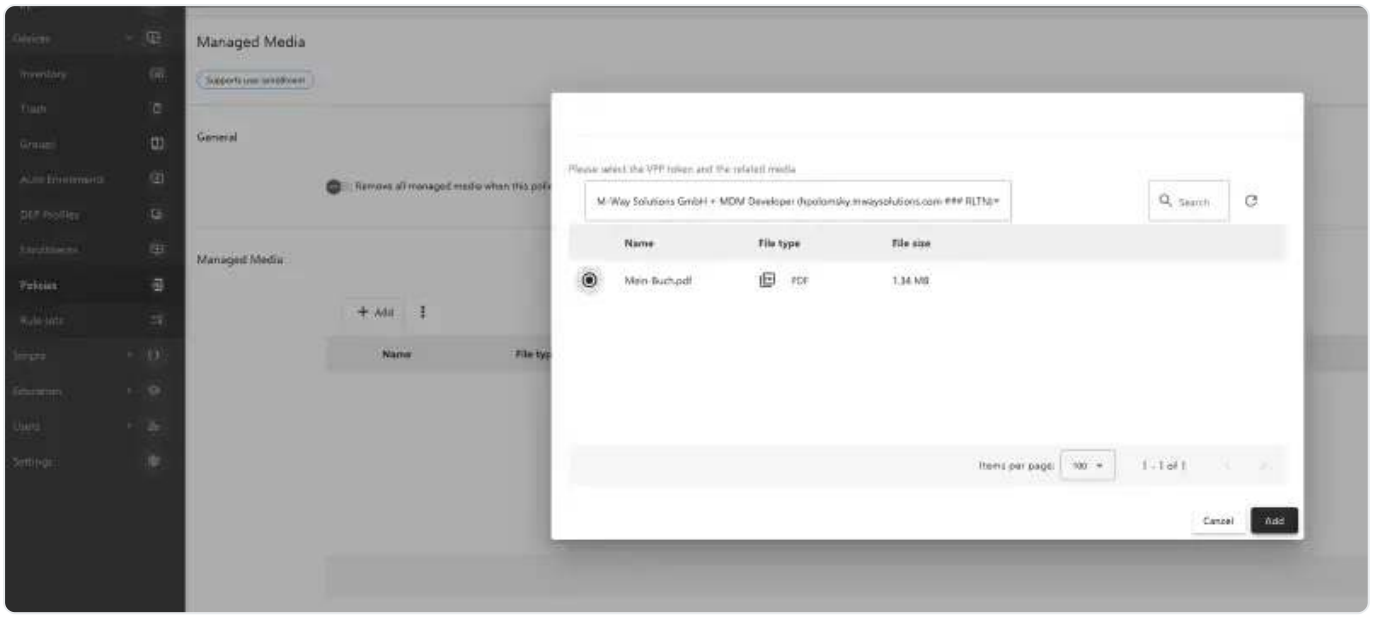
Policy configuration

For version 26.4.0

As already described, this policy configuration is available from Relution Server 5.20 and can thus be selected in an iOS policy.

In the Managed Media configuration, the previously added files can be linked and brought to the device via the policy.





A configuration parameter is also available that forces or prevents the automatic removal of the files after removing the policy from the device.

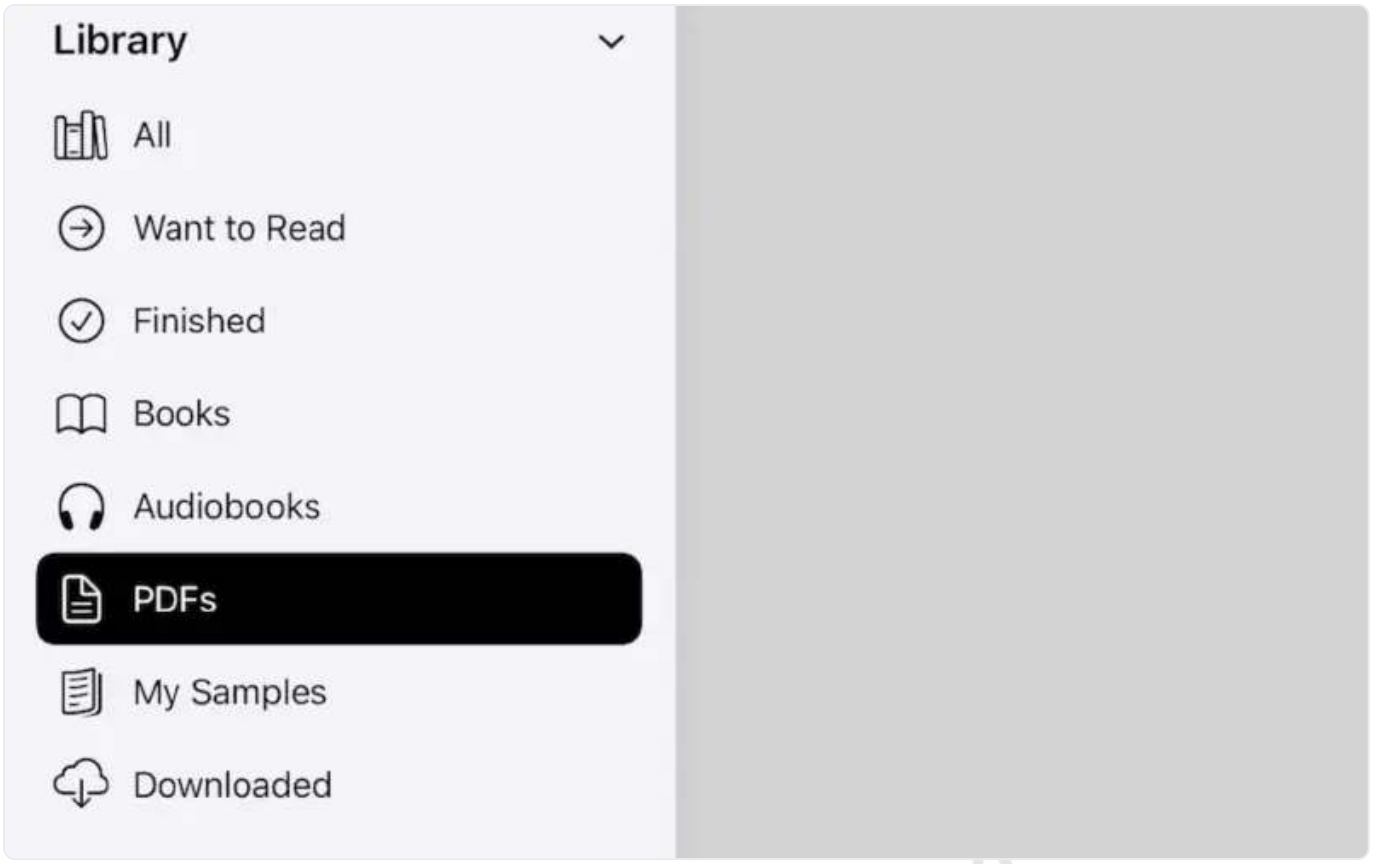
Execute as action

In addition to the policy configuration, previously uploaded media can also be installed on or removed from a device directly via an action. The corresponding actions are called Install Media and Remove Media.

For version 26.4.0

On the iPad

On the iPad, the linked PDF is then available under the corresponding category.



For version 26.4.0

Restrictions

The following is an overview of the available iOS/iPadOS restrictions in Relution `5.28.3`. Please note the additional information at the individual configuration points in Relution, such as `supervised`, `User Enreollment`, `deprecated`, `deprecated on non-supervised Devices`, as well as the min. OS version such as `iOS 16+`

Recommended Restrictions →

Device

Show all restrictions

Safari

Show all restrictions

For version 26.4.0

SIRI

Show all restrictions

Other Apps

Show all restrictions

Restrictions for managed apps and documents

Show all restrictions

Restrictions of settings

Show all restrictions

Classroom Restrictions

Show all restrictions

Restrictions for the media

Show all restrictions

Restrictions on changes

Show all restrictions

For version 26.4.0

iCloud Restrictions

Show all restrictions

Lockscreen restrictions

Show all restrictions

Restrictions for backups and synchronization

Show all restrictions

General

Show all restrictions

For version 26.4.0

App distribution

Companies are increasingly choosing to support specific work processes with a mobile app. In addition to many other conceptual questions, the question quickly arises as to how this app should be distributed to the users. Often, the use case looks like that not only employees but also external people should get the app – this may include, for example, service providers, partners or customers. This app is in most cases explicitly not intended for a wide range of customers but is aimed at selected professional users. The following sections in this Insight are intended to help in deciding on the best distribution method.

Distribution via public app stores

Apple and Google each provide an infrastructure for the distribution of apps. Apple provides apps to end users through the Apple App Store. The App Store app is preinstalled on every iOS device.

Apps are managed and published through the Developer Portal and the iTunesConnect portal. Google provides end-user apps through the Play Store. On every Android device, the App Play Store is preinstalled.

The administration and publishing of apps are done through the Developer Portal. Apple and Google define the framework for publishing apps through their systems.

If a device is managed via an MDM system, the store app can also be blocked for the user and may, therefore, be blocked and probably not available to the end user.

For version 26.4.0

Distribution via Apple App Store – Advantages

- Apps are available to end users through Apple's standard mechanism.
- Apps do not have to be re-signed and deployed after one year with an updated Provisioning Profile.
- Apps do not need to be re-signed and re-provisioned with an updated provisioning profile after one year.
- Apps can – if necessary – be selectively enabled or disabled for individual countries.
- Apps can be offered for a fee in defined structures – if desired – (Apple requires a commission fee of 15%).
- Apple provides the infrastructure for distribution and billing.

Distribution via Apple App Store – Disadvantages

- Users need an Apple ID on their devices to install apps from the Apple App Store.
- For enterprise customers with managed devices, the Apple App Store may be probably blocked by MDM.
- It must comply with all Apple requirements, such as support for new device classes such as iPhone X.
- Apple reserves the right to publish in a review before the app or remove subsequently.
- The review may lead to delays of up to 10 days (currently the average review time is around 3 working days).
- Apps can only be made available to a limited extent to selected user groups.

Distribution via Google Play Store – Advantages

- Apps are available to end users through Google's standard mechanism.
- Apps can – if necessary – be selectively enabled or disabled for individual countries.
- Apps can – if desired – be offered for a fee in defined structures (Google requires a commission fee of 15% for this).
- Google provides the infrastructure for distribution and billing.

Distribution via Google Play Store – Disadvantages

- Users need a Google Account to install apps from the Play Store.
- For enterprise customers with managed devices, the Play Store may be probably blocked by MDM.
- It must comply with all Google requirements – such as the Cordova version.
- Google reserves the right to remove the app from the store after automated app scans.
- Technical scans can delay app publishing by a few hours.
- Apps can only be made available to a limited extent to selected user groups.

Distribution via beta programs of public app stores

Apple and Google also provide a beta testing program in addition to the distribution of public apps. At Apple, apps for end-user beta testing are provided through the TestFlight app. On iOS devices, this app can be installed from the Apple Store app.
To manage and publish apps, use the Developer Portal and the iTunesConnect portal in the TestFlight section. Google provides apps for alpha or beta testing through the Play Store.

For version 26.4.0

The Play Store is pre-installed on every Android device. App management and publishing are done through the Developer Portal for Alpha and Beta Testing. Apple and Google define the framework for publishing apps through their systems.

Distribution via Apple Testflight – Advantages

- Apps are available to users through an Apple-provided mechanism.
- Apps can be selectively enabled for individual users.
- Apple provides the infrastructure for distribution and billing.

Distribution via Apple Testflight – Disadvantages

- Users need an Apple ID to install apps from the Apple App Store.
- The installation of the app requires a one-time installation of the TestFlight app.
- Apple reserves the right not to publish the app in a "reduced" review.
- The review may lead to delays of up to 10 days (currently the average review time is about two working days).
- The signature of apps expires after 90 days.

The TestFlight service is primarily intended for a short trial period prior to the release of an iOS app. For a permanent operation, the solution is not suitable because of the short validity of the signature.

Distribution via Google Alpha and Beta Testing – Advantages

- Apps are available to users through a mechanism provided by Google.
- Apps can be selectively enabled for individual users.
- Google provides the infrastructure for distribution and billing.

Distribution via Google Alpha and Beta Testing – Disadvantages

- Users need a Google ID to install apps from the Play Store.
- For enterprise customers with managed devices, the Play Store may be probably blocked by MDM.

Distribution via internal Enterprise App Store

Apple and Google offer not only the distribution of apps through the respective public stores but also mechanisms for the internal distribution of apps primarily for companies. Apple requires the Apple Enterprise Program and an Enterprise App Store such as Relution.

The apps are made available to end users through a separate App Store app or mobile web page. Apps are managed through the Developer Portal.
The distribution of apps through the respective provider of the Enterprise App Store. At Google, apps can be made available via a web service for download and installation.
For special devices such as Samsung optimized installation and distribution mechanisms can be used. Apple and Google are defining ways to distribute apps in parallel with their systems.

For version 26.4.0

Distribution of iOS Apps via Enterprise App Store – Advantages

- Apps can be distributed to selected user groups, for example, as a deep link or after logging in with a previously configured username and password.
- Users do not need an Apple ID to install apps from an in-house Enterprise App Store.
- Not all Apple requirements must be met.
- The release of app updates is not delayed by a review by Apple.
- Some enterprise app stores (such as Relution) can also be used without device management (MDM).
- An existing user management system (ActiveDirectory / LDAP) can be connected so that users do not need new access data.

Distribution of iOS Apps via Enterprise App Store – Disadvantages

- Apps are available to end users through a special mechanism approved by Apple but requiring initial configuration by the user (see here →).
- *Apps need to be re-signed & deployed after one year with an updated Provisioning Profile. This is not a disadvantage in this case, because Relution can automate these tasks.*
- The infrastructure for distribution can be provided, for example, as a cloud service or on-premises.
- According to Apple guidelines, the distribution of apps may only be made to employees, prospects and partners, but above all, to a known group of users.

Distribution of Android Apps via Enterprise App Store – Advantages

- Apps can be distributed to selected user groups, for example, as a deep link or after logging in with a previously configured username and password.
- Users do not need Google ID to install apps from an internal enterprise app store.
- Not all Google requirements must be met.
- The publication of app updates is not delayed by technical scans by Google.
- Some enterprise app stores (such as Relution) can also be used without device management (MDM).
- An existing user management system (ActiveDirectory / LDAP) can be connected so that users do not need new access data.

For version 26.4.0

Distribution of Android Apps via Enterprise App Store – Disadvantages

- Apps are available to end users through a special mechanism approved by Google but requiring an initial configuration by the user
- The infrastructure for distribution must be provided, for example, as a cloud service.

Identity Certificate

An expired identity certificate can block the secure communication between Relution and your devices. Learn how to identify affected Apple and Windows devices and manually renew the certificates here.

Apple and Windows devices enrolled in Relution receive an Identity Certificate. This is valid for one year and is automatically renewed as long as active communication with the device exists.

However, it can happen that devices are stored or inactive, preventing the identity certificate from being renewed in time. For security reasons, Relution blocks all communication with the device if the identity certificate has expired.

Checking and Renewing the Identity Certificate

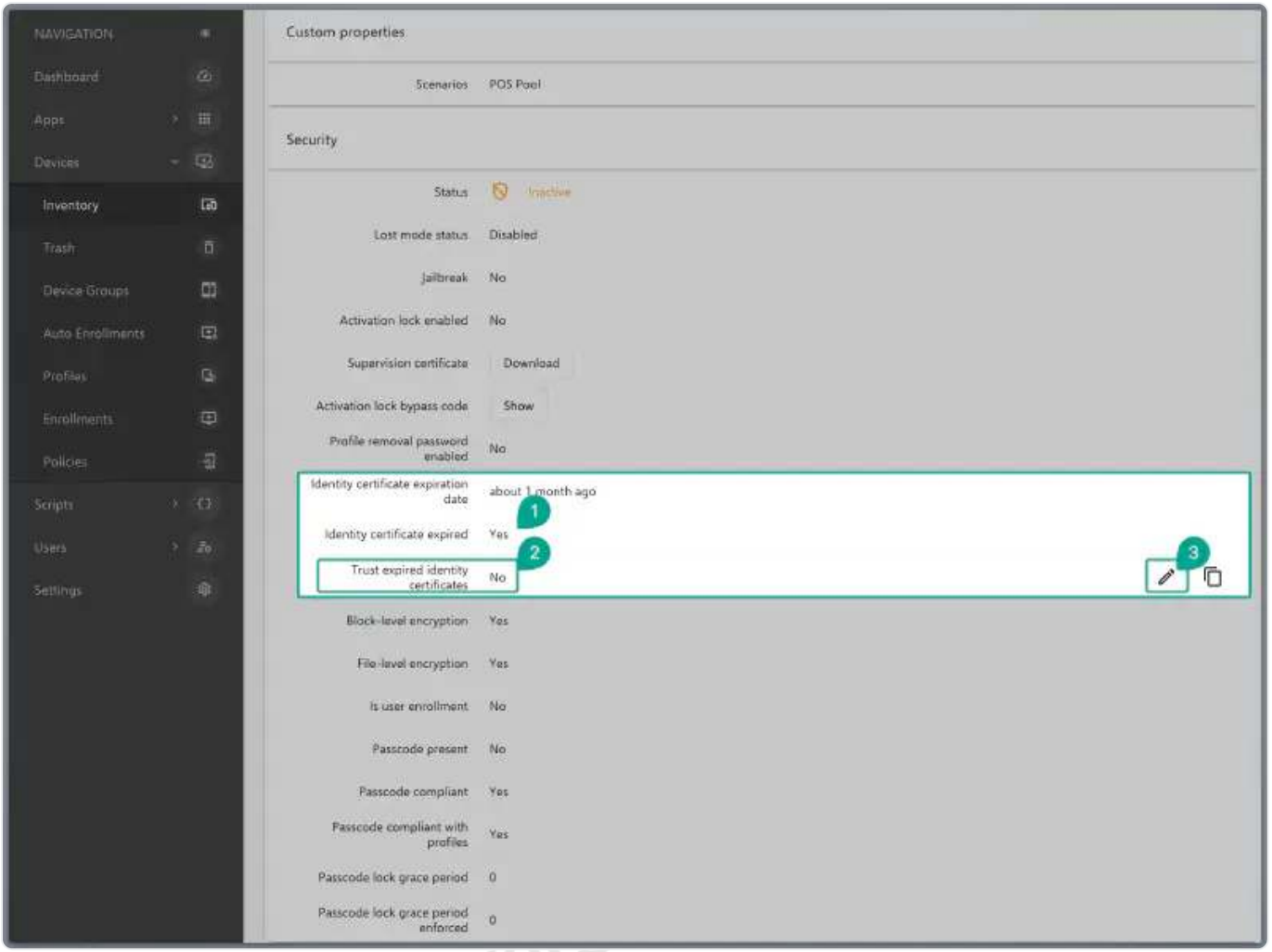
Affected devices can be checked under `Navigation` → `Devices` → `Inventory` → `[Your Device]` in the Information tab within the Security block.

The following three relevant fields are shown here:

- Identity Certificate Expiration Date
- Identity Certificate has expired
- Trust expired identity certificates

If an identity certificate has expired, the edit mode can be activated by hovering the mouse over the point Trust expired identity certificates, and the certificate can be renewed. This action restores the communication with the device as trustworthy, allowing MDM commands to be processed.

For version 26.4.0



Important Note: This action can be performed in the portal at any time. As soon as the devices are online, they will automatically update to the valid certificate.

Alternative app marketplaces

iOS 17.4 introduces support for third-party app marketplaces for devices in the European Union (EU). With the introduction of a special developer permission, third-party developers can now create their own alternative app marketplaces that can be downloaded and installed on devices running iOS 17.4 and later. Alternative app marketplaces offer a new distribution method for applications that allows users in the EU to download apps outside of Apple's App Store

Configuration via Relution restriction

The configuration `Allow installation of alternative app marketplaces` has been added to the restrictions. This allows the value to be easily adjusted in Relution

Configuration via Apple Configurator 2 Configuration in Relution

1. create a new policy with the name `Restrict Marketplace`
2. add an `Apple Configurator 2 configuration` in this policy
3. create an empty text file with the following content and save it as `restrictMarket.mobileconfig`

For version 26.4.0

> Show full configuration example

1. assign a name in the `Apple Configurator 2 configuration` and upload the mobileconfig file created.
2. publish the policy and assign it to devices with iOS 17.4 or higher

> Important! If the policy is assigned to devices under iOS 17.4, it must be removed and reassigned.

Data separation

When using mobile devices, data of all kinds is accessed. Data protection conformity must be guaranteed. A distinction is made between company-owned devices, so-called “Corporate Owned devices” (COD) and user-owned devices, so-called “Bring Your Own Devices” (BYOD). For both types of use, the manufacturers of the mobile device operating systems iOS and Android now offer their own technologies for data separation. In the following, these “on-board means” and their implementation in Relution are described in detail.

iOS – Corporate Owned Devices

Differentiation managed / unmanaged

Since iOS12, Apple basically distinguishes between “managed” and “unmanaged” for the following objects:

Managed Devices

1. Apps- pushed by Relution or installed via the Relution Enterprise Appstore, server configurable.
2. Mail Accounts - configured by Relution via a policy.
3. Contacts - loaded from managed mail account to the device (synchronized).
4. Documents - loaded from managed mail account to the device (synchronized).

For version 26.4.0

Unmanaged Devices

1. Apps - installed by the user from the Apple AppStore, non-server configurable.
2. Mail Accounts - configured on the device by user.
3. Contacts - created by user.
4. Documents - generated by user in unmanaged apps or received in unmanaged mail accounts.

An unmanaged app can be converted into a managed app by being pushed by Relution again. It replaces the unmanaged app of the same name on the device. However, unmanaged mail accounts, contacts and documents cannot be transferred to managed.

Access restrictions

In iOS, the data is separated on the system side by means of a policy that determines whether access to managed data from unmanaged apps is allowed or not. For this purpose, the configuration Restrictions as part of a policy in Relution offers the following restriction options:

- Prohibit opening managed documents in unmanaged apps.
- Allow opening of unmanaged documents in managed apps.
- Deny unmanaged apps access to managed contacts.
- Allow managed Apps to write unmanaged contacts.
- Generally consider AirDrop targets as unmanaged.
- Prohibit moving mails to unmanaged mail accounts.

For example the following can be prevented:

- A private app (e.g. WhatsApp) that sees business (Exchange) contacts.
- A business mail is forwarded at will.
- An attachment of a business mail is opened in any app (e.g. Dropbox).

Which web content iOS treats as managed, e.g. downloads from the intranet, is defined via the configuration Managed Domains →. Email domains can also be specified there so that the Mail app marks external recipients.

iCloud restrictions

In order to prevent the uncontrolled outflow of data, Relution offers the possibility to prohibit or at least restrict cloud accounts completely. The following functions can be switched off:

- iCloud backups
- iCloud keychain synchronization
- Allow managed apps to store data in the iCloud
- Saving photos in the iCloud
- Synchronization of iCloud documents.

Functional restrictions

Finally, there are some iOS system functions that can be considered under data security criteria and can also be switched off by restriction:

- App Block-/Allowlisting
- Web-URL Block-/Allowlisting
- AirDrop (can be switched off completely)
- Share password
- Access to Apple AppStore
- Screenshots and recordings
- Camera (can be switched off completely, also for in-app functions)
- Creating and modifying accounts (Mail, Apple IDs)
- Bluetooth
- Installation of VPN profiles
- USB connections.

For version 26.4.0

Via app VPN

As an important data protection measure, iOS offers the option of permanently coupling the data connection of apps to a VPN connection, which in turn can be reconfigured by the Relution server. This ensures that certain apps only run over the company's own network and external access is prevented (intranet-only).

iOS – Bring Your Own Devices

Until iOS 12, it was common to use a container app on iOS BYOD devices that could be configured on the server side and thus ensured separation of business and private data.

In the meantime, however, iOS offers a built-in “container solution” to separate business from private applications and data. For this purpose, an iOS device is added to Relution via a (BYOD) enrollment in the inventory. This installs an MDM profile on the device, allowing it to be managed via Relution. Technically, a distinction is then made between “managed” and “unmanaged” apps and content. This turns the iOS device into a “dual persona” device and completely separates the data. Restrictions can also be used to control whether data can be shared between “managed” and “unmanaged” apps.

Different configurations can be loaded on the devices and managed via Relution:

- Apps
- VPN configuration
- Notes (more system apps will follow in future iOS versions)
- iCloud account
- Keychain
- Mail accounts / attachments
- Calender accounts / attachments.

If the MDM profile is removed, all managed apps and content are deleted. This action can be performed via Relution or on the device itself.

For version 26.4.0

Class lists (Shared iPad)

The Class Lists for Shared iPads feature in Relution optimizes the login process for students using Managed Apple Accounts. Instead of manually typing in the full, often long Managed Apple ID, students can simply select their class and their name or initials.

Prerequisites

To use this feature, the following conditions must be met:

- DEP Token: At least one valid DEP token at the respective location.
- Managed Apple IDs: Availability of Managed Apple Accounts.
- Compatible Device: An Apple Shared iPad configured via the same DEP token used to manage the Managed Apple Accounts.

Configuration

For version 26.4.0

Follow these steps to activate the class lists:

1. Open Policies: Navigate to the Policies section in Relution.
2. Create Policy: Create a new iOS policy or edit an existing one.
3. Add Configuration: Add the Shared iPad configuration.
4. Select Classes: Choose the classes to enable for login on the Shared iPad.
5. Completion: After assigning the policy, the available classes will be offered for selection on the iPad lock screen.

Important Troubleshooting Notes

Login issues are often caused by a discrepancy in the account data:

- Account Alignment: Check the Apple Account stored for the user in Relution.
- Example of Discrepancies:
  - Account in Relution: `student@relution.io`
  - Account in Apple School Manager: `student@appleid.relution.io`
- Solution: The accounts must match exactly for the class list login to function.

> Tip: Test the login manually using the traditional Sign in to iPad method. If the credentials work there but not via the class list, there is likely a discrepancy in the stored user data.

Recommended restrictions

A large number of restrictions can be configured for iOS devices. Not always, every setting is useful or leads to the desired result. Sometimes, the settings also bring problems if their effects are not fully understood. In this article, we will limit ourselves to some potential problems that one can run into as a user and name recommended settings.

> Many restrictions can only be configured on devices in supervised mode. These are indicated by the note Being supervised

Allow connecting to Macs or PCs

This setting only has an effect if the connection to Macs or PCs has basically been allowed in the DEP profile. If this is not the case, the corresponding setting in the restrictions has no effect.

Activate delay of operating system updates

A value between one and 90 days can be defined here. During this time, new system updates are not displayed to the users and are therefore not installed. This also includes security updates.

For version 26.4.0

Allow USB connection in locked state

If devices are no longer online, they can be brought back online e.g. by an external network card (Lightning/ Ethernet adapter). However, if devices are locked, e.g. in Lost Mode, the external accessories cannot be released by users and therefore do not work. This setting prevents this.

Allow to delete all contents & settings

This is the factory reset. To make it unavailable, uncheck it.

Prohibit turning off the WiFi

If this option is enabled, users will not be able to turn off the WiFi, even in flight mode. Switching between WiFi networks is still allowed.

Force automatic date and time setting

The setting only works if location services have been enabled on the devices. The devices will set the date and time automatically. This is also done based on the time zone it is in. This cannot be determined if location services are disabled.

Force WiFi whitelisting

If this option is enabled, devices will only be able to connect to networks that have been brought to the devices via policy. Before enabling this feature, make sure that the transferred networks are working on the devices. It is not possible to manually add WiFi connections afterwards.

Silent app installation

To install apps `silently` on iOS devices, it is necessary that the devices are in `supervised mode` and either VPP licenses are available for the app, or users are logged in to the devices with an Apple ID.

If these conditions are met, apps can be installed on devices via Relution without users having to confirm this on the end devices. Make sure that sufficient VPP licenses are available.

> If there is a lack of VPP licenses, a prompt to log in to the App Store may appear on devices. This can also happen if Relution and the Apple VPP server are not running in sync. In this case, switch to the Purchased Apps section and perform a synchronization there.

For version 26.4.0

Add and update native apps

With Relution it is possible to distribute native iOS apps and to do release management. This means that different versions can be provided for different groups of people. For example, users can have version 1.0 of an app in productive use, while a group of key users tests version 1.1 without the users noticing. To do this, version 1.0 must be uploaded to Relution at the beginning and set to the status `Productive`.

Automatic distribution and installation of native apps is not possible with Android Enterprise.

Create a new app.

To do this, click on `Apps` → `App Store` in the menu. Here, an `App type` can be selected via the `Add` button. Click on `Native App`.

Now select the appropriate file of the app to upload.

> Pay attention to the size of the file. For large apps, problems may occur if the database or reverse proxy does not allow it. In this case, the configuration will need to be adjusted.

Specify the appropriate release status and click `Save`.

This app can now be seen and installed in the `Relution Agent` of the corresponding platform by members of the groups `Appstore User` and `Device Manager`. The permissions can also be adjusted at this point. Regardless of this permission, administrators can also distribute this app to devices via the Relution portal.

For version 26.4.0

Update app

If a new version is to be tested for the app, it can be set to the status ‘Development’ or ‘Testing’ in advance. Before that, the new version must be selected and uploaded via the ‘New Version’ button.

In the example the app is in the status `testing`. It will be automatically moved to `Productive` status on 5/31/2022. The `release date` can be used optionally.

Both versions can be viewed in the app properties.

Users:inside with appropriate permission can also view, install and test the app on endpoints.

Manual go-live of the new version

In the Relution portal the respective versions can be viewed and configured. By clicking on the button ‘Productive’ the new version is moved to this status. If a version is already in the productive status, it will be automatically moved to the ‘Archive’.

The app is not automatically updated on endpoints. This must be done manually by the users through the Relution Agent or triggered by the administrators through a manual Install App action.

For version 26.4.0

Manage App Store apps

Apps from the Apple App Store can be distributed to managed devices through Relution. An app license is required in every case — including for free apps.

Obtaining a license

An app license can be obtained in two ways:

- through the Apple `Volume Purchase Program` (VPP),
- or through an Apple ID signed in on the device.

Which route makes sense depends on the deployment scenario. On devices operated without an Apple ID, a VPP license is mandatory.

Setting up VPP →

Apps from Apple School Manager and Business Manager

Apps purchased in Apple School Manager or Apple Business Manager are synchronised to Relution automatically (from version 5.10). They appear there with the release status productive and are ready for distribution straight away.

If an app is not meant to be available to all users, the release status can be changed manually.

For version 26.4.0

Adding apps manually

Apps can also be added to the Relution App Store by hand at any time. Two restrictions apply:

- No VPP licenses are available automatically for manually created apps.
- Installation only succeeds on devices where a user is signed in with an Apple ID.

VPP licenses for such apps can be obtained later.

Forcing an update

App Store apps are updated by the operating system on its own. In rare cases this does not happen. The device action Install app triggers an update: the device starts the installation again and compares the app version against the App Store. If a newer version is available there, the existing app is updated.

Actions Not Being Processed

In school environments and other scenarios where iOS devices are centrally managed using Mobile Device Management (MDM), disruptions can occasionally occur. One common issue is the failure of devices to process MDM actions, which can cause significant problems – either during ongoing lessons or in the general operation of the devices. This article describes potential error patterns, analyzes their underlying causes, and provides solutions to address such situations.

Expired Certificates

Error Pattern: MDM actions remain in the `pending` status and are not executed by the device.

Cause: The identity certificate of the iOS device has expired. This often occurs in devices that have been stored for an extended period and were not in communication with the MDM server shortly before the automatic renewal of the certificate.

See also: Identity Certificate → — it describes the validity period and automatic renewal, as well as manually renewing an expired certificate via the `Device Details` section.

VPN Apps

For version 26.4.0

Error Pattern: iOS devices get stuck during lessons, or time-based configurations, such as starting or ending a lesson, are not executed.

Cause: Often, end users, particularly in educational contexts, install VPN apps on their own, which blocks communication with the MDM server. Some VPN apps also offer a `Kill-Switch` feature, allowing users to intentionally disconnect all internet communication. This interrupts MDM actions, such as starting or ending lessons. On affected devices, VPN apps can be identified in Relution under `Installed Apps`.

Solution: In Relution, it is possible to restrict the installation or use of VPNs. To achieve this, go to the Restrictions and enable the option `Disable VPN Configuration`. With this setting, it will no longer be possible to create unmanaged VPN configurations on the devices.

DNS

Error Pattern: iOS devices get stuck during lessons, or time-based configurations – such as starting or ending a lesson – are not executed.

Cause: A common reason is that end users, especially in schools, configure an alternative DNS manually. This can block communication with the MDM server, causing MDM actions to fail. On affected devices, navigate to `Settings` → `WiFi` → `DNS` to check for custom DNS configurations.

Solution: To prevent such issues, a configuration for `Encrypted DNS Settings` can be applied in Relution. This ensures that changes made to the DNS by end users will not take effect (even if the configuration remains possible), prioritizing communication through the managed DNS server.

Reliable Providers and Configuration Guides

- Google DNS →
- Cloudflare DNS →

For version 26.4.0

Optimize Relution Shared Device

When a user changes in `Relution Shared Device Mode`, depending on the configuration, many apps resp. several gigabytes of data are downloaded. This can lead to delays in teaching due to the high data volume with a large number of downloads and installations.

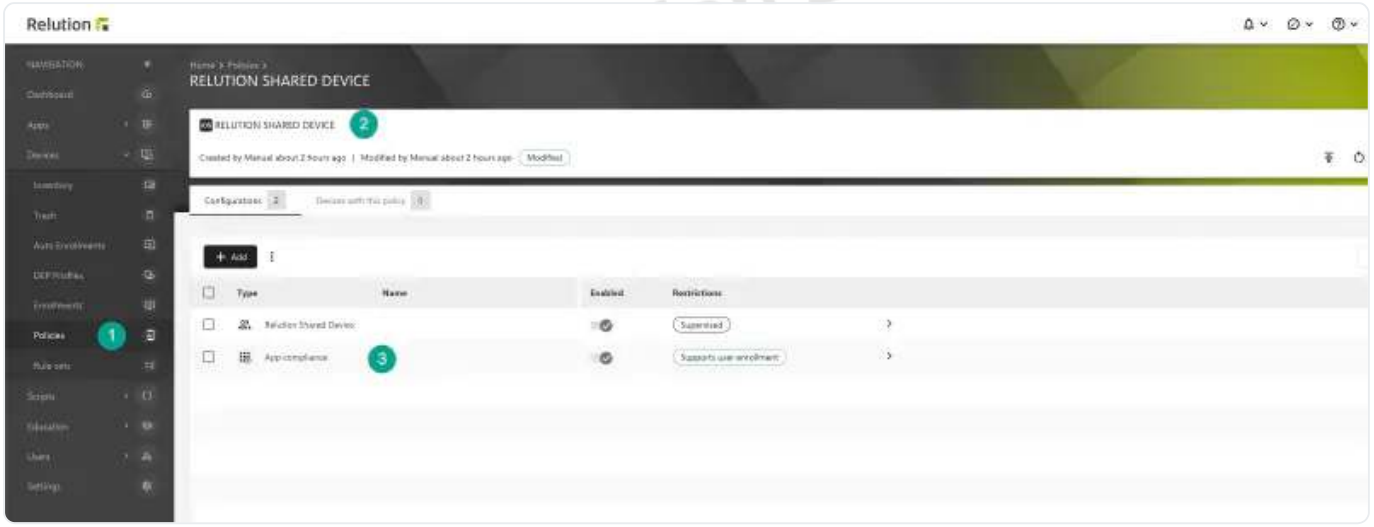
In order to be able to remove temporary content from used apps when the devices are used by multiple users, Relution must delete the apps from the devices during a user logout. More information is available at the following link
. Multi-user mode →

Optimizations

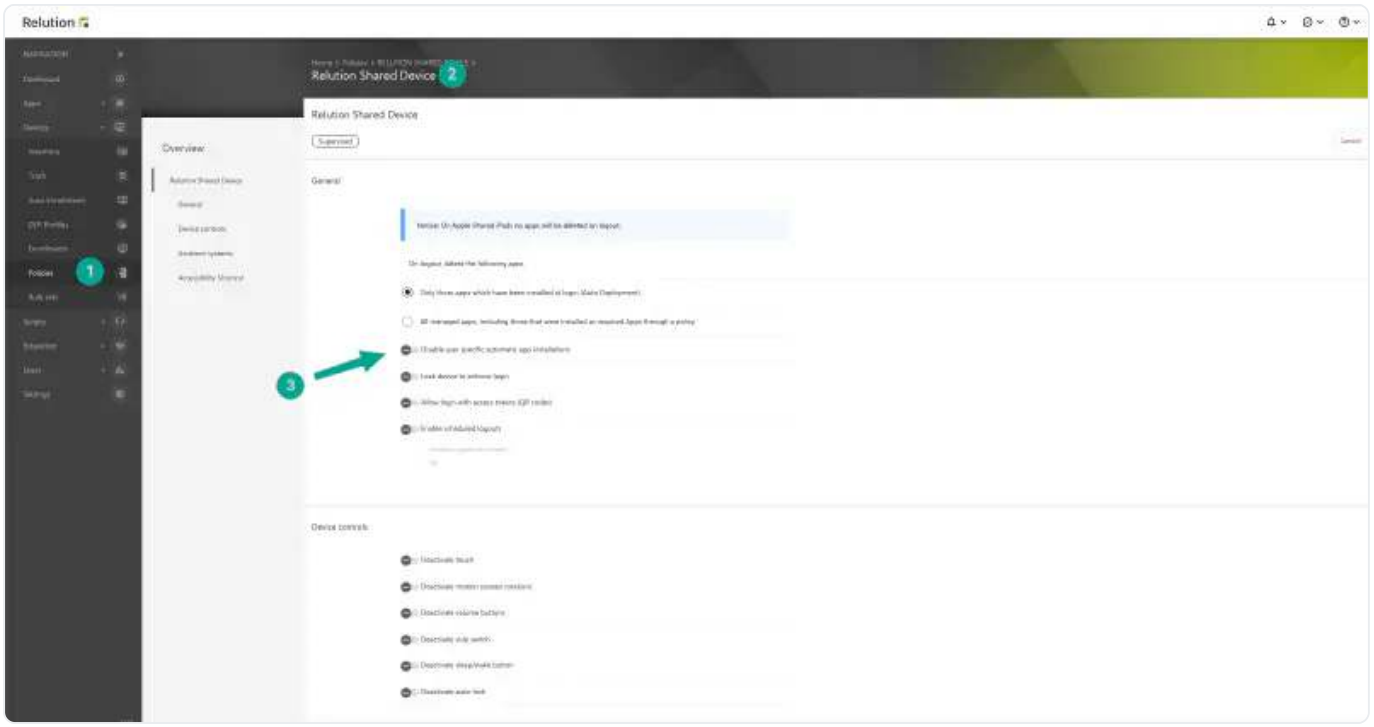
The following measures are recommended to keep class delays as minimal as possible:

Minimize App Conformance and Auto Deploys.

Keep the `Required Apps` list in their `App Conformance` policy configuration relatively small. A small base set of apps for all devices is usually sufficient. Note that each app must be transferred through the network multiple times, once for each device on which the policy applies. So 50 MB quickly becomes 5 GB when classes start.



In addition, `auto-deployments` for user-specific apps can be disabled to keep the user login footprint as small as possible.



Alternatively, required apps can be retrofitted to user devices at any time via the Relution Agent.

Teaching profiles via Relution Teacher.

After following the above measure, if there are no or only a few apps stored in `App Conformance` and `Auto Deployments`, teachers can use the Relution Teacher App and `Teaching Profiles` to predefine all required apps for the lessons. This way, only the apps needed for the particular lesson will be loaded.

For version 26.4.0

Not Now

Actions for iOS devices are shown as `Delivered` and never complete.

Actions are commands that Relution executes on enrolled devices. These can be triggered either implicitly by a policy configuration or explicitly by applying an action. An overview of all pending and executed actions can be found in device details under the `Actions` tab.

Device has been restarted

- The device has been restarted and has not yet been unlocked
  - The digital keychain is locked until a device is unlocked for the first time after a restart. As a result, the operating system cannot yet access stored passwords and therefore cannot connect to an encrypted Wi-Fi network

Action in the User channel

- The action was sent on the user-channel and no user is currently signed in on the device

For version 26.4.0

Device has connection status Not now

In some cases, iOS/iPadOS devices respond to commands from the MDM server with `Not now`. This always happens when the device is not ready to communicate with the MDM server at that moment

There are various reasons that can lead to a `Not now` response. The following list contains possible triggers currently known to us, but the list is not exhaustive.

- The device is locked / user interaction is required
  - Some commands cannot be executed while the device is locked, including
    - Applying certain restrictions
    - Configuring a Wi-Fi connection
    - Installing or updating apps
    - Installing certificates that require user consent
- Network or battery status
  - The device has too low a battery level to start the process
  - The device's network connection is unstable
- User delays software updates
  - An update is to be scheduled (`ScheduleOSUpdate` or `InstallLater`) and the user explicitly delays the update
- The device is not yet fully enrolled
  - Some commands can only be executed after the device has completed the DEP enrollment and/or supervision process
- The device is otherwise busy
  - The system is currently performing a critical task (Update, iCloud backup, or restore)

Solution

- Unlock the devices and establish a stable Wi-Fi connection
- If necessary, log in to the device with a user account
- Confirm any dialog boxes from the operating system
- Charge the device beforehand if necessary

Further information

The “Not Now” status is normal behavior of iOS/iPadOS and is not specific to Relution

Since version 5.8.1, Relution is able to understand `Not Now` responses from devices. If a device responds to a command with `Not now` Relution changes the connection status for that device in the inventory accordingly. To get devices in this state to communicate with the MDM again, they usually need to be unlocked and any pending operating system updates need to be performed, for example.

Some actions, such as `Lost Mode` and `Reset Password` are prioritized by the device and accepted even in this state. Since version 5.9, Relution also treats these actions as a priority and skips all currently pending actions. This ensures that devices that previously responded to actions with `Not now` can still be put into Lost Mode or that a forgotten password can still be changed.

Apple Dev-Doku Not Now Status →

For version 26.4.0

Device names

- DEP devices lose the previously assigned device name in the device inventory after reset.
- Export of `CSV` file from `Devices` → `Inventory` cannot be imported at `Devices` → `Auto enrollment` and vice versa.

Cause

- The name from `Auto enrollment` overwrites the subsequently changed device name from the device inventory.
- The format of the exported `CSV` file is different from the format of the imported `CSV` file and contains different fields.

Solution.

Export the `CSV` file with the desired device names from the `inventory` and transfer the data to the template format of the `CSV` file of `auto enrollment` to be imported.

`CSV` file templates for `Auto enrollment` and `Inventory` can be downloaded. This provides the correct format template for the name changes in each case.

> The first line of the format template is required and should not be changed.

For version 26.4.0

Copy the serial number and device name from the exported data and then import it at `Auto Enrollments`. If devices are newly enrolled, the correct device name will now be entered at the `Auto Enrollments`.

Instruction

1. Export the inventory list.
2. Download the format template for import at `Auto enrollments`.
3. Import the corresponding data from the export into the format template for import. Import the filled format template at `Auto enrollments`.

Multi-user mode

Relution and Apple each offer their own multi-user mode.

Relution Shared Device and Apple Shared iPad.

Both modes bring different features. A detailed description of this can be found in our Insights:

Relution Shared Device →

With iOS 17.x, using the restriction configuration allowCloudKeychainSync false leads to a slower login on Apple shared devices

Defined requirements to support decision-making.

Define requirements for multi-user mode devices to better decide on one of the two solutions. The following points provide guidance:

- GDPR-compliant work
- Availability of `Apple Classroom` for teachers
- Simple log in without user name and password
- Low available bandwidth
- No users and/or classes created in Relution
- Shortest possible login times
- Use of system apps necessary
- Use of personal drives
- Use of `Relution Teacher`

For version 26.4.0

Comparison of requirements

The requirements are only partially supported by both modes:

Function	Relution Shared Device	Apple Shared iPad
GDPR-compliant operation	Yes	Only in guest mode
Are students shown online in the Classroom app?	Yes	Not in guest mode
Login without username and password	No	Yes
Low available bandwidth	Configuration-dependent	Yes
No users and/or classes created in Relution	No	Yes
Shortest possible login times	Configuration-dependent	Yes
Use of system apps required	No	Yes
Use of personal drives	Yes	No
Use of the Relution Teacher Console	Yes	Only in combination with Relution Shared Device
Use of a SIM/eSIM	Yes	No

For ver

Guest mode

If the fastest possible log in time is required and little bandwidth is available, Apple ‘Split iPad’ is suitable. It allows logging in in the so-called `Guest Mode`, which ensures anonymous use. As a `guest`, however, the devices are not displayed as `online` in `Apple Classroom`. To work in a GDPR-compliant manner and use `Apple Classroom`, Apple’s multi-user mode is out of the question. With the `Relution Shared Device` mode, this combination is possible.

System apps

Since Relution can only delete temporary data and content from apps by uninstalling them from devices, it is not recommended to use system apps that store data. For example, the Safari browser is one such system app. It cannot be uninstalled, which means that content and open tabs of previous users are still available and can be viewed when a user changes. To get around this problem, alternative apps can be used, such as the Firefox browser, which can be deleted from the device.

Photos

When it comes to photos, the native camera should also be disabled on iOS devices. Otherwise, created pictures are automatically saved in the system app `Photos`, which cannot be deleted either. Thus, created photos cannot be removed by Relution. Alternatively, Relution Camera offers the option to save created photos not on the devices, but on a configured network drive.

Microsoft applications

When using Microsoft apps such as `Teams` or `Excel`, the following special feature must be taken into account:

If devices are operated in `Relution Shared Device` mode and users do not log out of these apps, the log ins are stored in the digital keychain of the devices and cannot be removed by uninstalling them. Users need to be made aware that logging out of these apps is mandatory. Alternatively, Apple `Shared iPad` can be used.

Combination of both multi-user modes

It is possible to activate `Relution Shared Device` and `Apple Shared iPad` at the same time. The combination combines the advantages of both solutions. Through the Apple `Guest Mode` system apps can be used without leaving any data on the devices. At the same time, through the `Relution Agent`, teachers can apply `Teaching Profiles` with relevant apps and features on student devices.

> When using Guest Mode on student devices, Apple Classroom cannot be used by teachers.

For version 26.4.0

Folder homescreen layout

With Relution Homescreen Layout it is possible to arrange apps and place them clearly in different folders.

Problem

When setting up the policy configuration `Homescreen Layout`, no folders are created in the simulator.

Solution

In order to create a folder, when using the `drag & drop` functionality of the simulator, make sure to position the app absolutely still over another app icon for a short period of time so that a folder is automatically created.

> Homescreen layout is currently limited to 20 apps per page.

For version 26.4.0

Create an Apple Case

After operating system updates on Apple devices, unexpected malfunctions or issues may occur in some cases. In such situations, we recommend opening a Case with Apple directly to expedite the analysis and resolution of the issue.
Afterward, send us the Case ID of the Apple ticket via our support team. We will forward it to our Apple contacts to further support and expedite the process.

Creating an Apple Case

1. Visit the website:
   Apple Feedback Assistant →
2. Log in with the ASM/ABM ID.
3. On the first visit, there is an option to select between:
   - Beta Program
   - Developer Program
     Select Beta Program.

Which topics can be reported?

For version 26.4.0

Cases can be submitted for the following Apple platforms:

- iOS / iPadOS
- watchOS
- tvOS
- macOS
- HomePod
- visionOS
  Of particular importance to us are iOS / iPadOS and macOS.

Important details when submitting a case

For example, when reporting issues with *iOS / iPadOS*, the following fields should be completed:

- Title of the Issue
- Category:
  `Something Else Not on the List`
- Type of Issue:
  `Incorrect / Unexpected Behavior`
- Description of the Issue (in English)
  → Provide a detailed and precise description.

Required information in the issue description

Please ensure the following details are included:

- Operating system version of affected devices
- Time/conditions under which the issue occurs
- Reproducibility: How can the issue be reproduced?
- Attach system diagnostics
  → How to generate this is explained via the ?-Symbol in the form.

Filter for content (Built-In)

Google search results contain inappropriate search results despite enabled `Auto-Filter`. Web pages containing inappropriate content are blocked as expected. However, inappropriate content is still displayed in the search results under the category `Pictures and Videos`.

Problem

Apple's content filter does not offer the possibility to restrict Google's search (e.g. Safe-Search). Apple's automatic filter filters web pages based on `adult language` and not on media content like images or videos. Google's image search is not restricted by this.

For version 26.4.0

Solution

To further restrict the search results, appropriate third-party apps or a network-level content filter (proxy/VPN) are required.

Link collection

The following websites give an overview of apps that can be used to filter inappropriate content. On the part of Relution, the recommended apps of the external sites have not been tested - therefore, explicitly no binding statement can be made about the quality and/or suitability of these apps.

wondershare →

WithSecure →

QR code cannot be scanned

On iOS devices, it can happen that in the course of an applied policy configuration with ‘app compliance’, the QR code scanner of the camera is disabled. The camera recognizes an existing QR code, but does not offer the link to open it in the browser. The problem only occurs in conjunction with a `positive list` in the `App Conformance` configuration.

How To

The app or plugin must be manually added to the `positive list` of `app compliance`.

1. Go to the configuration of the corresponding policy.
2. Create a new `positive list` entry for `add app manually`.
3. The name can be chosen freely. As `internal name` enter `com.apple.barcodesupport`.
4. Save and publish the policy.

For version 26.4.0

Locked Device

If iOS devices are protected with a PIN and are restarted, they cannot be connected to a password-protected WALN until they are unlocked, as the OS cannot access the keychain. A similar situation can be brought about by activating lost mode. Therefore, without a network connection, no actions such as resetting the password or deactivating Lost Mode are performed.

LAN to Lightning / USB-C adapter

This can be used to establish a LAN connection to the end device via an RJ45 adapter so that the device can establish an Internet connection and process MDM actions. However, the prerequisite for this is that the option `Allow USB accessories in locked state` has been set in the restrictions before locking the device.

Known open WLAN

If an open / unprotected WLAN was known to the device before it was locked, the connection to this WLAN can be established automatically by the device without unlocking and MDM actions can be processed again.

> Outdated for iOS 18.X

For version 26.4.0

Reset device

Resetting the affected devices to the factory settings is always a valid option. It is always possible to completely reset iOS devices via DFU mode → to reset them completely.

Weblinks

Weblink can be deployed as an app in Relution. This is useful if, for example, a weblink is to be deployed user- or group-specifically (auto-deployments) or placed in the policy configuration `Homescreen Layout`.

1. Create Weblink

1. Click on `Add` in Relution under `App Store`.
2. Select `Web Link`.
3. Click on `Next`.
4. Enter the URL of the link.
5. Click on `Add details`.
6. Activate the sharing status `Productive`
7. Assign a name
8. Optionally enable Open in full screen so that the weblink starts as a web app (see Open a weblink as a web app →)
9. Click on `Save` in the upper right corner.

2. Deploy weblinks on iOS devices

For version 26.4.0

Option ‘2a’ or ‘2b’ must be selected here. If web links are distributed via the autodeployments, it is possible to arrange them in the home page layout (3).

2a. Distribute Weblink via auto deployments

Weblink cannot be deployed as a `Required App` in the `App Compliance` policy configuration. However, it is possible to automatically deploy Weblink to specific users or user groups via `Auto Deployments`.

1. Open the corresponding user account or group.
2. Click the `Add` button at the bottom of the `Auto Deployments` section.
3. Select the created web links and click `Add`.
4. Click `Save` at the top.

The added web links will be immediately displayed on the devices where the corresponding user or a member of the corresponding user group has logged in.

2b. Provide a web link via the policy

Web links can also be provided with the configuration `Web link`, for this purpose, a configuration via policies must be created as follows:

1. In the page navigation, go to `Devices` > `Policies` > `Add` or open an existing policy
2. Click on the button `Add` > `Weblink` > `Add Details` to create a weblink configuration
3. Label and URL (e.g. `https://relution.io`) are mandatory.
4. Application to open weblink with: A third-party browser app can be selected here, e.g. Firefox. If no entry is made, Safari is used. For display as a web app, the field remains empty.
5. Removable: The web link can be removed by the user.
6. Precomposed icon: If enabled, iOS does not add any visual effects to the uploaded icon. The option dates back to older iOS versions that added a gloss effect to icons.
7. Full screen: The web link starts as a web app instead of in Safari (see Open a weblink as a web app →).

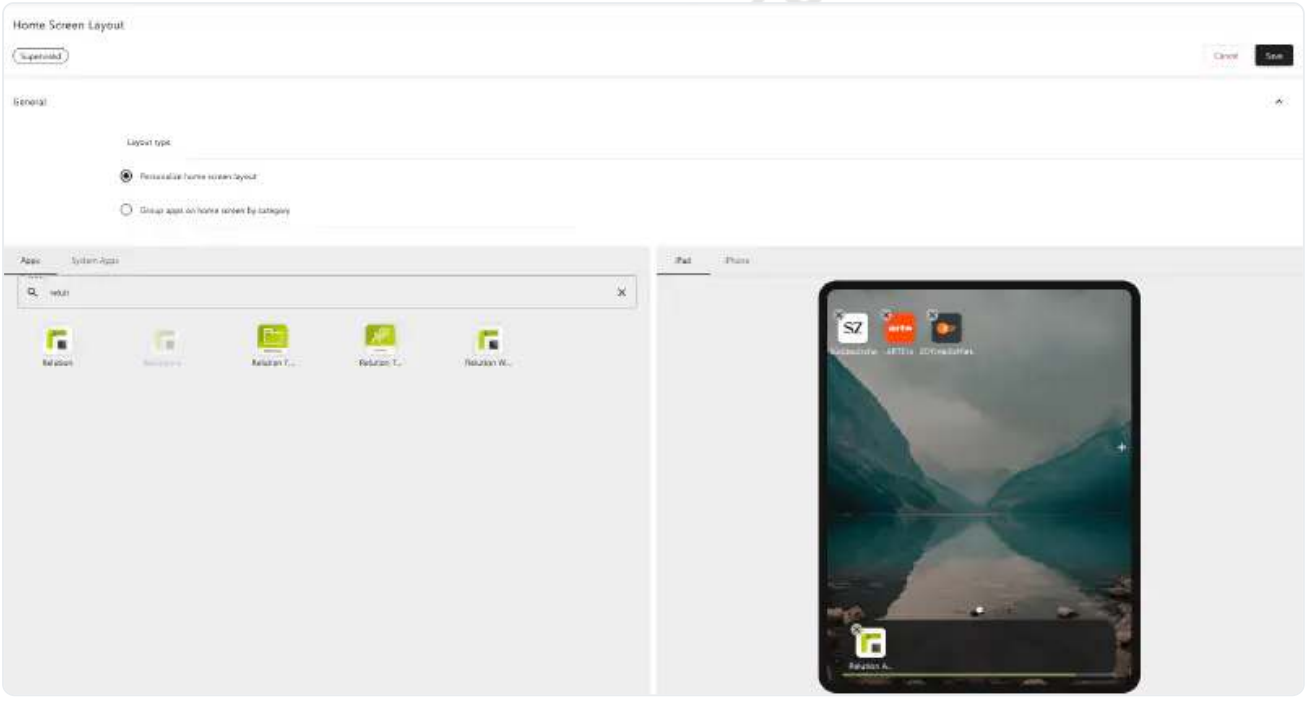
With Relution 5.32.0, placeholder can be used on Web links to include a user name.

---

3. Optional: Arrange Weblink in Homescreen Layout

The policy configuration `Homescreen Layout` can be used to place apps and web links specifically on the homescreen of iOS devices.

1. Navigate to the menu item `Devices` → `Policies` in the Relution portal and click on `Add`.
2. Create an iOS policy and assign a `name`. Click on `Save`.
3. After clicking `Add`, select `Homescreen Layout` option and proceed to `Add Details`.
4. If existing web links have previously been assigned to a category, they can be automatically placed in created folders on the homescreen. To arrange them manually, uncheck the option `Group icons by category`.
5. Then place the relevant apps and web links in the desired order using drag & drop.



6. Click `Save` and publish the current version of the policy.
7. To apply the policy to iOS devices, add the desired devices using the `Devices with this policy` tab. The selected settings will then be automatically applied to the devices.

> To display a web link in the home screen layout, steps 1+2 or 1+3 are necessary. The URL in the web link must be identical when creating it in the Relution store and in the web link configuration.

Open a weblink as a web app

On the device, a weblink starts either as a bookmark in Safari or as a standalone web app. This is controlled by the option Open in full screen (weblink in the App Store) or Full screen (configuration `Weblink` in a policy):

- Option disabled: The weblink opens the page in Safari, with address bar and tabs.
- Option enabled: iOS starts the page as a web app in its own window without the Safari interface. In the app switcher it appears as a separate app.

Whether the page is actually displayed as a web app also depends on the website itself. It must support web app mode, e.g. via a web app manifest with `"display": "standalone"` or the meta tag `apple-mobile-web-app-capable`. Without this support, iOS displays the page as in Safari even if the option is enabled.

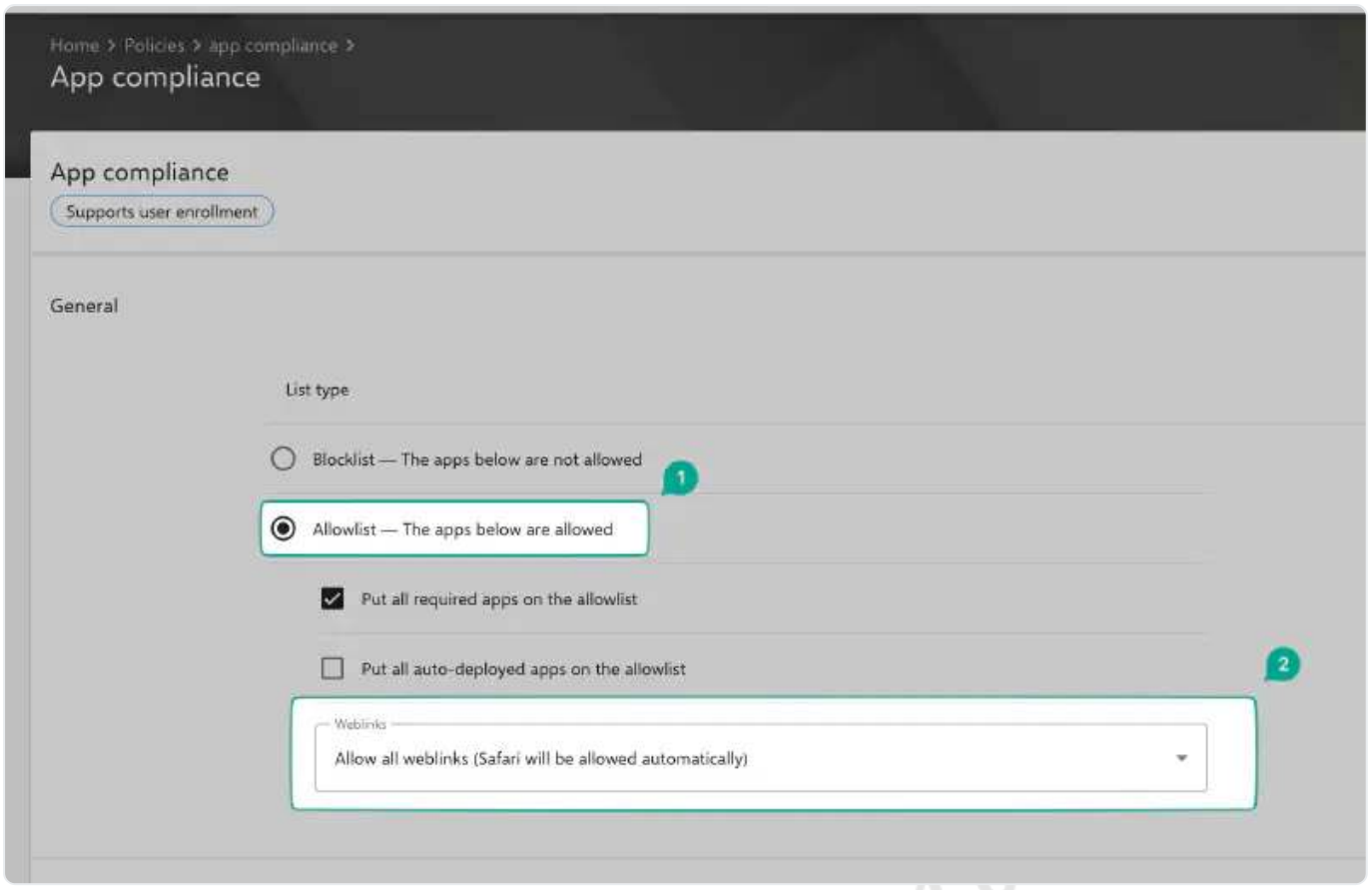
In the policy configuration, Application to open weblink with remains empty for display as a web app. If an app is selected there, the weblink opens in that app.

Web Links on Relution Shared Devices

To display and use web links on Relution shared devices, the devices must be assigned an app compliance policy. This policy needs to be configured as follows:

- Set List Type to `Allowed`
- Set Web Links to `Allow all web links (Safari will be automatically allowed)`

For version 26.4.0



For version 26.4.0

Backup

Apple iOS backups allow users to back up their important data such as contacts, photos, messages and settings and restore them when needed. These backups can be created either via iCloud or iTunes and serve as a protection against data loss in case of device replacement, damage or theft.

Standard restore via the setup wizard

A registered DEP device is restored from a backup to the same state with device monitoring status and MDM profile it was in when the backup was created. The general steps for restoring a device from a backup are described by Apple at the following link: Apple Backup→.

Data Transfer Quick Start

Quick Start data transfer allows content to be moved directly from an old iPhone or iPad to a new one by placing both devices next to each other. The requirements are that Bluetooth and Wi-Fi are enabled on both devices and that iOS/iPadOS 12.4 or later is installed.

During the setup assistant on the new device, a prompt appears on the old device asking for confirmation to continue. By scanning the animated pattern on the new screen with the camera of the old device, the devices are paired. After entering the passcode and Apple ID, select the option Transfer from iPhone or iPad, and the data will be migrated directly and securely over a wireless connection.

For version 26.4.0

Apple Quick Start →

For a device registered via Apple School/ Business Manager (DEP) to be offered the Quick Start option at all during initial setup, the following setup steps must not be skipped in the assigned DEP profile (leave the checkboxes disabled):

- `Quickly Set Up iPad`
- `Restoring from backup`

If either of these options is enabled, the corresponding step in the setup assistant is hidden, and the new device will no longer be able to receive data via Quick Start from the old device.

> On the existing device, Allow Proximity Setup must be enabled in the restrictions.

Backup

Create a backup on the device using Apple ID via iCloud or locally on a Mac or PC.

Preparation

Configure a new DEP recovery profile with the following settings:

- Enable `Allow connecting to Macs or PCs and configuring with Apple Configurator`.
- Do not enable `Allow device location`.
- Do not enable `Import backup`.
- Do not enable `Log in with Apple ID`.

Integration in Relution

Assign the device via Apple School/ Business Manager to the corresponding Relution server with the DEP recovery profile created before. After assigning, click on `Synchronize DEP devices`.

Restore backup

Start the reset device and follow the setup wizard. In the setup wizard, select `Restore apps and data`. For an iCloud backup, use the same Apple ID for the restore that was used for the backup.

During setup, the device automatically goes through the DEP registration process. Settings related to device management are not applied from the backup, but from the DEP profile configured in Relution. After a successful backup, switch back to the original default DEP profile. The setup step to restore the backup to the device will then no longer be displayed.

For version 26.4.0

Registering an unmanaged device with Apple DEP and restoring via backup

An unmanaged iOS device can be registered with Apple DEP afterwards without its users losing their data and content. However, Apple's documentation states that a restore keeps the device management status from the backup when restoring to the same device (see example below) - so an unmanaged device cannot be moved directly into a supervised DEP state from its own backup. The workaround below routes the backup through a second, temporary device: because the restore then counts as a restore to a different device, Apple takes the management status from Apple School/ Business Manager instead.

Apple documentation states:

- When you restore from a backup to the same iPhone or iPad, your device management status is restored from your backup.
- If you restore from a backup to a different iPhone or iPad, your device management status will come from Apple School/ Business Manager.

Example

If a device is configured to be supervised and automatically registered in the MDM system, but is subsequently restored from a backup created when the same device was unsupervised, the device is not supervised. In other words, an unmanaged device cannot be restored directly from its own backup when enabling `Supervised mode` and registering the device with Apple DEP in the process - which is exactly why the detour via a second device is needed.

Backup

Create a backup on unmanaged device-01 via iCloud or locally on a Mac or PC. Restore this backup onto a second device, device-02. Then back up device-02 again via iCloud or locally - this second backup is later restored onto device-01 and, since it is technically device-02's backup, counts as a backup "from a different device".

Preparation

Reset device-01 to factory settings. Add device-01 to the Apple School/ Business Manager via Apple Configurator 2. Read more in our Insight Add Apple devices to DEP afterwards →. Also configure a DEP recovery profile for device-01 as described in the previous "Preparation" section.

Integration in Relution

Assign device-01 via Apple School/ Business Manager to the appropriate Relution server with the DEP recovery profile created before. Set up the device by following the setup wizard on the device.

For version 26.4.0

Restore backup

On device-01, select `Restore apps and data` in the setup wizard and choose the backup previously created from device-02. For iCloud backup, use the same Apple ID for restore that was used for backup.

Because the backup is technically from device-02, the restore counts as a restore to a different device: settings related to device management are not taken from the backup, but from the DEP profile configured in Relution - this is what supervises and DEP-registers device-01.

After a successful restore, switch back to the original default DEP profile. The setup step to restore the backup to the device will then no longer be displayed.

Teamviewer Support invite

With TeamViewer, remote support sessions can be created and shared with recipients. Via Relution, a session link can be sent to a device via message. Prerequisite: The TeamViewer QuickSupport app is installed on the device.

This guide describes how to create a session, share the link, and get the recipient to connect.

Requirements

- TeamViewer
- TeamViewer QuickSupport App on the target device (e.g. iPhone or iPad)
- Access to Relution to send the message
- Permission to use remote support

Steps to create a remote session

1. Create message with link:
    - Log in to Relution.
    - Under Devices > Inventory > Select device > Select action > Send message, a message can be sent.
    - A link to the TeamViewer session is inserted into the message.
    - The message is sent to the desired device.
2. Open the link on the device:
    - The recipient receives the message on his device.
    - The recipient opens the message and clicks on the link.
    - The TeamViewer QuickSupport app opens automatically.
3. Start session:
    - The message sender can now start the session on their computer.
    - The recipient must confirm the connection on their device.

For version 26.4.0

Notes

- Make sure that the TeamViewer QuickSupport app is up to date.
- The link to the TeamViewer session is only valid for a limited time.
- The recipient must have a stable internet connection.

Miscellaneous

- Further information about TeamViewer can be found on the official website: teamviewer.com →

Security advice

- Links to TeamViewer sessions should only be shared with trusted individuals.
- Connections from unknown senders should not be confirmed.

For version 26.4.0

AirDrop

Since the update to iOS 26.2 (as well as iPadOS 26.2 and macOS 26.2), Apple has tightened the security requirements for data exchange via AirDrop. Many users, especially in schools and businesses, have noticed that sending files suddenly requires entering a code—a behavior that did not exist under iOS 18.x.

Attempting to send a file to a person who is not stored in contacts blocks the transfer until a numerical code is entered. This significantly complicates quick data exchange in classrooms or working groups.

Cause

According to official Apple documentation, this is a deliberate security feature designed to protect privacy:

- Identity Verification: People who are not saved in contacts must now use an AirDrop code to send items.
- Process: The recipient must select Continue, after which a code appears on their display. This code must be entered by the sender to authorize the transfer.
- MDM Limitation: Administrators currently have no way to globally disable this prompt via Mobile Device Management (MDM). Apple does not offer MDM providers any more options in this regard than it does for end users.

Prerequisite: Apple Account and iCloud

> Important: Using AirDrop in Contacts Only mode as well as maintaining a permanent code-free connection to known contacts requires a signed-in Apple Account (iCloud) on the device. More information can be found in the Apple documentation →

On iPads without an Apple Account, a confirmation dialog appears when switching AirDrop to “Contacts Only,” indicating that iCloud is required. Without signing in, this setting cannot be used.

To ensure AirDrop works reliably in Contacts Only mode, the email address or phone number associated with the sender’s Apple Account must also be saved in the recipient’s contact card.

Workaround

The following approaches can be used to bypass the constant code entry:

Use the 30-Day Rule

Once a code has been successfully entered, the system remembers the connection. Items can then continue to be exchanged with this person via AirDrop for 30 days without needing to use an AirDrop code again.

For version 26.4.0

Permanent Solution: Add to Contacts

The code prompt is permanently suppressed if the sender and recipient save each other in their Contacts.

- After receiving an item, select the option Create New Contact or Add to Contact.
- Once the person is saved as a known contact, the exchange will proceed as usual without additional verification.

Manage or Ignore Known Contacts

To terminate a connection before the 30-day period expires:

- Open the Contacts app.
- Look for the person in the Other Known Contacts list.
- Select the Ignore This Person option to end the automated exchange.

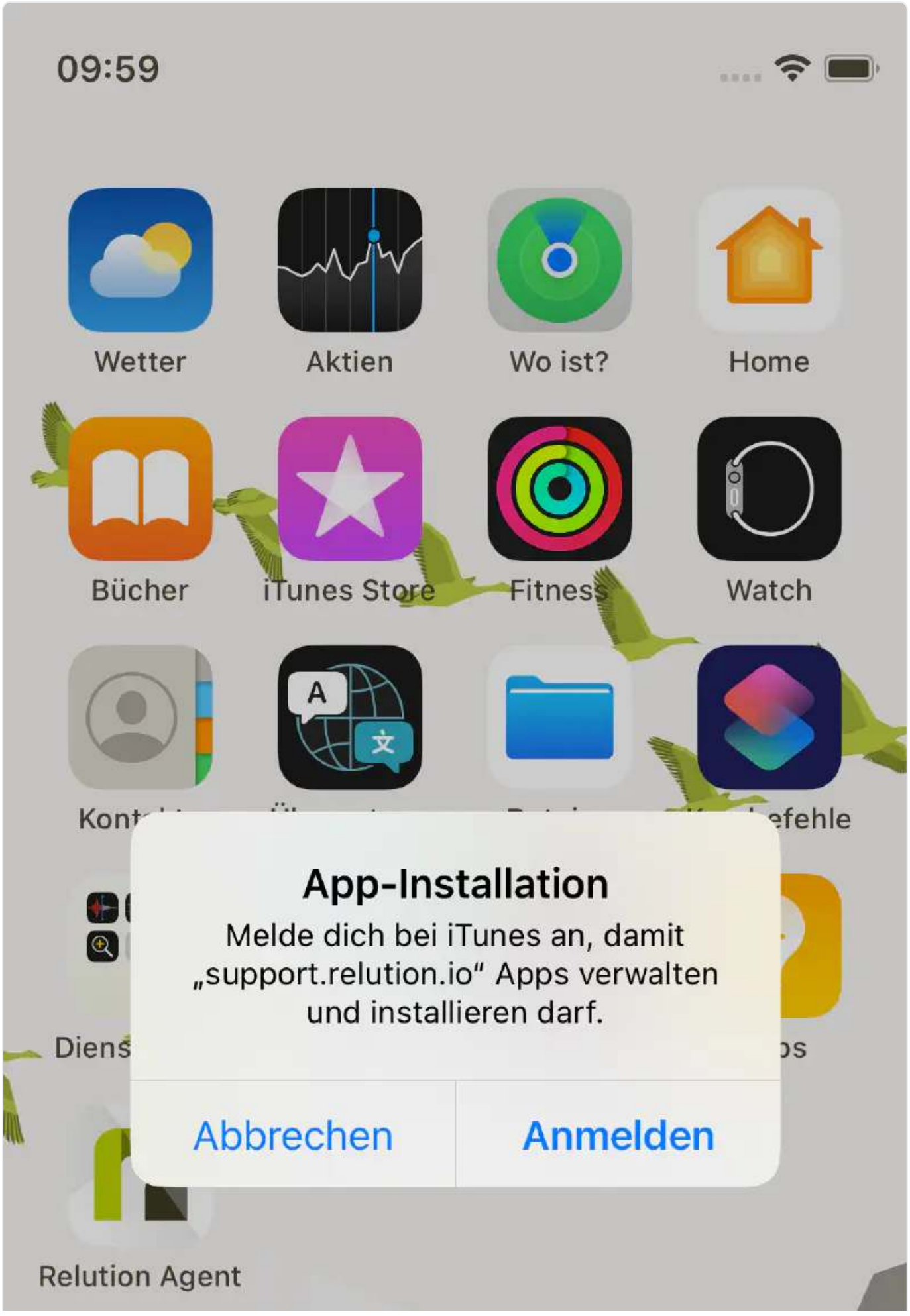
For version 26.4.0

Sign in to iTunes

If Apple Appstore apps are distributed via an MDM (in relation to an app install action, via a policy or via auto-deployment), the following message may appear on the end device.

> App Installation - Log in to iTunes so that your organisation can manage and install apps.

For 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

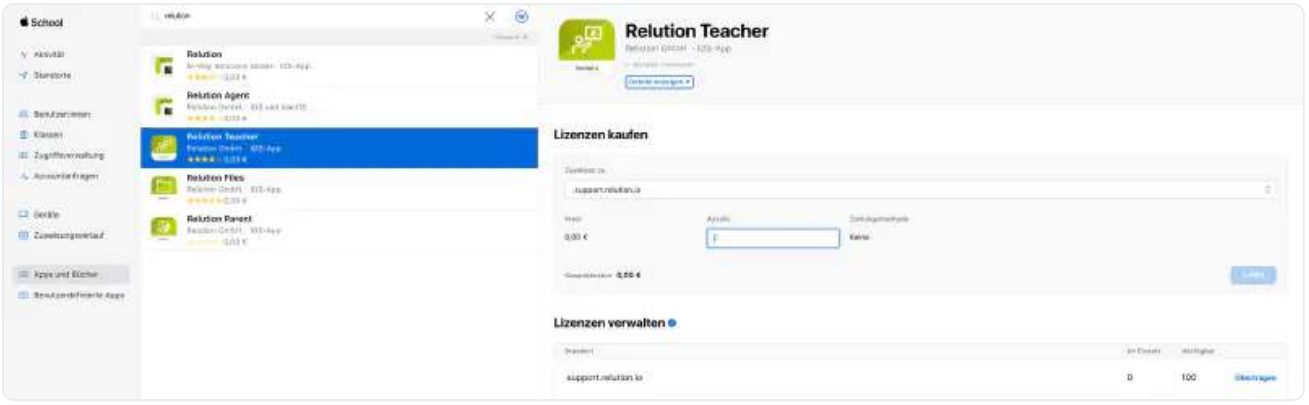


Cause

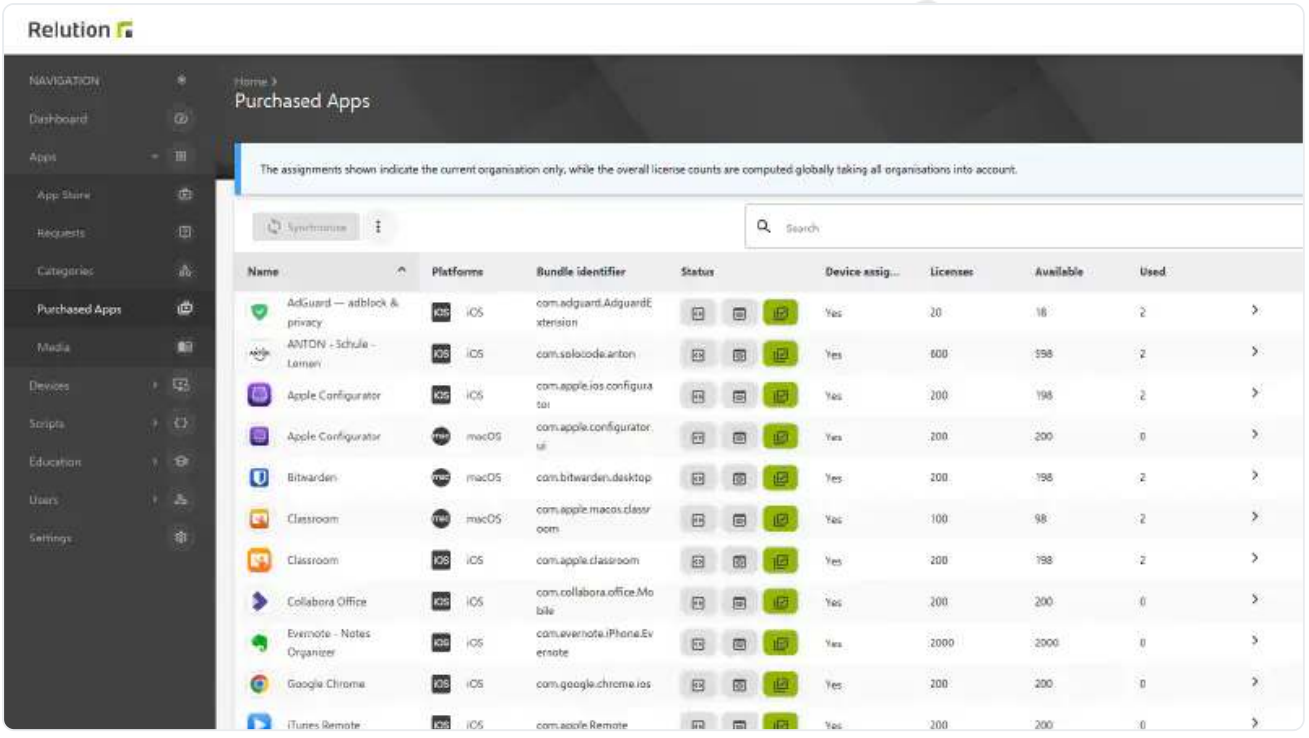
Appstore apps (even free ones) always require a licence. In the private environment, this is done via the AppleID and is done automatically when an app is downloaded from the store. For MDM providers, this is done via the Apple VPP (Volume Purchase Program). For this purpose, licences must be purchased in advance in ASM / ABM (Apple School / Business Manager) for each app to be distributed.

Solution

1. To do this, log in to the ASM / ABM portal and purchase a sufficient number of licences for the desired app for the (distributing) organisation under Apps & Books.



2. After a short time, the app is also visible in relation under ‘Purchased apps’ in the side menu.



3. all pop-ups (one message per unlicensed app) must be cancelled on the end devices with the message. The action or policy can then be executed again and the apps are installed without a message.

Setup VPP →

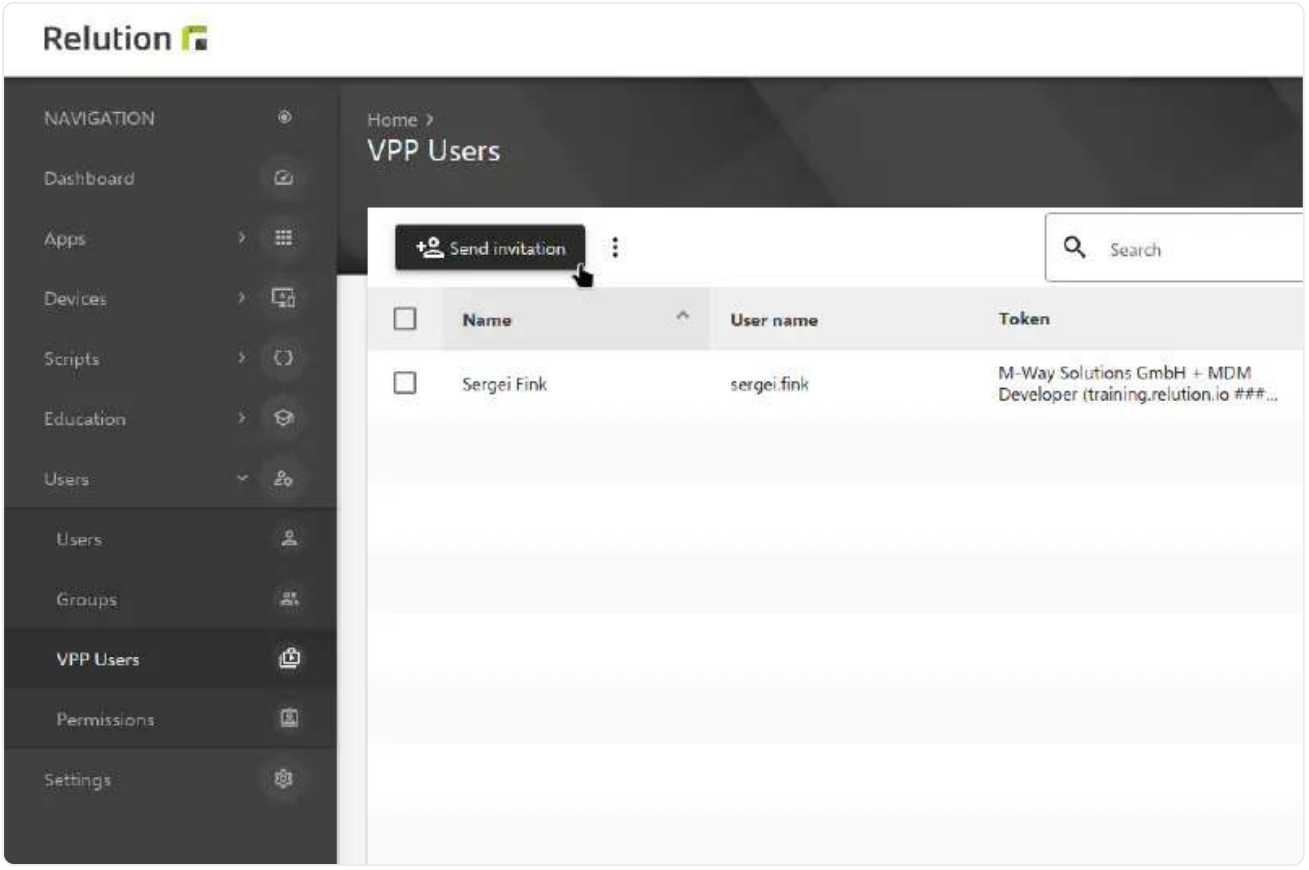
Assign purchased books to users

Books purchased through Apple can be assigned to individual users in Relution. It is not sufficient to create a Managed Apple ID for these users; they must receive an invitation via Relution and then follow the instructions on the screen.

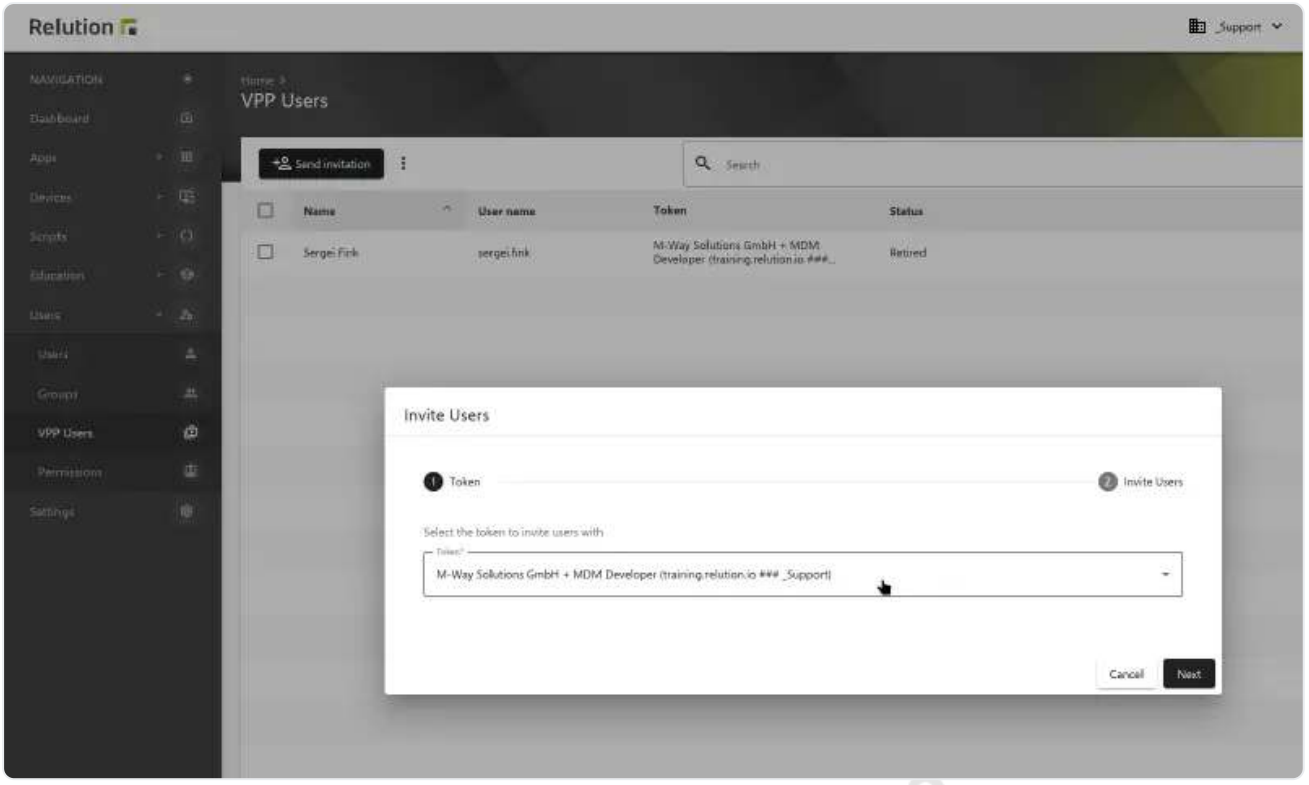
For version 26.4.0

How To

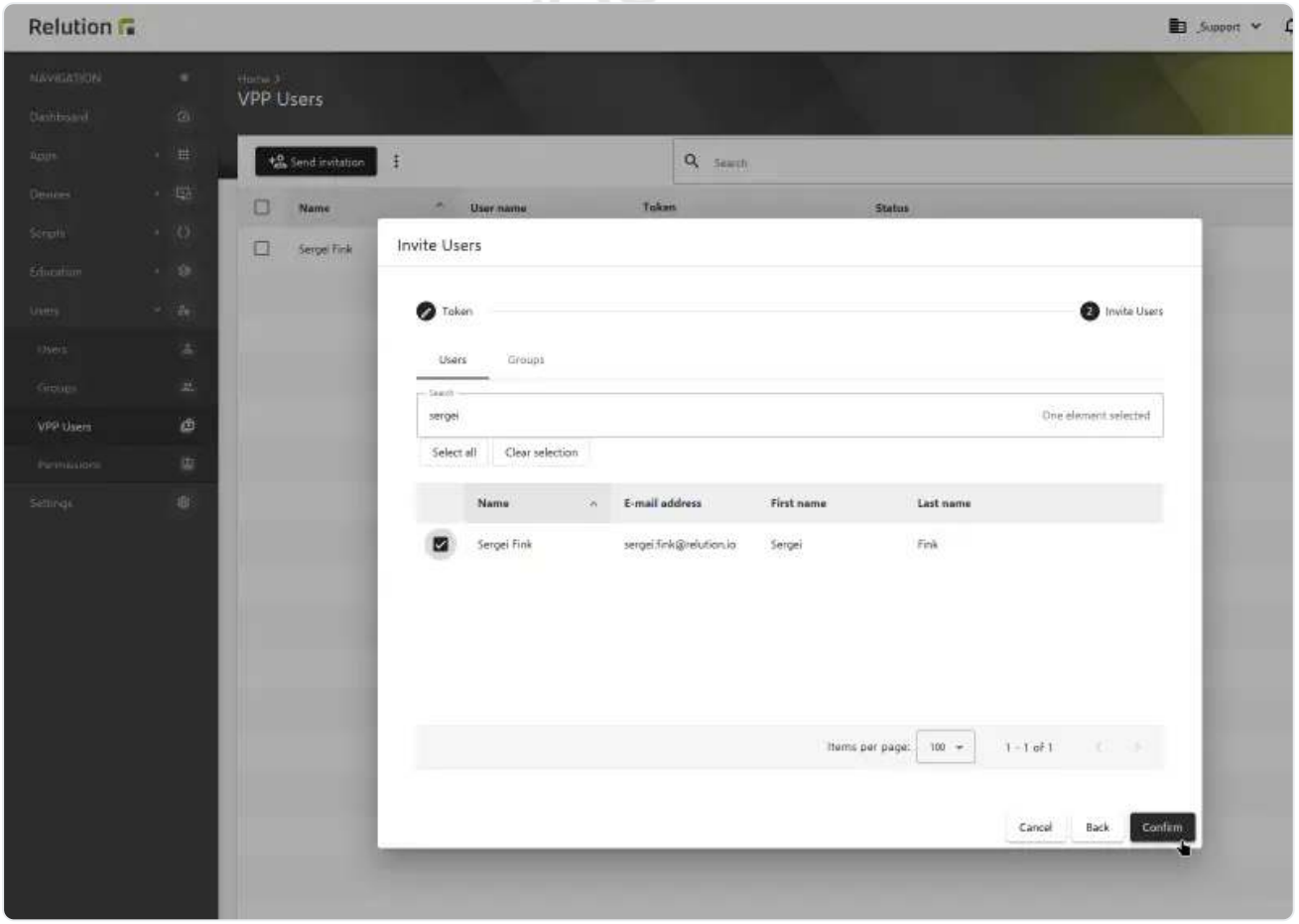
1. Create the desired users in Relution, if not already done.
2. Go to the `Users` → `VPP Users` section.
3. Select `Send Invitation`.



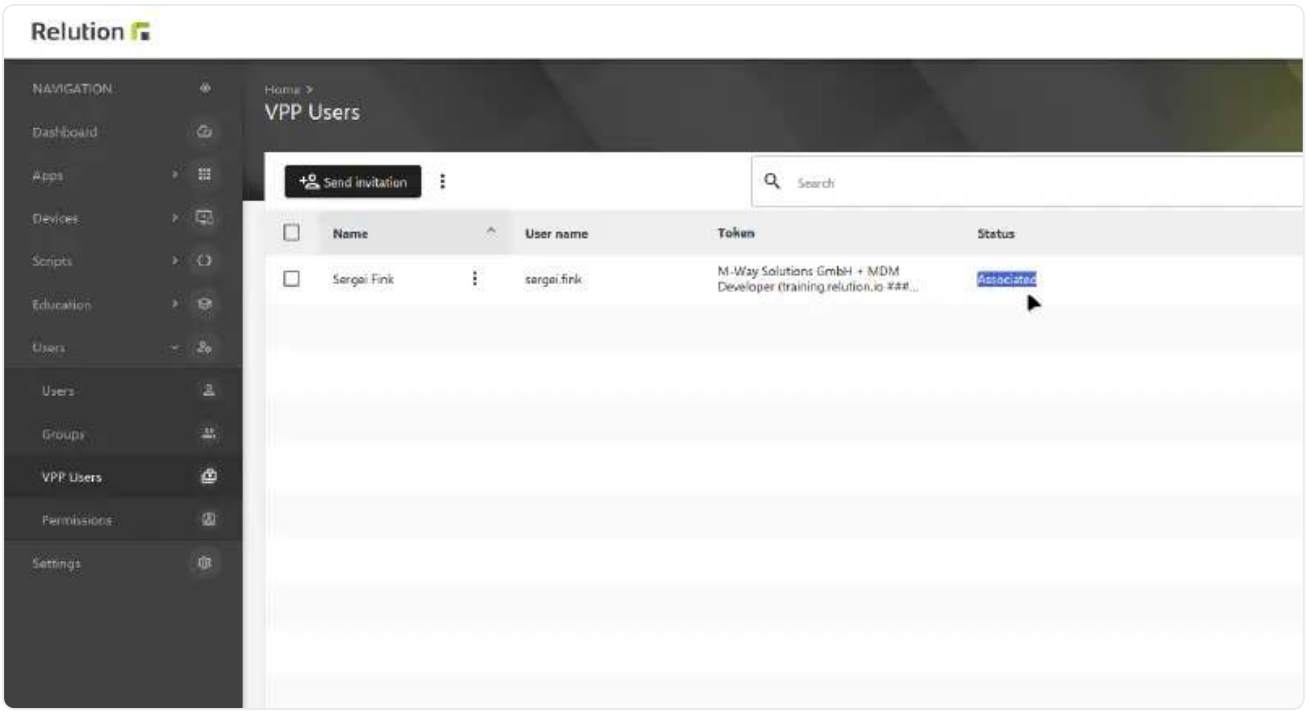
4. Select the desired VPP token and click `Next`.



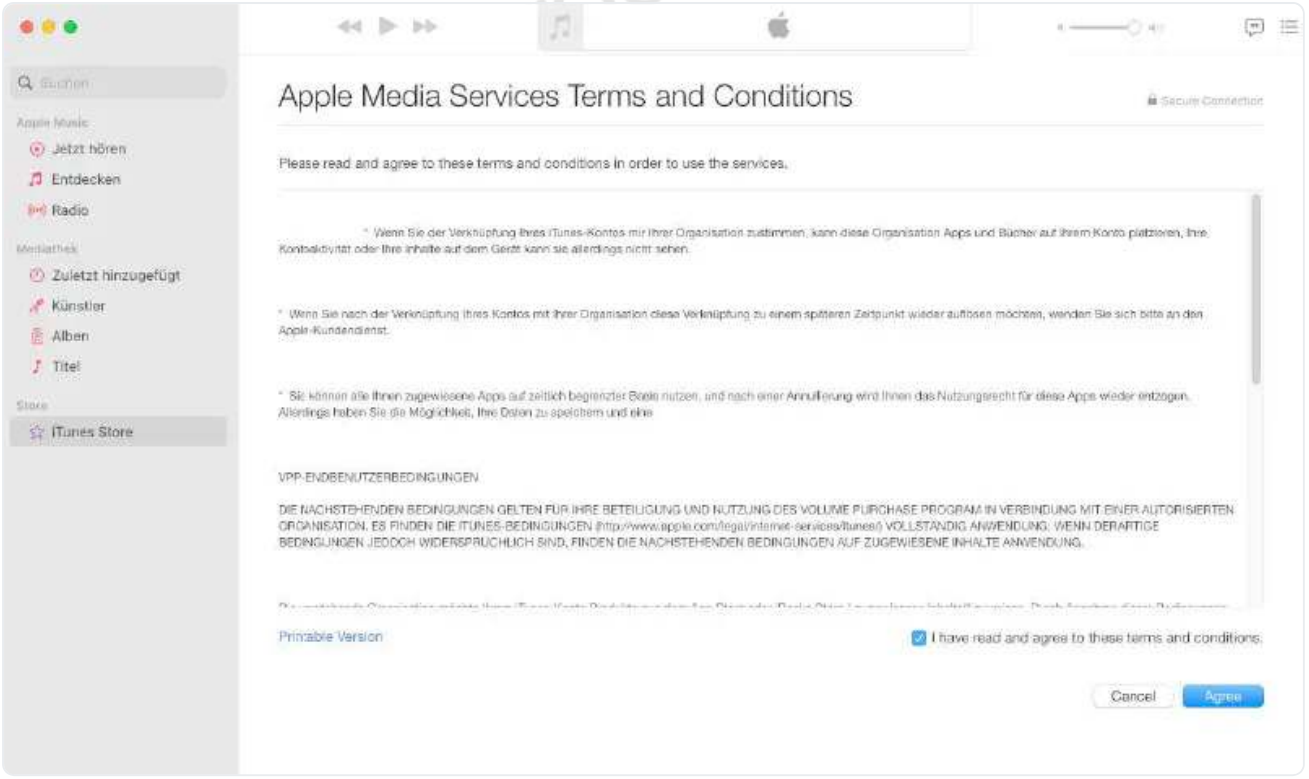
5. Select the desired user to invite and click on `Confirm`.



6. The user will be added to the list with the status `Registered`. The user should get an email.

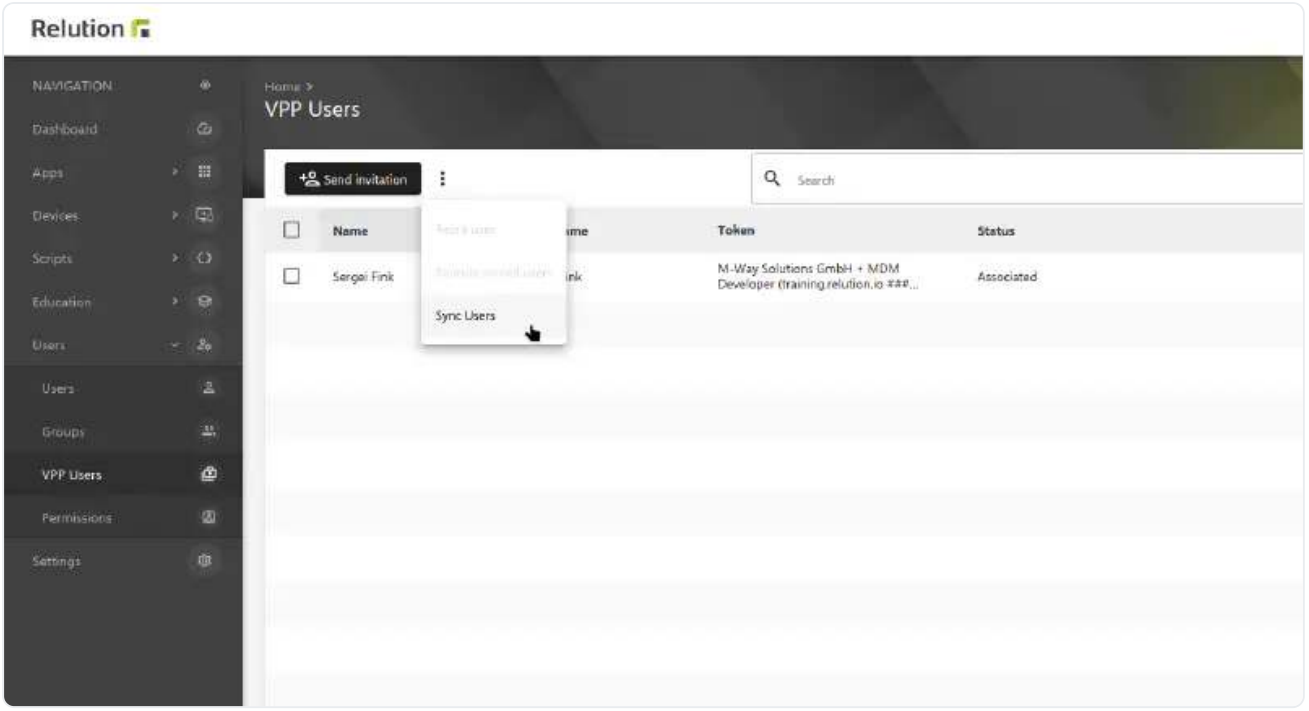


7. In the email, there is a link which has to be opened - either with `iTunes` or `Apple Music`. Here, the user has to accept and confirm the terms and conditions. If no user is logged in on the device yet, a username and password may have to be entered.



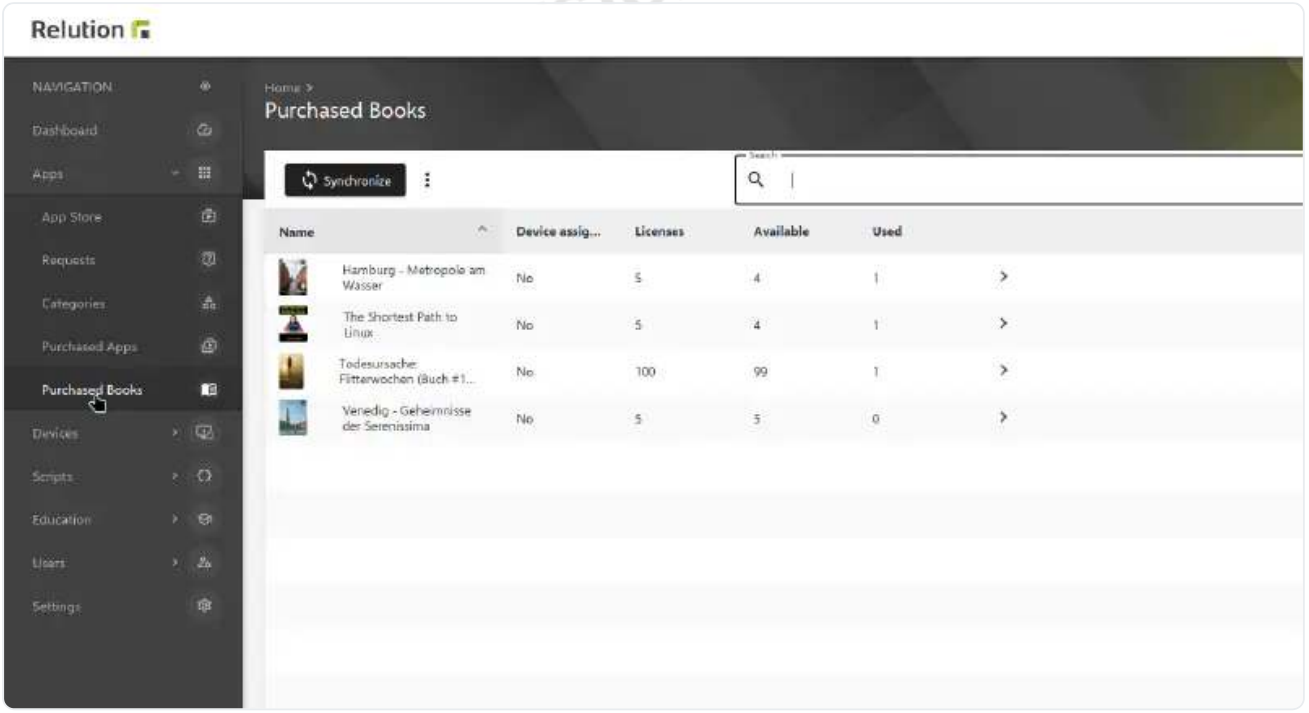
8. In Relution, the assignment of apps must be allowed again.

9. In Relution the VPP users must be synchronized now.

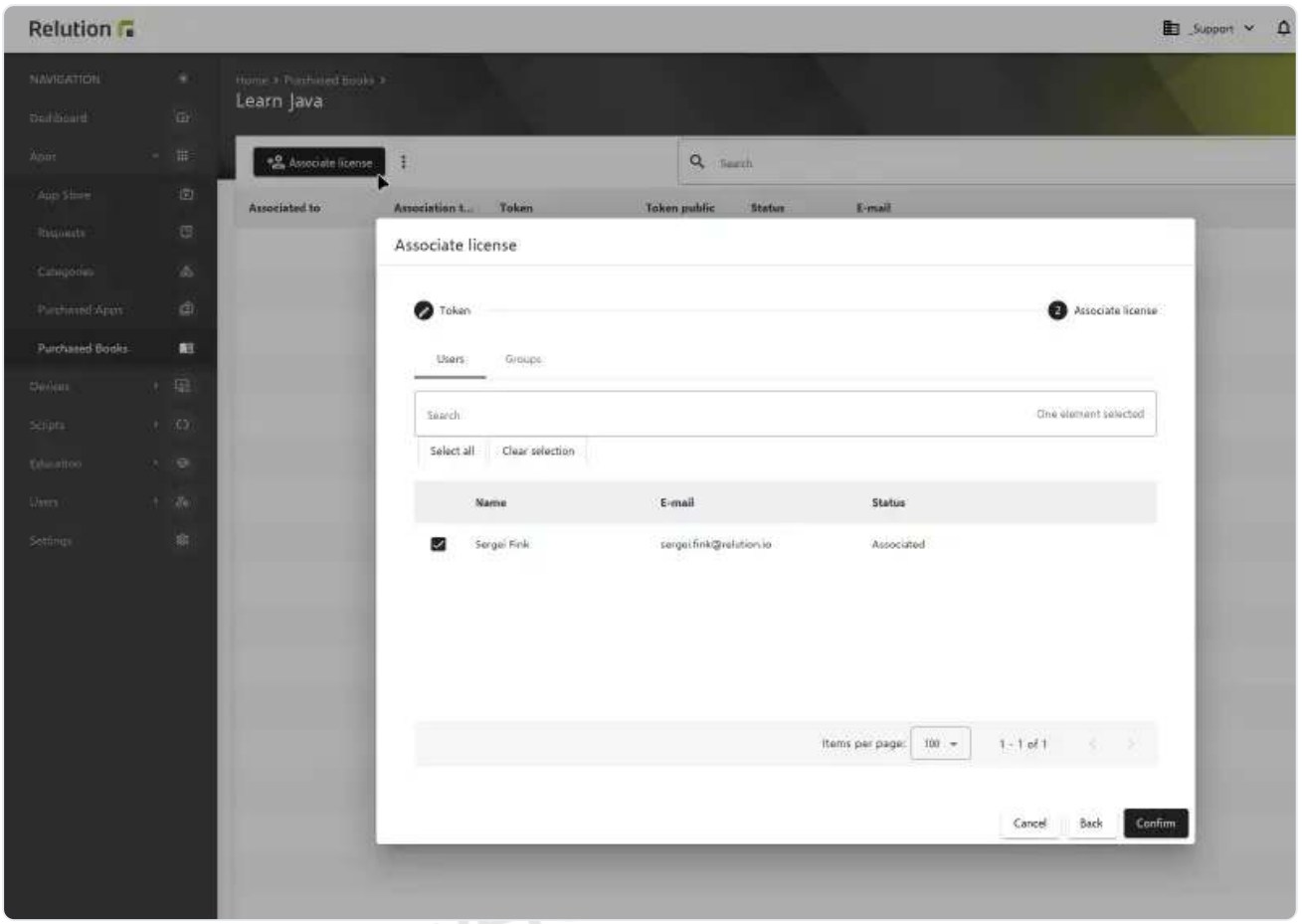


10. If the display is updated afterwards, the user is shown as `Assigned`.

11. Under `Purchased books` click on the book to assign.



12. In the next step click on `Assign license`, select the corresponding token and then the desired user. Finish the selection by clicking on `Confirm`.



Now the user is assigned a book.

Overview of enrollments

Apple TVs are becoming a significant entity in organizations. They are one of the most promising streaming tools used in organizational infrastructures today. Relution supports the management of Apple TVs with multiple enrollment methods: Automated Device Enrollment (ADE, DEP in the portal), subsequent addition via `Apple Configurator 2`, and manual enrollment.

Automated Device Enrollment (ADE) with a DEP profile

Apple School or Business Manager was introduced by Apple to help organizations and educational institutions deploy Apple devices remotely. With the aid of ASM/ABM, brand-new Apple devices can be enrolled in Relution without a technician ever having to get hold of them.

Profile for ADE →
DEP General →

Requirements

- tvOS 10.2 or later.
- Organization should be enrolled in Apple School / Apple Business Manager.
- Devices must have been ordered after March 1, 2011, whether purchased directly from Apple or an authorized reseller.
- If devices were purchased directly from Apple, the Apple customer number assigned to the organization is required to link eligible orders and devices to Apple School / Business Manager.
- If devices were purchased directly from an authorized reseller or carrier, the devices must be linked to that reseller's Reseller ID. The actual date of eligibility is determined by the sales history of the authorized reseller or network operator.
- An APNs certificate stored in Relution (APNS Push Certificates →).
- A DEP account connected to Relution and a DEP profile assigned to the devices. A minimum OS version cannot be set in the DEP profile for tvOS.

For version 26.4.0

Options for Apple TVs in the DEP profile

Two settings in the DEP profile specifically concern Apple TVs:

- Auto advance setup for macOS and tvOS: Setup Assistant automatically advances through its screens. The Apple TV requires an Ethernet connection for this. As long as the toggle is enabled, the setup steps to be skipped cannot be selected.
- Among the setup steps to be skipped, the tvOS specific group contains the screens that only appear on Apple TVs: Aerial screensavers setup and Tap To Set Up option screen (tvOS 10.2 and later) as well as TV home screen layout sync screen, TV provider sign in screen and "Where is this Apple TV?" screen (tvOS 11 and later). Enabled steps are skipped during setup.

Subsequent enrollment via Apple Configurator 2

`Apple Configurator 2` is a free app from the Mac App Store that can be used to subsequently add Apple TVs that were not already registered for ADE by an authorized reseller to Apple School / Business Manager. They are then enrolled like any other ADE device.

Requirements

- Apple TV with tvOS 10.2 or higher.
- macOS device with `Apple Configurator 2.5` or higher.
- The macOS device and the Apple TV are connected to the same Wi-Fi or Ethernet network.

For tvOS devices, the following path must be specified as the MDM server URL if the devices are to be managed on the Relution live system. For a self-hosted Relution instance, `live.relution.io` is replaced with the host name of the organization's own server.

```
https://live.relution.io/api/enrollment/v1/appleMdm/depenroll
```

Adding devices to ADE subsequently →
Supervised Mode / Supervision →

For version 26.4.0

Manual enrollment

Apple TVs can also be added to Relution without ADE via a manual enrollment. To do so, an enrollment with the platform tvOS is created under `Devices` → `Enrollments`. The platform can only be selected if an APNs certificate is stored in Relution. Since Apple TVs have no web browser, the enrollment's MDM profile is installed on the Apple TV using `Apple Configurator 2`.

Manual enrollment →

Available actions

Relution provides a selection of actions to directly control and manage Apple TV devices. The actions can be applied to a single device or, via multiple selection in the device list, to several devices at once. They can also be triggered by event or on a schedule through device group membership: Device group actions →

The action dialog is opened under `Devices` → `Inventory` via Apply action, either for the devices selected in the list or in the detail view of a device. Only actions supported by all selected devices are offered.

Action overview

Action	Description
Remove app	Uninstalls an app from the device.
Wipe device	Resets the device to factory defaults and deletes all data from the device.
Reboot device	Restarts the device. Only available for supervised devices.
Refresh device info	Refreshes all available information about the device listed under Details.
Continue in device Setup Assistant	Informs the device that the pre-configuration is completed and it can proceed in the Setup Assistant. Only available for devices enrolled via Automated Device Enrollment (ADE, DEP in the portal). Only takes effect if the Await configuration option is enabled in the DEP Profile.
Update MDM profile	Reinstalls the MDM profile on the device. The identity certificate is renewed and current settings such as certificate pinning are applied. The MDM server URL remains unchanged; a changed external URL is therefore not transferred to the device. Relution renews the MDM profile automatically before the identity certificate expires. The manual action is therefore only required in special cases.
Deploy Relution store app	Searches for an app in the Relution Store and installs it on the devices.
Return to Service	Resets the device to factory defaults; afterwards it tries to re-enroll itself automatically. Requires tvOS 18 or later; on older versions the action fails. A policy with a tvOS Wi-Fi configuration must be selected in the action dialog. The action is only available if all selected devices belong to the same platform.
Install Update	Installs a chosen update on the selected device. Only available for supervised devices. The action is only offered if Relution has determined an available update for all selected devices. Available updates are determined again whenever the device information is refreshed, e.g. via Refresh device info.

If at least one of the selected devices is not supervised, Reboot device and Install Update are not shown in the action dialog. The same applies to Continue in device Setup Assistant as soon as a selected device was not enrolled via Automated Device Enrollment.

For version 26.4.0

Overview

A policy is a collection of one or more configurations. Each policy can be applied to one or more devices at the same time. Likewise, each device can be linked to one or more policies.

Available configurations

Configuration	Description
AirPlay Security →	Applies AirPlay security settings that prevent unauthorized streaming to Apple TVs via AirPlay
App compliance →	Manages app-specific restrictions
Apple Configurator 2 configuration →	Applies a configuration profile (`.mobileconfig`) created with Apple Configurator 2 to devices
Single App Mode	Limits devices to a single app
Device settings	Configures general device settings (supervised devices only)
Device name	Configures the device name (supervised devices only)
Conference room →	Manages Conference Room mode
Restrictions	Manages device restrictions
Software update settings →	Controls the update behavior of devices, e.g. automatic installation and deferral of updates (tvOS 18.4 or later)
System updates	Manages updates of Apple devices (supervised devices only; deprecated, successor: Managed Software Updates)
Managed Software Updates →	Enforces operating system updates, targeting a specific version by a deadline (tvOS 18.4 or later, supervised devices only)
WiFi	Manages Wi-Fi settings
Time zone	Configures the time zone (tvOS 14 or later, supervised devices only)
Certificate	Selects a certificate to be installed on the device by default

The WiFi, Certificate and Apple Configurator 2 configuration configurations can be added to a policy multiple times; all other configurations only once.

Apple Configurator 2 Configuration

This policy configuration can be used to transfer `.mobileconfig` files to Apple devices. Such a file can contain, for example, a Wi-Fi connection together with the matching identity certificate (PKCS#12, `.p12`).

Configuration

The Name field sets a name for the configuration. The file is uploaded via Select .mobileconfig file. Its content then replaces the file selection in the Payload content field, where it can be edited. The content must be valid XML. Signed profiles are not readable XML and therefore cannot be used, so the file is saved without a signature in Apple Configurator 2. If the Payload content field is cleared, a file can be selected again.

User, device and certificate placeholders can be used in the Payload content field. The available placeholders are listed below the form and are replaced when the configuration is transferred to the device, see Advanced placeholders →.

Several Apple Configurator 2 configurations can be created per policy. This allows multiple configuration types to be split across separate configurations.

File requirements

The content is validated when the configuration is saved. The file must meet the following conditions:

- The top level contains the keys `PayloadType`, `PayloadVersion` (as a number), `PayloadIdentifier`, `PayloadUUID` and `PayloadDisplayName`.
- `PayloadContent` contains exactly one configuration type. Certificate payloads may be included in addition.

Files that cannot be read, that lack one of these keys, or that contain no payload or several configuration types are rejected when saving.

> Only certificates in PKCS#12 format (`com.apple.security.pkcs12`) are transferred along with the configuration. PKCS#1 certificates (`com.apple.security.pkcs1`) pass validation but are not transferred to the device. Other certificates such as root certificates (`com.apple.security.root`) count as a separate configuration type. Combined with another configuration, they cause an error when saving and are therefore stored in a configuration of their own.
>
> The actual configuration must be the first entry in `PayloadContent`. If the file contains several payloads of the same type, only the first one is transferred to the device.

If the file contains a configuration type that Relution also offers as a separate configuration allowed only once per policy, that configuration can no longer be added to the same policy. On tvOS, this applies to:

Payload type in the file	Blocked configuration
`com.apple.airplay.security`	AirPlay Security →
`com.apple.conferenceroomdisplay`	Conference room →
`com.apple.applicationaccess`	Restrictions
`com.apple.app.lock`	Single App Mode

Conversely, such a file is rejected when saving if the policy already contains the corresponding configuration or another active Apple Configurator 2 configuration with the same payload type.

Example

The following file transfers a Wi-Fi connection (`com.apple.wifi.managed`). SSID, password, identifiers and UUIDs are sample values and are replaced with actual values. Each `PayloadUUID` must be unique.

For version 26.4.0

```
<?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>Wi-Fi-password</string>
   <key>PayloadDisplayName</key>
   <string>Wi-Fi</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>Company-WiFi</string>
  </dict>
 </array>
 <key>PayloadDescription</key>
 <string>Wi-Fi configuration for Apple devices</string>
 <key>PayloadDisplayName</key>
 <string>Wi-Fi</string>
 <key>PayloadIdentifier</key>
 <string>com.example.wifi</string>
 <key>PayloadOrganization</key>
 <string>Example Inc.</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>
```

Remove Supervised Mode

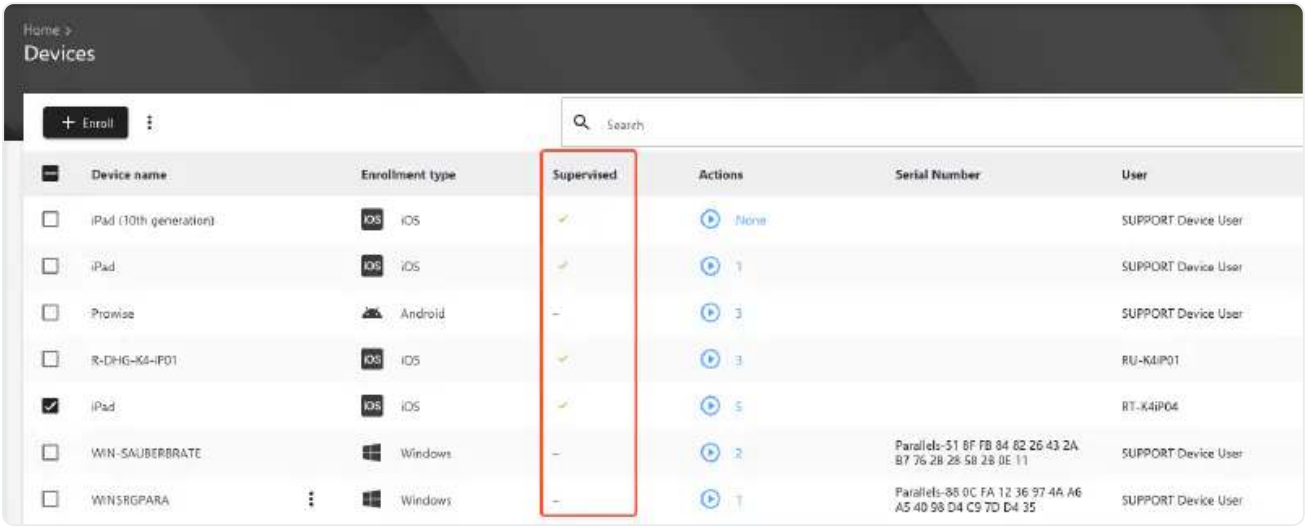
Every now and then it may be necessary to revoke this mode from Apple devices that are running in Supervised Mode.

> For iOS and tvOS devices, this state can be undone. macOS devices, on the other hand, can only be operated in Supervised Mode as of version 11.

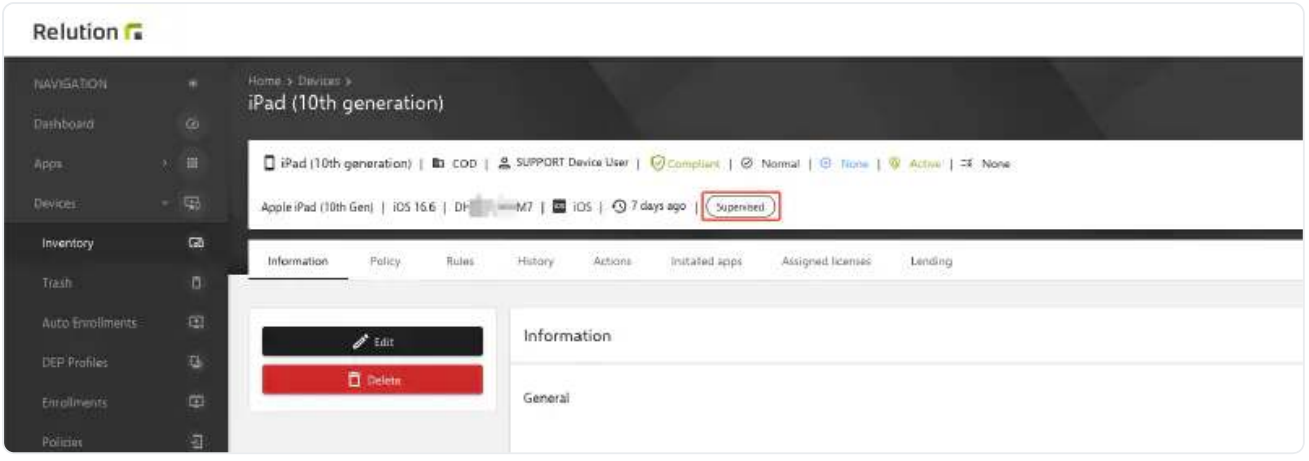
Identify supervised devices

Supervised devices can be located as follows:

1. The Supervised column can be displayed in the inventory. The corresponding devices are marked with a check mark. Alternatively, the list can be narrowed down with the Supervised filter.



2. In the device details, the status is shown by the Supervised badge in the info box.



Devices enrolled via Apple Configurator

> Note that this operation will also remove the MDM profile from the devices and they cannot be managed afterwards without re-enrolling them. In addition, all apps and data will be removed from the devices.

The devices can be reset using one of the following options:

1. A Wipe device action is sent to the devices.
2. The devices are reset on the device itself: on iPhone and iPad under `Settings` → `General` → `Transfer or Reset iPhone/iPad` → `Erase All Content and Settings`, on Apple TV under `Settings` → `System` → `Reset`.
3. The devices are connected to a Mac and the Apple Configurator 2 application is opened. The devices are right-clicked, then Advanced → Erase All Content and Settings is selected.

The Return to Service action is not suitable for removing Supervised Mode: it resets the device, but then re-enrolls it automatically (see Available actions →).

Devices enrolled via ADE through Apple School/Business Manager

For version 26.4.0

If devices have been added to the MDM system via Automated Device Enrollment (ADE, DEP in the portal) in Apple School/Business Manager, the link must be undone there. Otherwise, the devices will always automatically report back to the MDM system after a factory reset and be put into Supervised Mode again. This also applies to devices added by an authorized reseller.

1. After logging in to Apple School/Business Manager, Devices is selected.
2. The appropriate device is selected and Edit Device Assignment is clicked on the right-hand side.
3. Unassign is clicked.
4. The device is reset to factory settings.

ADE devices added later via Apple Configurator

Removing Supervised Mode from devices added to Apple School/Business Manager via Apple Configurator works in the same way as for ADE devices enrolled via an authorized reseller.

> However, users can manually remove the MDM profile on the devices within the first 30 days of adding the devices to Automated Device Enrollment (ADE). This will result in the loss of MDM enrollment as well as Supervised Mode.

Conference Room Configuration

Apple TV can share the screen of an AirPlay-supported device without giving users access to other Apple TV features. When the conference room screen is turned on, it displays network details and instructions on how to connect to Apple TV via AirPlay, along with the message stored in the configuration.

The Conference room configuration is only available in tvOS policies and can be added once per policy.

Set up the conference room for Apple TV

1. The configuration is created in the Relution portal via `Devices` → `Policies` → `{tvOS policy}` → `Add` → `Conference room` → `Add details`. Configurations can only be added to a draft version of the policy.

2. In the General section, the required Message field contains the text displayed on the Apple TV conference room screen. The text can include user and device placeholders (e.g. `${device.name}`) listed in the Available placeholders card; they are replaced with the corresponding values when the configuration is sent to the device. Without a message, the configuration cannot be saved.

3. Then, the policy must be published to be able to assign it to devices.

tvOS devices in Relution →

For version 26.4.0

AirPlay security configuration

AirPlay Security prevents unauthorized streaming to Apple TV via AirPlay. Administrators can thus control who can connect to Apple TV via AirPlay functionality. Either an AirPlay password can be set or the connection of devices in another network to the TV can be restricted. AirPlay Security can be used on Apple TVs running tvOS 11 or later.

Add the configuration

The configuration is created in the Relution portal via `Devices` → `Policies` → `{tvOS policy}` → `Add` → `AirPlay Security` → `Add details`. Configurations can only be added to a draft version of the policy. AirPlay Security is only available in tvOS policies and can be added once per policy.

Available AirPlay security settings

- Access (default: Devices on any Wi-Fi network) - Defines from which network an AirPlay-supported Apple device can connect to an Apple TV via AirPlay. The following options are available:
  - Devices on any Wi-Fi network: Allows Apple TV to connect to AirPlay-supported Apple devices on different networks.
  - Devices on the same Wi-Fi network: Allows connection between AirPlay-supported Apple devices and Apple TV that are on the same network (same Wi-Fi or Ethernet).
- Security (default: First-time passcode) - Defines how the connection is secured. The following options are available:
  - First-time passcode: When an Apple TV connects to an AirPlay-supported Apple device, a passcode appears on the TV screen. This passcode is entered on the AirPlay-supported Apple device to start streaming. The passcode is not required when the same devices connect again.
  - Passcode: Every time a device tries to stream content via AirPlay, a passcode is displayed on the TV screen. This passcode is entered on the AirPlay-supported Apple device to start streaming.
  - Password: Requires a fixed AirPlay password when an AirPlay-supported Apple device connects to the Apple TV. When this option is selected, the required Password field appears in the configuration, in which the AirPlay password is stored; without a password, the configuration cannot be saved. When a connection is made, the device connected to the Apple TV is prompted for this password; once the password from the policy is entered, streaming starts. Unlike First-time passcode, no code is displayed on the TV.

Then the policy must be published to assign it to devices.

tvOS devices in Relution →

For version 26.4.0

App Compliance

Installing apps from Apps and Books (VPP in the portal) on Apple TV devices is particularly straightforward thanks to Relution's App compliance policy. This configuration enables simple and central distribution of applications to a large number of devices.

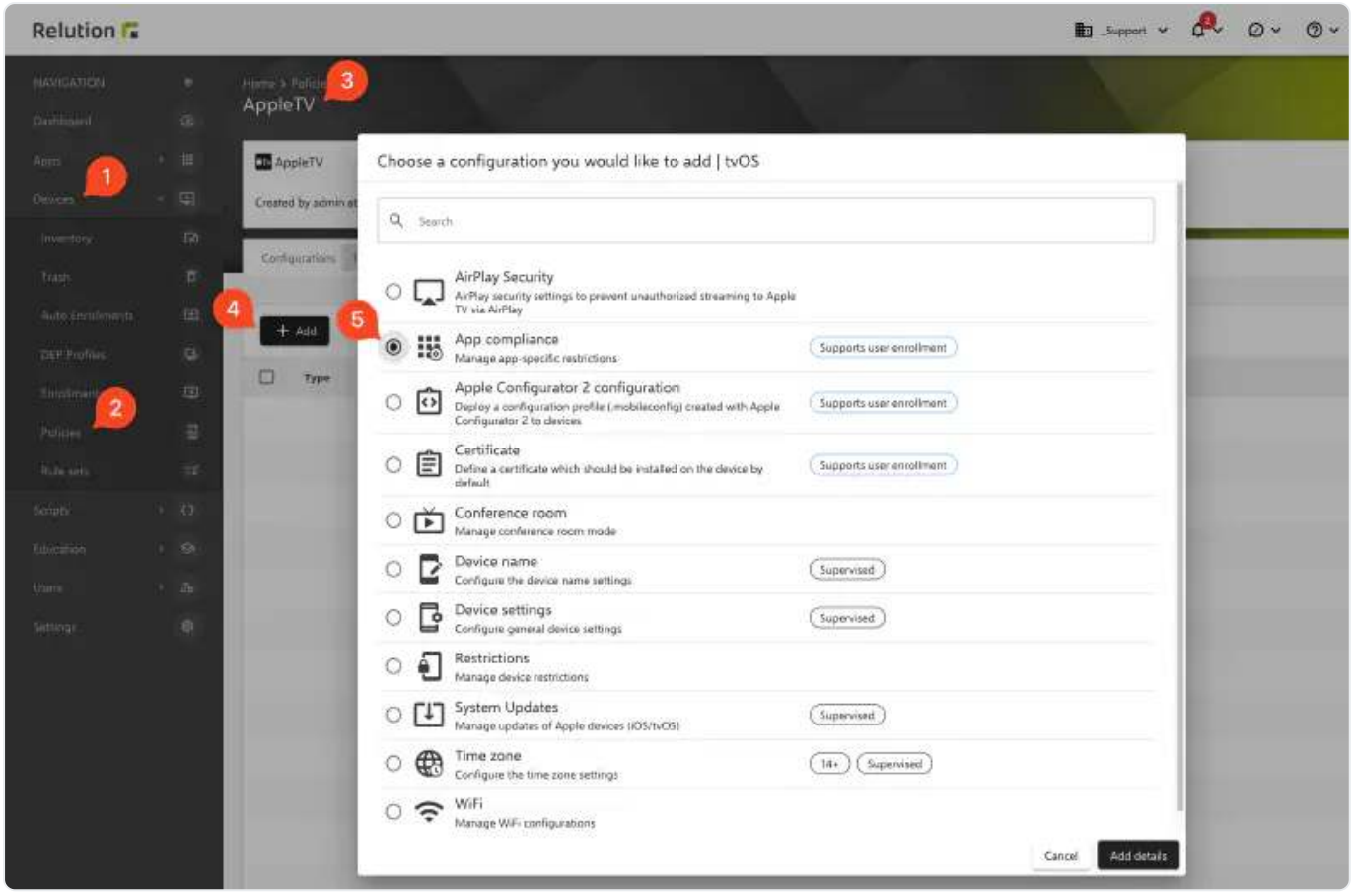
Starting the distribution only requires:

- An Apple School or Apple Business account.
- The integration of the organization's own Apps and Books token → in Relution.
- Acquired licenses for the desired apps from Apple School Manager (ASM) or Apple Business Manager (ABM).

tvOS devices in Relution →

Configuring App Compliance

The distribution of apps to Apple TV devices (analogous to iOS devices) is carried out via the App compliance policy configuration. It is selected under `Devices` → `Policies` in a tvOS policy via Add Configuration and created with Add details.



Similar to iOS devices, app availability is controlled under List type in the General section: either as a blocklist (Blocklist — The apps below are not allowed, the default for new configurations) or as an allowlist (Allowlist — The apps below are allowed). Only one of the two list types is active per configuration. The apps are entered via Add in the Blocked apps or Allowed apps section below.

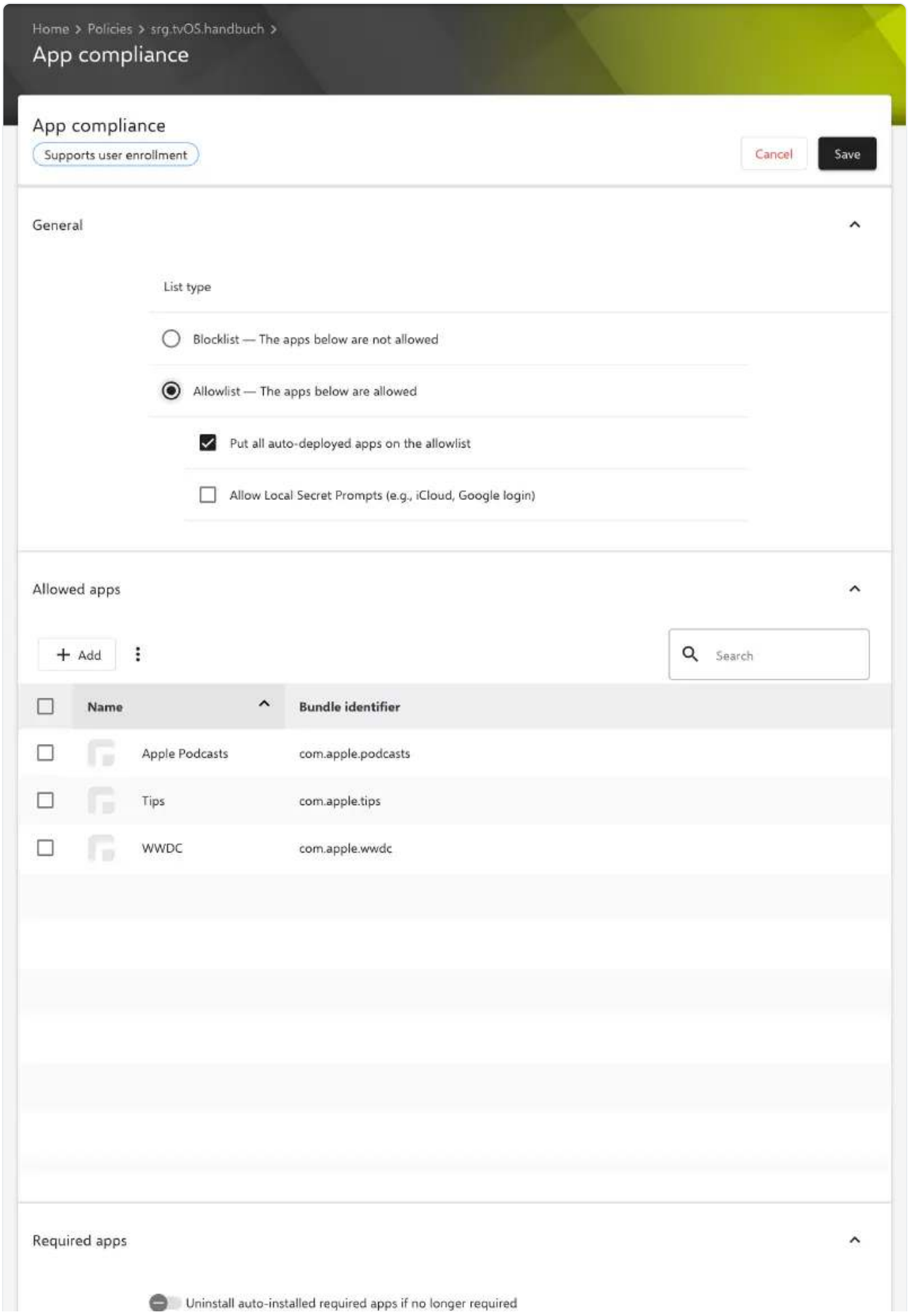
Allowlist and blocklist are only applied to supervised devices.

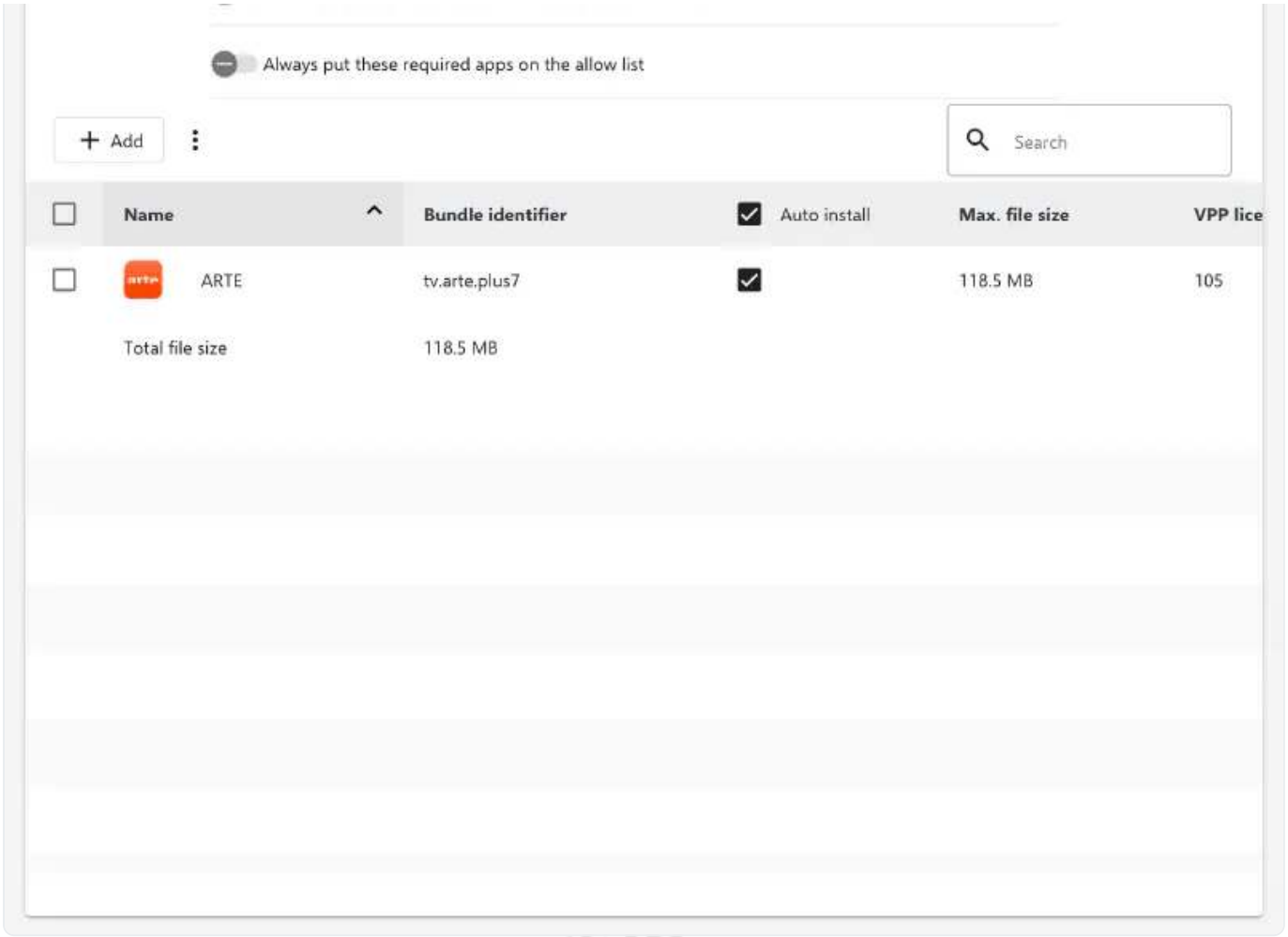
Allowlist (Permitted Apps)

The allowlist explicitly defines which apps are permitted to be available on the devices. Two additional options are available:

- Put all auto-deployed apps on the allowlist: Apps distributed to the devices' users via auto deployments are automatically added to the allowlist.
- Allow Local Secret Prompts (e.g., iCloud, Google login): The system dialog for local secret prompts is added to the allowlist so that such prompts are not blocked.

For version 26.4.0

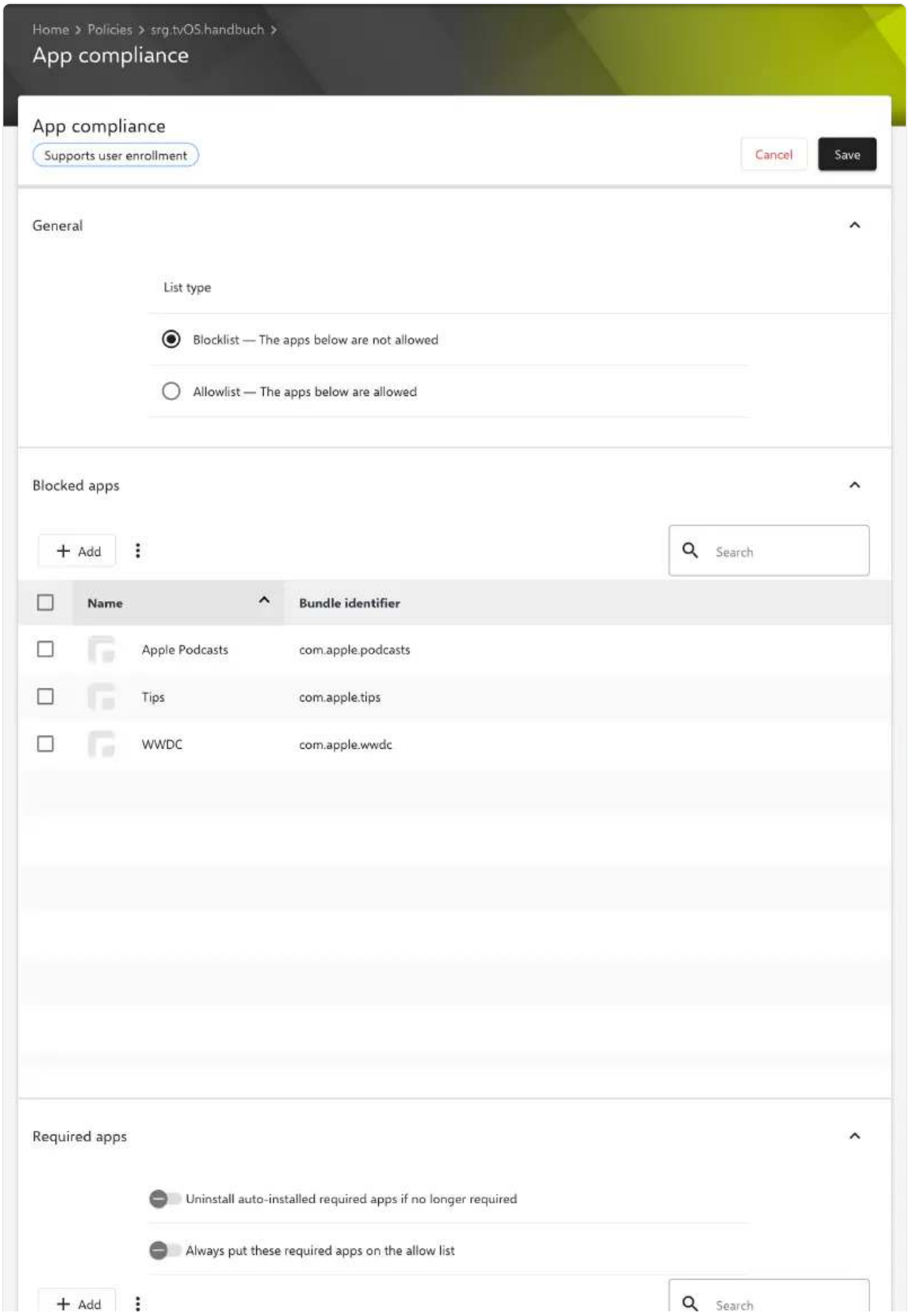

Home > Policies > srg.tvOS.handbuch >
App compliance
App compliance
Supports user enrollment
Cancel
Save
General
List type
Blocklist — The apps below are not allowed
Allowlist — The apps below are allowed
Put all auto-deployed apps on the allowlist
Allow Local Secret Prompts (e.g., iCloud, Google login)
Allowed apps
Add
Search
Name
Bundle identifier
Apple Podcasts
com.apple.podcasts
Tips
com.apple.tips
WWDC
com.apple.wwdc
Required apps
Uninstall auto-installed required apps if no longer required

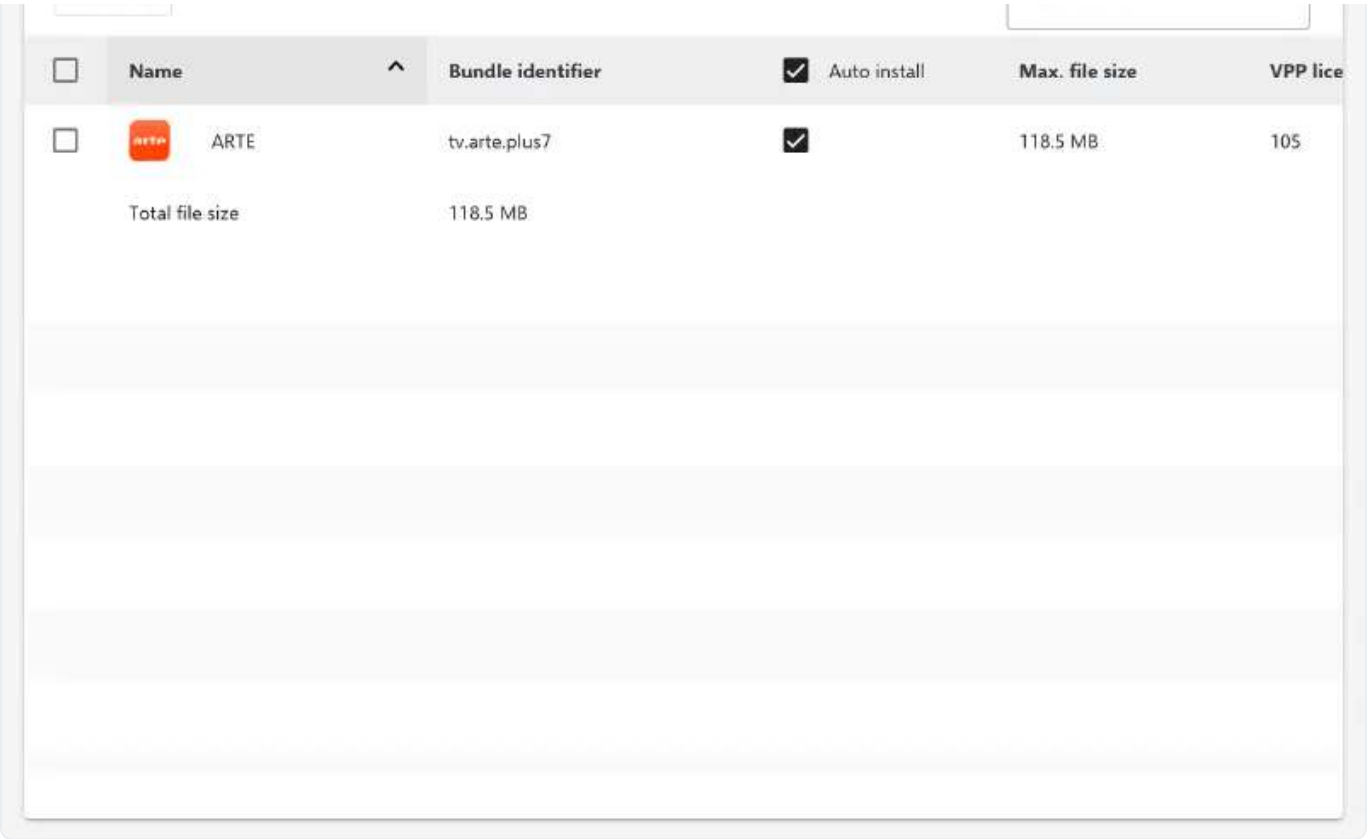


Blocklist (Blocked Apps)

The blocklist is used to hide or block specific apps on tvOS devices.

For version 26.4.0


Home > Policies > srg.tvOS.handbuch >
App compliance
App compliance
Supports user enrollment
Cancel
Save
General
List type
Blocklist — The apps below are not allowed
Allowlist — The apps below are allowed
Blocked apps
+ Add
Search
Name
Bundle identifier
Apple Podcasts
com.apple.podcasts
Tips
com.apple.tips
WWDC
com.apple.wwdc
Required apps
Uninstall auto-installed required apps if no longer required
Always put these required apps on the allow list
+ Add
Search

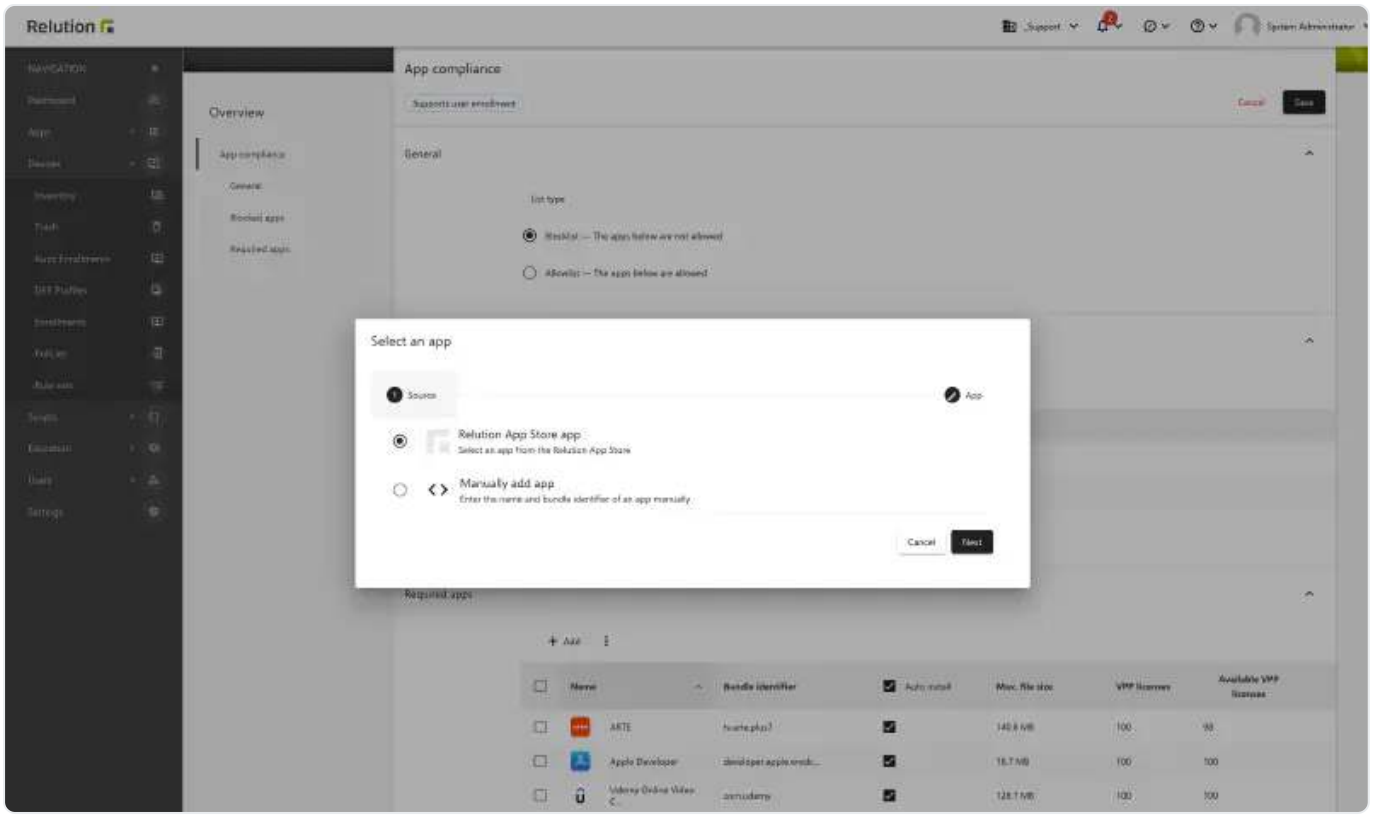


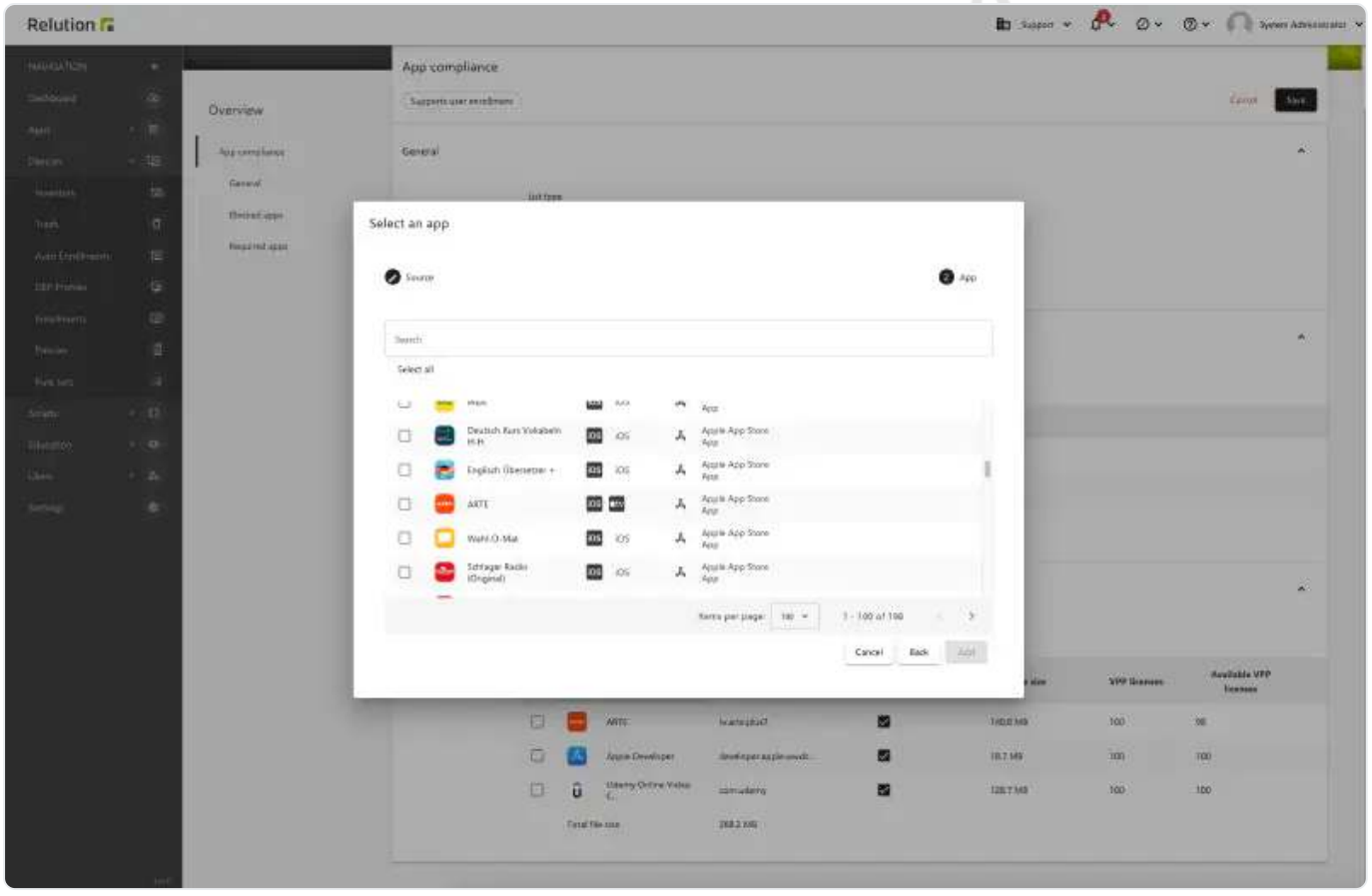
Required Apps

In the Required apps section, the applications that must be mandatorily installed on the devices are specified. Add offers the following sources (the same apply to the allowlist and blocklist):

- Relution App Store app: Selection of apps for the tvOS and iOS platforms from the Relution App Store. For required apps, native (self-uploaded) apps are offered, as well as public apps for which the organization holds Apps and Books licenses. There is no direct search in the public Apple App Store for tvOS.
- Manually add app: Entry of an app by Name and Internal name (bundle ID).

For Version 26.4.0





If a required app is not installed on the device, the device is considered noncompliant. The app is only actively installed if the checkbox in the Auto install column is selected; it is selected by default when an app is added. The VPP licenses and Available VPP licenses columns show the existing and the remaining free licenses per app.

Two toggles are available above the list:

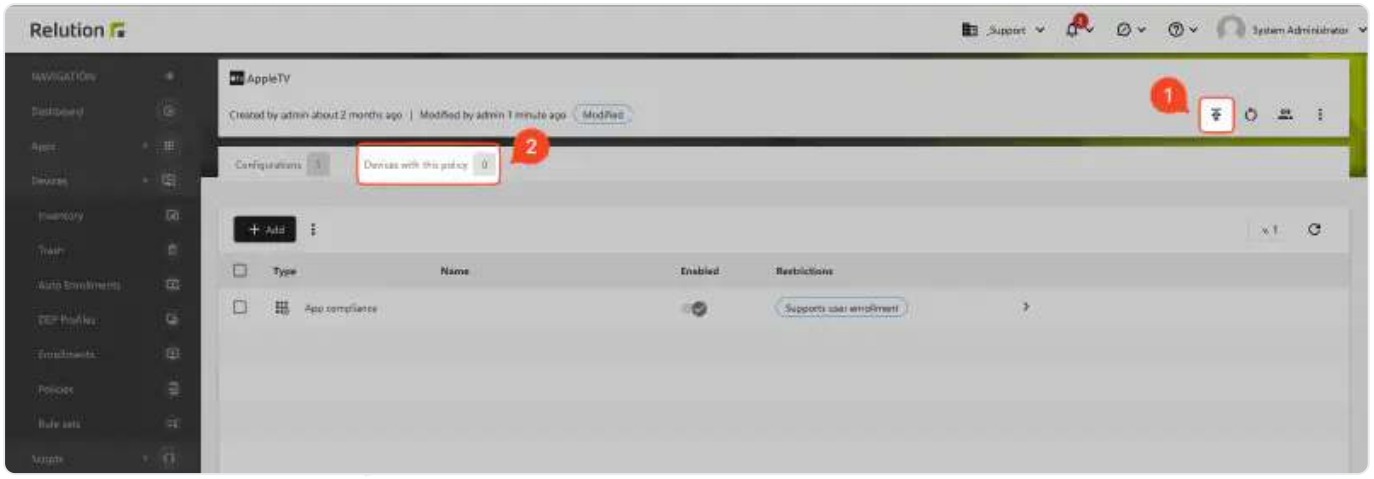
- Uninstall auto-installed required apps if no longer required: If an auto-installed required app is removed from the configuration, or the configuration is removed from the device, the app is uninstalled. The toggle is off for new configurations.
- Always put these required apps on the allow list: If this or another policy configures an allowlist for the device, the required apps are added to it.

When saving, the lists are checked for conflicts: a required app must not be on the blocklist. If the second toggle is off for an allowlist, all required apps must also be entered on the allowlist.

iOS apps can also be used on tvOS, as long as they are suitable for tvOS. Non-compatible apps will be installed on the device, but will disappear after the installation process and will not be available.

> Public apps without Apps and Books licenses as well as web links (browsers) cannot be installed on tvOS devices.

Once the configuration is complete, it can be saved, published, and assigned to the corresponding devices.



App Distribution

Companies are increasingly deciding to support certain work processes with a mobile app. Among many other conceptual issues, the question of how to distribute this app to users quickly arises. Often, the use case is that not only employees, but also external people should get the app - this can include service providers, partners or customers, for example. In most cases, this app is also explicitly not intended for a broad customer base, but is aimed at selected professional users. The following sections are intended to help in deciding on the best distribution method.

> Apps from Relution reach Apple TV devices exclusively through device management (MDM). Installation by users via a website, a deep link or a store app is not possible on tvOS, and web clips are not distributed to tvOS devices. In Relution, tvOS apps are listed under the iOS platform (Add and update native apps →). Apps from the App Store can only be installed on Apple TV with an Apps and Books (VPP in the portal) license (Manage App Store apps →, App Compliance →). The following sections describe the distribution methods in general for iOS and Android.

Distribution via public app stores

Apple and Google each provide an infrastructure for distributing apps. For Apple, apps are made available to end users through the Apple App Store. Every iOS device has the App Store app pre-installed.

Apps are managed and published via the developer portal and App Store Connect. On Google, apps are made available to end users via the Play Store. The Play Store app is preinstalled on every Android device.

The administration and publication of apps for this is done via the developer portal. Apple and Google define the framework for publishing apps via their systems.

For version 26.4.0

If a device is managed via an MDM system, the Store app can also be locked for the user and may therefore not be available to the end user.

Distribution via Apple App Store - Advantages

- Apps are available to end users via Apple's standard mechanism
- Apps do not need to be re-signed and re-provisioned with an updated provisioning profile after one year.
- Apps can be selectively enabled or blocked for individual countries, if necessary.
- Apps can be offered for a fee - if desired - in defined structures (Apple charges a percentage commission fee of 15% for this)
- Apple provides the infrastructure for distribution and billing

Distribution via Apple App Store - disadvantages

- Users need an Apple ID on the end devices to install apps from the Apple App Store
- For enterprise customers with managed devices, the Apple App Store may be blocked via MDM
- All Apple specifications must be met, such as support for new device classes like iPhone X
- In a review, Apple reserves the right not to publish the app or to subsequently remove it.
- The review can lead to delays of up to 10 days (currently, the average review duration is about 3 working days).
- Apps can only be made available to selected user groups on a very limited basis

Distribution via Google Play Store - advantages

- Apps are available to end users via Google's standard mechanism
- Apps can - if necessary - be selectively enabled or blocked for individual countries
- Apps can - if desired - be offered for a fee in defined structures (Google charges a percentage commission fee of 15% for this)
- Google provides the infrastructure for distribution and billing

Distribution via Google Play Store - disadvantages

- Users need a Google account to install apps from the Play Store
- For enterprise customers with managed devices, the Play Store may be locked down via MDM
- All Google requirements must be met - such as the Cordova version.
- After automated app scans, Google reserves the right to remove the app from the store at a later date.
- Due to technical scans, the release of apps can be delayed by a few hours
- Apps can only be made available to selected user groups to a very limited extent

Distribution via beta programs of the public app stores

Apple and Google each offer a beta testing program in addition to the distribution of public apps. At Apple, apps are made available for beta testing to end users via the TestFlight app. On iOS devices, this app can be installed from the App Store app.

The administration and publication of apps for this is done via the Developer Portal and App Store Connect in the TestFlight area. On Google, apps are made available for alpha or beta testing via the Play Store. The Play Store is preinstalled on every Android device.

The administration and publication of apps for this is done via the Developer Portal in the Alpha and Beta Testing area. Apple and Google define the framework for publishing apps via their systems.

For version 26.4.0

Distribution via Apple Testflight - Advantages

- Apps are available to users via a mechanism provided by Apple
- Apps can be selectively released to individual users
- Apple provides the infrastructure for distribution and billing

Distribution via Apple Testflight - Disadvantages

- Users need an Apple ID to install apps from the Apple App Store
- One-time installation of the TestFlight app is required to install the app
- Apple reserves the right not to publish the app in a "reduced" review
- Delays of up to 10 days may occur due to the review (currently, the average review duration is about two working days).
- App signature expires after 90 days

The TestFlight service is primarily intended for a short testing period before publishing an iOS app. It is not suitable for permanent operation due to the short validity of the signature.

Distribution via Google Alpha and Beta Testing - Advantages

- Apps are available to users via a mechanism provided by Google
- Apps can be selectively enabled for individual users
- Google provides the infrastructure for distribution and billing

Distribution via Google Alpha and Beta Testing - Disadvantages

- Users need a Google ID to install apps from the Play Store
- For enterprise customers with managed devices, the Play Store may be locked down via MDM

Distribution via internal enterprise app store

In addition to distributing apps via the respective public stores, Apple and Google also offer mechanisms for distributing apps internally, primarily for enterprises. In the case of Apple, the Apple Enterprise program and an enterprise app store such as Relution are required as prerequisites.

The apps are made available to end users via a separate App Store app or a mobile website. The apps are uploaded and managed in the enterprise app store (in Relution under `Apps` → `App Store`). At Apple, only certificates and provisioning profiles are created in the Apple Developer Portal.

Apps are distributed via the respective enterprise app store provider. At Google, apps can be made available for download and installation via a web service.

For special devices, such as Samsung, optimized installation and distribution mechanisms can be used. Apple and Google define the options for distributing apps in parallel with their systems.

For version 26.4.0

Distribution of iOS apps via Enterprise App Store - advantages

- Apps can be distributed to selected user groups, e.g. as a deep link or after logging in with previously configured user names and passwords
- Users do not need an Apple ID to install apps from an internal Enterprise App Store
- Not all Apple requirements have to be met
- The release of app updates is not delayed by a review from Apple
- Some enterprise app stores (e.g. Relution) can be used without device management (MDM)
- An existing user management system (ActiveDirectory/LDAP) can be connected so that users do not need new credentials

Distribution of iOS apps via enterprise app store - disadvantages

- Apps are available to end users via a special mechanism that is approved by Apple, but requires initial configuration by the user (see here →)
- Apps must be re-signed with an updated provisioning profile after one year and uploaded to Relution as a new version.
- The infrastructure for distribution can be provided as a cloud service or on-premise, for example.
- According to Apple's guidelines, apps may only be distributed to employees, interested parties and partners, but above all to a known group of users.

Distribution of Android Apps via Enterprise App Store - Advantages

- Apps can be distributed to selected user groups, e.g. as a deep link or after logging in with previously configured user name and password
- Users do not need a Google ID to install apps from an internal enterprise app store
- Not all Google requirements have to be met
- Release of app updates is not delayed by Google technical scans
- Some enterprise app stores (e.g. Relution) can be used without device management (MDM)
- An existing user management system (ActiveDirectory/LDAP) can be connected so that users do not need new credentials.

Distribution of Android apps via enterprise app store - disadvantages

- Apps are available to end users via a special mechanism that is approved by Google, but requires initial configuration by the user
- The infrastructure for distribution must be provided, for example, as a cloud service

For version 26.4.0

Add and update native apps

With Relution, native apps for tvOS can also be distributed and put under release management. There is no separate tvOS platform for this: tvOS apps are uploaded as an `.ipa` file and listed in Relution under the iOS platform. Apple TV devices receive them through this iOS app. The app must have been built for tvOS.

An app can have several versions in different release statuses, for example version 1.0 in the Release status and version 1.1, which is prepared and reviewed in the Development or Review status. Apple TV devices always receive the version in the Release status. Therefore, version 1.0 is uploaded to Relution first and set to the Release status.

Create a new app

Native apps are created in the menu under `Apps` → `App Store`. The Add button opens the Add a new app dialog. Under Source, the Native app option is selected.

After clicking Next, the app file (`.ipa`) is uploaded via Choose file. Add details then opens the app form.

> Attention has to be paid to the size of the file. For large apps, problems may occur if the database or reverse proxy does not allow it. In this case, the configuration has to be adjusted.

In the app form, the Release status is specified and the app is created with Save. Except for the Archive status, each release status can only contain one version of the app.

The Permissions section defines who may work on the app in the Relution portal:

- Owner: may apply any operation to the app in every status.
- Reviewer: may edit the app and move versions to the Release or Development status.
- Developer: may upload and edit versions in the Development status and move them to the Review status or to the Archive.
- User: may download, rate and comment on versions in the Release status.

Regardless of these permissions, administrators can distribute the app to devices via the Relution portal.

Distribute native apps to Apple TV

There is no Relution Agent for tvOS and therefore no self-service store on the device. Users cannot install native apps on the Apple TV themselves. Distribution takes place exclusively via the Relution portal:

- with the Deploy Relution store app device action (Actions →),
- under Required apps in the App compliance configuration, provided the checkbox in the Auto install column is selected (App compliance →),
- in the app view under Devices with this app with the Update app button, for devices on which the app is already installed.

The version in the Release status is always the one distributed. A version in the Development or Review status cannot be distributed to an Apple TV via the Relution portal. For tvOS, auto deployments only include public apps, not native apps.

For version 26.4.0

Update app

If a new version of the app is to be prepared, it can be set to the Development or Review status in advance. Before that, the new version must be selected and uploaded via the Add new version button.

A date can be entered for the new version in the Go Live date field. The version only switches to the Release status automatically on that day if an App Release Workflow → is active and the version in the Review status has passed all release steps. Without an active release workflow, the date only serves as a target date, and the version is set to the Release status manually (see below).

Both versions can be viewed in the app properties.

Manual go-live of the new version

In the Relution portal, the respective versions can be viewed and configured. If the new version is in the Review status, clicking the Release button moves it to this status. If it is still in Development, the change is made via `Move to` → `Release`. If a version is already in the Release status, it is automatically moved to the Archive.

> The app is not automatically updated on the devices. Administrators trigger the update with the Deploy Relution store app device action or in the app view under Devices with this app with the Update app button.

For version 26.4.0

Manage App Store apps

With Relution, it is possible to distribute apps from the Apple App Store to devices. To do this, an app license must always be purchased – regardless of whether the app is paid for or not. On iOS devices, an app license can either be purchased via Apps and Books (VPP in the portal) or obtained via an Apple ID signed in on the device. On Apple TV devices, however, apps from the App Store can only be installed with an Apps and Books license; the Apple ID route is not available there. The setup of Apps and Books is described in the corresponding chapter →.

Apps purchased in Apple School / Business Manager are automatically synchronized to Relution (from version 5.10). Apps are published in Relution with the release status Release and can be distributed to devices afterwards. Apps that should not be made available to all users can also be manually assigned to a different release status. An app can also be manually added to the Relution App Store at any time. However, Apps and Books licenses are not automatically available for these apps. On Apple TV devices, they can only be installed once Apps and Books licenses are available for them. These licenses can be obtained at a later date.

Distribute apps

Apps from the App Store are normally distributed to Apple TV devices as required apps via the App Compliance → policy configuration.

An app is assigned to individual devices via the device action Deploy Relution store app. In addition to native apps, it also offers the apps from the App Store that are listed under the iOS platform in the Relution App Store. The action Deploy an app from the Apple App Store is not available for tvOS devices.

For version 26.4.0

Manage apps

Apps from the App Store are updated automatically by the operating system. In rare cases, however, this does not work. In this case, there are two ways to trigger an update:

- In the app's detail view, the affected devices are selected on the Devices with this app tab and updated via Update app. The button is disabled as soon as one of the selected devices already has the version in the Release status installed.
- Alternatively, the action Deploy Relution store app is executed with the app in question on the affected devices.

In both cases, a reinstallation is triggered and the devices validate the app version with Apple's App Store. If the available version is more recent than the installed version, the existing app is updated.

User Enrollment

With user enrollment, private Macs can be enrolled without the owner having to give up all control over the devices. Based on the Bring Your Own Device approach (BYOD), private devices of students or employees can be integrated and used in the school or company context while maintaining the protection of private data. User enrollment of iPhone and iPad is described in the article User enrollment for iOS →.

> Devices must not be in Supervised Mode → for Apple user enrollment.

There are two variants of user enrollment: account-driven user enrollment, where sign-in on the Mac takes place with a Managed Apple Account (Managed Apple ID in the portal), and profile-based user enrollment via an enrollment link.

> Profile-based user enrollment is no longer supported as of macOS 15. For these Macs, account-driven user enrollment → is used.

Benefits

- Administrators cannot view privately installed apps.
- Devices remain under control of users.

For version 26.4.0

Disadvantages

- Not all actions and policy configurations are possible.
- Managed Apple Accounts are required.
- The macOS Companion is not deployed on Macs with user enrollment. Apps of type DMG can therefore not be installed on these Macs.

Account-driven user enrollment

Relution supports account-driven user enrollment for Macs that are not in Supervised Mode →.

Sign-in takes place on the Mac in System Settings by signing in with a work or school account, i.e. with the Managed Apple Account. Using Service Discovery, the Mac determines the responsible MDM server and redirects to the Relution sign-in page, where sign-in takes place with the Relution user account. The sign-in with the Managed Apple Account is then confirmed on the Mac, the MDM profile is installed, and the Mac appears in the device inventory of the corresponding Relution organization.

Requirements

- macOS 14 or later.
- An APNs certificate stored in Relution (APNS Push Certificates →).
- A Managed Apple Account and a Relution user account for each user. The Managed Apple ID is stored in the user details for this purpose; without a Managed Apple ID, Relution uses the user's E-mail address. This value must match the Managed Apple Account used to sign in on the Mac.
- Either the Account-driven Apple user enrollment setting enabled in the organization or a user enrollment → created for the user.
- Service Discovery for the domain of the Managed Apple Accounts, either automatically via Apple School/Business Manager or via a well-known file.

Enable account-driven Apple user enrollment

The setting is located under `Settings` → `Device Management` in the Account-driven Apple user enrollment section. It applies per organization; the section is not shown in the global organization.

When a user signs in, Relution first uses a macOS user enrollment created for this user with the status Created that is still valid for at least five minutes. If no such enrollment exists and the Account-driven Apple user enrollment toggle is enabled, Relution automatically creates a user enrollment with the ownership Bring Your Own Device (BYOD) and a validity of five days. The toggle is disabled by default; without a matching user enrollment, enrollment of the Mac then fails.

For version 26.4.0

Set up Service Discovery

Service Discovery must be configured so that Apple can direct devices to the correct MDM server. There are two ways to do this.

Automatically via Apple School/Business Manager

As of macOS 15.2, no separate file is required if Apple School/Business Manager is connected to Relution for Automated Device Enrollment (ADE, DEP in the portal) via a DEP account. Relution automatically stores the Service Discovery URL in Apple School/Business Manager during every synchronization of ADE devices. This requires Relution to be set as the default MDM server for Mac under `Preferences` → `Your MDM Servers` → `MDM Server Assignment` → `Default MDM Server Assignment`.

Via a well-known file

For Macs running a macOS version earlier than 15.2, or without a connected Apple School/Business Manager, an HTTP well-known resource file must be published on the domain users sign in with. Relution already answers this request itself for its own hostname; a separate file is therefore only required if the domain of the Managed Apple Accounts differs from it. Apple must be able to retrieve this file via an HTTP GET request at the following URL:

```
https://yourdomain.com/.well-known/com.apple.remotemanagement
```

Under `yourdomain.com`, the domain also used for the Managed Apple Accounts must be entered. The file must be hosted on a domain that can handle HTTP GET requests.

The file is created in JSON format with the content type `application/json`. To enter the correct information in the file, the required information can be copied directly from the Relution portal:

1. `Settings` → `Device Management` is opened.
2. In the Account-driven Apple user enrollment section, the JSON text shown under Response is copied in full, including the outer curly braces (Copy to clipboard button), and pasted into the file. The JSON text is shown regardless of the toggle.

> For the file to work correctly, it must not have a file extension.

Example: maxmustermann@musterhausen.de

In this example, the domain would be `musterhausen.de`. The Service Discovery file would need to be published there.

Create a user enrollment in Relution

A user enrollment is created under `Devices` → `Enrollments` via Add. macOS is selected as Platform and the User Enrollment button as Type. The type can only be selected with permission to read users.

A user enrollment is always assigned to exactly one user; a separate enrollment is created for each user. Either a Managed Apple ID or an E-mail address must be stored in the user details. If no Managed Apple ID is stored, the email address is used as the Managed Apple Account. Users assigned to devices can no longer be changed or removed from devices enrolled via user enrollment.

A user enrollment created this way is used for account-driven user enrollment when the user signs in on the Mac. On Macs up to macOS 14, it can also be used for profile-based user enrollment.

For version 26.4.0

Profile-based user enrollment (up to macOS 14)

The enrollment link of the created user enrollment is sent to the respective student or employee. Via the link, the enrollment is performed on the Mac using the user's Managed Apple Account, and the device automatically appears in the device inventory of the corresponding Relution organization.

Manual enrollment

Enrollment is performed by manually downloading and installing an MDM profile on the Mac. This requires either scanning a QR code or manually opening the corresponding URL in the browser. The MDM profile is then installed in System Settings.

Advantages

- Enrollment can be done without having to reset the devices to factory defaults.

Disadvantages

- Enrollment can be removed at any time in the settings on the devices (MDM profile), unless Use profile removal password is enabled in the enrollment.
- Only partially suitable for BYOD devices, as administrators can see which apps are installed. User enrollment → is intended for private devices.
- Not all actions and policy configurations are possible.
- Devices are often not supervised (Supervised Mode).

For version 26.4.0

Create the enrollment in Relution

An APNs certificate stored in Relution is required (APNS Push Certificates →). Without it, the Apple platforms cannot be selected when creating an enrollment.

To perform a manual enrollment, it must first be created in Relution. To do this, `Devices` → `Enrollments` is opened in the menu and Add is clicked.

Enrollments depend on the operating system. Therefore, macOS is selected as Platform and device enrollment as Type (button macOS, not User Enrollment). The Ownership is selected accordingly.

If a `User` is to be associated with the device to be enrolled, the user is selected under User. Optionally, a Device name and a Device description can be specified for display in the device inventory; without a device name, Relution generates the name automatically.

The Configuration section offers the following options for macOS:

- Use profile removal password: The MDM profile can then only be removed from the Mac with an automatically generated password. The password can be retrieved in the device details in the Security section under Profile removal password (see also Security optimizations for enrollments →).
- Static device groups: The device is added to these groups directly; policies assigned to these groups are applied after enrollment.
- Agreements: Selection of agreements created under `Settings` → `General` → `Agreements`. Relution provides their texts to the device during enrollment.

Each enrollment can be used only once unless the Multi-use enrollment switch is activated. If this is the case, new devices can be enrolled via the enrollment link until either the validity date has been exceeded or no more device licenses are available in Relution. The validity date is set under Valid until; the default is a date seven days after creation. Multi-use enrollment cannot be changed after saving.

If enrollment notifications by email or SMS are enabled in the organization settings, the enrollment link can be sent directly to the assigned user in the Notification section.

Once the enrollment is saved and thus created, the displayed URL can be opened in the browser on the Mac, or the created QR code can be scanned. The MDM profile is downloaded via the Enrollment button and then installed in System Settings (see steps below).

Step by step instructions

1. The enrollment is started by pressing the Enrollment button
2. Allow is then pressed
3. The next window is closed via Close
4. System Settings is opened
5. There in the section Profiles
6. The loaded MDM profile is selected
7. The MDM profile is checked, Install is pressed and the dialog is confirmed again with Install
8. A security message is displayed. Install is pressed here as well
9. The remote administration is trusted
10. Confirming with Done completes the installation of the MDM profile

For version 26.4.0

This completes the enrollment.
A new entry should now appear in the device inventory of the Relution portal. If licenses from Apps and Books (VPP in the portal) are available for the Relution Agent, the Relution Agent is then installed on the device automatically.

> The managed user should only be deleted once another user (ideally with administrator rights) already exists on the device. Otherwise, access to the Mac may be lost, and a factory reset could be required.

Available actions

Relution provides a selection of actions to directly control and manage Macs. The actions can be applied to a single device or, via multiple selection in the device list, to several devices at once. They can also be triggered by event or on a schedule through device group membership: Device group actions →

The action dialog is opened under `Devices` → `Inventory` via Apply action, either for the devices selected in the list or in the detail view of a device. Only actions supported by all selected devices are offered.

For version 26.4.0

Actions for macOS

Action	Description
Request mirroring	Enables wireless screen mirroring via AirPlay. - Use case: Presentations on a large screen.
Stop mirroring	Stops the AirPlay transmission. Only available for supervised devices. - Use case: Stopping screen mirroring.
Remove app	Uninstalls an app. - Use case: Removing apps that are no longer needed.
Deploy an app from the Apple App Store	Installs apps from the App Store. - Use case: Distribution of standard apps.
Enable Remote Desktop	Activates the Remote Management setting to allow others to access this computer using Apple Remote Desktop. macOS 10.14.4 or later. - Use case: Remote maintenance.
Disable Remote Desktop	Disables the Remote Management setting. macOS 10.14.4 or later. - Use case: Ending remote maintenance.
Enable or disable Bluetooth	Turns Bluetooth on the device on or off. macOS 10.13.4 or later. - Use case: Control for security reasons.
Wipe device	Resets the device to factory defaults and deletes all data. A 6-digit numeric PIN must be set when triggering the action. - Use case: Preparation for handing the device on.
Shutdown device	Shuts down the device. Only available for supervised devices, macOS 10.13 or later. - Use case: Shutting down devices centrally, e.g. at the end of the school or working day.
Reboot device	Restarts the device. macOS 10.13 or later. With the option Notify user to reboot the device (no forced reboot), the user is only prompted to restart (macOS 11 or later). - Use case: Troubleshooting software problems.
Lock device	Restarts the device and fully locks it for any use or login. The 6-digit PIN set when triggering the action is required to unlock it. On Macs with Apple silicon running a macOS version before 11.5, the action deactivates the Mac; reactivating it requires a network connection and authentication by a local administrator with Secure Token enabled. - Use case: Protection of sensitive data.
Refresh device info	Refreshes all available information about the device listed under Details. - Use case: Up-to-date information in Relution.
Continue in device Setup Assistant	Informs the device that the pre-configuration is completed and it can proceed in the Setup Assistant. Only available for devices enrolled via Automated Device Enrollment (ADE, DEP in the portal). Only takes effect if the Await configuration option is enabled in the DEP Profile. - Use case: Automated setup.

Action	Description
Update local administrator password	Changes the password of a local administrator account. The account is selected from the local users reported by the device or specified by its GUID via Enter manual. Only available if exactly one device is selected. - Use case: Increasing security.
Update MDM profile	Reinstalls the MDM profile on the device. The identity certificate is renewed and current settings such as certificate pinning are applied. The MDM server URL remains unchanged; a changed external URL is therefore not transferred to the device. Relution renews the MDM profile automatically before the identity certificate expires. The manual action is therefore only required in special cases.
Send message	Displays a text message on the device. - Use case: Short-term notice to users.
Deploy Relution store app	Installs an app from the Relution Store. Apps of type DMG can only be installed with the macOS Companion enabled. - Use case: Distribution of in-house apps.
Execute shell script	Runs a managed shell script on the device. Requires the macOS Companion to be enabled (`Settings` → `Relution Client Apps`, section macOS Companion, toggle Enable macOS companion). The macOS Companion is only deployed on Macs running macOS 12 or later. - Use case: Automated maintenance tasks.
Install Update	Installs a selected macOS update from the list of available updates reported by the device. In addition, the way the update is carried out is selected, e.g. download only, download and notify the user, or install with a forced restart afterwards. Only available for supervised devices. The action is only offered if Relution has determined an available update for all selected devices. Available updates are determined again whenever the device information is refreshed, e.g. via Refresh device info.
Set Recovery Lock →	Sets, changes or removes the Recovery Lock password. Only available for supervised devices, macOS 11.5 or later. - Use case: Prevent booting into Recovery Mode or from external media without knowing the password.
Verify Recovery Lock →	Checks whether a known password matches the Recovery Lock set on the device. Only available for supervised devices, macOS 11.5 or later. - Use case: Confirm that the stored Recovery Lock password is still valid.

If at least one of the selected devices is not supervised, Stop mirroring, Shutdown device, Install Update and the two Recovery Lock actions are not shown in the action dialog. The same applies to Continue in device Setup Assistant as soon as a selected device was not enrolled via Automated Device Enrollment. Execute shell script only appears if the macOS Companion is enabled.

For Macs enrolled via User Enrollment →, only the following actions are available: Request mirroring, Deploy an app from the Apple App Store, Refresh device info, Update MDM profile, Send message and Deploy Relution store app.

Recovery Lock

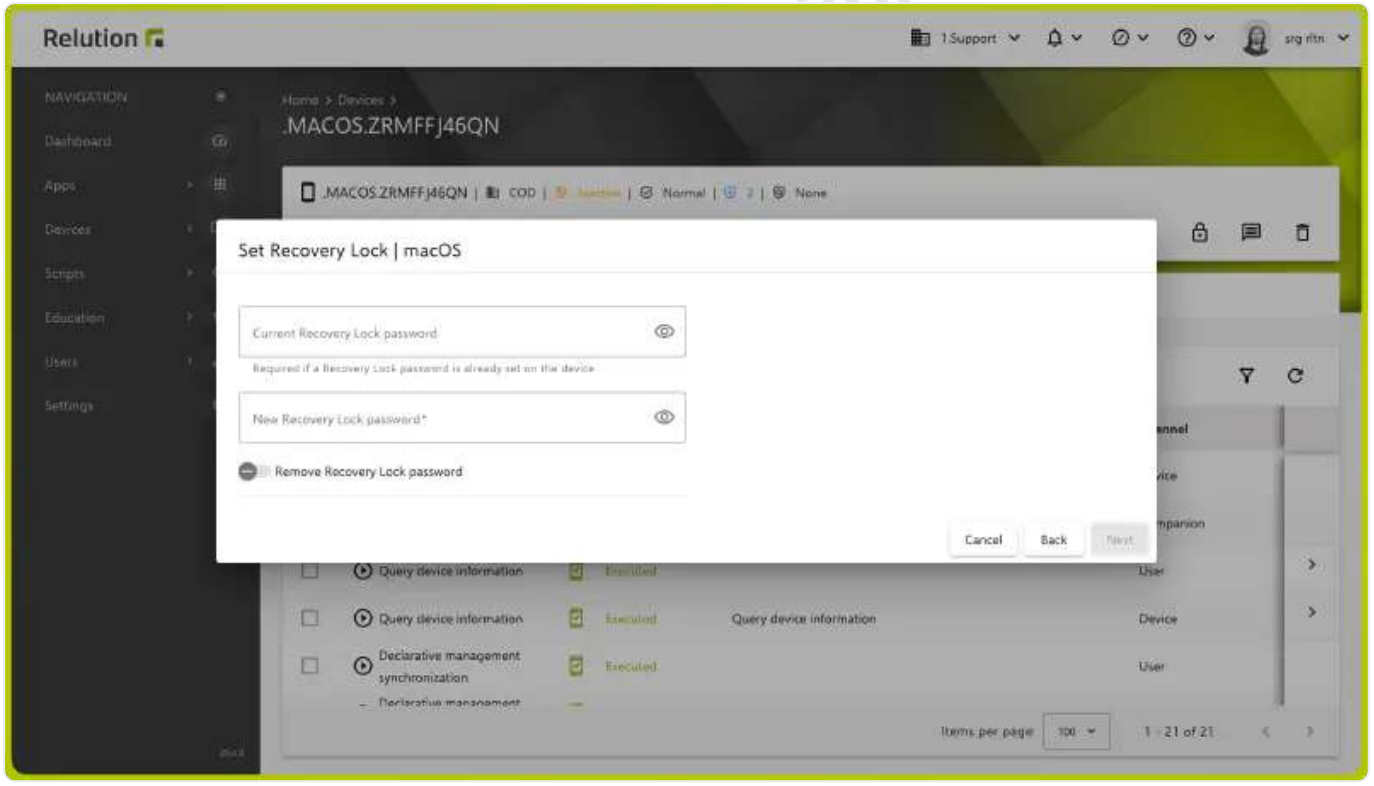
Recovery Lock prevents a Mac from being started into Recovery Mode or booted from external media without knowledge of a password. Two actions are available in Relution to manage this lock. Both require a supervised device running macOS 11.5 or later and are offered in the action dialog, either for a single device or, via multiple selection in the device list, for several devices at once: Available actions →

Relution does not output the passwords entered in these actions again; they cannot be viewed in the portal later and must therefore be stored separately.

Set Recovery Lock

New in 26.4

As of version 26.4, the Recovery Lock password can be set, changed or removed directly from Relution using the Set Recovery Lock action. If a Recovery Lock password is already set on the device, it must be entered in the Current Recovery Lock password field. The new password is entered in the required New Recovery Lock password field. If the Remove Recovery Lock password toggle is enabled, the existing password is removed without setting a new one; the new password field is then hidden and the Current Recovery Lock password field must be filled in.



Verify Recovery Lock

New in 26.5

The Verify Recovery Lock action checks whether a known password matches the Recovery Lock set on the device. The password to be checked is entered in the Recovery Lock password field; if no password is set on the device, the field is left empty. If the password matches, the action is given the status Executed. If it does not match, the action is given the status Error with the error message `The Recovery Lock password does not match`.

Recovery Lock status

Whether a Recovery Lock is active on a device at all can be viewed in the Security card of the device details via the Is recovery lock enabled value.

For version 26.4.0

Overview

Relution offers a variety of configuration options to efficiently control macOS devices. These configurations can be selected and customized in policies. The big advantage is that policies and the included configurations can be easily distributed to a large number of devices.

For version 26.4.0

Available Configurations

Configuration	Description
Active Directory →	Configures the Active Directory integration
Managed Domains	Defines managed email domains
AirPlay	Manages wireless content streaming to AirPlay-enabled receiver devices
AirPrint →	Manages AirPrint printer settings
Login Window	Manages the login window on the device
App compliance	Manages app-specific restrictions
App Store restrictions	Manages App Store restrictions
App to VPN Mapping →	Configures the VPN used by individual apps
Apple Configurator 2 Configuration →	Applies a configuration profile (`.mobileconfig`) created with Apple Configurator 2 to devices
Accessibility	Configures the accessibility features of the device
Conditional Access →	Requires the device to set up Conditional Access via the Relution Agent to use protected resources
Notifications	Configures notification settings for apps
Screen saver	Configures a password-protected screen saver
Parental Controls	Configures the parental controls settings
Desktop →	Configures the desktop settings
DNS Proxy	Configures a DNS proxy
Encrypted DNS settings	Configures encrypted DNS settings (macOS 11 or later)
Dock	Configures the Dock
Email	Adds email configurations for multiple users
Disk Management Settings	Installs disk management settings on the device (macOS 15 or later, supervised devices only)
Extensible Single Sign-On	Configures an app extension that performs single sign-on
Exchange	Configures Exchange accounts
External Intelligence Settings →	Controls external, cloud-based AI integrations via Siri and Apple Intelligence (macOS 26.4 or later)

Configuration	Description
FileVault →	Configures the disk encryption of a macOS device
Web Content Filter →	Allows or blocks specific web URLs (supervised devices only)
Finder settings	Configures the Finder settings of a macOS device
Firewall	Configures the firewall
Device settings	Configures general device settings (supervised devices only)
Device name →	Configures the device name (supervised devices only)
Global Preferences	Configures global preferences
Global ethernet settings	Manages the global Ethernet connection settings
Global HTTP Proxy	Configures global proxy settings (supervised devices only)
Content Caching	Configures the content caching service
Intelligence Settings →	Centrally controls Apple Intelligence features such as Genmoji, Image Playground and Writing Tools (macOS 26.4 or later)
Calendar →	Manages CalDAV accounts
Kernel Extensions →	Manages kernel extensions
Contact	Manages CardDAV accounts
Accounts	Configures account settings
Login Items	Manages items launched automatically at login
Managed App →	Pushes configurations to managed apps
Math Settings →	Centrally configures functions and modes of the Apple Calculator app (macOS 15 or later)
Migration Assistant Settings →	Controls the behaviour of Migration Assistant, including managed migration and excluded accounts and paths (macOS 26.4 or later, supervised devices only)
Passcode	Manages the passcode policy for Apple devices
Proxies	Configures proxies
Relution Decon →	DNS-based content filter for websites and apps
Restrictions →	Manages device restrictions
Safari settings →	Centrally controls the Safari browser’s behaviour, e.g. history, private browsing and start page (macOS 26 or later)
Safari Extensions	Manages Safari extension settings (macOS 15 or later, supervised devices only)

Configuration	Description
SCEP	Manages SCEP settings
Font	Adds fonts to the device
Script	Manages scheduled script execution via the macOS Companion (only selectable if the macOS Companion is enabled)
Setup Assistant →	Hide setup steps shown after the initial setup
Security Preferences	Configures security preferences
Siri Settings →	Centrally controls Siri's behaviour, including the profanity filter (macOS 26.4 or later)
Software update settings →	Controls the update behaviour of devices, e.g. automatic download, deferral and notifications (macOS 15 or later, supervised devices only)
System policy control	Configures system policy control settings
Energy saver	Configures the energy saver settings
System Extensions	Manages system extensions
System updates →	Manages updates of macOS devices (deprecated, successor: Managed Software Updates)
System preferences	Configures system preferences
Keyboard Settings →	Centrally controls keyboard features such as dictation and mathematical keyboard suggestions (macOS 26.4 or later)
Time Machine	Manages the Time Machine settings on the device
Managed Software Updates →	Enforces operating system updates, targeting a specific version by a deadline (macOS 14 or later, supervised devices only)
VPN	Manages VPN settings
Weblink	Adds a weblink to devices
WiFi	Manages Wi-Fi settings
Certificate	Selects a certificate to be installed on the device by default

The Active Directory, Apple Configurator 2 configuration, Encrypted DNS settings, Email, Extensible Single Sign-On, Exchange, Web Content Filter, Calendar, Contact, Managed App, Safari Extensions, SCEP, Font, Script, System policy control, VPN, Weblink, WiFi and Certificate configurations can be added to a policy multiple times; all other configurations only once. Once a configuration that is allowed only once is part of the policy, it is no longer offered in the selection dialog. The same applies if an Apple Configurator 2 configuration already contains a profile of this type.

In the selection dialog, badges indicate requirements, such as a minimum macOS version, supervised devices (Supervised) or support for User Enrollment → (Supports user enrollment). On Macs enrolled via User Enrollment, only some of the configurations are applied.

The Script configuration only appears in the selection dialog if the Enable macOS companion option is turned on under `Settings` → `Relution Client Apps` (enabled by default).

For version 26.4.0

Intelligence Settings

The Intelligence Settings configuration centrally controls Apple Intelligence features on managed macOS devices. The policy allows individual AI-powered features such as the Apple Intelligence Report, Genmoji, Image Playground, and Writing Tools, as well as app-specific Intelligence features in Mail, Notes, and Safari, to be allowed or blocked. In addition, the policy can enforce that dictation is processed exclusively on the device, without any connection to Apple's servers.

This configuration is available for macOS devices running version 26.4 or later and can only be applied with Device Enrollment, not with User Enrollment (BYOD). Only one configuration of this type is possible per policy. Devices that do not support these settings do not receive the configuration.

> The form is the same for iOS, macOS, and visionOS. The options Allow Image Wand, Allow personalized handwriting results, Allow Visual Intelligence summary and Force on-device only translation are also shown for macOS but are not supported by macOS. They are therefore not described here, see Intelligence Settings for iOS →.

Genmoji, Image Playground, Writing Tools, the Apple Intelligence Report and on-device only dictation can also be controlled via the Restrictions → configuration. The corresponding fields are marked as Deprecated there and are superseded by this configuration. For devices running versions earlier than macOS 26.4, they remain the only way to control these features. The summaries in Mail and Safari and the transcription summary in Notes are also available in the restrictions. The connection of external AI services is managed via the External Intelligence Settings → configuration.

For version 26.4.0

Settings

- Allow Apple Intelligence report
  - If disabled, the Apple Intelligence Report is disabled on the device. Enabled by default.
- Allow Genmoji
  - If disabled, the Genmoji feature is disabled. Enabled by default.
- Allow Image Playground
  - If disabled, Image Playground is disabled. Enabled by default.
- Allow Writing Tools
  - If disabled, Writing Tools are disabled. Enabled by default.
- Force on-device only dictation
  - If enabled, dictation is processed exclusively on the device, without any connection to Apple's servers. Disabled by default.

Mail

- Allow Smart Replies
  - If disabled, Smart Replies in Mail are disabled. Enabled by default.
- Allow summary
  - If disabled, the summary feature in Mail is disabled. Enabled by default.

Notes

- Allow transcription
  - If disabled, transcription in Notes is disabled. Enabled by default.
- Allow transcription summary
  - If disabled, the summary of transcriptions in Notes is disabled. Enabled by default.

Safari

- Allow summary
  - If disabled, the summary feature in Safari is disabled. Enabled by default.

External Intelligence Settings

The External Intelligence Settings configuration centrally controls whether and how external, cloud-based AI services (e.g. ChatGPT) may be used via Siri and Apple Intelligence on macOS devices. The policy is available starting with macOS 26.4 — only for devices with full device enrollment, not in User Enrollment/BYOD mode — and is delivered to the device via Declarative Device Management (DDM). Devices that do not support these settings do not receive the configuration. Only one configuration of this type is possible per policy. The same configuration is available in identical form for iOS and visionOS devices running the respective 26.4 version.

For version 26.4.0

> This DDM-based configuration supersedes the external intelligence integration fields in the Restrictions → configuration. These fields have been marked as Deprecated in the portal since Relution 26.3. For devices running versions earlier than macOS 26.4, external intelligence integrations can still only be controlled via these restriction fields.

External Intelligence Integrations

- Allow external intelligence integrations
  - When disabled, external AI integrations are fully blocked. Enabled by default.
- Allow sign-in for external intelligence integrations
  - When disabled, signing in to external AI integrations is not possible. Enabled by default.
- Allowed workspace ID
  - Sets the workspace ID that the external AI integration is restricted to. Currently limited to a single workspace ID. Leading and trailing spaces are removed. If the field is left empty, no workspace ID is specified.

Keyboard Settings

Starting with macOS 26.4 and Relution 26.3, the Keyboard Settings configuration is available, implemented via Declarative Device Management (DDM). This policy centrally enables or disables definition lookup, dictation, and mathematical keyboard suggestions on macOS. Additional keyboard options such as auto-correction, predictive text, spell check, slide to type, or text replacement are only available for iOS devices → through this policy.

> This configuration requires macOS 26.4 or later and is only available for devices managed via Device Enrollment. All settings are enabled by default; disabling a setting restricts the corresponding keyboard function.

A policy can contain one Keyboard Settings configuration. Relution only transfers it to devices that report this configuration type; devices running older macOS versions do not receive it, and no error message is shown.

Keyboard Settings

- Allow Definition Lookup
  - If disabled, looking up word definitions (Look Up) on the keyboard is no longer available.
- Allow Dictation
  - If disabled, the keyboard's dictation feature can no longer be used.
- Allow Math Keyboard Suggestions
  - If disabled, the keyboard no longer displays automatic solution suggestions for mathematical expressions.
  - The Math Settings → configuration also contains an option for mathematical keyboard suggestions, Enable keyboard suggestions.

For version 26.4.0

Siri Settings

As of macOS 26.4 and Relution 26.3, the Siri Settings configuration is available, implemented through Declarative Device Management (DDM). This policy centrally controls Siri's general availability and the profanity filter. Other options of this configuration — processing user-generated content and access to Siri while locked — are only available on iOS and are not shown in the form for macOS. Only one configuration of this type is possible per policy.

> This configuration requires macOS 26.4 or later and is only available for devices managed through Device Enrollment; it is not available for devices with User Enrollment (BYOD).

> Comparable Siri switches (Allow Siri, Enable Siri profanity filter) also exist in the Restrictions → configuration. They are marked as Deprecated there and are superseded by the Siri Settings. For devices running versions earlier than macOS 26.4, Siri can still only be controlled via the restrictions.

Siri settings

- Enable Siri
  - Enables or disables Siri on the device. Enabled by default.
- Force Profanity Filter
  - Enforces Siri's profanity filter. Disabled by default.

For version 26.4.0

Safari Settings

The “Safari Settings” configuration centrally controls the behavior of the Safari browser on managed macOS devices. This includes clearing the browsing history, private browsing, content summarization, and the start page shown when opening a new tab. On iOS devices, additional options for cookies, the fraud warning, JavaScript, and pop-ups are available; these are not part of this configuration on macOS.

> This configuration is only available for devices with a Device Enrollment profile (not for User Enrollment/BYOD) and requires at least macOS 26. It applies per signed-in, managed user account rather than device-wide across all local accounts.

Only one configuration of this type is possible per policy.

Safari Browser Settings

- Allow history clearing
  - When disabled, the browsing history in Safari cannot be cleared. Enabled by default.
- Allow private browsing
  - When disabled, private browsing mode is not available in Safari. Enabled by default.
- Allow summarization of content
  - When disabled, automatic content summarization in Safari is disabled. Enabled by default.
- Start page *(required field)*
  - Determines which page is displayed when opening a new tab in Safari.
    - Start – Safari uses its default start page; the homepage is disabled. *(default)*
    - Extension – Safari uses the Safari extension referenced by the specified identifier as the start page; the homepage is disabled. Requires an extension identifier in the Extension field of the same name, in the format `Identifier (TeamIdentifier)`, e.g. `com.example.app (ABCD1234)`.
    - Homepage URL – Safari uses the specified URL both as the start page for new tabs and as the homepage. Requires a URL in the Homepage URL field of the same name, which must start with `https://` or `http://`.

User and device placeholders can be used in the homepage URL. The available placeholders are listed below the form and are replaced when the configuration is transferred to the device, see Advanced placeholders →.

For version 26.4.0

Mathematical Settings

Starting with version 26.1.0, Relution also provides the Math Settings configuration for devices running macOS 15+.

This policy centrally manages the functions and modes of the Apple Calculator app and adapts them to educational or organizational requirements. Compared to iOS, the macOS Calculator additionally offers a Programmer Mode and input in reverse Polish notation (RPN), which can also be configured here.

> This policy is only available for devices managed through Device Enrollment, not User Enrollment (BYOD).

Configuration

In the portal, the configuration is divided into the sections Calculator and System behaviour. When the configuration is created, all options are enabled except Add Square root. A policy can contain one Math Settings configuration. Relution transfers the settings via Declarative Device Management (DDM) and only to devices that support this configuration type; older devices do not receive them.

Settings for the Apple Calculator App

For version 26.4.0

Basic Mode

- Add Square root: Adds a square root button to the basic calculator by replacing the +/- button. By default, the square root function is only available in scientific mode. This option makes the square root accessible even if scientific mode is restricted.

Math Notes Mode

- Enabled: Determines whether Math Notes mode can be used within the Calculator app.

Programmer Mode

- Enabled: Determines whether Programmer Mode can be used within the Calculator app. Only available on macOS.

Scientific Mode

- Enabled: Specifies whether the scientific mode of the Calculator app is available.

Global Input Options of the Calculator

- Enable reverse polish notation (RPN): Determines whether input in reverse Polish notation can be used. Only available on macOS.
- Enable unit conversion: Allows the use of the built-in unit conversion feature within the app.

System Behavior

- Enable keyboard suggestions: Controls whether keyboard suggestions automatically display mathematical solutions. The Keyboard Settings → configuration also contains an option for mathematical keyboard suggestions, Allow Math Keyboard Suggestions.
- Enable Math Notes for other apps: Determines whether the `Math Notes` feature can also be used in other apps (e.g., Notes).

For version 26.4.0

Software Update

For macOS devices running version 15 or later in supervised mode, Relution offers the Apple configuration Software update settings. It is based on Apple's Declarative Device Management and replaces the legacy general settings of the System updates configuration, which is marked as deprecated by Apple. Enforcing updates is handled by the Managed Software Updates configuration (see below).

To ensure updates across the entire device fleet, both Software update settings and System updates can be configured in parallel and deployed to all macOS devices.

> The deprecated System updates configuration will be phased out by Apple in the medium term.

General

Allow standard user to perform OS Updates

- Enable / Disable (default: enabled)

Show all software update enforcement notifications

- Enable / Disable (default: enabled)

If disabled, the device only shows the notifications triggered one hour before the enforcement deadline and the restart countdown notification.

Beta program enrollment *(macOS 15.4+)*

- Allowed (default) — the user can enroll in beta programs associated with their Apple Account.
- Always Off — the device is not allowed to enroll in beta programs and is removed from any beta programs it is already enrolled in.

Automatic Software Update Actions *(supervised only)*

User choice is preset for all three settings.

Automatically download available OS Updates

- User choice
- Always Off
- Always On

Automatically install available OS Updates

- User choice
- Always Off
- Always On

For version 26.4.0

Automatically install available security update

- User choice
- Always Off
- Always On

Deferral of OS Updates *(supervised only)*

- Number of days to defer a major OS software update on the device (1–90)
- Number of days to defer a minor OS software update on the device (1–90)
- Number of days to defer system or non-OS updates (1–90)

Rapid Security Response

- Allow background security improvements to the user
- Allow rollbacks of background security improvement to the user

Both toggles are enabled by default.

Managed Software Updates

For version 26.4.0

New in 26.4

The Managed Software Updates configuration enforces operating system updates, targeting a specific version by a deadline. It is the successor to the deprecated System updates configuration and complements the Software update settings configuration described above: those settings control the update *behaviour* (automatic download, deferral, notifications), while Managed Software Updates defines bindingly *which* version has to be installed by *when*.

It requires macOS 14 or later in supervised mode. The configuration is also available for iOS 17 and later, tvOS 18.4 and later and visionOS 26 and later.

Target version

- Version to enforce (default: Latest minor version)
  - Latest major version — the device is raised to the most recent available major version.
  - Latest minor version — updates happen within the installed major version.
  - Minimum specific version — a concrete version is set as the minimum level. It is selected in the mandatory Version field from the operating system versions released by Apple. A version that has already been saved remains selectable even if it is no longer offered in the list.

Enforcement

- Enforcement schedule (default: Relative to release date)
  - Relative to release date — the deadline results from Days after release (mandatory, 0 or more) and Time of day (preset to 00:00). The same rule then applies automatically to every future version.
  - Specific date and time — the Deadline is set as a fixed point in time.
- Grace period after enrollment — optional. Postpones the deadline until this many days after a device was enrolled, so that freshly enrolled devices are not forced to update immediately. It applies to both enforcement schedules and only ever extends a deadline, never shortens it. Leaving the field empty disables the function.

> If the available operating system versions cannot be loaded in the portal, the configuration reports this when opened. Selecting a minimum specific version is then not possible, while the other two modes remain usable.

A deadline that has already passed is still sent to the device; the update is then enforced at the next restart. If there is no suitable update for a device, e.g. no newer minor version, no enforcement is sent.

Details

- Details page URL — optional link that macOS shows to users in the update announcement.

Triggering Updates

For version 26.4.0

There are two ways to perform macOS updates:

Policy Configuration The Managed Software Updates configuration sets a target version that has to be installed by a deadline (see above). The deprecated System updates configuration still defines weekdays (Repeats on) and a Start time for scheduled updates. The latest available update is installed, optionally limited by Max. version to update to. If both configurations are active on a device, Managed Software Updates takes precedence.

Device Action The Install Update device action in the device inventory installs an update selected from the updates available for the device. In addition, the action defines how the update is performed, e.g. Download and install updates, Only download updates, don’t install, Download updates and install later (with Maximum user deferrals) or Download, install and force restart afterwards.

For macOS devices to successfully perform an update, the following applies:

- Devices must be sufficiently charged or connected to a power source.
- Devices must be unlocked; otherwise, users must enter their device passcode.
- Updates can take a long time, depending on network infrastructure and number of devices.
- Supported macOS devices check for updates once per day, independently of the System updates configuration.
- The System updates configuration overrides any restrictions on deferring updates.

Desktop

With the Desktop configuration for macOS devices, the desktop background is defined by specifying a path to an image file. Unlike the comparable Wallpaper → configuration for iOS, Android and Windows devices, no image file is uploaded to or distributed through Relution as part of this policy.

> The path entered in the “Path to the desktop image to be used” field refers to a file that must already exist locally on the macOS device — not a URL. Relution passes this path directly to Apple's native Desktop configuration profile, which only tells the operating system where to look for an existing background image; it does not fetch or install the file itself.

Settings

The configuration can be added once per policy and contains a single field in the General section:

- Path to the desktop image to be used: path to the image file on the macOS device, e.g. `/Library/Desktop Pictures/Company.jpg`. Relution passes the value unchanged into the configuration profile. Placeholders are not replaced in this field. If the field is left empty, a Desktop profile without an image setting is installed.

For version 26.4.0

Providing the Image File

Because the referenced file must already be present on the device before the policy is applied, the image itself needs to be distributed separately — for example through a script configuration (only for devices with device enrollment, not with User Enrollment), an installer package, or another file-distribution mechanism that places the file at the configured path beforehand.

FileVault

With the FileVault configuration for macOS devices, full-disk encryption is enabled centrally on managed Macs. The configuration can be added once per policy and is only available for devices with device enrollment, not for devices with User Enrollment →.

> Installing the FileVault configuration does not start disk encryption immediately, since FileVault derives its encryption key from the user's login password. When the user is asked to enable FileVault depends on the options for deferring the activation.

Time of activation

With the default settings, the following applies:

- Defers enabling FileVault until the designated user logs out. is enabled.
- Do not request enabling FileVault when user logs out is disabled.
- The maximum number of times users can bypass enabling FileVault is `0`.

The user is then asked to enable FileVault at the next logout. At the latest, enabling is required at the next login.

A value greater than `0` (at most `9999`) allows the corresponding number of bypasses. With `-1`, enabling is not enforced at login. If Do not request enabling FileVault when user logs out is enabled, the request at logout is omitted. Both sub-options are only available while deferring is enabled. If deferring is disabled, the user name and password of a user must be specified in the profile.

For version 26.4.0

Settings

The General section provides the following settings:

- FileVault status: On enables FileVault, Off disables it (required, default On).
- Recovery key type: institutional and personal recovery key, institutional recovery key only, or personal recovery key only. An institutional key requires a Certificate.
- Recovery key path: location for the recovery key and the computer information, e.g. `/Library/Keychains/recovery.plist`.
- Allow displaying the personal recovery key after enabling FileVault on the device: defines whether the personal key is shown to the user after activation.
- FileVault Open Directory user and Password: user to be added to FileVault. Alternatively, Enable to prompt for missing user name or password has the device prompt for missing information.
- Options for deferring the activation (see above).

In the Personal recovery key handling section, Allow that Relution can access the personal recovery key defines whether Relution stores the personal recovery key (default: enabled). The key can then be retrieved in the device details in the Security card under FDE personal recovery key. This is only possible if the option was already enabled before FileVault was activated; if FileVault is already enabled on the Mac, the option has no effect.

The Additional options section provides Prohibit the deactivation of FileVault, Prohibit the activation of FileVault and Delete FileVault key on standby.

Deployment via Automated Device Enrollment (ADE)

The FileVault configuration can be deployed via Automated Device Enrollment (ADE, DEP in the portal) before or during Setup Assistant, so it is already present when the device starts up for the first time. Since deriving the encryption key requires a user account and its login password, actual encryption cannot begin until after a user account has been created and that user has logged in for the first time.

If Relution is to store the personal recovery key, the configuration with Allow that Relution can access the personal recovery key enabled must be on the device before FileVault is activated. In the DEP profile, the FileVault step of Setup Assistant can be skipped. Relution does not support forcing FileVault activation in Setup Assistant.

For version 26.4.0

Kernel Extensions

KEXTs (Kernel Extensions) are modules that integrate deeply into the macOS operating system to extend its functionality or support specific hardware and system requirements. They operate at the kernel level — the “nervous system” of the operating system — and therefore provide access to resources and functions that are not directly accessible in user space.

Why are KEXTs needed?

- Support for non-native hardware such as specific graphics cards, network adapters, or external storage devices.
- Implementation of file systems (e.g., NTFS, FUSE) that are not available by default in macOS.
- Extension of network functionality, e.g., for VPN protocols or virtual network interfaces.
- Integration of security solutions and checks at the kernel level.
- Development of virtualization platforms and their interaction with the kernel.

Advantages of KEXTs

- Deep system access: They enable features that would otherwise not be possible without direct kernel access.
- Hardware compatibility: Devices and features not natively supported by macOS can be fully integrated through KEXTs.
- Flexible expandability: Developers can create custom solutions for specific requirements.

For version 26.4.0

General

The Kernel Extensions configuration is added to a macOS policy under `Devices` → `Policies` via Add. Each policy can contain one configuration of this type. It is only available for devices enrolled via device enrollment, not for user enrollments.

The following configuration options are available in the General section:

- Allow nonadministrative users to approve kernel extensions in Security & Privacy preferences: toggle, off by default. When enabled, users without administrator privileges can also approve additional kernel extensions. Effective as of macOS 11.
- Allow user to approve additional kernel extensions: toggle, off by default. When enabled, users can approve kernel extensions that are not explicitly allowed by the configuration.
- Allow any kernel extensions signed by these team identifiers: list field for team identifiers. Validly signed kernel extensions with these team identifiers are allowed to load. If the list is left empty, no team identifier is transferred.

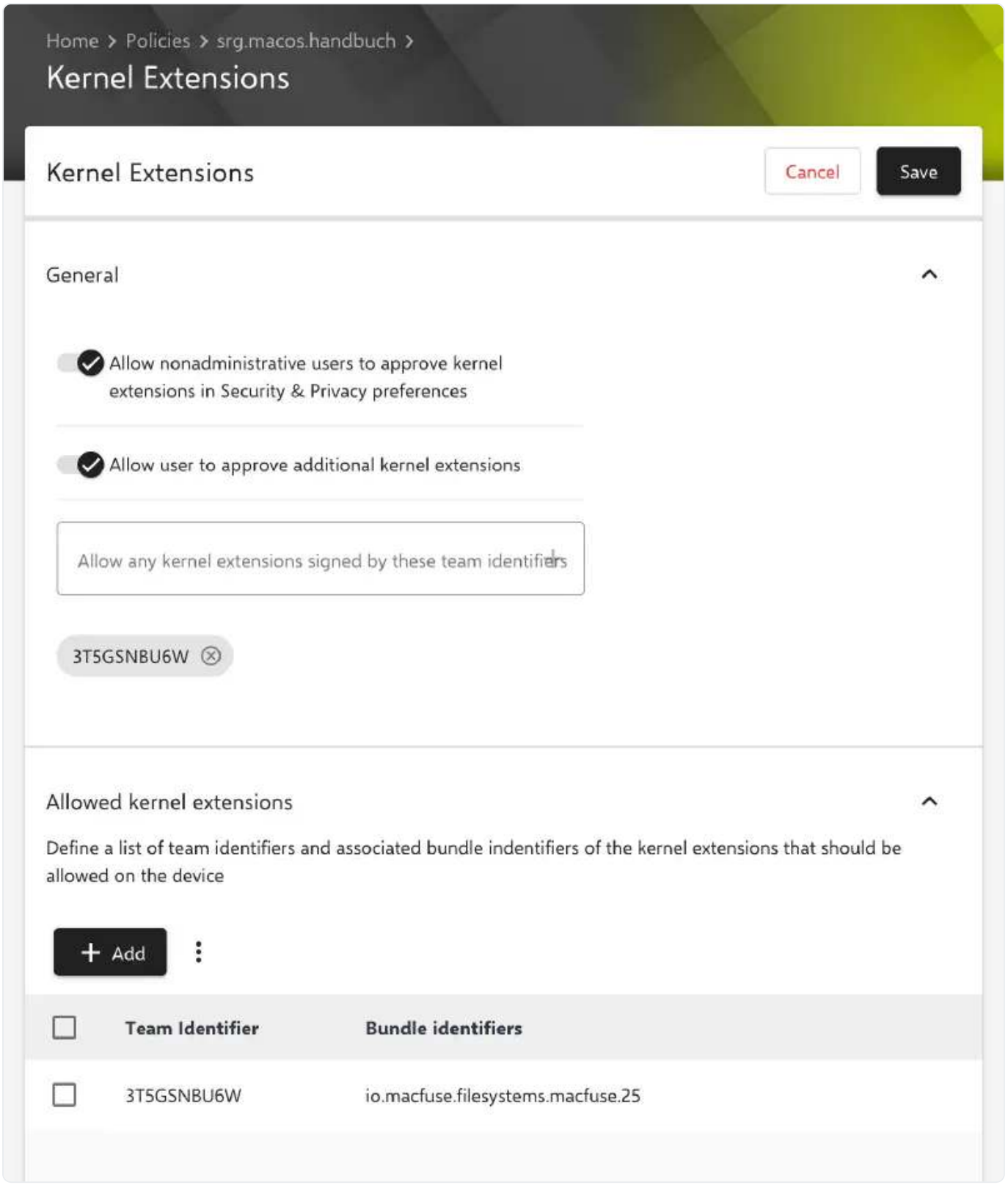
In general, all KEXTs with the same team identifier can be allowed. Alternatively, explicit extensions can be defined in the next section using a team identifier.

Allowed kernel extensions

Add opens the Add new Team identifier mapping dialog. The Team Identifier (required) is entered there, and the associated bundle IDs are listed under Bundle identifiers.

Team Identifier	Bundle identifiers
3T5GSNBU6W	io.macfuse.filesystems.macfuse.25

For version 26.4.0



Reading Team Identifier and Bundle ID

The Team Identifier can be extracted from the downloaded macfuse-5.1.1.dmg using the following command:

```
codesign -d --verbose=2 macfuse-5.1.1.dmg 2>&1 | grep -i teamidentifier
```

Output:

```
TeamIdentifier=3T5GSNBU6W
```

The Bundle ID can be obtained from a manually installed KEXT (example: macFUSE) as follows:

```
kextstat | grep -i fuse
```

Output:

```
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>
```

Thus, io.macfuse.filesystems.macfuse.25 is the required Bundle ID.

Note

Under Allowed kernel extensions, multiple bundle IDs can be assigned to one team identifier — either when creating a new entry via Add or when editing an existing entry via the three-dot menu and Edit.

Each team identifier can only be added once. A second entry with the same team identifier is rejected with the message Team identifier already exists; additional bundle IDs are therefore added to the existing entry.

Apple KEXT →

Migration Assistant

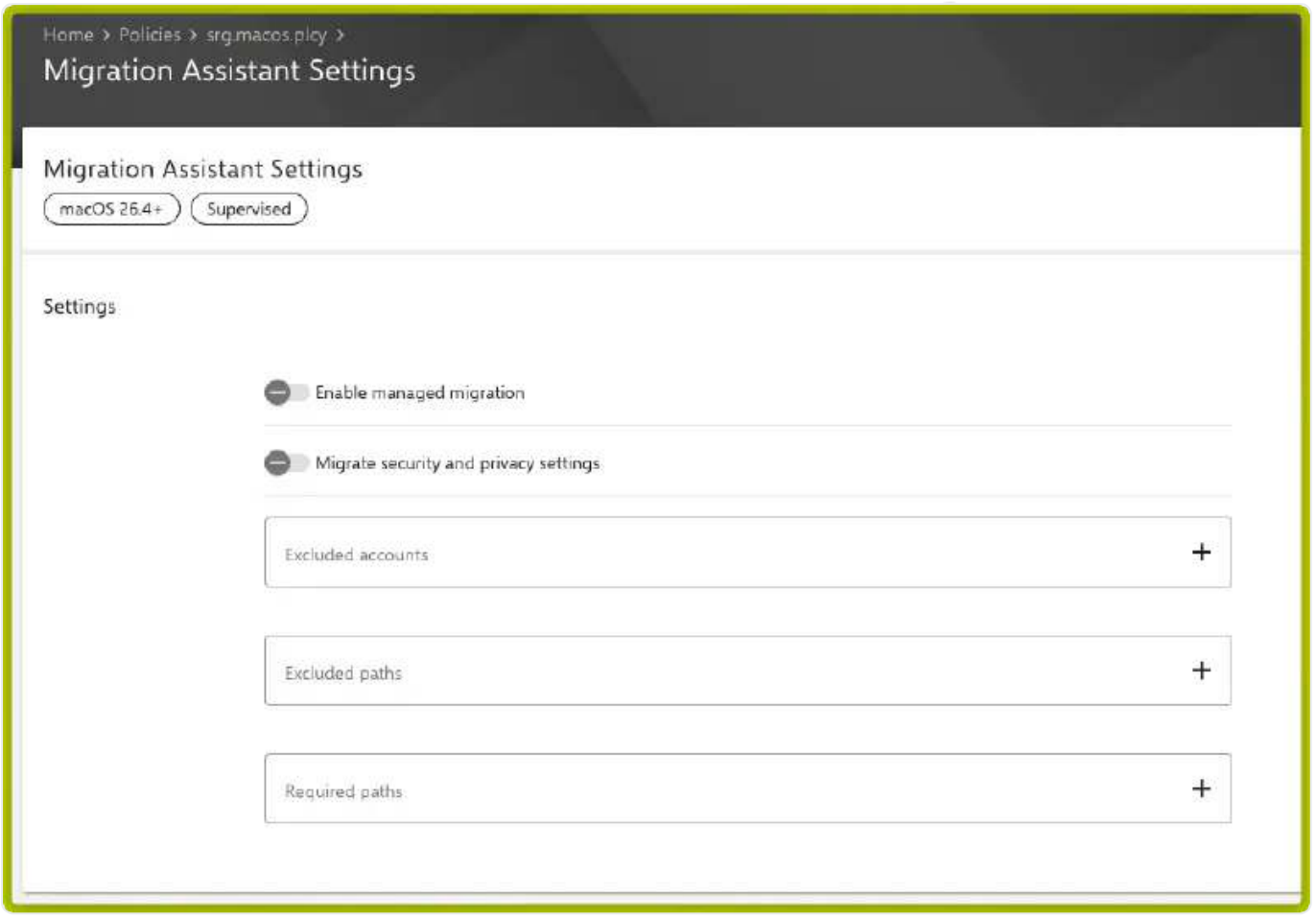
Migration Assistant is a built-in macOS tool that helps set up a new Mac. It transfers user data, apps, settings, and files from an old device to the new one — so nothing has to be set up from scratch.

Starting with macOS 26.4, Apple supports managing Migration Assistant through Declarative Device Management (DDM). Relution 26.3 implements this support fully: settings can be pushed to devices via policy, and the current migration status is reported back to Relution as a status report.

> The configuration requires macOS 26.4 or later and a supervised device.

Settings Declaration

New in 26.3



Enable managed migration

Activates managed migration on the device. While this toggle is off, no further restrictions apply. The toggle is off by default.

Migrate security and privacy settings

Determines whether security and privacy settings are transferred from the source to the new device. When disabled, only user data is migrated; system-wide security settings remain at their default state. The option is off by default.

Excluded accounts

List of user accounts to be excluded from the migration process. Each entry is the short name of a user account. Account names can be added individually using the + button.

Examples:

Account name	Use case
`administrator`	Local admin account should not be transferred
`guestuser`	Temporary guest account to exclude

For versi

Excluded paths

List of files and directories that will not be migrated. Paths can be added individually using the + button.

Paths are relative to the user's home directory and must not start with `/` or `~`; directory paths end with `/`. Invalid entries are rejected when they are added. System-wide paths outside the home directory cannot be specified.

Examples:

Path	Use case
`Library/Caches/`	Cache data will be rebuilt on the target device
`Downloads/`	Temporary downloads are not transferred
`Documents/Excluded/`	A specific documents folder is left behind

Required paths

List of files and directories that must be migrated. If a required path is missing on the source device, the migration is aborted. Paths can be added using the + button. The same format rules apply as for Excluded paths.

Examples:

Path	Use case
`Documents/`	Work documents must be transferred completely
`Library/Keychains/`	Keychains are required for operation

Status Reports

Relution automatically reads two status reports from the device. After selecting the device under `Devices` → `Inventory`, the values appear on the Information tab in the Device details card. The entries are only shown once the device has reported the respective values.

For version 26.4.0

Migration state

The Migration Assistant entry shows the current state of Migration Assistant on the device:

State	Meaning
Waiting	Migration Assistant has not been started yet or no migration has taken place
Migrating	The migration is currently running
Completed	The migration completed successfully
Failed	The migration failed
Cancelled	The user cancelled the migration
Unknown	The device reports a state that Relution cannot map

Migration report

Contains detailed information about the completed migration:

- Source user: user account on the source Mac
- Target user: user account on the new Mac
- Start time and Completion time: start and end of the migration
- Files transferred: files transferred compared to the total number of files
- Data transferred: amount of data transferred compared to the total data size
- Errors: errors reported during the migration

Configuration in Relution

1. Under `Devices` → `Policies`, create a macOS policy via Add or open an existing macOS policy.
2. Select the Migration Assistant Settings configuration via Add.
3. Enable Enable managed migration.
4. Configure the desired accounts and paths.
5. Save the configuration, publish the policy and assign it to the target devices.

Each policy can contain one Migration Assistant Settings configuration. If a device receives several of these configurations through multiple policies, only one of them is transferred to the device.

For version 26.4.0

Device Name

Relution allows the device name to be set for iOS, iPadOS, tvOS, and macOS. A policy with the Device name configuration can be created and distributed to device groups. The configuration can be added once per policy; the Device name field is required and accepts up to 255 characters.

The configuration is intended for supervised devices (badge Supervised) and is not available for devices with User Enrollment →.

The device name can be assigned statically, e.g. `Case iPad`, so all devices in the group receive the same name.

However, for multiple devices in a group, using placeholders might be more practical. The portal shows the available user and device placeholders below the form in the Available placeholders card.

For example, the device name could be composed as follows: `Case ${device.model} ${user.name}` This would result in a display like: `Case iPad12,1 Max.Mustermann` making it easier to manage the inventory.

Further functions such as substrings, default values for unset fields, or replacing umlauts are described in Advanced placeholders →.

If the configuration is active on a device, Relution takes the name reported by the device into the inventory with every device query. Without this configuration, the reported name is only taken over as long as no name is set in the inventory yet.

Active Directory

With Relution it is possible to configure macOS devices in such a way that login with accounts from a Windows domain is possible. The domain controller must be accessible for this.

Prerequisite

The usual requirements for the domain controller apply. The following instructions are based on tests and experience with a Windows Server 2019 Standard Edition.

- Domain Controller
- Administrative permissions in the domain
- The macOS device must be able to resolve FQDN from domain controller. (Entry in the hosts file is not sufficient).
- The macOS device must be able to reach the domain controller
- Computer account in the domain

Configuration of the Active Directory policy

The configuration shown here is only an example and has been tested with macOS 13 and higher.

For version 26.4.0

1. The Active Directory configuration is added to a policy for macOS.
2. At least the following parameters are configured:

Option	Value
Name (optional)	Name of the configuration; if left empty, the value of Active Directory domain to join is used
Active Directory domain to join	Name of the domain (e.g. relution.loc)
User name of the account for the domain	Username of a domain administrator
Password of the account for the domain	Password of the domain administrator
Create a mobile account at login	ON
Active Directory groups with admin access (optional)	DOMAIN\Group-name

The only required field is Active Directory domain to join; the value must be a valid host name. The portal does not enforce user name and password, but they are needed to join the domain.

3. Once the policy with the configuration has been applied to the Mac, the Mac should be restarted in any case to reduce login problems.

For version 26.4.0

When the policy is removed from the Mac, the computer account is also removed in AD.

Optional settings

In addition to the parameters above, the configuration offers further settings that are only set when needed:

- General: Client ID defines the name of the computer object in the domain. Allow authentication from any domain in the namespace permits logins from all domains of the forest.
- Accounts: Organizational unit to add the joining computer object to defines the OU for the computer account. For the mobile account, Warn before creating the mobile account, Force a local home directory, Network home protocol (AFP or SMB), Use UNC path from Active Directory to derive the network home location, Default user shell and Primary user account naming convention (Domain or Forest) are available.
- Advanced Options: Preferred domain server, Interfaces allowed for dynamic DNS updates, Packet signing policy, Packet encryption policy, the mapping of UID, GID and group GID to AD attributes, and Number of days before requiring a change of the computer trust account password (0 to 3650; `0` disables the change and is the default).

Further configuration

To enable login on a Mac, the Login Window configuration must also be added. The following parameters must be activated there:

- Show name and password fields instead of user list
- Show network users
- Show ‘Other…’ in user list

The Login Window configuration is only available for devices with device enrollment, not for devices with User Enrollment →.

Possible Errors

1. `(1) The 'Directory Binding Account' payload could not be installed. Attempts to bind to the server 'rltn.mway' returned an unspecified problem. (-319)`
    - It should be checked whether a computer account with the name of the device exists on the DC.
2. `(1) The 'Account for mounting in directories' payload could not be installed. The server 'rltn.mway' was not found or is not responding.`
    - It should be checked whether the domain controller can be reached from the Mac. The FQDN must be resolvable.

For version 26.4.0

App to VPN Mapping

When setting up a cross-device VPN, all device data is routed through the private network. Sometimes, a company may want to set up a VPN only for their enterprise applications. Apple allows VPN connections to be set up for iPhones, iPads and Macs on an app-by-app basis. Here, administrators can control exactly what data flows through the VPN. The policy configuration of an app-to-VPN mapping helps organizations keep app-level traffic apart, allowing for the separation of personal and corporate data.

Prerequisite

An app-to-VPN mapping can be set up directly through Relution. This only works for apps that are installed and managed by the MDM on the devices.

Relution supports the following connection types for establishing a per-app VPN connection on iOS and macOS devices:

- IPSec
- JuniperSSL
- SonicWALL
- AnyConnect Legacy
- AnyConnect
- IKEv2
- Custom SSL

For other VPN types, the VPN configuration points to the supported types; for the IKEv2 Always On type, the option is not available.

For version 26.4.0

Configuring app-to-VPN mapping for iOS and macOS devices

1. Per-app VPN requires two configurations in the same policy:
    - VPN
    - App to VPN Mapping
2. Within the VPN configuration, the option Per App and Account VPN has to be activated and depending on the VPN type, all necessary fields have to be filled in.
3. Within the App to VPN Mapping configuration, apps are assigned to a VPN configuration of the same policy. The configuration can be added once per policy. Via Add, the VPN configuration (Configuration) is selected first, followed by the Source of the app: Relution App Store app, Apple App Store App, iOS System or built-in app, App Compliance or Manually add app.
4. Once Per App and Account VPN is activated, the VPN configuration shows the Per account VPN section. There, Automatically connect to the VPN, if an associated app requests a network connection defines that the connection is established automatically when needed. In addition, Associated domains, Excluded domains, Safari domains and SMB domains can be specified. Under Select configurations, account configurations of the same policy can be assigned to the VPN; on macOS, these are email, CalDAV and CardDAV configurations.

The list of mappings shows in the columns Enabled and Per App VPN enabled whether the assigned VPN configuration is active and whether Per App and Account VPN is switched on there. The mapping only takes effect if both apply.

---

macOS specifics

In macOS policies, each assigned app additionally has the required fields Signing identifier and Designated requirement. When an app is added, Relution initially fills both fields with the bundle ID of the app; the values can be adjusted via Edit. The signing identifier is shown by `codesign -dv /Applications/Safari.app` in the `Identifier` line, the designated requirement by `codesign -d --requirements - /Applications/Safari.app`.

Calendar (CalDAV)

The Calendar configuration also hands a CalDAV account to the native Calendar app on macOS devices via a configuration profile. The configuration fields and the server-side requirement — automatic discovery according to RFC 6764 through a redirect at `/.well-known/caldav` — are identical to iOS.

Configuration and server-side requirement

The full description of the configuration fields, of automatic discovery via `/.well-known` and of the server-side setup of the redirect including troubleshooting is documented in the iOS article and applies to macOS unchanged:

- Calendar (CalDAV) for iOS →

Note in particular that the redirect must point to an `https://` address without an internal port, and that the Principal URL — if set — has to be given as a plain path.

---

macOS specifics

On macOS, Relution delivers the configuration via the user channel. The CalDAV account is therefore installed in the profile of the logged-in user and not device-wide. If the device does not support a user channel, the configuration is delivered via the device channel.

The configuration is also available for Macs with User Enrollment →.

For version 26.4.0

Apple Configurator 2 Configuration

This policy configuration can be used to transfer `.mobileconfig` files to Apple devices. Such a file can contain, for example, a Wi-Fi connection together with the matching identity certificate (PKCS#12, `.p12`).

Configuration

In the portal, the configuration is called Apple Configurator 2 configuration. The Name field sets a name for the configuration. The file is uploaded via Select .mobileconfig file. Its content then replaces the file selection in the Payload content field, where it can be edited. The content must be valid XML. Signed profiles are not readable XML and therefore cannot be used, so the file is saved without a signature in Apple Configurator 2. If the Payload content field is cleared, a file can be selected again.

User, device and certificate placeholders can be used in the Payload content field. The available placeholders are listed below the form and are replaced when the configuration is transferred to the device, see Advanced placeholders →.

Several Apple Configurator 2 configurations can be created per policy. This allows multiple configuration types to be split across separate configurations.

> On macOS, the portal points out that this configuration should only be used if the file does not contain any of the following configuration types: CardDAV, CalDAV, LDAP, Exchange, email and Web Clip. Relution provides separate configurations for these types.

For version 26.4.0

File requirements

The content is validated when the configuration is saved. The file must meet the following conditions:

- The top level contains the keys `PayloadType`, `PayloadVersion` (as a number), `PayloadIdentifier`, `PayloadUUID` and `PayloadDisplayName`.
- `PayloadContent` contains exactly one configuration type. Certificate payloads may be included in addition.

Files that cannot be read, that lack one of these keys, or that contain no payload or several configuration types are rejected when saving.

> Only certificates in PKCS#12 format (`com.apple.security.pkcs12`) are transferred along with the configuration. PKCS#1 certificates (`com.apple.security.pkcs1`) pass validation but are not transferred to the device. Other certificates such as root certificates (`com.apple.security.root`) count as a separate configuration type. Combined with another configuration, they cause an error when saving and are therefore stored in a configuration of their own.
>
> The actual configuration must be the first entry in `PayloadContent`. If the file contains several payloads of the same type, only the first one is transferred to the device.

If the file contains a configuration type that Relution also offers as a separate configuration allowed only once per policy, that configuration can no longer be added to the same policy. Conversely, such a file is rejected when saving if the policy already contains the corresponding configuration or another active Apple Configurator 2 configuration with the same payload type.

Affected payload types on macOS

Example

The following file transfers a Wi-Fi connection (`com.apple.wifi.managed`). SSID, password, identifiers and UUIDs are sample values and are replaced with actual values. Each `PayloadUUID` must be unique.

For version 26.4.0

```
<?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>Wi-Fi-password</string>
   <key>PayloadDisplayName</key>
   <string>Wi-Fi</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>Company-WiFi</string>
  </dict>
 </array>
 <key>PayloadDescription</key>
 <string>Wi-Fi configuration for Apple devices</string>
 <key>PayloadDisplayName</key>
 <string>Wi-Fi</string>
 <key>PayloadIdentifier</key>
 <string>com.example.wifi</string>
 <key>PayloadOrganization</key>
 <string>Example Inc.</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 Configuration

It is possible to pre-configure some apps with the policy configuration Managed App. This configuration is only available for iOS devices from version 7 and macOS devices from version 11+.

Configuration

The configuration contains the bundle ID of the app to be configured in the Bundle Identifier field and a valid app configuration payload in the Payload field. The bundle ID is taken from a selection dialog: from the apps stored in Relution, from the Apple App Store or by manual entry. The Payload field is prefilled with an empty plist skeleton. Invalid XML is marked as an error, and the configuration cannot be saved. A policy can contain several Managed App configurations, for example for different apps.

In the payload, the placeholders displayed at the bottom of the page can be used. For example, an email client app can be configured by using the placeholder `${user.email}`. This way, it is possible to make the configuration usable for different users. The placeholders are filled in when the configuration is pushed to the devices. Unknown or misspelled placeholders are replaced with an empty value without an error message.

> The app to be configured must be installed on the devices for the app configuration to be applied. If Relution installs the app – from the App Store, via Apps and Books (VPP in the portal) or as an enterprise app – and a policy with a Managed App configuration for the same bundle ID has already been applied on the device, Relution sends the configuration together with the installation command. The order of configurations in the policy has no influence on this.

For version 26.4.0

Basically, the manufacturer of each app is responsible for the configuration options. The following examples worked with the respective apps at the time of writing. There is no guarantee that this will continue to be the case.

Microsoft Outlook for 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>
```

For versi

Microsoft Outlook for an 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>
```

For versi

SecurePIM for 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>
```

For version 26.

Configuration incomplete

When an existing configuration is exported from another MDM system as XML and then converted into a `plist` file, a value that was marked as optional and left empty can turn into an empty `<string></string>` value in the `plist`. The key `subscriptionWebServiceEndPointURL` is affected by this, among others.

In this case, SecurePIM shows the persistent message “Configuration incomplete” on app start, even though the key worked without a value in the original system. Entering any non-empty value for the affected key, or removing the key from the `plist` entirely, resolves the issue.

FileBrowser for Education

```
com.stratospherix.filebrowsereducation
```

Configuration of an 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>
```

For versi

IBM Verse client

```
com.ibm.lotus.traveler
```

Show full configuration example

Web Content Filter

The Web Content Filter configuration integrates the content filter of a third-party app on macOS devices (filter type Plugin), for example a filter app with a Network Extension. The filtering itself is performed by this app.

> Relution has no control over the filtered content. Which content is filtered is determined by the provider of the filter app.

macOS policies do not offer a Filter Type selection: the filter type is fixed to Plugin. The built-in filter (Built In) with Enable Auto-Filter, Blocked URLs, Permitted URLs and Allowed Bookmarks is only available in iOS policies, see Web content filter on iOS →. A web filter built into macOS with deny and allow lists is provided by the macOS configuration Parental Controls in the Web content filter section.

Prerequisites

- The device is supervised (badge Supervised) and enrolled via device enrollment; the configuration is not available for user enrollments.
- The provider's filter app is installed on the device.

For version 26.4.0

Configuration

Under `Devices` → `Policies`, the Web Content Filter configuration is added to a macOS policy via Add. A policy can contain several of these configurations; they are distinguished by their User Defined Name.

Field	Description
User Defined Name	Required. Name of the filter
Plugin Bundle ID	Required. Bundle ID of the app that contains the filter provider
Service Address	Optional. Address of the filter service, e.g. host name or URL
Username	Optional. User name for signing in to the filter service
Password	Optional. Password for signing in to the filter service; only allowed together with a Username
Payload Certificate	Optional. Certificate (PKCS#1 or PKCS#12) from certificate management for signing in to the filter service
Traffic Filter Type	Socket (default) filters network traffic at socket level, WebKit filters traffic from WebKit browsers; exactly one option is active

Enforce Safari history retention

The Enforce Safari history retention toggle applies to macOS 26 and later and is enabled by default. When enabled, the Safari history cannot be cleared on the device and Private Browsing is disabled. When disabled, the history can still be cleared.

For version 26.4.0

Relution Decon (content filter)

Starting with version 26.5, Relution enables the setup of a DNS-based content filter for macOS devices. This feature ensures a secure and focused internet experience by restricting access to selected websites and apps. With AI-powered content categorization, Relution Decon also provides a comprehensive parental control filter with advanced configuration options.

What is Relution Decon?

Relution Decon is an AI-powered add-on for macOS that filters content in real-time, creating a safe digital environment. Using DNS-based content control, Decon blocks unwanted websites and apps, allowing users to work and learn in a protected, distraction-free space.

Relution Decon uses a DNS proxy to forward all requests to the Decon server. Websites are classified and either allowed or blocked according to policy rules. All data transfers are SSL-encrypted, ensuring user activities remain secure.

Decon App

For version 26.4.0

The Decon app is automatically deployed on macOS devices when the policy is installed. It monitors device DNS requests and ensures that only approved content is accessible.

App features:

- Activates a system-wide DNS proxy, which cannot be disabled by the user
- Displays the current status of Relution Decon
- Provides insight into blocked websites and applied filter categories

> Recommended: provide a sufficient number of licenses for the app via Apps and Books (VPP in the portal) before distribution.

Set up Apps and Books (VPP) in Relution →
Relution Decon in the Apple App Store →

Decon Policy

In the device policy, the configuration is added via `Add` → `Relution Decon`. This policy automatically installs the Decon app on the devices, where it acts as a proxy for all DNS requests. Unlike on iOS, macOS additionally requires a Managed App Configuration → and the approval of the system extension — Relution sets up both automatically.

Policy configuration is completed upon publishing.

On macOS, Relution Decon is only available for devices with device enrollment. With User Enrollment →, the configuration cannot be added.

A license that includes Relution Decon is required. Without it, the configuration shows a notice and cannot be saved.

> If the policies applied to a device already contain a **DNS Proxy** configuration, Relution does not set the DNS proxy for Decon. The device then receives the compliance notice **Cannot set DNS Proxy for Decon since configuration type already exists**.

Policy configuration hierarchy (highest to lowest priority)

1. Allowed apps
2. Blocked apps
3. Permitted domains
4. Blocked domains
5. Blocked categories

Decon in Relution Teacher

On macOS devices, Decon can be selected and managed in class profiles starting with Relution Server 26.5. Prerequisite: the student devices have a Decon policy assigned. Relution Teacher only shows a notice about a missing Decon configuration for iOS devices, not for macOS devices.

More about Relution Teacher →

Note: If Decon is enabled in the class profile, the otherwise valid Decon configuration is completely overwritten for the duration of the lesson. Permitted or blocked domains from the Relution Decon requests do not apply during this time.

For version 26.4.0

Filtering

In the Filtering section of the Decon policy, Filter Type determines how websites are filtered:

- Off: No filtering by categories or age level.
- Categories (default): The categories to be blocked are selected individually via toggles. The toggles are only shown for this filter type. Adult content, Advertising and Phishing are blocked by default.
- Age level: Filtering is based on an age level (0+, 6+, 12+ or 16+, default 12+).

Two further toggles are available regardless of the filter type:

- BPJM list: Additionally filters content classified as inadmissible by the BPjM. Entries under Permitted domains can still enable access to such content.
- Safe search: Set independently of the blocked categories and the age level. Blocking the Adult content category does not enable safe search.

If several Decon configurations are used on one device, the strongest filtering automatically takes effect: age-based filters take precedence over category-based filters. Configurations without filtering are ignored.

Category Classification

Relution Decon automatically assigns each website to a category. With the filter type Categories, administrators can define which categories are blocked:

Category	Description	Examples
Adult content	Sites inappropriate for youth	Pornography, Violence, Weapons, Drugs, Gambling, Adult Entertainment, Adult Shopping, Dating
Advertising	Advertising websites	Ad providers
Social media	Social media content	Facebook, Instagram, TikTok, etc.
Entertainment	Entertainment websites like streaming or games	Movies, Games, Videos
Music	Music streaming services	Spotify, Tidal, etc.
News	News and magazines	News, Weather
Shopping	Online shops (excluding adult content)	Amazon, eBay, etc.
Education	Learning websites	Wikipedia, Google Scholar
Generative AI	AI-specific websites	ChatGPT, Perplexity.ai, etc.
Phishing	Potential phishing websites	Potential scams, Data theft
Miscellaneous	Everything else	Remaining sites

Permitted and Blocked Apps and Domains

- Allowed apps / Blocked apps (Apps section): Internet access of individual apps is allowed or blocked specifically, while basic functions remain available.
- Permitted domains / Blocked domains (Domains section): Specific domains can be allowed or blocked independently of categories. Only the domain should be specified, not the path. Permitted domains remain accessible even if the filter deems them inappropriate. The number of blocked domains should be limited to about 500.

Regardless of these lists, the Relution server URL, the Decon server and the Relution apps (Relution Agent, Teacher, Files, Assets and Decon) are always allowed. In addition, Relution adds the domains allowed and blocked organization-wide under `Settings` → `Relution Decon requests` to every Decon configuration.

Advanced DNS Configuration

DNS servers on the device: Alternative DNS servers can be configured if the Relution Decon DNS is unavailable. Fallback: Cloudflare Families DNS (1.1.1.3).

DNS servers on the Relution Decon server: An alternative DNS server can replace the standard DNS on the Decon server. IP addresses (UDP) or DNS-over-HTTPS (DoH) such as Zero or Quad9 can be used.

Limitations

- Caching: Blocks and policy changes can take up to 1 minute to take effect.
- Path independence: DNS operates at domain level, subpages are not distinguished.
- App blocking: Only internet access is blocked, basic functions and cached content remain available.

AirPrint

The AirPrint policy configuration also provides AirPrint-capable printers to macOS devices via a configuration profile. The printers defined there are then available in the print dialog without having to be discovered on the local network via Bonjour — for example when the Mac and the printer are located in different subnets or VLANs.

For version 26.4.0

Configuration

The configuration is created under `Devices` → `Policies` in a macOS policy via Add Configuration → AirPrint. The fields Host Name or IP Address, Port, Resource Path and Use TLS, as well as the prerequisites and how to determine the resource path, are identical to iOS and are described in the iOS article:

- AirPrint for iOS →

Setup Assistant

The configuration Setup Assistant hides setup steps that macOS shows on a Mac that has already been set up, e.g. when another user signs in for the first time or after a software update. The configuration is not available for devices with User Enrollment (BYOD).

Difference from the DEP profile

The setup steps selected in the profile → of Automated Device Enrollment (ADE, DEP in the portal) only apply to the initial setup of the Mac. The configuration Setup Assistant, on the other hand, is installed on the enrolled device via a policy and affects setup steps that macOS shows afterwards.

The configuration is therefore not a prerequisite for enrollment. It is only needed if no additional setup steps should be shown after the initial setup either.

Settings

In the section General, each setup step can be set to be skipped:

- Skip accessibility
- Skip appearance
- Skip Cloud Setup (sign-in with the Apple Account)
- Skip iCloud storage setup
- Skip privacy setup
- Skip Siri setup
- Skip True Tone setup
- Skip screen time setup
- Skip Touch ID setup
- Skip unlock with watch
- Skip wallpaper

Apple has marked these individual settings as deprecated as of macOS 15. For newer macOS versions, Apple instead provides a list of setup steps to skip. Relution currently offers this list only in the iOS configuration.

Apple allows only one Setup Assistant configuration per device. A device should therefore not be assigned several policies with this configuration at the same time.

For version 26.4.0

Restrictions

The Restrictions policy configuration restricts or permits functions on managed macOS devices. The configuration corresponds to the Apple restrictions payload; which settings a device actually applies depends on the macOS version and on whether the device is managed in supervised mode.

The overview below follows the structure of the form in the portal. Many restrictions require a specific macOS version; the minimum version is shown as a hint on the restriction in the form (e.g. macOS 14+) and is stated in the overview. Restrictions marked Supervised only take effect on supervised devices, while restrictions marked Supports user enrollment also take effect on devices with user enrollment. Restrictions marked Deprecated have been deprecated by Apple; restrictions marked Deprecated on unsupervised devices are deprecated only on unsupervised devices.

> Relution sends every switch to the device with its current value. If a function is disabled, it is generally blocked on the device; options that enforce a behavior (such as “Force ⋯”) only take effect when they are enabled.

By default, all options are enabled except Force on device only dictation, the three Force delay of ⋯ visibility switches, Enable Siri profanity filter, Allow the presentation of a screen capture alert and the four Classroom restrictions. The age ratings are set to All, and the Allowed external integration workspace IDs list is empty. A new configuration therefore does not restrict any function unless it is adjusted.

The download icon at the top of the form (Export restrictions as CSV file) downloads the configured values, including unsaved changes, as a CSV file.

Of the Recommended restrictions for iOS/iPadOS →, only the notes on Erase All Content and Settings and on delaying operating system updates also apply to macOS.

For version 26.4.0

Device

The device restrictions are divided into three sections.

Device restrictions

Show all restrictions

Authentication Restrictions

Show all restrictions

Update Restrictions

> This section is marked Deprecated in the portal because Apple has deprecated these settings. For new policies, the Software Update → configuration is intended instead.

The fields for the delay in days can only be edited, and are only sent to the device, when the corresponding Force ⋯ switch is enabled. Values from 1 to 90 days are allowed.

Show all restrictions

Apps

The following restrictions apply to individual apps and services.

Apps restrictions

Show all restrictions

Relution does not offer Safari options for JavaScript, pop-ups or the fraud warning for macOS. Clearing the history, private browsing, content summarization and the start page for new tabs can additionally be controlled from macOS 26 using the Safari Settings → configuration.

For version 26.4.0

Settings

The following restrictions apply to the system settings of the device and to the Classroom app.

Settings restrictions

Show all restrictions

Classroom restrictions

Show all restrictions

Media

The following restrictions apply to media content. All options in this section require macOS 15 or later (macOS 15+).

Media restrictions

Show all restrictions

Modifications

These restrictions determine which settings may be modified on the device.

Modifications restrictions

Show all restrictions

iCloud

The following restrictions apply to the iCloud services on the device.

For version 26.4.0

iCloud restrictions

Show all restrictions

AI feature restrictions

These restrictions control the Apple Intelligence features.

> All restrictions in this section are marked Deprecated in the portal. For devices running macOS 26.4 or later, the Intelligence Settings → (Apple Intelligence report, Genmoji, Image Playground, writing tools) and External Intelligence Settings → (external intelligence integrations, sign-in, workspace ID) configurations are available instead. For devices running older macOS versions, the restrictions described here continue to apply.

General

Show all restrictions

Related topics

- Restrictions for iOS and iPadOS → — An overview of the settings for iOS and iPadOS.
- Software Update → — Successor to the update restrictions.
- Safari Settings → — Additional Safari options from macOS 26.
- Intelligence Settings → — Successor to the AI feature restrictions from macOS 26.4.
- External Intelligence Settings → — External intelligence services from macOS 26.4.

For version 26.4.0

MS Office Volume License 2024

How to license Microsoft Office LTSC 2024 on macOS devices using the VL Serializer in Relution.

To use Microsoft Office apps on macOS, they must be licensed using the `Microsoft_Office_LTSC_2024_VL_Serializer.pkg` package.

The challenge here is that the PKG changes its internal package name during installation. Since it is not a standard application, the usual procedure for native apps in Relution fails.

Therefore, additional steps are required to:

- Properly equip the devices with the PKG.
- Successfully license the Office apps.
- Maintain device compliance.

Preparing the VL Serializer

The required PKG can be downloaded from the Microsoft Admin Center →.

For version 26.4.0

Relution Configuration

1. The PKG is uploaded to the Relution App Store.
2. In the Detection rules section of the app, a rule of type Package Name is created via Add (the app cannot be saved without a detection rule), and the following value is entered in the Package name field so that Relution can correctly interpret the installation status:

```
com.microsoft.office.licensingV2.helper
```

Deploying the PKG

The PKG must be transferred to the endpoints. There are two ways to achieve this:

Manual Installation

The PKG is manually copied to the respective device and executed locally. However, this is not efficient for larger rollouts.

Automated Installation (Recommended)

- Deployment via a Relution script that is created under `Scripts` → `Scripts` and executed by the macOS Companion: once via the Execute shell script or Execute on device action, or on a schedule via the Script configuration of a macOS policy.
- Download of the file to `/Users/Shared/`.
- Subsequent silent installation via the terminal.

Download & Installation

This script downloads the serializer from an external source (e.g., a file server) and installs it directly.

```
#!/bin/bash

# Configuration
URL="https://your-share.com/link/to/file"
PKG="/Users/Shared/Microsoft_Office_LTSC_2024_VL_Serializer.pkg"

echo "Starting download..."
if ! curl -fL "$URL" -o "$PKG"; then
    echo "Error: Download failed."
    exit 1
fi

echo "Serializer found – starting installation..."
/usr/sbin/installer -pkg "$PKG" -target /

if [ $? -eq 0 ]; then
    echo "Installation completed successfully."
    rm "$PKG" # Optional: Delete installer after success
    exit 0
else
    echo "Error: Installation failed."
    exit 1
fi
```

Installing a Locally Available PKG

If the file has already been placed in the Shared folder, the following script can be used:

```
#!/bin/bash

PKG="/Users/Shared/Microsoft_Office_LTSC_2024_VL_Serializer.pkg"

if [ -f "$PKG" ]; then
    echo "Serializer found – starting installation..."

    sudo /usr/sbin/installer -pkg "$PKG" -target /

    if [ $? -eq 0 ]; then
        echo "Installation completed successfully."
        exit 0
    else
        echo "Error: Installation failed."
        exit 1
    fi
else
    echo "Error: PKG file not found at $PKG."
    exit 1
fi
```

For version 26.4.0

Distribution via App Compliance

Once the PKG is uploaded to Relution and the detection rule is stored, it can be managed via the App compliance configuration of a macOS policy:

1. In the configuration, the app is added under Required apps and the policy is published. If Auto install is enabled for the app, Relution installs the uploaded PKG itself on devices where the identifier is missing; the detection rule prevents repeated installations.
2. Relution uses the detection rule to check whether the identifier `com.microsoft.office.licensingV2.helper` is included in the device's list of installed apps (and, if version check is enabled, its version). Relution does not check whether Office is actually licensed.
3. Devices without this identifier are marked as Noncompliant, provided the option Add compliance violation when required apps are missing is enabled under `Settings` → `Device Management` → `Device Management` (default). The script can be run again on these devices.

Adobe Creative Cloud Apps

How to deploy Adobe apps (Creative Cloud) to macOS devices via Relution and keep them up to date with the Remote Update Manager.

Adobe apps cannot be installed like a classic native app through Relution. The reason: Adobe packages are not simple silent installers – during installation they start their own background processes (Creative Cloud Desktop / HyperDrive). These do not run reliably in the restricted context of the native MDM command – the PKG upload succeeds, but the installation hangs or fails.

The installation is therefore performed via a script (macOS Companion). Updates are managed centrally through the Remote Update Manager.

Why a script is needed

- Installation: `installer -pkg … -target /` runs in full root context, exactly as documented by Adobe. The signed-in user does not need administrator rights.
- No file push: The macOS Companion does not deliver a file. The PKG must therefore be obtained (downloaded) over the network.
- Updates: In the managed package, auto-update for end users is disabled. Updates are performed via a recurring update script that calls the Remote Update Manager (RUM).

For version 26.4.0

Create the package in the Admin Console

1. After signing in to the Adobe Admin Console →, the Packages area is opened.
2. A Managed Package is created, with all apps selected that are to be installed on the devices – multiple apps (e.g. Photoshop, Illustrator, Acrobat) are bundled into one PKG.
3. In the management options, Remote Update Manager (RUM) is enabled. This ships the RUM binary with the PKG to the devices, so it is available for updates later.
4. The finished package is then downloaded. The installer is located in the package folder under `Build/<PackageName>_Install.pkg`.

Note on splitting: If all users receive the same set of apps, one combined package is sufficient. If different groups need different apps, a separate package is created per app or bundle and assigned to the respective device group. The update script (see below) remains the same in both cases.

Deploying the PKG

Since the Companion does not deliver a file, the PKG must be hosted at a network-reachable location from which the script downloads it – e.g. an internal web server or cloud storage.

Important: A permanent storage location is required. The download link from the Adobe Admin Console is temporary and session-bound and is not suitable as a fixed source. The package is downloaded once and hosted on internal infrastructure. The file name must also contain no spaces.

Automation scripts

Prerequisite: The macOS Companion is switched on under `Settings` → `Relution Client Apps` via Enable macOS companion. The Companion is not deployed on devices running a macOS version lower than 12 or on user-enrolled devices; this procedure cannot be used there.

The rollout consists of a one-time initial installation and a recurring update. Both scripts are created under `Scripts` → `Scripts` via Add script as shell scripts for macOS and are executed on the device by the macOS Companion:

- Initial installation: The script is started once via the Execute shell script action on the device or device group, alternatively via Execute on device in the script list (see Overview of actions →).
- Update: In a macOS policy, the Script configuration is added and the update script is selected. In the Time based execution section, the weekdays (Repeats on) and the Start time are defined (see Overview of configurations →).

In addition to the log file on the device, the execution state as well as the result and error output of each run can be viewed in the history of the respective script under `Scripts` → `Scripts`.

Initial installation (recommended)

Adobe packages are often several gigabytes in size. A direct download within a Relution script can exceed the script timeout and is then aborted. The timeout is set on the script in the Timeout (in minutes) field (default 5, maximum 30 minutes). The following script avoids this: it installs a LaunchDaemon that performs the download, installation and first update run decoupled in the background. The Relution script itself finishes within seconds.

Per package, only `PKG_URL` and `APP_LABEL` need to be set.

For version 26.4.0

> Show full configuration example

The result is logged to `/var/log/relution_adobe_deploy.log`.

Ongoing updates

This script is assigned as a Script configuration in a macOS policy and is thus executed on a recurring basis (e.g. once a week). It requires no download – the Remote Update Manager fetches the updates directly from Adobe. Without specifying products, all installed Adobe apps are updated together; a separate script per app is not needed.

```
#!/bin/bash
RUM_BIN="/usr/local/bin/RemoteUpdateManager"
RUM_PRODUCTS=""   # empty = all apps; otherwise SAP codes, e.g. "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 "ERROR: RUM not found – is an Adobe app installed?"
    exit 2
fi

log "=== RUM update started ==="
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 finished (RC $?)."
```

SAP codes for updating individual apps: `APRO` (Acrobat), `PHSP` (Photoshop), `ILST` (Illustrator), `IDSN` (InDesign), `PPRO` (Premiere Pro), `AEFT` (After Effects).

For version 26.4.0

Alternative: Self-service

If users are to install their Adobe apps themselves instead of a central rollout, a Self-Service package is created in the Admin Console instead (alternatively, the options Enable self-service install and Allow non-admins to update and install apps are enabled in the package). The script then installs only the Creative Cloud Desktop app; users then select and install the actual apps themselves. This requires Named User Licensing with matching product profiles. A central update script is not needed, since updates run through the Desktop app.

> Show full configuration example

Note: If the package is very large and the direct download runs into the script timeout, the decoupled LaunchDaemon variant from Initial installation is the better choice: `PKG_URL` is set to the Creative Cloud Desktop app package and the RUM step is omitted.

Status monitoring via App Compliance

In this setup, installation is performed via the script – no PKG is uploaded to Relution. The App compliance configuration of a macOS policy therefore does not serve distribution but status monitoring: the app is created via Manually add app, and the bundle ID is entered in the Internal name field.

1. In the App compliance configuration, the source Manually add app is selected under Required apps via Add (without PKG upload).
2. A Name is assigned and the bundle ID is entered in the Internal name field, e.g. `com.adobe.acc.AdobeCreativeCloud`.
3. Relution regularly checks whether this bundle ID is included in the device's list of installed apps.
4. Devices without the app are flagged as Noncompliant, provided the option Add compliance violation when required apps are missing is enabled under `Settings` → `Device Management` → `Device Management` (default). The installation script can then be run (again) on those devices.

App-specific detection (e.g. Photoshop only): Relution checks every stored bundle ID against the device's list of installed apps. For an app-specific check, the bundle ID of the individual app is therefore stored instead of `com.adobe.acc.AdobeCreativeCloud` (via Manually add app). The bundle ID can be looked up in the list of installed apps of a device on which the app is already installed. This requires macOS to report the app in that list.

Notes

- Licensing (Named User Licensing): After installation, the user signs in with their Adobe ID on first launch. Each app requires a matching product profile in the Admin Console – without an entitlement the app is installed but not usable.
- Major upgrades: The Remote Update Manager only updates within the installed major version (base and security updates). Moving to a new yearly generation requires a new package.
- Education environments: For Adobe education customers, auto-update for end users is not available; management via the Remote Update Manager is the intended path here.
- Spotlight: The initial installation script indexes installed apps via `mdimport` so they are immediately findable through Spotlight search – not only in Finder.

For version 26.4.0

Platform SSO (PSSO)

With Relution, macOS devices can be configured so that users sign in with their Microsoft Entra ID account directly at the login window (Platform Single Sign-On). On the first sign-in, a local user account is created that is linked to the Entra ID identity.

Prerequisites

- macOS 13 (Ventura) or later for Extensible SSO, macOS 15 (Sequoia) or later for the login, unlock and FileVault policies, the grace periods and non-Platform SSO accounts, macOS 26 (Tahoe) for Setup Assistant registration and authenticated guest mode. Microsoft recommends at least macOS 14 (Sonoma).
- A Mac with Apple Silicon if the recommended *Secure Enclave Key* method is used (see Choosing the authentication method →). On Intel Macs, only the *Password* method is available.
- A Microsoft Entra ID tenant
- Permission to register devices in Microsoft Entra ID for the users
- Microsoft Company Portal for Mac must be available as an app and installed *before* users are targeted for PSSO. For registration during the Setup Assistant (macOS 26+), version 5.2604.0 (April 2026) is required. The latest version is always recommended — it meets both requirements.
- Network access to the Microsoft/Apple sign-in URLs (see General section →). These URLs must be reachable and excluded from any TLS inspection, otherwise registration fails.

Platform SSO itself does not require Relution to be connected to Microsoft Entra ID; the configuration works without this connection. The connection is only needed if users are also to be synchronized from Entra ID or if Conditional Access → is used: Connect Relution with Entra ID →. Conditional Access additionally requires OIDC →.

For version 26.4.0

Preparation in Microsoft Entra ID

Before the configuration is rolled out in Relution, the following points should be checked in the Microsoft Entra admin center:

- Device settings: Under `Identity` → `Devices` → `Device settings`, Users may join devices to Microsoft Entra ID must be set to All (or to the relevant target group).
- Multi-factor authentication: If classic per-user MFA is enabled on the account, PSSO registration can fail. Conditional Access should be used for the MFA requirement instead.
- Password complexity: For the *Password* method, the complexity requirements of the local account and Entra ID must match so that synchronization works.

Upload the Company Portal app

1. The latest version of Microsoft Company Portal for Mac (.pkg) is downloaded from Microsoft → and then uploaded to Relution under `Apps` → `App Store` via Add as a Native app (see Native apps for macOS →).
2. The app must be released to the target group or organization.

The Company Portal app contains the SSO extension `com.microsoft.CompanyPortalMac.ssoextension`, which is required for Platform SSO. It must be at least version 5.2404.0 (for Setup Assistant registration on macOS 26+: 5.2604.0).

Note on version numbers: Company Portal reports two version strings. The *"About this app"* version follows the scheme `5.YYMM.x` (e.g. `5.2604.0` = April 2026), while the build number visible in the package or via `pkgutil` looks different — e.g. `4.83.26040910`, where `260409` is the build date (2026-04-09). Both refer to the same release; a build from 2026 easily meets the PSSO requirement.

Assign the device group and configurations

1. A device group is created for the Mac devices on which PSSO is to be rolled out.
2. In the device group's Policies section, a macOS policy containing the following two configurations is assigned via Add (one combined policy or two separate ones):
   - Extensible Single Sign-On (see Configuring the Extensible Single Sign-On policy →)
   - App compliance: Under Required apps, the uploaded Company Portal app is added via Add. If the checkbox in the Auto install column is selected (the default when adding an app), Relution installs the app automatically. Without auto install, the device is merely reported as non-compliant if the app is missing.
3. The configurations only reach the devices once the policy has been published.

Without the Company Portal app installed, the SSO extension cannot register. Relution deploys the SSO profile independently of the app installation; no order between the two is enforced.

For version 26.4.0

Choosing the authentication method

The authentication method determines how users sign in to the device and to apps. It is the most important decision during setup and is set in the Platform SSO section → of the configuration.

Method	Passwordless	Local password	Min. macOS	Suitable for
Secure Enclave Key *(recommended)*	Yes, phishing-resistant	remains unchanged	13 / 14	Personalized devices, Apple Silicon only
Password	No	synchronized with Entra ID	13 / 14	Intel Macs, shared/lab devices
Smart card	Yes (via CBA)	remains unchanged	14+	Organizations with physical smart cards

Recommendation: For personalized company Macs (Apple Silicon), the Secure Enclave Key method is recommended — it is passwordless, hardware-bound, and meets phishing-resistant MFA. For Intel devices or shared devices, Password is the appropriate choice.

Smart card is not supported during the Setup Assistant.

Registration during the Setup Assistant (macOS 26+): If PSSO is registered already during the Setup Assistant (Enable registration during Setup Assistant set to ON), then Enable creating first user during Setup Assistant must also be ON — regardless of the selected method. Otherwise no local account is created during setup and registration fails (verified in practice):

- *Secure Enclave Key* method: sign-in ends up in a login loop.
- *Password* method: the message “Sign-in not possible – Registration failed” appears.

With the toggle set to ON, the first local account is created via PSSO and sign-in completes in both cases.

Configuring the Extensible Single Sign-On policy

In a macOS policy, the Extensible Single Sign-On configuration is added.

For version 26.4.0

General section

Parameter	Value
Extension Identifier	`com.microsoft.CompanyPortalMac.ssoextension`
Denied bundle identifiers	leave empty (default)
Extension data → `AppPrefixAllowList`	`com.microsoft.,com.apple.`
Extension data → `browser_sso_interaction_enabled`	`1`
Extension data → `disable_explicit_app_prompt`	`1`
Realm	leave empty
Registration token	leave empty (not required for Entra ID – see note)
Screen locked behavior	Do not handle (default: Cancel)
Team Identifier	`UBF8T346G9` (Microsoft Team ID)
Type	Redirect (default: Credentials)
URLs	`https://login.microsoftonline.com` `https://login.microsoft.com` `https://sts.windows.net`

Required fields are Extension Identifier, Team Identifier and, for the Redirect type, URLs. With the Credentials type, the Hosts field appears instead of URLs.

> Registration token: For Microsoft Entra ID, no registration token is needed in the Extensible SSO payload; the field remains empty. (The field is intended for other IdP/Kerberos scenarios.)

> URLs / TLS: The three sign-in URLs must be reachable on the network and excluded from TLS inspection.

Platform SSO section

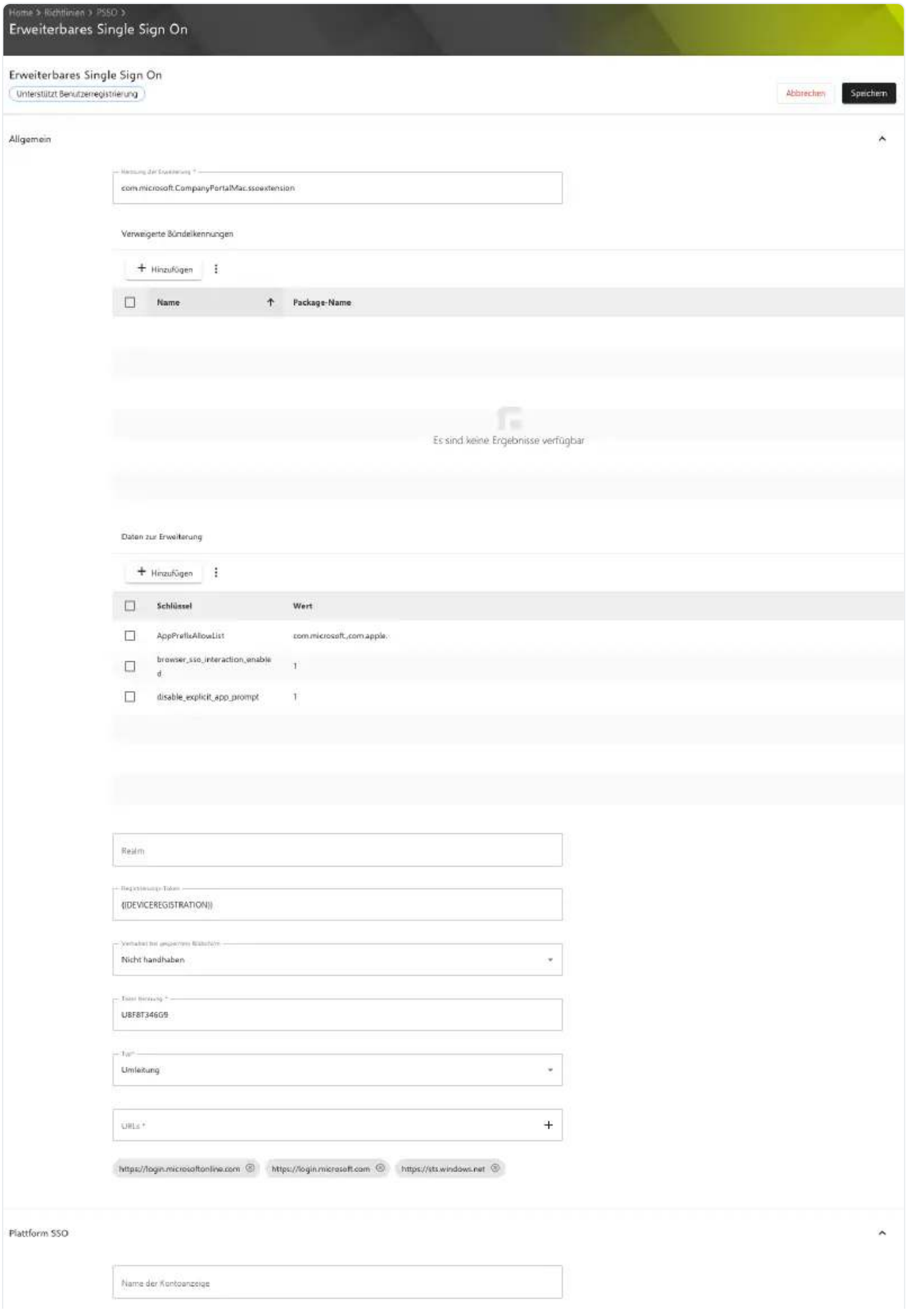
Parameter	Value	Note
Account display name	leave empty	optional
Authentication Method	User Secure Enclave Key	Recommended; for Intel/shared devices: *Password* (default for new configurations)
├── Login policy	– (not applicable)	only visible with the *Password* method; macOS 15+
├── Unlock policy	– (not applicable)	only visible with the *Password* method; macOS 15+
├── FileVault policy	– (not applicable)	only visible with the *Password* method; macOS 15+
├── Offline grace period	– (not applicable)	only visible with the *Password* method; macOS 15+
└── Authentication grace period	– (not applicable)	only visible with the *Password* method; macOS 15+
Non platform SSO accounts	not set	macOS 15+
Login frequency	`64800` (seconds, equals 18 hrs)	Re-auth interval; default `64800`, minimum `3600`
Use shared device keys	ON	Required for JIT account creation, see Shared device keys and account creation →; default: OFF
├── Enable Authorization	ON	
└── Enable create user at login	ON	Just-in-time provisioning of the local account
Additional groups	not set	optional
Administrator groups	not set	optional
Authorization groups	not set	optional
New user authorization mode	Standard	
User authorization mode	Standard	
Allow device identifiers in attestation	OFF	macOS 15.4+
Enable creating first user during Setup Assistant	ON (default)	macOS 26+ — required when registering during the Setup Assistant (otherwise registration fails)

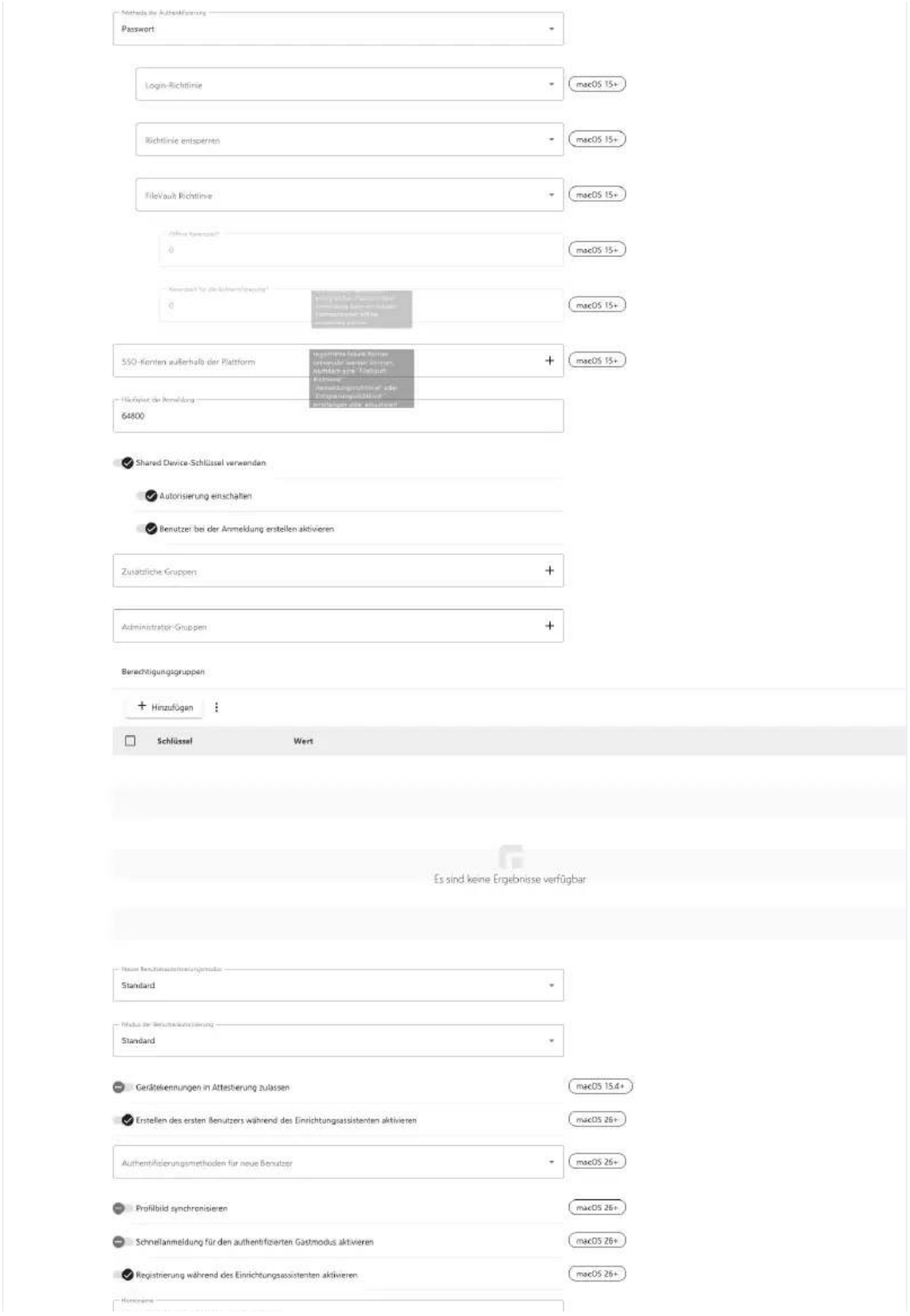
Parameter	Value	Note
New user authentication methods	not set	macOS 26+; options Password, Smart card and Access Key. With Access Key, additional fields appear for the reader group identifier, terminal identity, issuer certificate and express mode
Synchronize profile picture	OFF	macOS 26+
Enable quick login for Authenticated Guest Mode	OFF	macOS 26+
Enable registration during Setup Assistant	ON	macOS 26+
Account name	`com.apple.PlatformSSO.AccountShortName`	Placeholder for the local short name
Full name	`name`	Placeholder for the full name

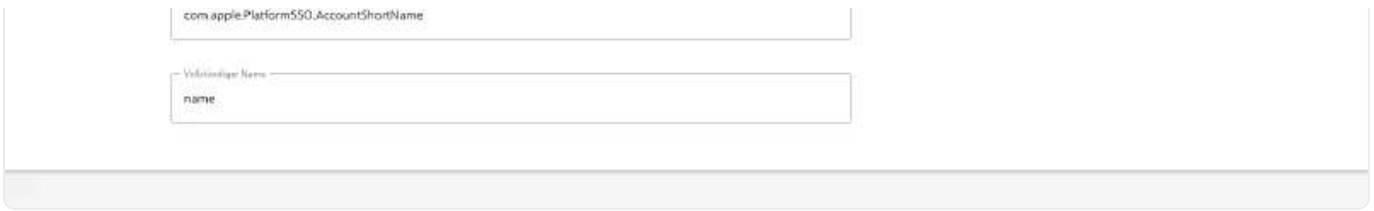
With the Password method, the portal additionally shows Login policy, Unlock policy and FileVault policy. Each of these policies offers the options Attempt authentication, Require authentication, Allow offline grace period and Allow authentication grace period; Unlock policy additionally offers Allow Touch ID or watch for unlock. The Offline grace period and Authentication grace period fields (prefilled with `0`) can only be edited once the corresponding option Allow offline grace period or Allow authentication grace period is selected in at least one of the three policies. With the Smart card and User Secure Enclave Key methods, these fields are neither shown nor transferred.

For version 26.4.0

> The fields marked macOS 26+ only take effect on devices running macOS Tahoe 26 or later and require that registration already occurs during the Setup Assistant.


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


Passwort
Login-Richtlinie
macOS 15+
Richtlinie entsperren
macOS 15+
FileVault Richtlinie
macOS 15+
macOS 15+
macOS 15+
SSO-Konten außerhalb der Plattform
macOS 15+
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
Standard
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+



The screenshot shows the *Password* method as an example. With *User Secure Enclave Key* (recommended, see table), the portal hides Login policy, Unlock policy, FileVault policy and both grace periods; the rest of the configuration is identical.

Further configuration

- A policy assigned to the device group must additionally contain the App compliance configuration for Company Portal (see Assign the device group and configurations →), so the extension is already available at the time of registration.
- For Automated Device Enrollment (ADE, DEP in the portal), it is advisable to assign the device group containing the PSSO configurations already in the auto enrollment (`Devices` → `Auto Enrollments` , in the device's entry section Device Groups → Static device groups), so registration can take effect during the Setup Assistant (macOS 26+).

Shared device keys and account creation

Use shared device keys must be ON, because in this flow the local accounts are provisioned via just-in-time provisioning (the Enable Authorization and Enable create user at login toggles). Without shared device keys, user-bound keys would be needed — but those cannot be generated while the user account does not yet exist (chicken-and-egg problem).

> Enable Authorization and Enable create user at login can only be changed while Use shared device keys is ON. If it is OFF, both are greyed out and not applied, even if they are still shown as ON. No account is then created at sign-in.

For version 26.4.0

Choosing the method by device type:

- Personalized device (recommended): *Secure Enclave Key* method — passwordless, hardware-bound, Touch ID.
- Shared / multi-user device (e.g. classroom, shift work): *Password* method, since changing users get by without pre-configured passwordless credentials. Such devices are registered without user affinity; Conditional Access is not supported on shared Macs.

Approving background items for Microsoft AutoUpdate

As of macOS Ventura, background processes such as Microsoft AutoUpdate (MAU) are blocked by default, or users receive a "Background item added" notification and have to confirm it manually. Without this approval, MAU cannot update automatically in the background — this also affects Company Portal, since its updates run through MAU.

Background items can be approved in advance with a profile containing the `com.apple.servicemanagement` payload (managed login items), for example with a rule for Microsoft's team ID (`UBF8T346G9`). Relution has no dedicated configuration for this payload; such a profile can, however, be distributed as a `.mobileconfig` file via the Apple Configurator 2 configuration (see Apple Configurator 2 Configuration →).

The Relution Login Items configuration is not suitable for this: it defines which apps are launched automatically at login, but does not approve background items.

Without this approval, users repeatedly get system notifications about new background items, and MAU may not reliably update the SSO-relevant components automatically.

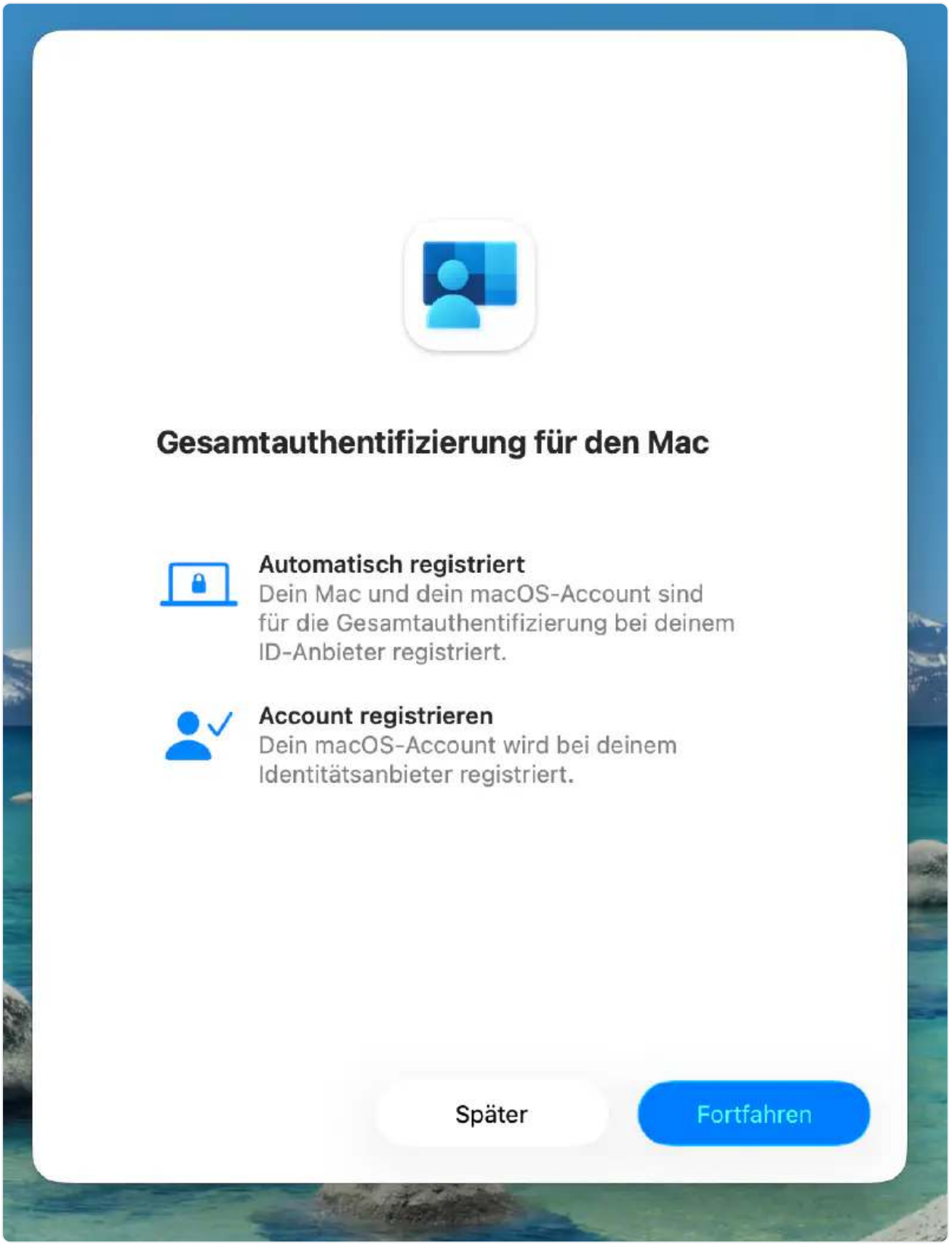
Registration by end users

Once the configuration has arrived on the device and the Company Portal app is installed, the initial registration proceeds as follows:

For version 26.4.0

1. A “Registration Required” notification appears on the device. Alternatively, it can be triggered from System Settings.

2. Right after the first sign-in, the “Single Sign-On for Mac” dialog opens with the “Register account” item. Registration continues via Continue (it appears equally for the *Password* and *Secure Enclave Key* methods).



3. Users sign in with their Microsoft Entra ID account and confirm MFA if required (e.g. via Microsoft Authenticator).

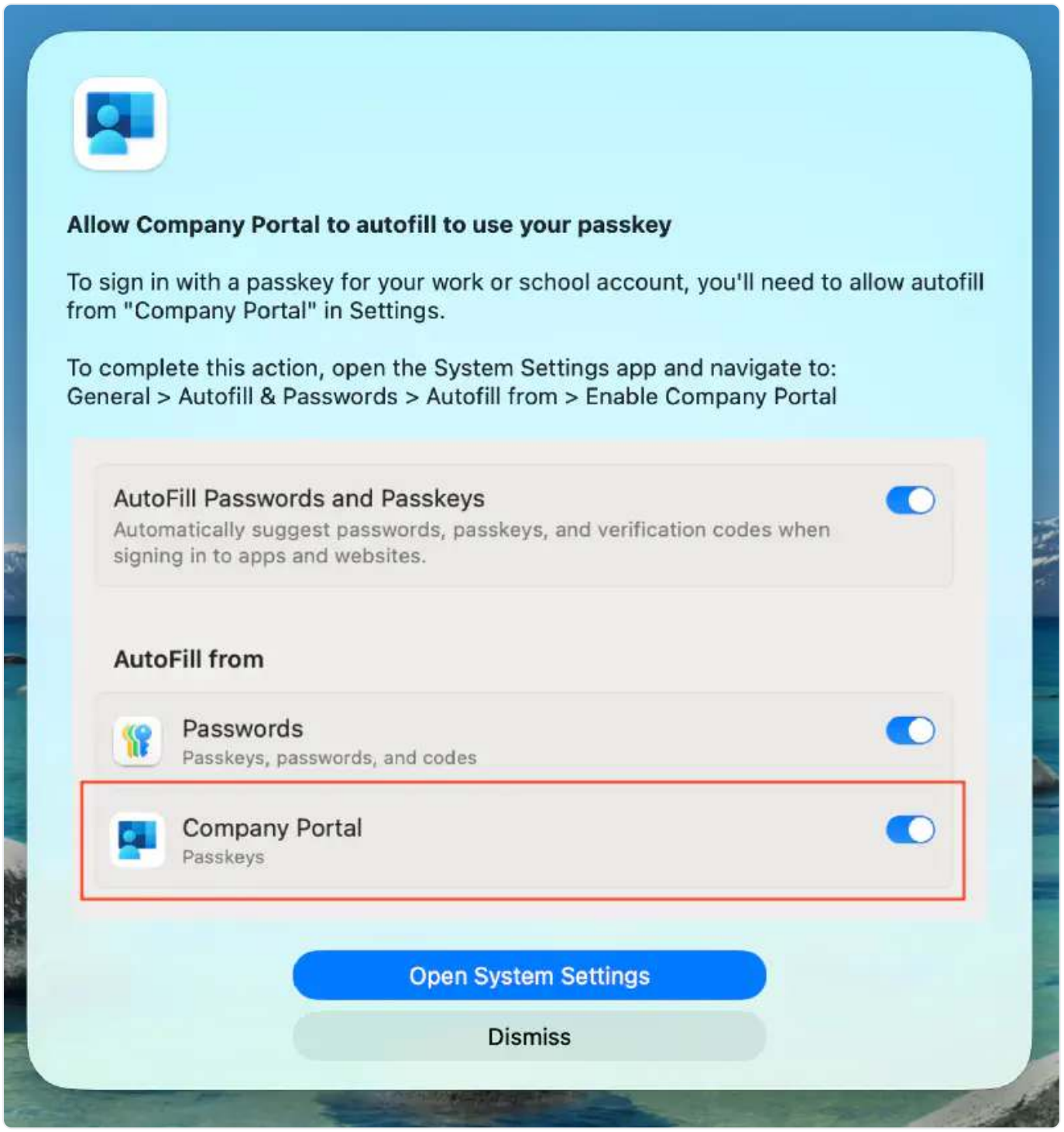
4. The local user account is linked to the Entra ID identity. From now on, single sign-on applies for apps and browsers that use Entra ID.

Allowing passkey autofill for Company Portal

After the first sign-in, a prompt “Allow Company Portal to autofill to use your passkey” appears. For passkey sign-in to work (Platform Credential, especially with the *Secure Enclave Key* method), users must enable autofill for Company Portal once:

1. System Settings are opened via Open System Settings (or manually).
2. There, `General` → `AutoFill & Passwords` is opened.
3. Under AutoFill from, the toggle for Company Portal is enabled.

For version 26.4.0



Without this approval, Company Portal cannot offer the passkey for sign-in; passwordless sign-in then fails or the prompt reappears repeatedly.

With the *Secure Enclave Key* method, the local password remains unchanged; after a reboot, the local password is first required to unlock FileVault, after which Touch ID can be used.

Verification

Registration success can be checked as follows:

- On the device (Terminal): `app-sso platform -s` shows the registration status of the Platform SSO extension.
- In Microsoft Entra: Under *Devices*, the device appears as registered/joined.
- Company Portal: The device status is shown as compliant/registered.

Possible errors

- Registration prompt does not appear → it should be checked whether Company Portal (version 5.2404.0+) is installed and the app compliance has already been evaluated.
- Sign-in fails → the Team Identifier, Extension Identifier, and URLs should be checked for typos; the URLs must be excluded from TLS inspection.
- Registration aborts at MFA → classic per-user MFA is disabled on the account and Conditional Access is used instead.
- Secure Enclave not available → affects Intel Macs; the *Password* method is used there.
- Login loop or “Sign-in not possible – Registration failed” → when registering during the Setup Assistant (macOS 26+), Enable creating first user during Setup Assistant must be ON — regardless of the method. If the toggle is OFF, no local account is created: with Secure Enclave a login loop occurs, with Password the “Registration failed” message.

For further known issues and diagnostics, see: Microsoft documentation →

For version 26.4.0

SFTP Upload

Relution can be used to create Managed Apple Accounts (Managed Apple IDs in the portal) in large numbers.
This is possible via the Relution Portal in the settings and makes it easier for schools and school authorities to automatically configure these accounts so that they can be made available to students and teachers.
This process also automatically migrates classes created in Relution to classes in Apple School Manager.

Requirements

- Port 22 outbound to the Apple servers allowed, especially for the URL: `upload.appleschoolcontent.com`
- An Apple School Manager
- An Education or Free license in Relution
- Read and update permission for Apple School Manager SFTP upload in the administrator's role (without update permission, the setup wizard cannot be completed)
- At least one verified domain in Apple School Manager (reserve addresses from Apple are not possible)
- A class in Relution with at least one teacher and one student user
- The teachers must be part of the `Teacher` system group, and the students must be part of the `Student` system group

For version 26.4.0

Configuration

- The Relution portal and Apple School Manager are opened.
- In Relution, the following item is opened: `Settings` → `Education` → `Apple School Manager SFTP upload`
- The setup wizard is continued until the server URL, user, and password are entered.
- In Apple School Manager, the following item is opened: the own `User` in the bottom left corner → `Settings` → `Managed Apple Accounts` → `Start the first steps of linking directory synchronization`.
- Create new accounts is clicked.
- Use CSV file in Apple format is clicked.
- Step 1: Set up SFTP
- The values are copied into the fields in Relution, then Next is clicked.
- The verified domain from Apple School Manager is entered in the Managed Apple ID domain field.
- Clicking Save Settings saves the settings and automatically starts the first SFTP upload.
- Next is clicked in Apple School Manager and the import is awaited.

The accounts are now displayed and can be checked for errors here.

In Apple School Manager, the same verified domain and the user name format `FirstName.LastName` are configured under Create Accounts and Classes for both instructors and students (e.g. `John.Doe@school.com`). For users that do not yet have a Managed Apple Account, Relution stores the address in exactly this format (`FirstName.LastName@<domain>`) on the user. If a different format is configured in Apple School Manager, the accounts created there will not match the addresses stored in Relution.

Upload and scope

After the setup, Relution uploads the data to Apple School Manager automatically once a day by default. In addition, an upload can be triggered manually under `Settings` → `Education` → `Apple School Manager SFTP upload` via Start upload. Apple School Manager sends an email once the import is complete.

The following is transferred:

- all members of the `Teacher` system group as instructors and all members of the `Student` system group as students, even if they belong to the group only via a subgroup; a user in both groups is transferred as an instructor only
- the organization's classes with the instructors and students assigned directly or via groups

On the same page, Password policy for students defines which password policy the students' Managed Apple Accounts receive:

- Use location default: New accounts use the default password policy of the location in Apple School Manager; existing accounts keep their current policy.
- Set 8-digit policy (Standard), Set 6-digit policy or Set 4-digit policy: New and existing accounts are switched to the respective policy.

Location

The SFTP upload creates a new location in Apple School Manager for each Relution organization that uses SFTP upload. The name of this location is the same as the unique name of the respective Relution organization.

For example:

- Organization Name: `User-Import-Test`
- Unique Name of the Organization: `UIT`
- New Location in ASM: `UIT`

If the location in Apple School Manager used for purchasing apps and already exists has the same name, this can cause problems.
This should be discussed with the server operator or partner beforehand.

Disconnecting

The SFTP upload connection must never be disconnected if the accounts are still actively in use and additional accounts are to be created in the future. Disconnecting changes all accounts created via SFTP upload to the source Manually from SFTP. Reconnecting afterward may result in duplicate Managed Apple Accounts. Since Relution version 5.26 also introduced user import, this can create a vicious cycle.

In Relution, the settings are reset via Clear SFTP server settings → Delete. This only removes the settings in Relution: the SFTP credentials remain valid until the directory sync is disconnected in the Apple School Manager preferences.

For version 26.4.0

Install native macOS apps

Relution allows native macOS applications to be uploaded centrally to the App Store and distributed to managed Macs. The supported file formats are `.pkg` (installer package) and `.dmg` (disk image). Reliable, unattended distribution depends on the interplay of a suitable package format, a correct detection rule, and valid signing. The following sections describe these components in detail.

> Native macOS apps are installed through the Relution App Store or a distribution action. A Mac that is managed (enrolled) in Relution is required.

PKG and DMG compared

The choice of package format determines how an app is installed and whether the process can be automated.

Characteristic	`.pkg` (installer package)	`.dmg` (disk image)
Structure	installer with optional scripts (`preinstall` / `postinstall`)	container/archive, usually contains one `.app`
Install location	flexible, several target locations possible	usually a copy to `/Applications`
Install logic	the package's own installation routine	copy operation of the contained `.app`
Automated installation	possible in the background without interaction	usable only if exactly one `.app` is contained
Recommendation	preferred for MDM distribution	suitable when no PKG is available

A `.pkg` is the more robust format for automated distribution, because the installation routine is contained within the package itself and can run silently in the background. Scripts inside the package can perform additional steps, such as creating configuration files. During the upload, Relution reads the package's Distribution file and takes the product ID and version from it. Packages without a Distribution file (plain component packages) are rejected as an unsupported file.

A `.dmg` is a disk image. It is only suitable for distribution if it contains a single application (`.app`) that is copied to `/Applications`. Images with an interactive installation assistant or multiple items cannot be installed unattended.

One essential difference concerns the distribution channel: `.pkg` apps are installed directly via the MDM protocol, whereas `.dmg` apps are deployed via the macOS Companion. This requires the macOS Companion to be switched on under `Settings` → `Relution Client Apps` with Enable macOS companion. The macOS Companion is not available on Macs running a macOS version earlier than 12 or on Macs with User Enrollment; DMG apps cannot be distributed to these devices.

Note: If an app is available both as a `.pkg` and as a `.dmg`, the `.pkg` is preferable for centralized distribution.

Add a native app in Relution

Native macOS apps are created in the menu under `Apps` → `App Store`. The Add button opens the Add a new app dialog. Under Source, the Native app option is selected.

After clicking Next, the `.pkg` or `.dmg` file is uploaded via Choose file. Add details then opens the Add app form.

> For large packages, the file size may be limited by the database or reverse proxy. In this case, the server-side configuration needs to be adjusted accordingly.

The following entries are required in the form:

- Internal name: For `.pkg` files, the product ID is taken from the Distribution file. For `.dmg` files, the file name is pre-filled as a placeholder and is replaced by a unique name. If an app with the same internal name already exists, saving creates a new version of that app.
- Version name: For `.pkg` files, the version is taken from the Distribution file; for `.dmg` files, it is entered manually.
- Detection rules: At least one detection rule is entered in the section of the same name – without a detection rule, the app cannot be saved (see the section on the detection rule below).

After specifying the desired Release status, the app is created via Save.

For version 26.4.0

Version management and release status

Native macOS apps also support release management: different versions of an app can be made available in parallel to different groups of people. For example, one version can be in productive use while a new version is tested by a selected group, without affecting the remaining users.

Each version goes through one of the following states:

- Release: the version that is regularly distributed and installed via the Relution Agent.
- Development or Review: states used for versions that are tested before release.
- Archive: state of a previous version that has been superseded by a newer released version.

Except for the Archive status, each release status can only contain one version of the app.

Testing a new version in parallel

To test a new version alongside the existing released version, it is uploaded via the Add new version button and initially set to the Development or Review state. For `.pkg` files, the internal name of the new version must match that of the existing app. For `.dmg` files, a mismatch can be allowed with Ignore internal app name mismatch.

A date can be entered for the new version in the Go Live date field. The version only switches to the Release status automatically on that day if an App Release Workflow → is active and the version in the Review status has passed all release steps. Without an active release workflow, the date only serves as a target date, and the version is set to the Release status manually (see below).

Both versions remain visible in the app properties in the meantime; users with the appropriate permission can already view, install, and test the new version on endpoints.

Manual go-live

If the new version is in the Review status, it is moved to the Release status on the app detail page via the Release button. If it is still in Development, the change is made via `Move to` → `Release`. An already released version is then automatically moved to the Archive state. Released versions of global apps cannot be moved to a different state.

> The app is not automatically updated on endpoints. An update is triggered by users in the Relution Agent or by administrators with the Deploy Relution store app device action or in the app view under Devices with this app with the Update app button.

Detection rule via the bundle identifier

The detection rule tells Relution how to recognize the installed state of an app. For native macOS apps, the Package Name rule type is available for this purpose. It contains the bundle identifier of the installed app (e.g. `com.vendor.appname`); letters, digits, dots and hyphens are allowed. This value is used to check in the device's list of installed apps whether the app is already present and whether an installation is considered successful.

Detection rules are created in the Detection rules section via Add new detection rule – in the Add app form during the upload, and for existing apps on the app detail page in the Settings tab. Optionally, a version check also compares the installed version: under Operator, Version is equal to (=) or Version does not equal (≠) is selected, and the version is entered under Value. An app can have several detection rules, for example if a package installs several apps. The app is only considered installed if all rules match.

For version 26.1.0

The most reliable way to determine the correct bundle identifier is via a Mac that is already managed:

1. The app is installed manually once on a Mac that is managed in Relution.
2. In the Relution portal, the device is opened under `Devices` → `Inventory`.
3. On the Installed apps tab, the app is located. The bundle identifier is shown in the Internal name column.
4. This value is entered in the Package name field of the detection rule.

> After a manual installation, it may take a moment until the next inventory sync shows the app in the portal. The Refresh device info action speeds up the display.

Alternatively, the bundle identifier can be read directly on the Mac via the Terminal:

```
osascript -e 'id of app "App-Name"'
```

If the path of the application is known, the value can also be read from the package metadata:

```
mdls -name kMDItemCFBundleIdentifier -raw /Applications/App-Name.app
```

If the detection rule is to be determined before an installation, the contents of a `.pkg` can be inspected with a third-party tool such as Suspicious Package. Such a tool shows the bundle identifier in addition to the install paths and contained scripts, without the package having to be run.

Note: Third-party tools serve analysis purposes only. The authoritative bundle identifier remains the value reported in the Relution inventory after an installation.

Alternatives without a working detection

For some native apps, Relution cannot reliably check the installed state – for example because no unique bundle identifier is available or the package places the app in an atypical location. Automatic installation via App compliance is not suitable in these cases: Relution only recognizes a PKG or DMG app as installed if all detection rules are met. Otherwise, the installation is scheduled again with every compliance check.

Two options work without a reliable detection rule:

- Provisioning via the Relution App Store: The app is made available to users in the Relution Agent and installed there manually. Because the installation is actively triggered, no automatic state check is required.
- Distribution via an action: The Deploy Relution store app action on selected devices or groups triggers the installation specifically. The install command is transmitted to the device and executed there, independent of a detection rule.

> Without a matching detection rule, Relution can only assess the success of the installation to a limited extent. In this case, the actual installation state has to be verified on the device.

For version 26.4.0

Signing and notarization

macOS uses Gatekeeper to check whether software comes from a trusted source. Packages that are neither signed nor notarized by Apple may be blocked or require user interaction – which prevents unattended distribution.

- Signing: The package is signed with a valid Developer ID. This makes the origin traceable and rules out tampering.
- Notarization: The package has additionally been checked by Apple (notarized). Only then is it accepted on current macOS versions without a warning.

Whether a package is correctly signed and notarized can be verified on the Mac in the Terminal:

```
spctl --assess --type install -vv /path/to/App.pkg
pkgutil --check-signature /path/to/App.pkg
```

Note: If an installation fails silently only for individual packages, missing signing or notarization is one of the most common causes.

Troubleshooting via logs and device logging

If an installation remains unsuccessful, the causes can be narrowed down via logging.

Device logging in Relution

Device logging is switched on for a single device in the global organization: the device is selected in the device inventory, and Activate device based logging is set via Manage device logging for the time specified under Duration (in minutes). During this period, commands such as the app installation are logged together with the device's response. The captured Device logs are downloaded as a file in the same dialog. This makes it visible whether an install command has reached the device and with which status it was acknowledged.

> Logging ends automatically after the configured duration. The log file is deleted one day after logging ends and does not survive a restart of the Relution server.

Installation logs on the Mac

In addition, the Mac's system logs provide information about the installation process. The progress of a PKG installation is logged locally and can be evaluated in the Terminal:

```
tail -n 100 /var/log/install.log
```

For live observation during an installation, the live stream of the system log is suitable:

```
log stream --predicate 'process == "installer"' --info
```

These outputs reveal whether the package was unpacked, a script was executed, or the process was aborted by Gatekeeper.

Uninstallation

Native macOS apps that were installed through Relution can also be uninstalled through Relution – both `.pkg` and `.dmg` apps. This requires a bundle identifier (detection rule) that uniquely addresses the app on the device. Without a valid bundle identifier, no uninstallation is triggered. As with installation, the removal runs over different channels depending on the format – `.pkg` via MDM, `.dmg` via the macOS Companion – but the procedure in the portal is identical.

There are two ways to uninstall:

- Specifically via an action: The Remove app action on selected devices or groups uninstalls the app. In the device's command history, the operation appears as `Remove <bundle identifier>`.
- Automatically when the assignment no longer applies: If an app that was installed automatically via App compliance (checkbox in the Auto install column) is no longer required after the policy is changed or removed, Relution uninstalls it automatically. Unlike on iOS, the macOS App compliance configuration offers no option to switch this uninstallation off.

> What matters for the uninstallation is the bundle identifier, not the package format. Without a valid detection rule, Relution cannot resolve the app on the device and therefore cannot remove it specifically.

Apps without a bundle identifier, as well as apps installed manually – outside of Relution – cannot be removed through Relution. For `.dmg` apps, the macOS Companion is additionally required; if it is disabled or cannot be used on the device (macOS earlier than version 12, User Enrollment), uninstallation through Relution is not possible. In these cases, the removal is implemented via a script that quits the app and removes the associated directories, distributed specifically to the affected devices or groups via an action.

For version 26.4.0

Manage App Store apps

With Relution, it is possible to distribute apps from the Apple App Store to devices. To do this, an app license must always be purchased – regardless of whether the app is paid for or not. An app license can either be purchased via Apps and Books (VPP in the portal) or obtained via an Apple ID signed in on the device. Depending on the use case, one or the other scenario makes more sense. For devices without an Apple ID, there is no way around an Apps and Books license. The setup of Apps and Books is described in the corresponding chapter →.

Apps purchased in Apple School / Business Manager are automatically synchronized to Relution (from version 5.10). Apps are published in Relution with the release status Release and can be distributed to devices afterwards. Apps that should not be made available to all users can also be manually assigned to a different release status. An app can also be manually added to the Relution App Store at any time. However, Apps and Books licenses are not automatically available for these apps, and installation is only possible if users with an Apple ID are signed in on the corresponding end devices. Apps and Books licenses for these apps can be obtained at a later date.

If Apps and Books licenses are available for an app, Relution automatically assigns a license during installation – including manually added apps once the licenses have been synchronized later on. On Macs with User Enrollment, a user-based license is used for this.

Distribute apps

For version 26.4.0

Apps from the App Store are normally distributed to Macs as required apps via the App compliance policy configuration.

Two device actions are available for individual devices:

- Deploy Relution store app: offers the apps from the Relution App Store, i.e. in addition to native apps also the App Store apps created there.
- Deploy an app from the Apple App Store: the app is searched for directly in the Apple App Store and installed without having to be created in the Relution App Store first.

Manage apps

Apps from the App Store are updated automatically by the operating system. In rare cases, however, this does not work. In this case, there are two ways to trigger an update:

- In the app's detail view, the affected devices are selected on the Devices with this app tab and updated via Update app. The button is disabled as soon as one of the selected devices already has the version in the Release status installed.
- Alternatively, the action Deploy Relution store app (or Deploy an app from the Apple App Store) is executed again with the app in question on the affected devices.

In both cases, a reinstallation is triggered and the devices validate the app version with Apple's App Store. If the available version is more recent than the installed version, the existing app is updated.

Managed App Configuration for native apps

Native macOS apps – that is, applications uploaded manually as `.pkg` or `.dmg` – can be pre-configured in Relution. However, the intended path differs from the one for apps from the App Store. The decisive factor is the source of the app, as it determines which method is available.

The app source determines the configuration method

The Managed App → policy configuration requires the app to have been installed through a channel managed by Apple. macOS only applies it to apps installed from the App Store or via Apps and Books (VPP in the portal). For these apps, the operating system handles the assignment of the configuration to the app based on the bundle ID.

For native apps, this mechanism does not take effect, because they were not installed through the managed App Store channel. Although they can be selected in the Managed App configuration in the portal, the configuration has no effect on them. The configuration of a native app must therefore be transmitted as a payload via the Apple Configurator 2 Configuration → policy configuration.

App source	Configuration method
App Store / Apps and Books	Managed App
Native app (`.pkg` / `.dmg`)	Payload via Apple Configurator 2 configuration

Configuring native apps via Apple Configurator 2

Which keys and values are supported in the payload (property list) is specified by the respective app vendor. The setup is done in a few steps:

1. The native app is first provisioned as usual so that it is installed on the target devices (see Install native macOS apps →).
2. The desired app configuration is assembled as a `.mobileconfig` file (see the recommendation below).
3. An Apple Configurator 2 configuration is added to the policy, a Name is entered, and the complete `.mobileconfig` file is uploaded via Select .mobileconfig file. Its content is then shown in the Payload content field and can be adjusted there if necessary.
4. The policy is published and assigned to the affected device groups.

> The app must already be installed on the device before the configuration takes effect. The order of the configurations within a policy cannot be specified. If the app is installed via the same policy, the Apple Configurator 2 configuration may therefore reach the device before the app.

A `.mobileconfig` file may contain only one configuration type (payload type) in `PayloadContent`; additional certificate payloads are allowed. If the file contains several types, for example settings for several apps, the configuration cannot be saved. A separate Apple Configurator 2 configuration is therefore created for each app. If the file contains several payloads of the same type, only the first one is transmitted. Further requirements for the file are described in the Apple Configurator 2 Configuration → article.

Recommendation: create the payload with the iMazing Profile Editor

Writing a payload manually is error-prone. For convenient creation, the third-party tool iMazing Profile Editor is recommended. It allows the configuration to be assembled through a graphical interface, without writing the underlying property list by hand.

The procedure is as follows:

1. In the iMazing Profile Editor, the desired settings for the app are set via the interface.
2. The result is exported unsigned as a `.mobileconfig`. Relution reads the file as XML; signed profiles cannot be saved.
3. The complete `.mobileconfig` file is uploaded to the Apple Configurator 2 configuration in Relution.

> The iMazing Profile Editor is a third-party tool and not part of Relution. It serves only to create the payload.

The payload can also use the placeholders provided by Relution (e.g. `${user.email}`) to fill in the configuration on a per-user basis. The available placeholders are shown below the configuration form and are replaced when the configuration is transmitted to the devices, see Advanced placeholders →.

For version 26.4.0

Overview of enrollments

Vision Pro is becoming a central component of modern organizations, opening up entirely new possibilities. Relution supports multiple enrollment methods to ensure Vision Pro can be integrated seamlessly and used to its full potential. Besides Automated Device Enrollment (ADE, DEP in the portal), Apple User Enrollment is also available.

Automated Device Enrollment (ADE) with a DEP profile

Apple School or Business Manager was introduced by Apple to help organizations and educational institutions deploy Apple devices remotely. With the aid of ASM/ABM, brand-new Apple devices can be enrolled in Relution without a technician ever having to get hold of them.

Profile for ADE →
Configure DEP →

Requirements

- visionOS 1.1 or later.
- Organization should be enrolled in Apple School / Apple Business Manager.
- If devices were purchased directly from Apple, the Apple customer number assigned to the organization is required to link eligible orders and devices to Apple School / Business Manager.
- If devices were purchased directly from an authorized reseller or carrier, the devices must be linked to that reseller's Reseller ID. The actual date of eligibility is determined by the sales history of the authorized reseller or network operator.
- An APNs certificate stored in Relution (APNS Push Certificates →).
- A DEP account connected to Relution and a DEP profile assigned to the devices. The Minimum visionOS version field in the DEP profile can additionally be used to define a minimum visionOS version for enrollment.

For version 26.4.0

Account-driven user enrollment

This is the typical enrollment method for Bring Your Own Device (BYOD) scenarios. Users can carry out the enrollment themselves, and the devices do not need to be reset to factory settings.

Relution supports account-driven user enrollment for visionOS devices that are not in `Supervised Mode`.

Sign-in takes place on the Vision Pro in the device settings with a Managed Apple Account (Managed Apple ID in the portal). Using Service Discovery, the device determines the responsible MDM server and redirects to the Relution sign-in page, where sign-in takes place with the Relution user account. Relution then automatically creates a user enrollment with the ownership Bring Your Own Device (BYOD). For visionOS, user enrollments cannot be created manually in the portal.

Requirements

- An APNs certificate stored in Relution (APNS Push Certificates →).
- A Managed Apple Account and a Relution user account for each user.
- The Account-driven Apple user enrollment setting enabled in the organization.
- Service Discovery for the domain of the Managed Apple Accounts, either automatically via Apple School/Business Manager or via a well-known file.

Enable account-driven Apple user enrollment

The setting is located under `Settings` → `Device Management` in the Account-driven Apple user enrollment section. It applies per organization; the section is not shown in the global organization.

If the Account-driven Apple user enrollment toggle is enabled, Relution automatically creates a user enrollment when a user signs in. The toggle is disabled by default; in that case, enrollment of visionOS devices fails.

Set up Service Discovery

Service Discovery must be configured so that Apple can direct devices to the correct MDM server. There are two ways to do this.

Automatically via Apple School/Business Manager

As of visionOS 2.2, no separate file is required if Apple School/Business Manager is connected to Relution via a DEP account. Relution automatically stores the Service Discovery URL in Apple School/Business Manager during every synchronization of ADE devices. This requires Relution to be set as the default MDM server for Apple Vision Pro under `Preferences` → `Your MDM Servers` → `MDM Server Assignment` → `Default MDM Server Assignment`.

For version 26.4.0

Via a well-known file

For devices running a visionOS version earlier than 2.2, or without a connected Apple School/Business Manager, an HTTP well-known resource file must be published on the domain users sign in with. Relution already answers this request itself for its own hostname; a separate file is therefore only required if the domain of the Managed Apple Accounts differs from it. Apple must be able to retrieve this file via an HTTP GET request at the following URL:

```
https://yourdomain.com/.well-known/com.apple.remotemanagement
```

Under `yourdomain.com`, the domain also used for the Managed Apple Accounts must be entered. The file must be hosted on a domain that can handle HTTP GET requests.

Create the file in JSON format with the content type `application/json`. To enter the correct information in the file, the required information can be copied directly from the Relution portal:

1. `Settings` → `Device Management` is opened.
2. In the Account-driven Apple user enrollment section, the JSON text shown under Response is copied in full, including the outer curly braces (Copy to clipboard button), and pasted into the file. The JSON text is shown regardless of the toggle.

For the file to work correctly, it must not have a file extension.

Example: maxmustermann@musterhausen.de

In this example, the domain would be `musterhausen.de`. The Service Discovery file would need to be published there.

Subsequent enrollment via Apple Configurator 2

`Apple Configurator 2` is a free app available from the Mac App Store. The application can be used to manually configure Apple devices connected via USB to a macOS device before the devices are handed out to users. For this purpose, so-called profiles can be created and applied to the devices. In addition, `Apple Configurator 2` allows Apple devices that have not already been registered for ADE by an authorized reseller to be added subsequently. Overall, it is recommended to purchase ADE-capable devices directly, as adding them later involves manual effort.

Requirements

- visionOS 1.1 or later.
- macOS device with `Apple Configurator 2.5` or higher.
- Make sure the macOS device and Vision Pro are connected to the same Wi-Fi or Ethernet connection.

For visionOS devices, the following path must be specified as the MDM server URL if the devices are to be managed on the Relution live system. For a self-hosted Relution instance, replace `live.relution.io` with the server's hostname.

```
https://live.relution.io/api/enrollment/v1/appleMdm/depenroll
```

Apple devices that are subsequently registered in Apple School / Business Manager via `Apple Configurator 2` will not function like devices registered directly via ADE when purchased through an authorized reseller for the first 30 days after deployment. Even if manual removal of MDM management on devices has been blocked via the associated DEP profile in the MDM system, users can remove the MDM management under `Settings` → `General` → `Profiles`.

Once the 30-day period from registration has elapsed, users will be prevented from removing MDM management on devices.

Detailed guide on adding Apple devices to ADE after the fact →

Available actions

Relution provides a selection of actions to directly control the Vision Pro. The actions can be applied to individual devices, to several devices at once via multiple selection in the device list, or automatically via Device group actions →.

Action overview

Action	Description
Refresh device info	Refreshes the device information, which is listed in Details.
Deploy Relution store app	Installs an app from the Relution Store on the devices. In addition to visionOS apps, iOS apps are also available for selection.
Update MDM profile	Reinstalls the MDM profile on the device. The identity certificate is renewed and current settings such as certificate pinning are applied. The MDM server URL remains unchanged; a changed external URL is therefore not transferred to the device. Relution renews the MDM profile automatically before the identity certificate expires. The manual action is therefore only required in special cases.
Continue in device Setup Assistant	Informs the device that the pre-configuration is completed and it can proceed in the Setup Assistant. Only takes effect on devices enrolled via Automated Device Enrollment (ADE, DEP in the portal) whose DEP Profile has the Await configuration option enabled. The action is not available for devices enrolled via User Enrollment.

The actions Reboot device, Lock device, Shutdown device and Wipe device are not offered for visionOS devices.

Overview

A policy is a collection of one or more configurations. Each policy can be applied to one or more devices at the same time. Likewise, each device can be linked to one or more policies.

Available configurations

Configuration	Description
App Compliance →	Manages app-specific restrictions
Apple Configurator 2 Configuration →	Applies a configuration profile (`.mobileconfig`) created with Apple Configurator 2 to devices
External Intelligence Settings →	Controls external, cloud-based AI integrations via Siri and Apple Intelligence (visionOS 26.4 or later)
Intelligence Settings →	Centrally controls Apple Intelligence features such as Genmoji, Image Playground, and Writing Tools (visionOS 26.4 or later)
Passcode →	Passcode policy for Apple devices
Restrictions →	Manages device restrictions
Siri Settings →	Centrally controls Siri's behavior, including the profanity filter and access while locked
Software update settings →	Controls the update behavior of devices, e.g. automatic downloads, deferral, and notifications (visionOS 26 or later)
Managed Software Updates →	Enforces operating system updates, targeting a specific version by a deadline (visionOS 26 or later, supervised devices only)
WiFi	Manages Wi-Fi settings
Certificate	Selects a certificate to be installed on the device by default

Passcode

The Apple passcode policy defines security requirements for device passcodes on visionOS devices. On visionOS, this configuration is intended for device enrollment.

The policy offers a wide range of options to further adapt passcode security. These include requirements for complexity, length, validity period, and the number of allowed failed attempts.

As soon as the policy is applied to a device, a device passcode is always required. Fields left empty are not sent to the device; the policy imposes no requirement for these settings.

> This requires at least visionOS 2.x.

Configuration options

- Allow simple passcode (enabled by default): Allows passcodes with repeated or ascending/descending character sequences such as `aaa`, `abc` or `123`.
- Require alphanumeric values (disabled by default): Specifies whether the passcode must contain letters or whether digits are sufficient.
- Minimum passcode length: Values from 0 to 25 characters.
- Required number of special chars (1-4): Values from 0 to 4.
- Maximum passcode age (in days): Number of days after which a new passcode has to be set; values from 0 to 730.
- Inactivity time (in minutes): Maximum auto-lock time after inactivity that the user can select on the device.
- Passcode history: Number of previously used passcodes that cannot be set again; values from 1 to 50.
- Grace period for device lock (in minutes): Period after locking during which the device can still be unlocked without entering the passcode. With Immediately, the passcode is required every time the device is unlocked. This setting does not determine when the device locks – that is controlled by Inactivity time (in minutes).
    - Immediately
    - 1 minute
    - 5 minutes
    - 15 minutes
    - 60 minutes
    - 4 hours
- Maximum number of failed attempts: Values from 2 to 11.

> If the limit is exceeded, a wipe action is triggered.

For version 26.4.0

Apple Configurator 2 Configuration

This policy configuration can be used to transfer `.mobileconfig` files to Apple devices. Such a file can contain, for example, a Wi-Fi connection together with the matching identity certificate (PKCS#12, `.p12`).

Configuration

The Name field sets a name for the configuration. The file is uploaded via Select .mobileconfig file. Its content then replaces the file selection in the Payload content field, where it can be edited. The content must be valid XML. Signed profiles are not readable XML and therefore cannot be used, so the file is saved without a signature in Apple Configurator 2. If the Payload content field is cleared, a file can be selected again.

User, device and certificate placeholders can be used in the Payload content field. The available placeholders are listed below the form and are replaced when the configuration is transferred to the device, see Advanced placeholders →.

Several Apple Configurator 2 configurations can be created per policy. This allows multiple configuration types to be split across separate configurations.

File requirements

The content is validated when the configuration is saved. The file must meet the following conditions:

- The top level contains the keys `PayloadType`, `PayloadVersion` (as a number), `PayloadIdentifier`, `PayloadUUID` and `PayloadDisplayName`.
- `PayloadContent` contains exactly one configuration type. Certificate payloads may be included in addition.

Files that cannot be read, that lack one of these keys, or that contain no payload or several configuration types are rejected when saving.

> Only certificates in PKCS#12 format (`com.apple.security.pkcs12`) are transferred along with the configuration. PKCS#1 certificates (`com.apple.security.pkcs1`) pass validation but are not transferred to the device. Other certificates such as root certificates (`com.apple.security.root`) count as a separate configuration type. Combined with another configuration, they cause an error when saving and are therefore stored in a configuration of their own.
>
> The actual configuration must be the first entry in `PayloadContent`. If the file contains several payloads of the same type, only the first one is transferred to the device.

If the file contains a configuration type that Relution also offers as a separate configuration allowed only once per policy, that configuration can no longer be added to the same policy. On visionOS, this applies to Passcode → (`com.apple.mobiledevice.passwordpolicy`) and Restrictions → (`com.apple.applicationaccess`).

Conversely, such a file is rejected when saving if the policy already contains the corresponding configuration or another active Apple Configurator 2 configuration with the same payload type.

Example

The following file transfers a Wi-Fi connection (`com.apple.wifi.managed`). SSID, password, identifiers and UUIDs are sample values and are replaced with actual values. Each `PayloadUUID` must be unique.

For version 26.4.0

```
<?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>Wi-Fi-password</string>
   <key>PayloadDisplayName</key>
   <string>Wi-Fi</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>Company-WiFi</string>
  </dict>
 </array>
 <key>PayloadDescription</key>
 <string>Wi-Fi configuration for Apple devices</string>
 <key>PayloadDisplayName</key>
 <string>Wi-Fi</string>
 <key>PayloadIdentifier</key>
 <string>com.example.wifi</string>
 <key>PayloadOrganization</key>
 <string>Example Inc.</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 Settings

With Relution, the Intelligence Settings configuration can be centrally managed to control Apple Intelligence features on managed visionOS devices. This policy makes it possible to allow or block individual AI-powered features such as the Apple Intelligence Report, Genmoji, Image Playground, Image Wand, and Writing Tools. It also allows the Intelligence features in Mail and Safari to be controlled and enforces that dictation is processed exclusively on the device, without any connection to Apple's servers.

This configuration is available for visionOS devices running version 26.4 or later.

> The form is the same for iOS, macOS, and visionOS. The options Allow Personalized Handwriting Results, Allow Visual Intelligence Summary, Force On-Device-Only Translation as well as Allow Transcription and Allow Transcription Summary in the Notes section are also shown for visionOS but are not supported by visionOS. They are therefore not described here, see Intelligence Settings for iOS →.

Settings

- Allow Apple Intelligence Report
  - When disabled, the Apple Intelligence Report is disabled on the device. Enabled by default.
- Allow Genmoji
  - When disabled, the Genmoji feature is disabled. Enabled by default.
- Allow Image Playground
  - When disabled, Image Playground is disabled. Enabled by default.
- Allow Image Wand
  - When disabled, Image Wand is disabled. Enabled by default.
- Allow Writing Tools
  - When disabled, Writing Tools are disabled. Enabled by default.
- Force On-Device-Only Dictation
  - When enabled, dictation is processed exclusively on the device, without any connection to Apple's servers. Disabled by default.

For version 26.4.0

Mail

- Allow Smart Replies
  - When disabled, Smart Replies in Mail are disabled. Enabled by default.
- Allow Summary
  - When disabled, the summary feature in Mail is disabled. Enabled by default.

Safari

- Allow Summary
  - When disabled, the summary feature in Safari is disabled. Enabled by default.

Restrictions

Below is an overview of the available visionOS restrictions.

Most restrictions require visionOS 2 (hint visionOS 2+ in the form); different minimum versions such as visionOS 1.1+, visionOS 2.4+ or visionOS 26+ are stated in the overview below. Restrictions marked Supervised only take effect on supervised devices, while restrictions marked Supports user enrollment also take effect on devices with user enrollment; both are marked accordingly in the overview. The AI feature restrictions are marked Deprecated in the portal.

By default, all options are enabled except on-device-only dictation, the two contact options under Managed Apps and Documents, applying the Allow opening ⋯ settings to copy and paste, AirDrop targets considered as unmanaged, Force Automatic Date and Time and Force WiFi whitelisting. The Allowed external integration workspace IDs list is empty. With the default values, all features are therefore allowed; only Force authentication before auto fill is enabled by default, so authentication is required before autofill.

The download icon at the top of the form (Export restrictions as CSV file) downloads the configured values, including unsaved changes, as a CSV file.

Of the Recommended restrictions for iOS/iPadOS →, only the notes on Erase All Content and Settings, Force Automatic Date and Time and Force WiFi whitelisting also apply to visionOS.

Device

Show all restrictions

For version 26.4.0

Apps

The app restrictions are grouped by area of use.

General

Show all restrictions

Safari

Show all restrictions

Siri

Show all restrictions

Other apps

Show all restrictions

Managed apps and documents

These settings control the exchange of data between managed and unmanaged apps.

Managed apps and documents restrictions

Show all restrictions

Settings

The following restrictions apply to the system settings of the device.

For version 26.4.0

Settings restrictions

Show all restrictions

Media

The following restrictions apply to media content and its playback.

Media restrictions

Show all restrictions

Modifications

These restrictions define which settings may be changed on the device.

Modifications restrictions

Show all restrictions

iCloud

The following restrictions apply to the iCloud services on the device.

iCloud restrictions

Show all restrictions

AI feature restrictions

These restrictions control the Apple Intelligence features.

For version 26.4.0

All restrictions in this section are marked Deprecated in the portal. For devices running visionOS 26.4 or later, the Intelligence Settings → (Genmoji, Image Playground, writing tools, Image Wand) and External Intelligence Settings → (external intelligence integrations, sign-in, workspace ID) configurations are available instead; the article on external intelligence settings describes the configuration using iOS as an example. For devices running older visionOS versions, the restrictions described here continue to apply.

General

Show all restrictions

App Compliance

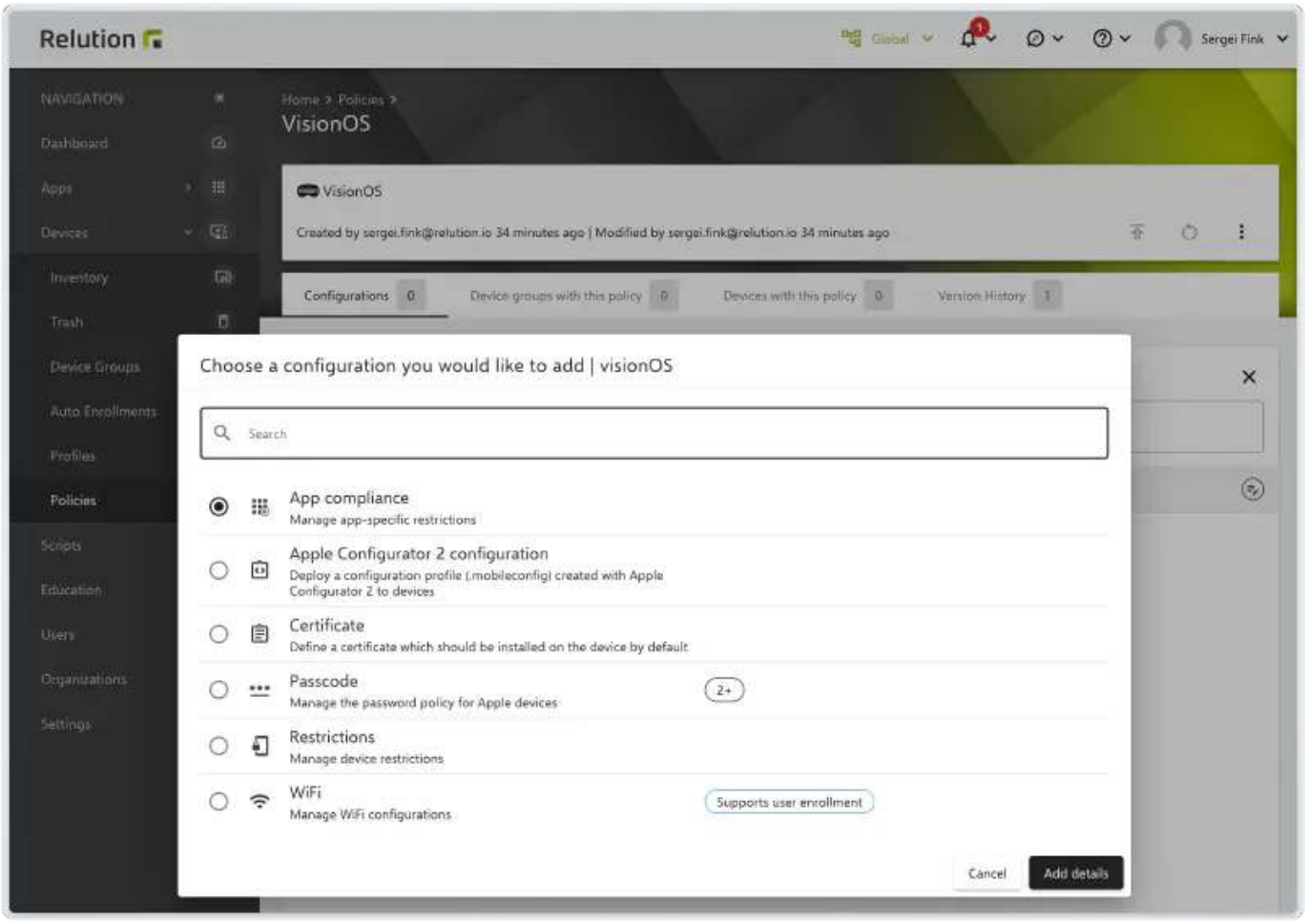
Installing apps from Apps and Books (VPP in the portal) on Apple Vision devices is particularly straightforward thanks to Relution's App compliance policy. This configuration enables simple and central distribution of applications to a large number of devices.

Starting the distribution only requires:

- An Apple School or Apple Business account.
- The integration of the organization's own Apps and Books token → in Relution.
- Acquired licenses for the desired apps from Apple School Manager (ASM) or Apple Business Manager (ABM).

Configuring App Compliance

The distribution of apps to Apple Vision devices (analogous to iOS devices) is carried out via the App compliance policy configuration. It is selected under `Devices` → `Policies` in a visionOS policy via Add Configuration and created with Add details.



Similar to iOS devices, app availability is controlled under List type in the General section: either as a blocklist (Blocklist — The apps below are not allowed, the default for new configurations) or as an allowlist (Allowlist — The apps below are allowed). The apps are entered via Add in the Blocked apps or Allowed apps section below.

Allowlist and blocklist are only applied to supervised devices.

Allowlist (Permitted Apps)

The allowlist explicitly defines which apps are permitted to be available on the devices. Two additional options are available:

- Put all auto-deployed apps on the allowlist: Apps distributed to the devices' users via auto deployments are automatically added to the allowlist.
- Allow Local Secret Prompts (e.g., iCloud, Google login): The system dialog for local secret prompts is added to the allowlist so that such prompts are not blocked.

Blocklist (Blocked Apps)

The blocklist is used to hide or block specific apps on visionOS devices.

Required Apps

The Required apps section defines which applications are to be installed mandatorily on the devices. Add offers the following sources (the same apply to the allowlist and blocklist):

- Relution App Store app: Selection of apps from the Relution App Store. Apps for the visionOS and iOS platforms are offered, i.e. public apps (e.g. with Apps and Books licenses) and native, self-uploaded apps. iOS apps can only be used on Apple Vision devices if they are compatible with visionOS.
- Apple App Store App: Search for an app in the public Apple App Store.
- Manually add app: Entry of an app by Name and Internal name (bundle ID).

For version 26.4.0

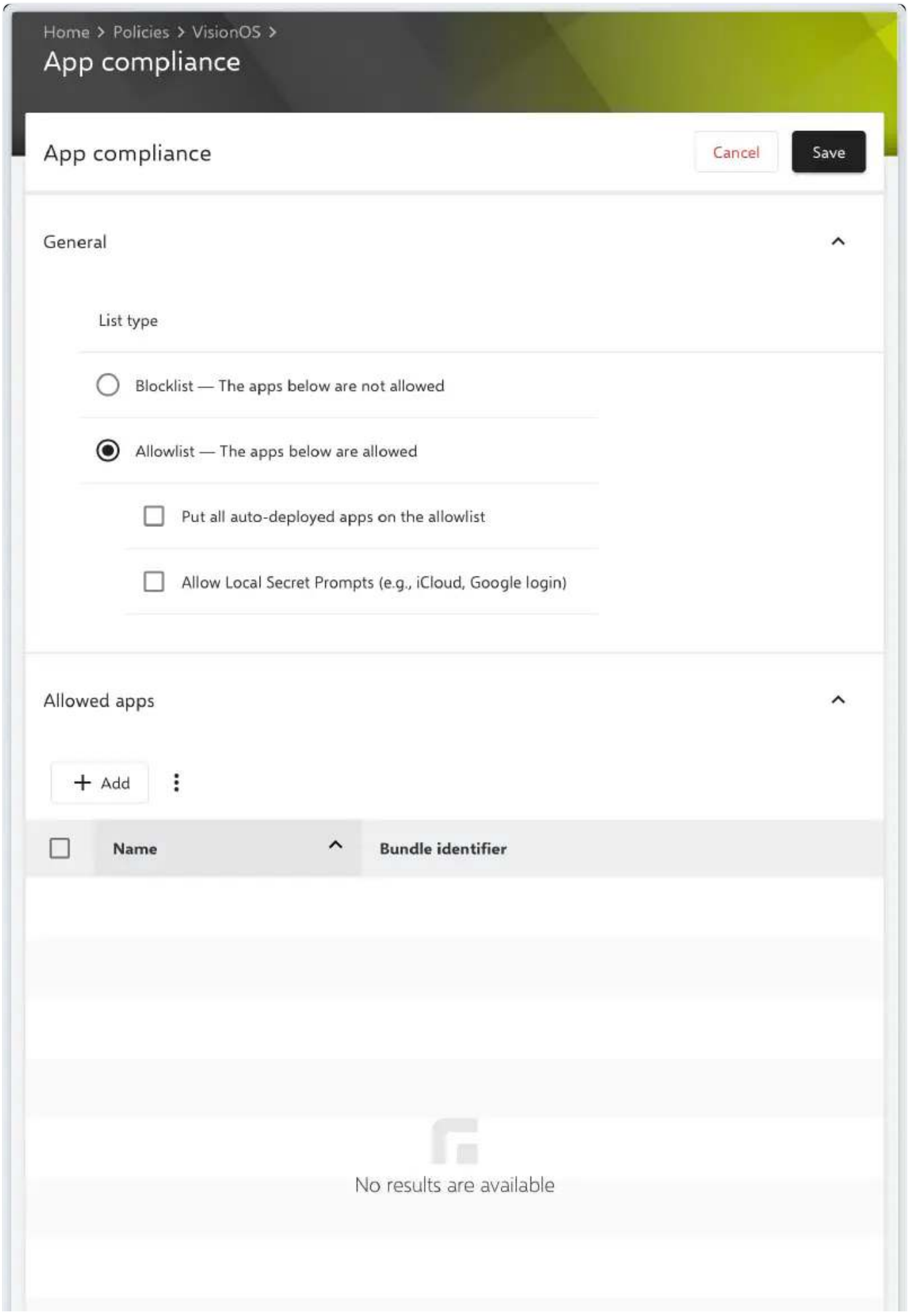
If a required app is not installed on the device, the device is considered noncompliant. The app is only actively installed if the checkbox in the Auto install column is selected; it is selected by default when an app is added. Native apps from the Relution App Store and App Store apps whose Apps and Books licenses are assigned to the devices can be installed automatically. The VPP licenses and Available VPP licenses columns show the existing and the remaining free licenses per app.

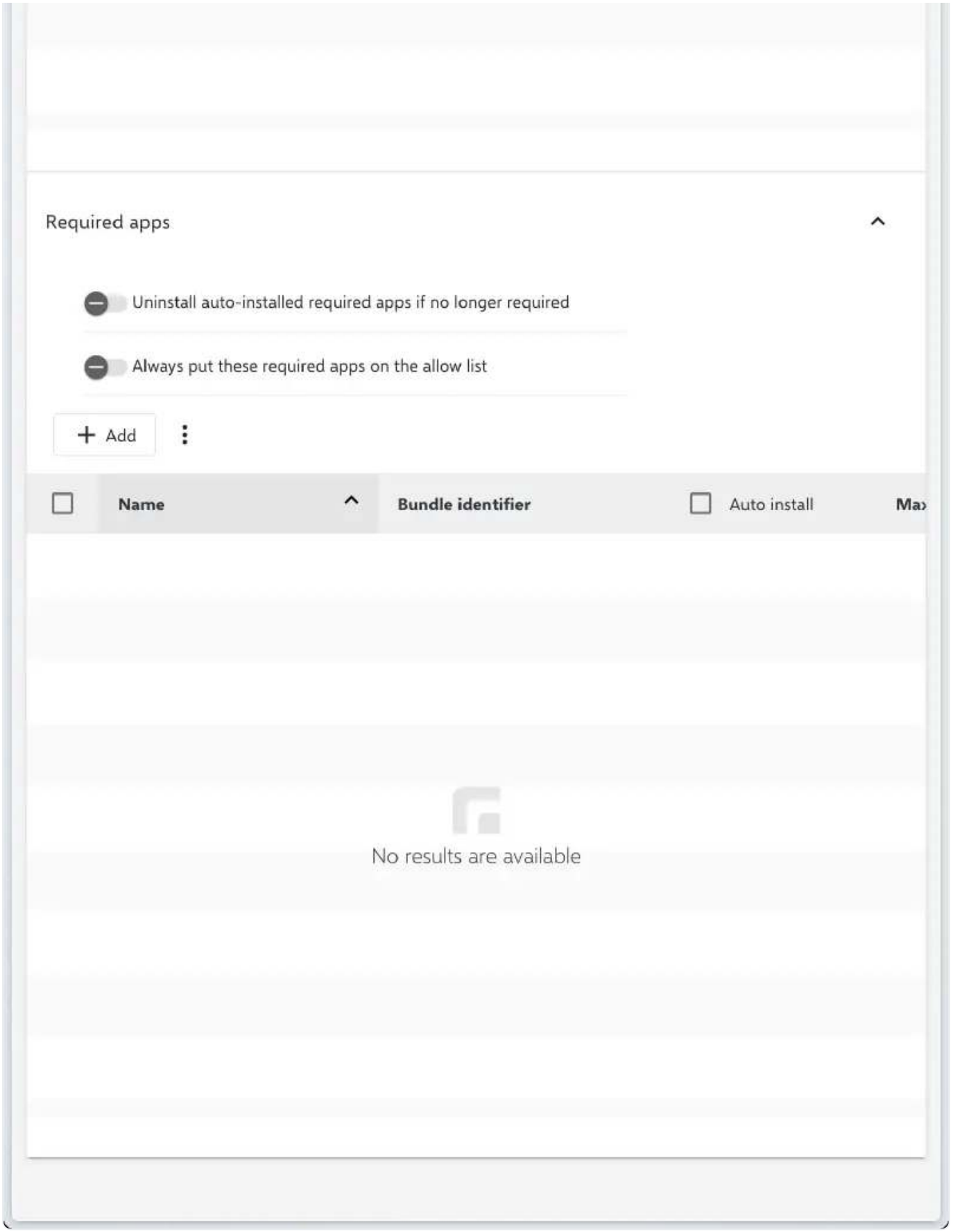
Two toggles are available above the list:

- Uninstall auto-installed required apps if no longer required: If an auto-installed required app is removed from the configuration, or the configuration is removed from the device, the app is uninstalled. The toggle is off for new configurations.
- Always put these required apps on the allow list: If this or another policy configures an allowlist for the device, the required apps are added to it.

When saving, the lists are checked for conflicts: a required app must not be on the blocklist. If the second toggle is off for an allowlist, all required apps must also be entered on the allowlist.

Once the configuration is complete, it can be saved, published, and assigned to the corresponding devices.


Home > Policies > VisionOS >
App compliance
App compliance
Cancel
Save
General
List type
Blocklist — The apps below are not allowed
Allowlist — The apps below are allowed
Put all auto-deployed apps on the allowlist
Allow Local Secret Prompts (e.g., iCloud, Google login)
Allowed apps
+ Add
Name
Bundle identifier
No results are available


Required apps
Uninstall auto-installed required apps if no longer required
Always put these required apps on the allow list
+ Add
Name
Bundle identifier
Auto install
Ma
No results are available

Enrollment under watchOS

With the iOS configuration Apple Watch Enrollment, Apple Watch devices (watchOS) can be enrolled and managed in Relution via a managed iPhone. The Apple Watch itself cannot be enrolled in Relution directly - it is registered through a paired iPhone that is already managed in Relution.

Requirements

- An iPhone running iOS 17 or later that is already enrolled and managed in Relution. The configuration is delivered via Apple's Declarative Device Management and only reaches devices that support it. Older iPhones do not receive it, and no notice is shown.
- An Apple Watch that can be paired with this iPhone.
- An active internet connection on the iPhone.
- Pairing with an Apple Watch is allowed on the iPhone. If the Allow paired watch option is disabled in the Restrictions →, pairing is not possible; any Apple Watch that is already paired is unpaired and erased immediately.

Procedure

For version 26.4.0

1. Create the configuration
    - Under `Devices` → `Policies`, the Apple Watch Enrollment configuration is created in an iOS policy via Add Configuration.
2. Apply the configuration
    - The policy is assigned to the managed iPhone.
    - Pairing should only begin once the iPhone has received the configuration.
    - The configuration is transferred via Declarative Device Management. In the iPhone's Actions tab, the Declarative management synchronization action shows whether the iPhone has accepted the synchronization. Relution does not show separately whether the configuration itself has been applied.
3. Pair the Apple Watch
    - The Apple Watch is held close to the configured iPhone.
    - The pairing process is started on the iPhone.
    - During pairing, a prompt requests consent to enrollment in Relution.

Once this prompt is confirmed, the Apple Watch is registered in Relution. Once pairing is successful, the Apple Watch appears as a standalone device (watchOS) in the device inventory. It inherits the organization and user of the iPhone and is listed as a Corporate Owned Device (COD). In the iPhone's device details, it is also listed in the Paired devices tab. Policies can then be used to apply certain restrictions or profiles that are supported for watchOS.

Notes

- If the Apple Watch is unpaired from an iPhone, it automatically loses its MDM assignment.
- If the iPhone is deleted or withdrawn in Relution, the paired Apple Watch is also removed from management.
- Only compatible watchOS versions can be enrolled using this method.

Available actions

Relution provides a selection of actions to directly control and manage the Apple Watch. The actions can be applied to a single device or, via multiple selection in the device list, to several devices at once. They can also be triggered by event or on a schedule through device group membership: Device group actions →

Action overview

Action	Description
Refresh device info	Refreshes the device information, which is listed in Details.
Deploy Relution store app	Searches for an app in the Relution Store and installs it on the devices.
Update MDM profile	Renews the MDM enrollment data on the device to ensure it matches the current server and profile settings.

Overview

A policy is a collection of one or more configurations. Each policy can be applied to one or more devices at the same time. Likewise, each device can be linked to one or more policies.

Available configurations

Configuration	Description
App Compliance →	Manages app-specific restrictions
Apple Configurator 2 Configuration →	Applies a configuration profile (`.mobileconfig`) created with Apple Configurator 2 to devices
Passcode →	Passcode policy for Apple devices
Restrictions →	Manages device restrictions
Siri Settings	Manages Siri settings
WiFi	Manages Wi-Fi settings
Certificate	Selects a certificate to be installed on the device by default

The WiFi, Certificate and Apple Configurator 2 configuration configurations can be added to a policy multiple times; all other configurations only once.

Passcode

The Apple passcode policy defines security requirements for device passcodes on watchOS devices.

The policy offers a wide range of options to further adapt passcode security. These include requirements for complexity, length, validity period, and the number of allowed failed attempts.

As soon as the policy is applied to a device, a device passcode is always required. Fields left empty are not sent to the device; the policy imposes no requirement for these settings.

> This requires at least watchOS 10.x.

Configuration options

- Allow simple passcode (enabled by default): Allows passcodes with repeated or ascending/descending character sequences such as `aaa`, `abc` or `123`.
- Require alphanumeric values (disabled by default): Specifies whether the passcode must contain letters or whether digits are sufficient.
- Minimum passcode length: Values from 0 to 25 characters.
- Required number of special chars (1-4): Values from 0 to 4.
- Maximum passcode age (in days): Number of days after which a new passcode has to be set; values from 0 to 730.
- Inactivity time (in minutes): Maximum auto-lock time after inactivity that the user can select on the device.
- Passcode history: Number of previously used passcodes that cannot be set again; values from 1 to 50.
- Grace period for device lock (in minutes): Period after locking during which the device can still be unlocked without entering the passcode. With Immediately, the passcode is required every time the device is unlocked. This setting does not determine when the device locks – that is controlled by Inactivity time (in minutes).
    - Immediately
    - 1 minute
    - 5 minutes
    - 15 minutes
    - 60 minutes
    - 4 hours
- Maximum number of failed attempts: Values from 2 to 11.

    > If the limit is exceeded, a wipe action is triggered.

For version 26.4.0

Apple Configurator 2 Configuration

This policy configuration can be used to transfer `.mobileconfig` files to Apple devices. Such a file can contain, for example, a Wi-Fi connection together with the matching identity certificate (PKCS#12, `.p12`).

Configuration

The Name field sets a name for the configuration. The file is uploaded via Select .mobileconfig file. Its content then replaces the file selection in the Payload content field, where it can be edited. The content must be valid XML. Signed profiles are not readable XML and therefore cannot be used, so the file is saved without a signature in Apple Configurator 2. If the Payload content field is cleared, a file can be selected again.

User, device and certificate placeholders can be used in the Payload content field. The available placeholders are listed below the form and are replaced when the configuration is transferred to the device, see Advanced placeholders →.

Several Apple Configurator 2 configurations can be created per policy. This allows multiple configuration types to be split across separate configurations.

File requirements

The content is validated when the configuration is saved. The file must meet the following conditions:

- The top level contains the keys `PayloadType`, `PayloadVersion` (as a number), `PayloadIdentifier`, `PayloadUUID` and `PayloadDisplayName`.
- `PayloadContent` contains exactly one configuration type. Certificate payloads may be included in addition.

Files that cannot be read, that lack one of these keys, or that contain no payload or several configuration types are rejected when saving.

> Only certificates in PKCS#12 format (`com.apple.security.pkcs12`) are transferred along with the configuration. PKCS#1 certificates (`com.apple.security.pkcs1`) pass validation but are not transferred to the device. Other certificates such as root certificates (`com.apple.security.root`) count as a separate configuration type. Combined with another configuration, they cause an error when saving and are therefore stored in a configuration of their own.
>
> The actual configuration must be the first entry in `PayloadContent`. If the file contains several payloads of the same type, only the first one is transferred to the device.

If the file contains a configuration type that Relution also offers as a separate configuration allowed only once per policy, that configuration can no longer be added to the same policy. On watchOS, this applies to Passcode → (`com.apple.mobiledevice.passwordpolicy`) and Restrictions → (`com.apple.applicationaccess`).

Conversely, such a file is rejected when saving if the policy already contains the corresponding configuration or another active Apple Configurator 2 configuration with the same payload type.

Example

The following file transfers a Wi-Fi connection (`com.apple.wifi.managed`). SSID, password, identifiers and UUIDs are sample values and are replaced with actual values. Each `PayloadUUID` must be unique.

For version 26.4.0

```
<?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>Wi-Fi-password</string>
   <key>PayloadDisplayName</key>
   <string>Wi-Fi</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>Company-WiFi</string>
  </dict>
 </array>
 <key>PayloadDescription</key>
 <string>Wi-Fi configuration for Apple devices</string>
 <key>PayloadDisplayName</key>
 <string>Wi-Fi</string>
 <key>PayloadIdentifier</key>
 <string>com.example.wifi</string>
 <key>PayloadOrganization</key>
 <string>Example Inc.</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>
```

Restrictions

Below is an overview of the available watchOS restrictions.

The Restrictions configuration is available for watchOS devices running watchOS 10 or later (hint watchOS 10+ in the form). Individual restrictions are marked Supervised in the portal and only take effect on supervised devices; they are marked accordingly in the overview below.

In the portal, the restrictions are grouped into the areas Device, Apps (with the sections General and Siri), Settings, Modifications and Lockscreen. By default, all switches are enabled except Force Apple Watch wrist detection and the two options for performing dictation and translation on the device only. With the default values, the device is therefore not restricted.

The download icon at the top of the form (Export restrictions as CSV file) downloads the configured values, including unsaved changes, as a CSV file.

Device

Show all restrictions

For version 26.4.0

Apps

The Apps area is divided into the sections General and Siri.

General

Show all restrictions

Siri

Show all restrictions

Settings restrictions

Show all restrictions

Modifications restrictions

Show all restrictions

Lockscreen restrictions

Show all restrictions

For version 26.4.0

App Compliance

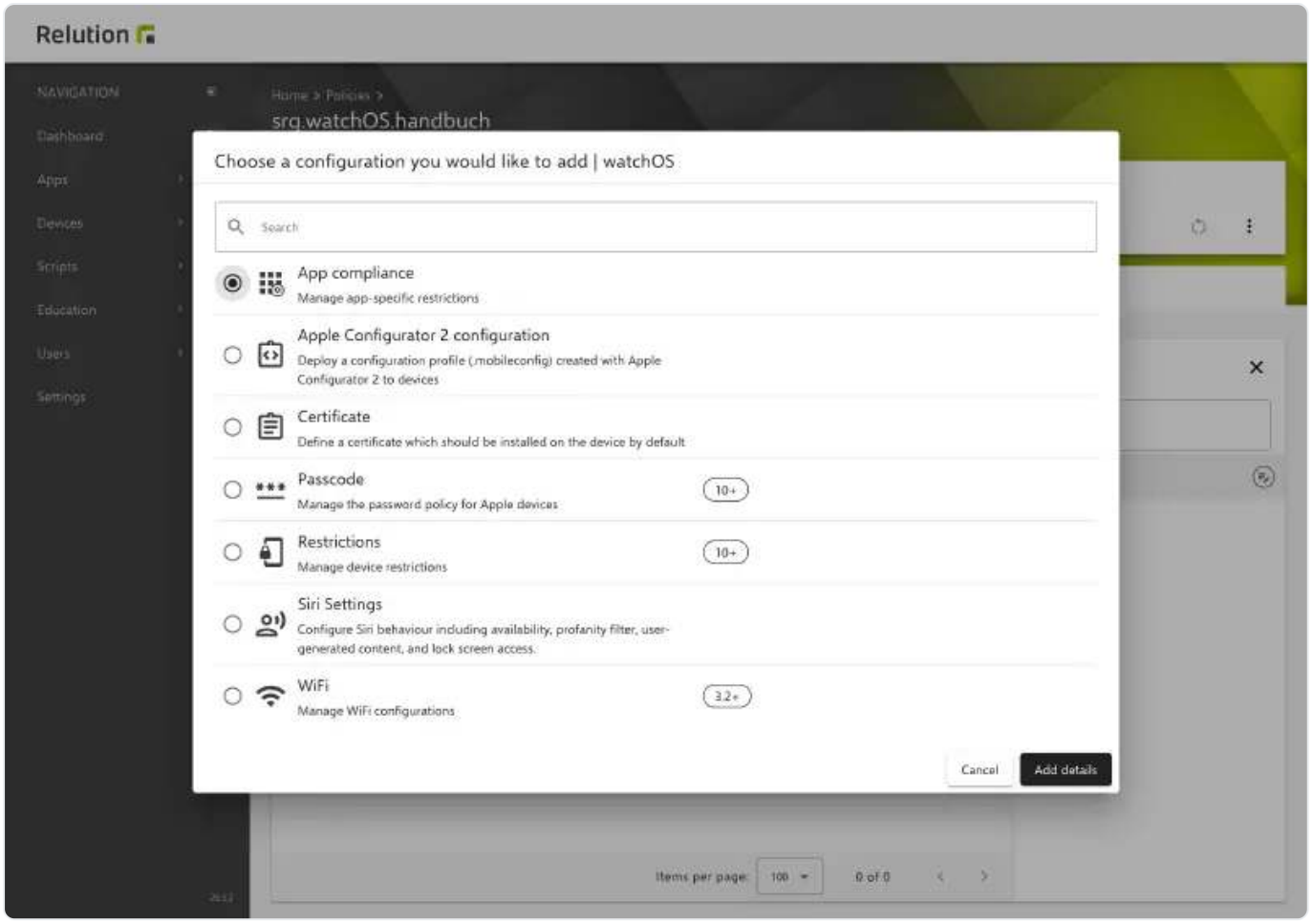
Installing apps from Apps and Books (VPP in the portal) on Apple Watch devices is particularly straightforward thanks to Relution's App compliance policy. This configuration enables simple and central distribution of applications to a large number of devices.

Starting the distribution only requires:

- An Apple School or Apple Business account.
- The integration of the organization's own Apps and Books token → in Relution.
- Acquired licenses for the desired apps from Apple School Manager (ASM) or Apple Business Manager (ABM).

Configuring App Compliance

The distribution of apps to Apple Watch devices (analogous to iOS devices) is carried out via the App compliance policy configuration. It is selected under `Devices` → `Policies` in a watchOS policy via Add Configuration and created with Add details.



Similar to iOS devices, app availability is controlled under List type in the General section: either as a blocklist (Blocklist — The apps below are not allowed, the default for new configurations) or as an allowlist (Allowlist — The apps below are allowed). The apps are entered via Add in the Blocked apps or Allowed apps section below.

Allowlist and blocklist are only applied to supervised devices.

Allowlist (Permitted Apps)

The allowlist explicitly defines which apps are permitted to be available on the devices. Two additional options are available:

- Put all auto-deployed apps on the allowlist: Apps distributed to the devices' users via auto deployments are automatically added to the allowlist.
- Allow Local Secret Prompts (e.g., iCloud, Google login): The system dialog for local secret prompts is added to the allowlist so that such prompts are not blocked.

Blocklist (Blocked Apps)

The blocklist is used to hide or block specific apps on watchOS devices.

Required Apps

In the Required apps section, the applications that must be mandatorily installed on the devices are specified. Add offers the following sources (the same apply to the allowlist and blocklist):

- Relution App Store app: Selection of public apps with watchOS support from the Relution App Store, e.g. apps with Apps and Books licenses. There is no direct search in the public Apple App Store for watchOS; the apps must have been added to the Relution App Store beforehand.
- Manually add app: Entry of an app by Name and Internal name (bundle ID).

Native (self-uploaded) apps are not available for selection in watchOS policies, because Relution assigns them the iOS platform.

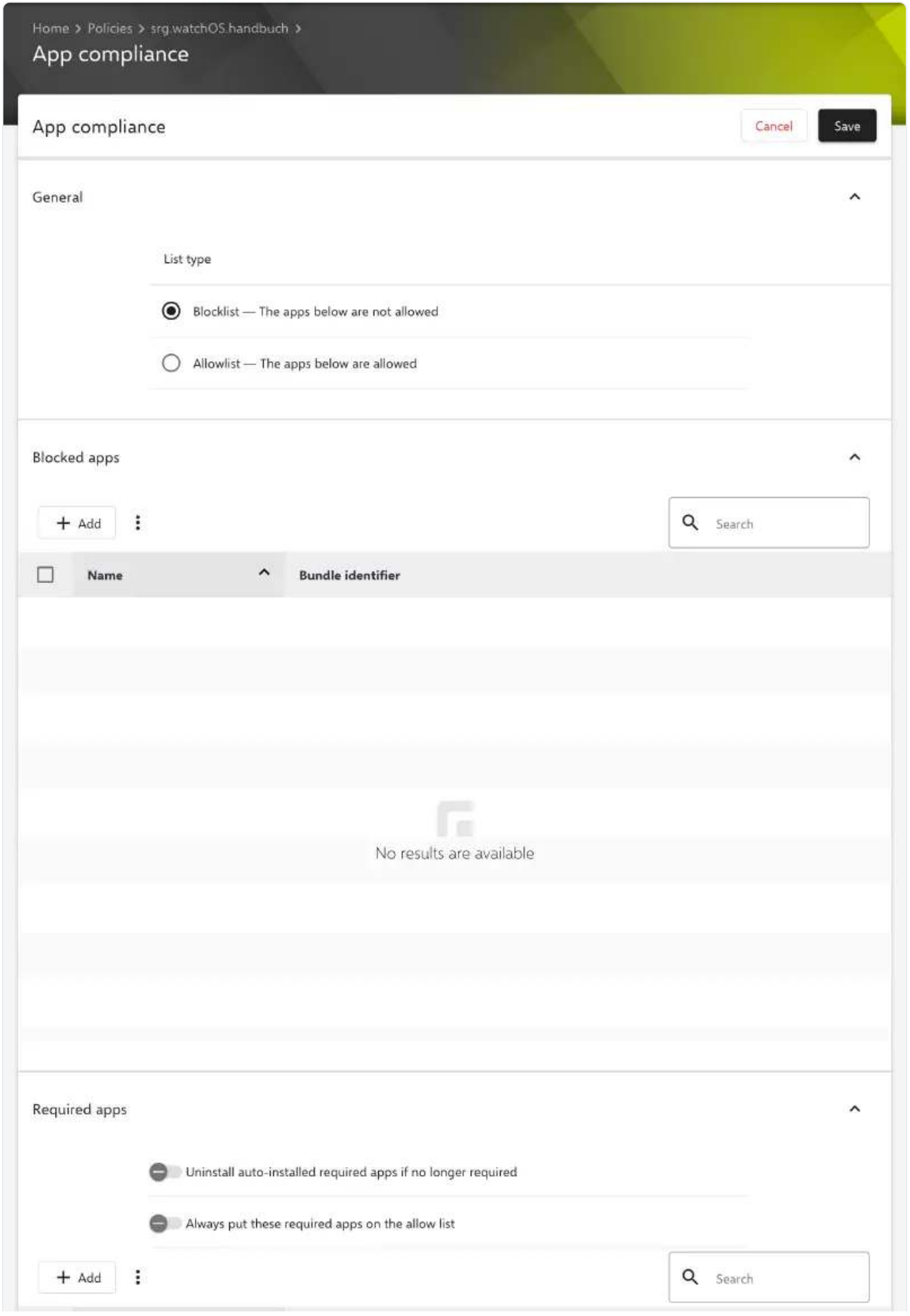
If a required app is not installed on the device, the device is considered noncompliant. The app is only actively installed if the checkbox in the Auto install column is selected; it is selected by default when an app is added. The VPP licenses and Available VPP licenses columns show the existing and the remaining free licenses per app.

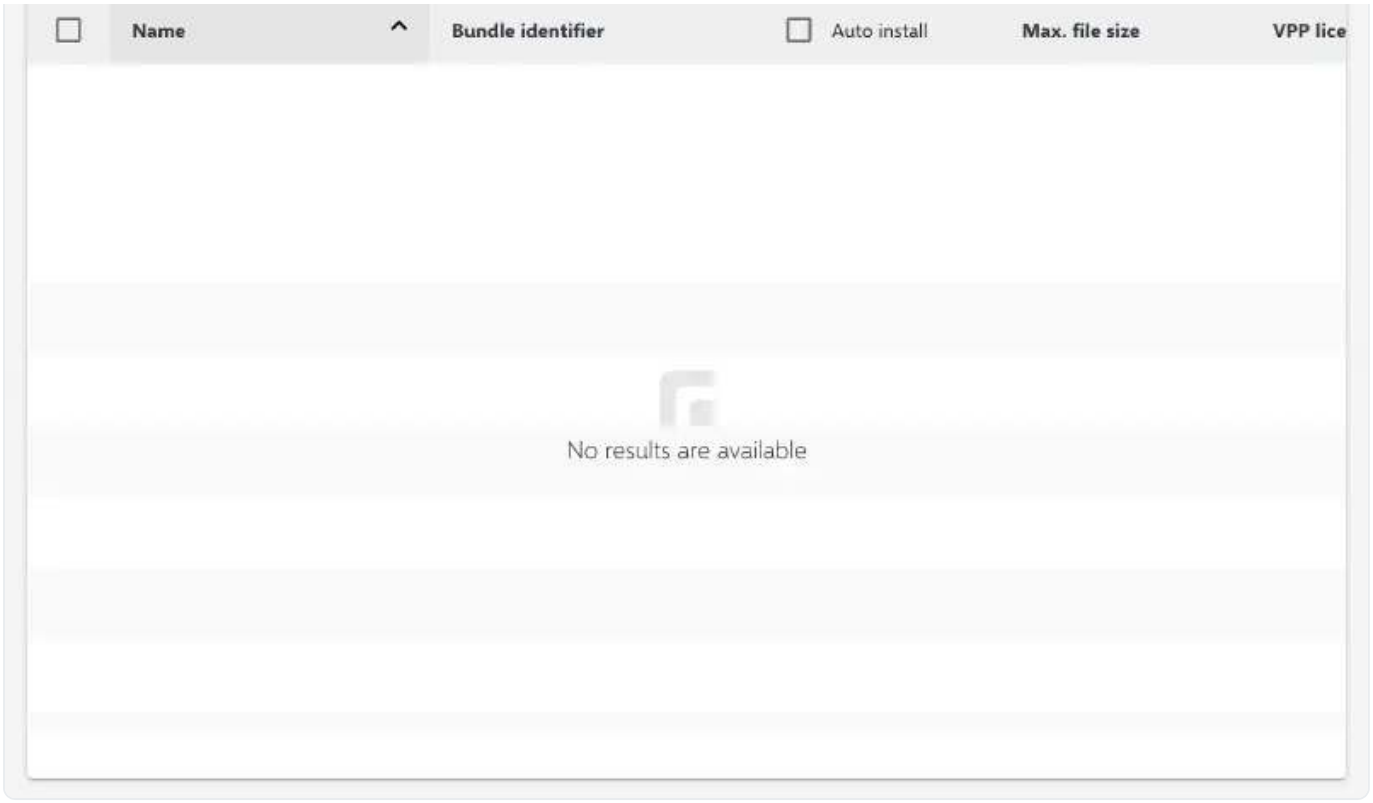
Two toggles are available above the list:

- Uninstall auto-installed required apps if no longer required: If an auto-installed required app is removed from the configuration, or the configuration is removed from the device, the app is uninstalled. The toggle is off for new configurations.
- Always put these required apps on the allow list: If this or another policy configures an allowlist for the device, the required apps are added to it.

Once the configuration is complete, it can be saved, published, and assigned to the corresponding devices.

For version 26.4.0


Home > Policies > srg.watchOS.handbuch >
App compliance
App compliance
Cancel
Save
General
List type
Blocklist — The apps below are not allowed
Allowlist — The apps below are allowed
Blocked apps
Add
Search
Name
Bundle identifier
No results are available
Required apps
Uninstall auto-installed required apps if no longer required
Always put these required apps on the allow list
Add
Search



For version 26.4.0

Education groups

Education groups are device groups of type Education. They bundle policies that are automatically applied to the devices of participating students for the duration of a lesson. The group and its policies are prepared in the portal; in Relution Teacher, they are selected as Configurations in the lesson template. This makes it possible to roll out even extensive MDM settings only while the lesson is running.

How it works

For an education group, only the policies are configured. Relution manages membership automatically through lessons: the devices of participating students are added when a lesson that uses this group as a configuration starts and removed when it ends. Devices cannot be assigned manually to this group type, and no filter is evaluated. The teacher's devices do not become members of the group.

- When the lesson starts, the student devices are added to the group and receive the linked policies.
- During the lesson, the assignment is updated as soon as students are added or removed. If the configurations of the running lesson are changed, the student devices are added to the newly selected education groups and removed from the deselected ones.
- When the lesson ends, the devices are removed from the group again and the policies no longer apply.

> Infrastructure policies such as Wi-Fi should not be distributed through an education group: they would be withdrawn from the devices when the lesson ends.

For version 26.4.0

Creating an education group

Education groups are created like other device groups under `Devices` → `Device Groups` using Add. Education is selected as the Group type. The desired policies are then assigned to the group. The Education type is only available with an Education or Free license.

> If an existing static or dynamic device group is later switched to Education, Relution removes all previous devices from the group when saving. The linked policies therefore no longer apply to these devices.

The name, description and linked policies are displayed in Relution Teacher. Meaningful names and descriptions therefore make the selection easier during lessons.

General information on device groups: Device groups →.

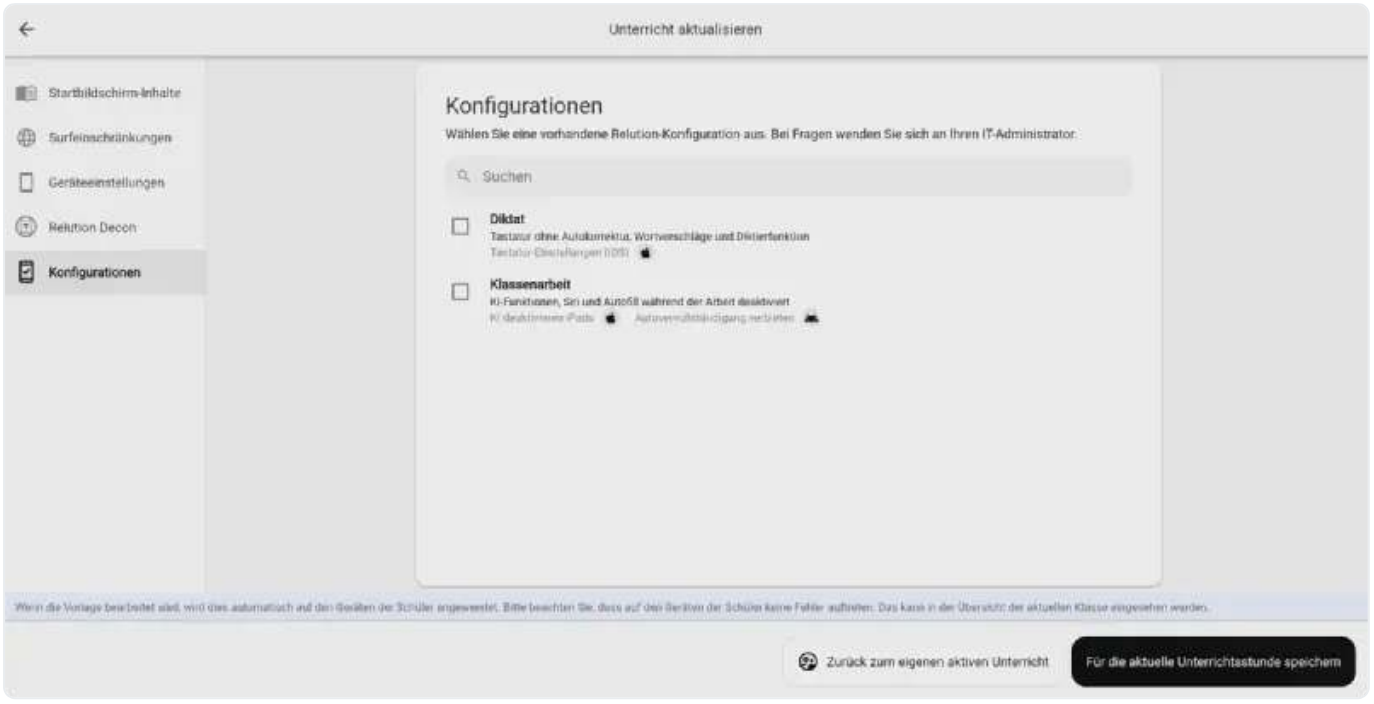
Permission for teachers

Which teachers can see and select configurations is controlled by the read permission `Education` → `Lesson Device Groups` in the role editor. It complements the `Education` → `Use Teacher App` permission; both are required to select configurations. Without this permission, no configurations are displayed in Relution Teacher. It is already included in the predefined roles that allow the use of the Teacher App. Custom roles do not receive it automatically; there, `Education` → `Lesson Device Groups` is added manually if required.

More on roles and rights: Permissions →.

Use in Relution Teacher

In the lesson template, the Configurations area lists the organization's education groups with their name, description and linked policies. One or more configurations can be selected. If no education group exists, the note No configurations available is displayed; the template can still be used as usual.



Details on the lesson template: Relution Teacher →.

Apple Classroom

Relution distributes the configuration for using the Classroom app to Apple devices managed by Relution (iPadOS / macOS). Apple Classroom is an app used in the education sector to enable teachers to control and monitor student devices during lessons.

Requirements

1. Two devices registered in Relution (Supervised).
2. At least two users.
3. The Apple Classroom app must be installed on one device (teacher).
4. A valid Education or Free license for Relution.

Network preparation

1. The devices must be on the same network if Classroom is to be used.
2. Client-to-client communication must be possible in the Wi-Fi network.
3. Port 3284: For sharing documents via Classroom.
4. Port 3285: For communication with the Classroom app.

For version 26.4.0

User preparation

1. At least two users are required (one teacher and one student).
2. Classes must be created under `Education` → `Classes`. This step can be automated by importing via an interface (e.g. LDAP or Apple School Manager); alternatively, users and classes can be imported via a CSV file. Relevant manual articles:
   - CSV import: Import users via CSV →
   - LDAP integration: LDAP configuration →
   - ASM import: Apple School Manager Import →
   - SchulConnex import: SchulConnex Import →
   - OneRoster: OneRoster Interface →
3. Teachers and students are added to the class either individually or via user groups, e.g. via the groups `UIT - Teacher` / `UIT - Student`. No specific group membership is required for Apple Classroom; what counts is only the entry as a teacher or student in a class. For the default groups `Teacher` / `Student` and their permissions in Relution, see Education function →.

Configuration

Relution distributes so-called `education configurations` to the devices. These configurations contain information about which classes and students can be controlled by which teachers. Classes that do not contain at least one teacher and one student are not included in the education configuration and therefore do not appear in Apple Classroom. In addition to the classes, an active ad-hoc lesson from Relution Teacher is included in the education configuration as a separate group, see Relution Teacher →.

In order for the distribution of the education configuration to be successful, users must be assigned to the devices. The assignment can be done either manually or via CSV file. Alternatively, users can be assigned during Automated Device Enrollment (ADE, DEP in the portal): in the DEP profile under `Devices` → `Profiles`, User authentication is set to Username + Password. The device is then assigned to the user who signs in during enrollment. Details: Profile for ADE →. If users are assigned this way, devices that are already enrolled must be reset (`deleted`) and then re-enrolled.

Shared iPads without an assigned user receive the education configuration via the classes stored in the Shared iPad settings configuration of a policy, see Class lists (Shared iPad) →.

Troubleshooting

Occasionally, individual or multiple users may be displayed as `offline` for the teacher. Possible causes and solutions:

1. Invalid or expired education configuration:
    - If the configuration is invalid, it must be reinstalled. To do this, the user must be removed from the class and reassigned.
    - If classes were created automatically via LDAP, the user must be removed from the device and reassigned. Note: Problems may occur when using dynamic device groups on a user basis.
2. Incorrect network configuration (ports or Wi-Fi networks):
    - If the required ports are closed or the devices are in different WLAN networks, connection problems may occur.
    - To check this, a mobile hotspot can be used to connect the devices to each other. If the devices are displayed as `online` in this environment, the network configuration must be adjusted accordingly.

For version 26.4.0

Apple School Manager import

The ASM Import Configuration enables Relution to create new users based on data from the Apple School Manager (ASM) or to synchronize existing users with the Managed Apple Accounts (Managed Apple ID in the portal) from the ASM. In addition, the classes from ASM can be imported.

The opposite direction, creating Managed Apple Accounts in ASM from the data in Relution, is described under SFTP Upload →.

Prerequisites

- A valid ADE token (Automated Device Enrollment, DEP token in the portal) within the organization where the configuration is to be created.
- Managed Apple Accounts that have been grouped into at least one class in the ASM (minimum of one student and one teacher).

Configuration

For version 26.4.0

1. Navigate to Settings: `Settings` → `Education` → `Apple School Manager Import Configuration`
2. Add a New Configuration: A new configuration is created via Add.
3. Enter the Provider Name: A unique name is entered under Provider name. The name cannot be changed after saving, because Relution uses it to match previously synchronized objects.
4. Select the DEP Account: Under DEP account, Select is used to choose the DEP account through which Apple School Manager is accessed. Without a DEP account, Check connection, Locations and Preview are not available, and the configuration cannot be saved.
5. Test the Connection: Check connection verifies whether a connection to Apple School Manager is possible with the DEP account.
6. Select Locations: Under Locations, one or more ASM locations are chosen for the import via Select. Only the classes of these locations are imported, together with the teachers and students who are members of one of these classes.
7. Preview Available Classes: Under Preview, Show displays the classes that will ultimately be imported.

In the global organization and in meta organizations, the Locations option does not exist. There, the configuration is first saved with the DEP account. Afterwards, the Map locations to organizations section in the Map objects to organizations area defines which ASM locations are imported into which organization. Without mapped locations, no synchronization takes place.

Synchronization Settings

The Synchronization settings area defines which objects Relution creates from ASM and what happens to objects that are no longer delivered by ASM.

Create New Relution Users

- Enabled by default.
- Relution creates a new user for every ASM user for whom no matching Relution user is found. The search uses the link from previous synchronizations, the Managed Apple Account and the matching rules enabled under Advanced.
- Matching users without a source system (e.g. created manually) or from the same ASM configuration are linked and taken over instead. They get the ASM configuration as their source system.
- Users of other source systems (e.g. LDAP) are not linked. If they have the same email address or the same username as the user to be created, creating the user fails (sync error Duplicate e-mail or Duplicate username).
- If the option is disabled, only existing users are linked. ASM users without a matching Relution user are not imported.

Update Managed Apple ID for Matching Relution User of Any Source System

- Disabled by default.
- Overwrites the Managed Apple ID field of a user from another source system (e.g. LDAP) if the ASM user can be matched to this user via one of the matching rules enabled under Advanced. The user's other data and source system remain unchanged.
- The option only applies to ASM users that were neither linked nor newly created, in practice only when Create new Relution users is disabled.

Synchronize Classes

For Version 26.4.0

- Enabled by default.
- Imports the classes of the selected locations from ASM and creates or updates them in Relution.
- Classes for which no synchronized teacher or no synchronized student exists in Relution are skipped (sync error Class members are missing).
- Recommended only in cases where:
  - No class data exists in Relution.
  - Manual class configuration in Relution is not planned.
  - No LDAP system is in use.
- Important: If classes are already synchronized via LDAP, this option should not be enabled.

Action When a User Is Removed in ASM

- Defines what happens to users of this configuration that are no longer delivered during a synchronization:
  - None (default): The users remain unchanged.
  - Deactivate: The users are deactivated in Relution.
  - Delete: The users are deleted in Relution.
- This applies to all users that have the ASM configuration as their source system, i.e. newly created users as well as linked users that previously had no source system (e.g. created manually).
- Users of other source systems (e.g. LDAP) whose Managed Apple Account was only updated remain unchanged. Their Managed Apple Account is not removed.
- If a synchronization does not deliver a single user, for example because of a connection problem or a misconfiguration, no users are deactivated or deleted.

Action When a Class Is Removed in ASM

- Specifies whether classes in Relution are deleted when they are removed from ASM: None (default) or Delete.
- If no classes are synchronized, this option has no effect.

Automatic Synchronization via Cron Expression

- Defines the frequency at which Relution automatically imports information from ASM.
- By default, the synchronization runs daily at 6 a.m. and 9 p.m. (`0 0 6,21 * * ?`).

Advanced

The Advanced area defines how ASM users are matched to existing Relution users and which ASM value is used as the username.

ASM User to Relution User Matching

- Defines the rules by which an ASM user is matched to an existing Relution user. Several rules can be active at the same time.
- Before these rules are applied, the synchronization always first looks for a Relution user that is already linked to the ASM user or has the same Managed Apple Account.
- The enabled rules are then checked in this order. The first matching rule applies:
    1. Match the ASM user's Managed Apple ID to the Relution user's email (default: enabled)
    2. Match the ASM user's email to the Relution user's email (default: disabled)
    3. Match the ASM user's name to the Relution user's username (default: disabled)
    4. Match the ASM user's first and last name to the Relution user's first and last name (default: disabled)
- Only Relution users of the same organization that have no source system or come from this ASM configuration are considered. Users of other source systems (e.g. LDAP) are not taken over. If Update Managed Apple ID for matching Relution user of any source system is enabled, the same rules (without the preceding check) determine for which user of another source system only the Managed Apple Account is updated.
- Note: If Create new Relution users is not enabled and none of the rules allows a match, no linkage will occur between the systems.

For version 26.4.0

ASM User to Relution User Mapping

- ASM user field to use as Relution user name specifies which value from ASM is used as the username in Relution. The options are Name (default), Managed Apple ID and E-mail.
- Note: With every synchronization, the username as well as the first and last name are taken over from ASM for matched users. The email address in Relution is replaced by the Managed Apple Account, and the user is activated.

Synchronization

The synchronization runs automatically according to the configured schedule. It is started manually in the list of configurations via Sync in the context menu, or in the detail view of a configuration via the Sync icon.

Synchronized teachers and students are added to the respective default group `Teacher` or `Student` of their organization. For more on these groups, see Education function →.

The detail view shows the synchronization results separately for Users and Courses, including Next planned synchronization, Last completed and Success. The Sync Errors column shows the individual errors, e.g. Duplicate e-mail, Duplicate username, Class members are missing or Roster object synchronization failed.

For version 26.4.0

Link Organization

Before Android devices can be enrolled via Android Enterprise, the Relution organization must first be linked to a Google organization. This linking allows organizations to have full control over their Android devices and manage them effectively; including configuration, app management, and security policies.

Relution organization registration for Android Enterprise

For this purpose, an appropriate Google account is created in the Relution portal under `Settings` → `Device platform specific` → `Android Enterprise`:

- Via Sign up now, an existing Google account is selected or a new one is created
- When creating a new Google account, a choice is made between For myself or For my company, and the linked agreement to Google Managed Play Store is read
- After accepting the agreement, the I have read and agree to the Google Play Agreement field is confirmed and Confirm is clicked
- Clicking Complete Registration returns to the Relution portal

On return, the link is saved automatically; no further save step is required. The General tab then shows the Organization ID and the Enterprise Type. Display name, primary color and logo can optionally be adjusted in the Account information tab, see Account information →.

For version 26.4.0

> Only non-managed Google accounts can be used to link to the Google Managed Play Store. Managed accounts from organizations for employees are not possible.

> The new Multi EMM feature is now available. This feature will now allow an IT admin to bind multiple EMMs to their managed Google domain account. Google Multiple EMM Provides →

To remove an existing link including the consequences, see Delete/Remove organization →.

Organization ID

In Relution, every tenant / organization should be linked to its own Google account. This ensures that every tenant receives a unique Organization ID from Google and can be managed accordingly.

For Relution organizations that were linked to Google Enterprise several years ago, the enterprise type often still shows GooglePlay Enterprise account. For newly linked organizations, Google now automatically creates a Managed Google domain with its own unique Organization ID. For older organizations, Google offers an upgrade from GooglePlay Enterprise account to Managed Google domain. For this purpose, Relution shows a notice and the Upgrade button under `Settings` → `Device platform specific` → `Android Enterprise` in the General tab (permission to edit the Android Enterprise settings required). The button opens the upgrade wizard provided by Google in a new tab; once it is completed, Relution updates the enterprise type automatically (see also the Upgrade enterprise → section).

Upgrade from GooglePlay Enterprise account to managed Google domain

> Tested and confirmed by Google (as of 08/2026): the upgrade can be carried out without risk – even if several Relution organizations are linked to the same Google Play Enterprise account and the same Organization ID.

- Risk during the upgrade: no risks are known. The process has been tested successfully and runs without errors.
- Effect on Android devices that are already enrolled: they are neither reset nor otherwise changed by the upgrade.
- Google Play Enterprise account linked multiple times: even if a Google Play Enterprise account is linked to several Relution organizations that share the same Organization ID, the upgrade is possible without problems. A separate upgrade of individual Relution organizations does not exist; the upgrade automatically applies to all linked Relution organizations (see Scope of the upgrade).
- Recommendation: the upgrade to a managed Google domain should be carried out.
- Scope of the upgrade: the upgrade applies to the entire Google Organization ID and thus to all Relution organizations linked to it. It is therefore sufficient to trigger the upgrade once via one of the linked Relution organizations.

Do not split a Google Organization ID by disconnecting individual Relution organizations

For version 26.4.0

> If several Relution organizations are linked to the same Google Organization ID, none of these connections may be removed in the Account settings tab via Remove Android Enterprise in order to split the Organization ID afterwards. As described in the article Delete/Remove organization →, the affected Relution organization loses control over its Android Enterprise devices regardless of the selected option. With the options Remove enterprise and devices known to Relution and Remove enterprise and devices, all existing enrollments of the affected Relution organization are also irrevocably lost and the devices are reset. The Remove enterprise and devices option additionally deletes devices that Relution does not know in this organization, i.e. also devices of the other Relution organizations with the same Organization ID. Restoring the connection afterwards to regain control over the devices is not possible.

For a permanently unique assignment between Relution organization and Google Organization ID, only new Relution organizations should instead be linked, each with its own new Google account.

Settings of the linked organization

After linking, the `Settings` → `Device platform specific` → `Android Enterprise` page is divided into the tabs General, Managed Google Play, Account information, Enrollments and Account settings. Changes require permission to edit the Android Enterprise settings.

Account information

The Account information tab contains two areas:

- Appearance: Enterprise Display Name and Primary color (hex color code, e.g. `#ffffff`) are mandatory and are applied with Save. An Organization logo in JPEG or PNG format is applied directly after uploading. Relution transfers this information to the Android Enterprise at Google.
- Contact information: shows the information stored at Google in read-only form, divided into Notification contact (email), Data protection officer and EU representative (each with name, email and phone number). According to the notice in the portal, it is edited at play.google.com/work/adminsettings →. The area only appears if Google provides contact information.

Terms and conditions

In the Enrollments tab, the Terms and conditions area maintains texts that Relution transfers to the Android Enterprise at Google. Each entry consists of Header and Content. When adding or editing, a separate tab is available for each language, in which both fields are mandatory; the text of the default language serves as the default text. The order of the entries can be changed by drag and drop. Changes are applied with Save.

Zero-Touch

Also in the Enrollments tab, Relution embeds Google's zero-touch view in the Android Enterprise Zero Touch area, see Zero Touch Enrollment →.

Repair signup

New in 26.5

In the Account settings tab, the Repair signup area is available above Remove Android Enterprise. According to the notice in the portal, it serves to regain control of the devices if Google has removed the binding to the Android Enterprise. The registration with Google is run through again without removing the existing link beforehand.

For Version 26.4.0

Before starting, it must be checked whether the displayed Organization ID matches the one at Google:

- GooglePlay Enterprise account: at play.google.com/work →
- Managed Google domain: at admin.google.com → under `Devices` → `Mobile and endpoints` → `Settings` → `Third-party integrations`

Start redirects to the registration with Google. For a managed Google domain, sign-in is restricted to this domain. On completion, Relution checks whether the signed-in enterprise matches the previously connected one; if the Organization ID differs, the repair is aborted with an error message.

Enrollment types

There are three different types of enrollment available for Android Enterprise. Each has special functionalities suitable for specific use cases.

Enrollment type	Factory reset required	Personal use	Administrator access
Managed Device →	required	not possible	full access to the entire device
Personal profile (COPE) →	required	possible in the personal profile	full access to the device, no insight into the personal profile
Work profile / BYOD →	not required	possible on the rest of the device	no access to private areas of the device

For version 26.4.0

Managed Device

The Managed Device enrollment type is suitable, for example, for organizations or schools to hand over devices to users who use them exclusively for official or school activities.

- Administrator access: full access to the device, including insight into the list of installed apps and the ability to reset the device to factory settings.
- Requirement: the device must be reset to factory settings before it is commissioned.
- Restriction: no personal profile, the device is intended exclusively for work use. Relution does not automatically prevent additional accounts, such as a private Google ID, from being added. The Disable adding and removing accounts option in the Restrictions → configuration is available for this purpose.

Details on setup: Managed Device →

Managed Device with Personal Profile (Company Owned, Personally Enabled COPE)

The enrollment type is the counterpart to the work profile and allows devices of an organization to be issued to users who may also use them for private purposes.

- Personal profile: users register their private GoogleID there and install their own apps; private and company-related data are strictly separated.
- Administrator access: full access to the device, but no insight into the personal profile (e.g. no view of installed apps or activated settings).
- Factory reset: required before the device is commissioned; a later factory reset performed by administrators deletes both private and company-related data completely.

Details on setup: Personal profile →

Work Profile / BYOD

The Work Profile enrollment type is the right choice for the Bring Your Own Device (BYOD) approach: users provide their private device, on which the organization sets up a work profile.

- Requirement: no reset of the device is necessary.
- Usage: the mail app or other apps of the organization can, for example, be made available within the work profile; private and organization-related data are strictly separated.
- Administrator access: no insight into installed private apps, no access rights to functions or settings of the private device.
- Removal: if the work profile is removed, only the organization-related data is deleted — private data is retained.

Details on setup: Work profile / BYOD →

For version 26.4.0

Enrollment options

When an enrollment is created under `Devices` → `Enrollments`, the form shows further options for the Android Enterprise platform in addition to Type and Ownership. They are available for all three enrollment types; restrictions are noted where they apply.

> Relution includes Language, Allow cellular enrollment, Keep system apps enabled and the settings in the WiFi area exclusively in the QR code shown for Managed device and Personal profile under `Enrollment information` → `Using QR Code`. The DPC identifier, the KME Custom JSON and the Android Enterprise Zero Touch custom JSON do not contain them. For the Work profile, the QR code only contains the link to the enrollment.

Authentication, Multi-use enrollment and Allow cellular enrollment cannot be changed after saving. According to a notice in the form, every change to an existing Android Enterprise enrollment recreates the registration on Google's servers; the previous QR code and DPC identifier become invalid as a result.

Authentication

The Authentication selection field in the Assignment section defines whether a user has to sign in during enrollment:

- Not required (default): the enrollment takes place without sign-in.
- Using Relution Companion app (supports single-use & expiration): the Relution Companion app requires the user to sign in during enrollment. Multi-use enrollment and Valid until remain available.
- Using Android's built-in app (enforces multi-use): sign-in takes place without the Companion app during device setup via the Relution login page. If exactly one Relution user has the email address of the account signed in to Google, this user is signed in automatically; otherwise the login page appears. If a user with an email address is assigned to the enrollment, it is pre-filled with this user's email address, otherwise with that of the Google account. The enrollment is assigned to the signed-in user, with Relution creating a separate single-use copy of the enrollment for each device. The form hides Multi-use enrollment and Valid until.

The sign-in flow via Android's built-in app is only used if the Show Google work account sign-in option is enabled as well. This option is only offered for the Managed device type and requires a managed Google domain, see Google Work-Account-Setup →. Enrollments with this option can always be used for multiple devices and do not expire.

Expiration

In the Expiration section, Multi-use enrollment defines whether the enrollment can be used for multiple devices. After the date set under Valid until, the enrollment can no longer be used; the default is a date seven days after creation. With the Using Android's built-in app (enforces multi-use) authentication, the section is not shown.

Compliance

The Compliance section contains the following options:

- Always require a device password (enabled by default): a device password is required even without an explicit password policy. For this purpose, Relution adds a device password requirement to the enrollment's default policy, as well as a compliance rule that disables apps as long as no password has been set.
- Allow cellular enrollment: setup may take place via mobile data. Relution adds a corresponding entry to the QR code.
- Language: the selected language is included in the QR code as the language for device setup. Without a selection, the entry is omitted.
- Keep system apps enabled: non-vital system apps remain enabled after enrollment, see Managed Device →.

For version 26.4.0

WiFi

In the WiFi area, a network for device setup can be stored:

- Connection section: The network's SSID, This network is hidden, Encryption type (None / Open, WEP or WPA/WPA2 PSK) and, for WEP and WPA, the Password.
- Proxy type section: None, Manual with Host, Port and Bypass proxy for (list of addresses that should not be routed through the proxy) or Automatic configuration with PAC URL (address of the PAC file).

Relution only includes WiFi and proxy in the QR code if The network's SSID is filled in. A restriction applies to enrollment via NFC, see Enroll devices via NFC →.

Agreements

In the Configuration section, Agreements can be selected that were created under `Settings` → `General` → `Agreements`. Relution provides their texts to the device during enrollment. The selection is only shown to users with read permission for agreements.

Managed Device

The Managed Device enrollment type is suitable, for example, for organizations or schools to hand out devices to users. Administrators have full access to the devices and can, for instance, view the list of installed apps and reset the devices to factory settings. A factory reset is necessary for commissioning. Relution does not automatically prevent additional accounts, such as a private Google ID, from being added. The Disable adding and removing accounts option in the Restrictions → configuration is available for this purpose. As a rule, this enrollment type is used for company-owned devices that are provided to employees or students to be used exclusively for professional or school activities (no private use).

> The Relution organization must be linked to a Google organization to enroll Android devices via Android Enterprise.

Creating an Enrollment in Relution

- Under `Devices` → `Enrollments`, Add is clicked.
- Android Enterprise is selected as the platform and, under Type, the Managed device icon (the name appears as a tooltip; preselected by default).
- The ownership would be COD (Company Owned Device) in this case.
- A device name is assigned and the enrollment is saved.

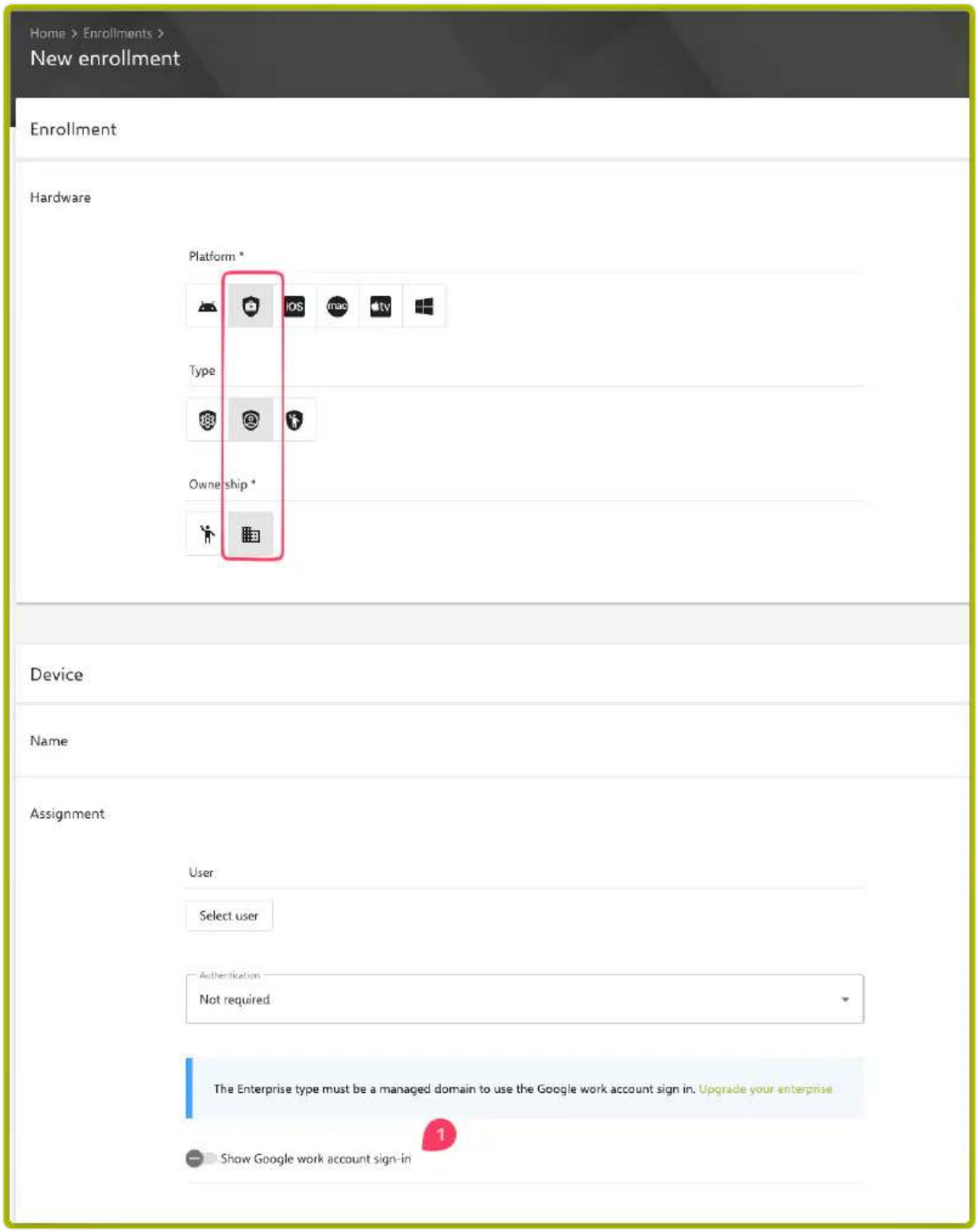
> Starting with Relution 5.33, it is possible to keep pre-installed system apps such as Samsung Internet or other 3rd party apps. For this, there is the switch Keep system apps enabled during enrollment. Conversely, unwanted apps must be blocked in the Manage apps configuration.

For version 26.4.0

Ownership is a mandatory field and is applied to the device during enrollment. Together with the settings under `Settings` → `Device Management` → `Enrollment`, it determines which device actions are allowed (Wipe device, Lock device, Locate device, Reset lock passcode) and whether the ownership can still be changed after enrollment. With COD, all of these actions are allowed by default, and the ownership can be changed afterwards.

Google Work-Account-Setup

During enrollment, the option Show Google work account sign-in is available. When enabled, the device is still set up using the enrollment QR code. After scanning, the user signs in with their Google work account (Google Workspace). If Using Android's built-in app (enforces multi-use) is additionally selected under Authentication, Relution signs the user in automatically based on the email address of the Google account; if this fails, the Relution login page is displayed. This assigns the device to a named Relution user, see Enrollment options →. Enrollments with this option can always be used for multiple devices and do not expire.



For details on the Work Account policy configuration, see Work Account Setup →.

Prerequisite: managed domain

Android Enterprise distinguishes between two enterprise types:

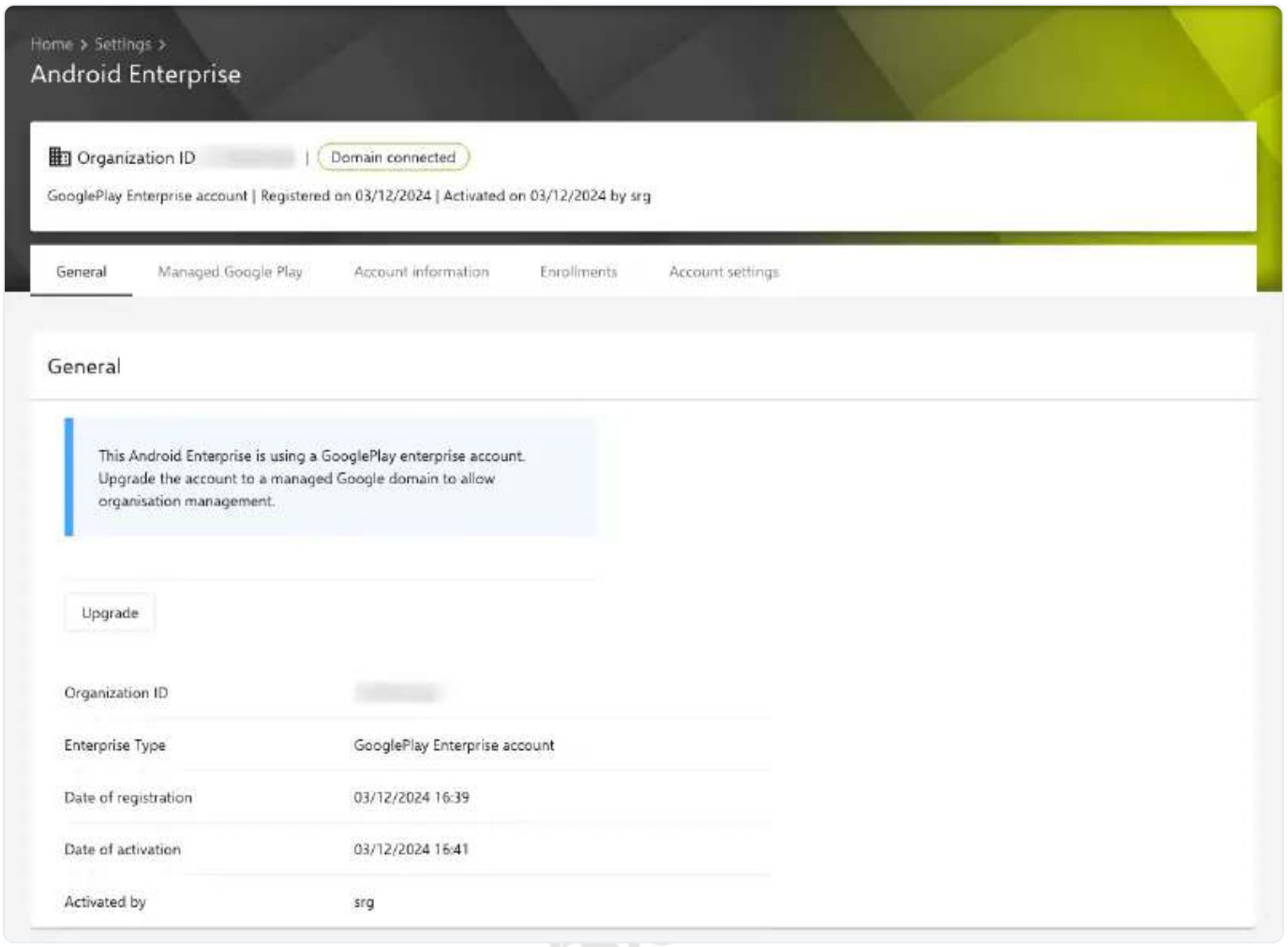
Enterprise type	Setup	Google Work-Account-Setup
Managed Google Play Accounts	Default – registered with any Google account. Users automatically receive a managed Google account during enrollment.	Not available
Managed domain	Requires an active Google Workspace license with a verified company domain. Users sign in with their existing `@company.com` account.	Available

If the Relution organization was initially linked using a personal Google account (Managed Google Play Accounts), the form shows the following notice for the Managed device type above the Show Google work account sign-in switch:

“The enterprise type must be a managed domain to use the Google Work Account sign in.”

Upgrade enterprise

For version 26.4.0



The Upgrade your enterprise link opens the `Settings` → `Android Enterprise` page. There, the Upgrade button on the General tab launches a Google-provided wizard in a new browser tab that links the existing Android Enterprise to the organization's Google Workspace. The link is only shown to users with read access to the Android Enterprise settings; all other users see a notice to contact an administrator for the upgrade instead. The following prerequisites must be met:

- An active Google Workspace license (Business, Enterprise, Education, etc.)
- Administrator access to the Google Workspace Admin Console
- A company domain verified in Google Workspace

After a successful upgrade, the Show Google work account sign-in option becomes available in the enrollment. In addition, user authentication must be enabled for the connected enterprise in the Google Admin Dashboard (admin.google.com). If it is not enabled, the enrollment form shows the following notice:

"The connected Enterprise Account needs to enable User Authentication. This can only be done in the Admin Dashboard at admin.google.com."

Once both prerequisites are met, users can enroll using their existing `@company.com` accounts.

Necessary Information for Performing the Enrollment

In the created enrollment, a QR code is displayed under Enrollment Information, which can be used to enroll Android devices. This can also be accessed via the QR Code column in the Enrollments overview. Alternatively, the device can be enrolled via the Using DPC identifier tab, see Enroll devices without camera →.

Resetting Android Devices

To start the enrollment for Managed Device, Android devices must first be reset to factory settings.

Welcome Screen on the Devices

A spot on the welcome screen is tapped 6 times quickly.

Scanning the Relution QR Code

The devices will then display a prompt to scan the QR code from the created enrollment.

For version 26.4.0

Completing the Enrollment

The further instructions are followed to set up the devices. After successful enrollment, administrators have full access to the managed devices.

Actions

- Install app from the Google Play Store
- Remove app
- Install app from the Relution Store
- Clear app data (Android 9 and later)
- Send file to device
- Remove eSIM
- Add eSIM
- Reset device to factory state
- Shutdown device
- Restart device
- Locate device →
- Fully lock device
- Update device information
- Enable lost mode (Android 11 and later)
- Disable lost mode
- Send message
- Reset password

Policy Configuration

For version 26.4.0

The available configurations include the following:

- Work Account Setup →
- Manage apps →
- Advanced keyguard feature management →
- Advanced security overrides →
- Device password →
- Global proxy →
- Kiosk Mode →
- Runtime permission management →
- Play Store Management →
- Restrictions →
- Samsung Classroom Management →
- Location mode →
- System updates →
- Wi-Fi →

All configurations are described in the Overview → article.

Personal profile

The enrollment type Company Owned, Personally Enabled (COPE) allows to issue devices of an organization to users who are allowed to use them also for private purposes. Users have the option of logging their private GoogleID into a private profile and installing their own apps. Private and organization-related data is strictly separated on the devices. Administrators have no insight or access to the private profile and cannot, for example, see which apps are installed in the private profile and which settings are activated. However, administrators have full access to the devices and can, for example, perform a factory reset, which deletes all data, both private and work-related. A factory reset is required to put the operating mode into operation.

Relution organization must be associated with a Google organization to enroll Android devices via Android Enterprise.

Create enrollment in Relution

- Under `Devices` → `Enrollments`, Add is clicked
- Android Enterprise is selected as the platform and, under Type, the Personal profile icon (the name appears as a tooltip; Managed device is preselected by default)
- Ownership in this case would be COD (Company Owned Device)
- A device name is assigned and the enrollment is saved

Ownership is a mandatory field and is applied to the device during enrollment. Together with the settings under `Settings` → `Device Management` → `Enrollment`, it determines which device actions are allowed and whether the ownership can still be changed after enrollment. With BYOD, Wipe device, Locate device and Reset lock passcode are disabled by default, and the ownership cannot be changed afterwards. COD is therefore the appropriate choice for devices with a personal profile.

For version 26.4.0

Necessary information to perform the enrollment

In the enrollment created, a QR code is displayed under Enrollment information that can be used to enroll Android devices. This can also be accessed via the QR Code column in the Enrollments overview. Alternatively, the device can be enrolled via the Using DPC identifier tab, see Enroll devices without camera →.

Reset Android devices

To start enrollment for managed device with personal profile, Android devices must first be reset to factory defaults.

Welcome screen on devices

The welcome screen is tapped 6 times quickly.

Scan Relution QR Code

The devices will then display a prompt to scan the QR code from the enrollment created earlier. The further instructions are followed to set up the managed devices.

Container personal profile on COD devices

After successful enrollment, two separate areas personal and work are available on the user interface of the Android devices, which can be switched between at any time.

Actions

The available actions include the following:

- Enterprise wipe (Android 8 and later): removes the work profile and all policies; apps and data of the personal profile are preserved
- Wipe device
- Refresh device info

All actions are described in the Overview → article.

For version 26.4.0

Policy configuration

The available configurations include the following:

- Manage apps →
- Work profile passcode →
- User messages →
- Display →
- Advanced keyguard feature management →
- Advanced security overrides →
- Device password →
- Global proxy →
- Wallpaper →
- Kiosk Mode →
- Runtime permission management →
- Personal Usage →: settings for the personal profile
- Play Store Management →
- Restrictions →
- Samsung Classroom Management →
- Location mode →
- System updates →
- Wi-Fi →

All configurations are described in the Overview → article.

The Enable Factory Reset Protection (FRP) option in the Restrictions configuration can block factory resets via the Android device settings. Resetting via the recovery menu remains possible. If the device has no network connection, Relution cannot send a reset action to the device. Further details can be found in the Restrictions → article.

For version 26.4.0

Work profile / BYOD

The enrollment type Work Profile is the right choice for the Bring Your Own Device (BYOD) approach. Users can provide their private devices to have a Work Profile installed on them by the organization. No resetting of the devices is necessary for the commissioning of a work profile. The mail app or other apps of the organization can then be made available within a work profile. Private and organization-related data are strictly separated on the devices. In addition, administrators have no insight into installed apps and no access rights to functions or settings on private devices. When a work profile is deleted, all organization-related data is removed from the devices, whereas all private data is retained.

Relution organization must be associated with a Google organization to enroll Android devices via Android Enterprise

Create enrollment in Relution

- Under `Devices` → `Enrollments`, Add is clicked
- Android Enterprise is selected as the platform and, under Type, the Work profile icon (the name appears as a tooltip; Managed device is preselected by default)
- Ownership in this case would be BYOD (Bring Your Own Device)
- A device name is assigned and the enrollment is saved

Ownership is a mandatory field and is applied to the device during enrollment. It has no effect on how the work profile is set up. Together with the settings under `Settings` → `Device Management` → `Enrollment`, however, it determines which device actions are allowed (Wipe device, Lock device, Locate device, Reset lock passcode) and whether the ownership can still be changed after enrollment. With BYOD, wiping, locating and resetting the passcode are disabled by default, and the ownership cannot be changed afterwards. Locking the device is allowed by default.

For version 26.4.0

Necessary information to perform the enrollment.

In the enrollment created, a QR code is displayed under Enrollment information to enroll Android devices. This can also be called up via the QR Code column in the Enrollments overview.

The link must be opened with Google Chrome, other browsers such as Samsung Browser only show a white page

Complete enrollment

The newly created QR code is scanned with the camera app. The steps shown are then followed to complete the enrollment process.

Container work profile on the private devices

After successful enrollment, two separate areas personal and work are available on the user interface of the Android devices, which can be switched between at any time.

> No other work should be done on the device while the work profile is being created.

Actions

- Install apps from the Google Play Store
- Remove apps
- Clear app data (Android 9 and later)
- Send file to device
- Remove eSIM
- Add eSIM
- Shutdown device
- Locate device (disabled by default for ownership BYOD)
- Lock device completely
- Update device information
- Request device info (Android 13 and later)
- Send message
- Reset lock passcode (disabled by default for ownership BYOD)
- Select Play Store app from the Relution Store

For Version 26.4.0

Policy configuration

The available configurations include the following:

- Always-On VPN →
- Manage apps →
- Work profile passcode →
- Compliance enforcement →
- Advanced security overrides →
- Device password →
- Runtime permission management →
- Play Store Management →
- Restrictions →
- Samsung Classroom Management →
- Default Applications → (Android 16 and later)
- StrongSwan Restrictions →
- StrongSwan VPN Profile →
- Work account setup →
- Certificate →

All configurations are described in the Overview → article.

Unavailable configurations

- User messages →
- Display →
- Advanced keyguard feature management →
- Global proxy →
- Wallpaper →
- Kiosk Mode →
- Personal Usage →
- Location mode →
- System updates →
- Wi-Fi →

For version 26.4.0

Knox Mobile Enrollment

Knox is a security platform for Samsung devices that enables centralized and secure management of mobile endpoints in enterprise environments. The platform supports efficient device provisioning, configuration, and protection.

Samsung Knox Mobile Enrollment (KME)

Samsung Knox Mobile Enrollment (KME) enables automated provisioning of Samsung devices for management in a Mobile Device Management (MDM) system such as Relution.

After a device is powered on for the first time and connected to the internet, the setup process starts automatically. Even after a factory reset, the device automatically re-enrolls into the assigned MDM system.

KME provides functionality comparable to Apple's Device Enrollment Program (DEP).

Requirements

1. The Samsung device must be Knox-capable. A list of supported devices is available on the Samsung Knox support page →.
2. Samsung devices can be registered in the KME program directly by authorized resellers using the device serial number.
3. Devices not purchased through authorized resellers can be added manually:
    - by scanning a dedicated QR code during device setup
    - or by using the Knox Mobile Deployment app on an additional Samsung device

The KME program is provided free of charge after registration in the Samsung Knox Portal. Samsung Knox Portal →

> The Knox Mobile Enrollment configuration available in the Relution settings must not be used. This configuration is outdated, intended exclusively for Android Legacy, and only supported up to Android version 10.
>
> Instead, the following guide applies: Link organization →

Combining KME with Android Enterprise

Samsung Knox Mobile Enrollment can be combined with the following Android Enterprise enrollment types:

- Managed Device
- Managed Device with Personal Profile (COPE – Company Owned, Personally Enabled)

For version 26.4.0

Preparing Enrollment in Relution

1. Navigation to `Devices` → `Enrollments`.
2. Selection of Add.
3. Settings:
    - Platform: Android Enterprise
    - Type: Managed device or Personal profile (icon buttons; the label appears as a tooltip)
    - Ownership: COD (Corporate Owned Device); the enrollment cannot be saved without a selection
4. Activation of the Multi-use enrollment option in the Expiration section.
5. Selection of a long-term date under Valid until (e.g., 100 years).
6. Saving the enrollment.

Since these steps require Multi-use enrollment and Valid until, Authentication remains set to Not required or Using Relution Companion app (supports single-use & expiration). With Using Android's built-in app (enforces multi-use), the form hides both fields. Settings for WiFi, Language and Allow cellular enrollment are not contained in the KME Custom JSON. If the enrollment is changed later, Relution recreates the registration on Google's servers; the JSON stored in the Knox Portal must then be replaced. Details: Enrollment options →

After saving:

- Opening the created enrollment.
- Switching to `Enrollment information` → `Using DPC identifier`.
- Copying the provided KME Custom JSON for later use in the Knox Portal.

For Version 26.4.0

Creating a KME Profile in the Samsung Knox Portal

1. Sign-in to the Samsung Knox Portal →.
2. Navigation to Profiles.
3. Selection of CREATE PROFILE.

Profile Settings

- Assignment of a profile name and description.
- Activation of EMM.
- Deactivation of Knox Service Plugin.
- Continuation with Next.
- Completion of the contact information.

EMM Information

- Under Select your EMM (required), selection of: Other
- Entry in Link to agent APK (required):

```
https://play.google.com/managed/downloadManagingApp?identifier=setup
```

- Continuation with Next.
- Insertion of the DPC identifier shown in Relution under `Enrollment information` → `Using DPC identifier` into DPC Extras. The KME Custom JSON already contains the DPC identifier.
- Insertion of the previously copied JSON into Custom JSON Data.
- Completion with Create.

Optional: Creating a QR Code

A QR code can be created for device enrollment or for adding new devices to KME.

Procedure:

1. Selection of ADD A QR CODE.
2. Activation of Also allow QR Code enrollment for devices not uploaded by a reseller if devices were not pre-registered by a reseller.
3. Optional configuration of Wi-Fi settings to simplify bulk device provisioning.
4. Completion with ADD.

To use the QR code, a plus sign (+) is drawn on the Samsung welcome screen. This opens the QR code scanner.

Linking Devices to the Profile

For version 26.4.0

If no QR code is used:

1. Navigation to Devices in the Knox Portal.
2. Selection of the desired devices.
3. Selection of `Actions` → `Configure Devices`.
4. Powering on the devices.

Zero Touch Enrollment

Android Zero-Touch Enrollment is a service that enables organizations to deploy large numbers of Android devices automatically — without requiring additional manual configuration by administrators or end users.

Once a device is unboxed, powered on, and connected to the internet, it is automatically configured with predefined corporate policies, apps, and settings. This allows for fast, standardized, and secure provisioning of Android devices in enterprise environments.

Android Zero-Touch Enrollment

The functionality of Android Zero-Touch Enrollment is comparable to Knox Mobile Enrollment (KME) →.

In the Zero-Touch portal, a configuration is created first and then assigned to the desired devices from the device list.

> Devices for Android Zero-Touch Enrollment (ZTE) cannot be added manually by end customers. Adding devices to the Zero-Touch portal must always be handled by an authorized reseller or OEM.

For version 26.4.0

Preparing Enrollment in Relution

1. Navigation to `Devices` → `Enrollments`.
2. Selection of Add.
3. Settings:
    - Platform: Android Enterprise
    - Type: Managed device or Personal profile (icon buttons; the label appears as a tooltip)
    - Ownership: COD (Corporate Owned Device); the enrollment cannot be saved without a selection
4. Activation of the Multi-use enrollment option in the Expiration section.
5. Selection of a sufficiently late date under Valid until.
6. Saving the enrollment.

Since these steps require Multi-use enrollment and Valid until, Authentication remains set to Not required or Using Relution Companion app (supports single-use & expiration). With Using Android's built-in app (enforces multi-use), the form hides both fields. Settings for WiFi, Language and Allow cellular enrollment are not contained in the Zero-Touch JSON. If the enrollment is changed later, Relution recreates the registration on Google's servers; the JSON stored in the Zero-Touch configuration must then be replaced. Details: Enrollment options →

After saving:

- Opening the created enrollment.
- Switching to `Enrollment information` → `Using DPC identifier`.
- Copying the provided Android Enterprise Zero-Touch custom JSON to the clipboard.

Zero-Touch in Relution

In addition to the Zero-Touch Portal →, Relution embeds Google's zero-touch view under `Settings` → `Device platform specific` → `Android Enterprise` in the Enrollments tab, in the Android Enterprise Zero Touch area. The view is loaded in the portal language and is pre-set to Android Device Policy as DPC. The functions it offers are determined by Google.

Creating a Zero-Touch Profile

1. Sign-in to the Zero-Touch Portal →.
2. Navigation to Configurations.
3. Selection of the + symbol in the top section.
4. Assignment of a name for the configuration.
5. Selection of Android Device Policy under EMM DPC. (If multiple entries are listed, any of them may be used.)
6. Insertion of the previously copied JSON into the DPC extras field.
7. Completion of the remaining fields as required.
8. Completion with ADD.

Linking Devices and Configuration

1. Navigation to Devices in the Zero-Touch portal.
2. Assignment of the desired configuration to the respective devices.
3. Powering on the devices.

Scanning a QR code is not required. When powered on for the first time, Android devices automatically contact the Zero-Touch service, which forwards the enrollment request to Android Enterprise and subsequently to Relution.

For version 26.4.0

Enroll devices via NFC

With the Relution Agent, Android Enterprise devices can be enrolled easily via NFC (Near Field Communication).
Both devices must support NFC, and the source device (enrollment device) must already be enrolled in Relution.

The target device can only be enrolled as Fully Managed or with a Personal Profile. Android Work Profile or Legacy enrollment is not possible.

Setup

1. In Relution, an enrollment is created under `Devices` → `Enrollments` for the platform Android Enterprise with the type Managed device or Personal profile (not Work profile).

   Tip: If several devices are to be enrolled one after the other, Multi-use enrollment is enabled in the Expiration section and a late date is selected under Valid until. The Expiration section is missing if Using Android's built-in app (enforces multi-use) has been selected under Authentication, see Enrollment options →.

   > Currently, no Wi-Fi profile may be included during NFC enrollment.

2. On the enrollment (source) device, the Relution Agent App is opened.
3. The following path is opened: `Menu` → `Device information` → `Share NFC enrollment`
4. Scan enrollment is tapped.
5. The QR code of the previously created enrollment is scanned.

   The device is now ready to enroll other devices via NFC. Alternatively, an NFC tag can be written with the enrollment information.

6. The target device must be reset and on the initial setup screen.
7. The carrier device or NFC tag is held close to the target device, and the instructions on the target device are followed.

For version 26.4.0

Enroll devices without camera

Some Android devices do not have a camera or a functioning QR code scanner. These devices can still be enrolled in Relution as fully managed devices using a DPC Identifier code (Device Policy Controller Identifier).

Enroll devices without camera/ QR code

In a created enrollment, the DPC identifier is displayed under Enrollment information in the Using DPC identifier tab (the highlighted code above Enrollment process). It must not be confused with the Enrollment code field under Details. The same tab is also available in the QR code dialog of the enrollment. The DPC identifier is used as follows:

- The devices are reset to factory settings.
- The initial device setup is started and the instructions are followed.
- If the devices ask for the Google account credentials, the code `afw#setup` is entered as the username.
- If the devices ask for the DPC identifier, the corresponding code is entered.
- The instructions are followed to set up the managed devices. After setup, the device is fully enrolled in Relution – just like using the QR code method.

For version 26.4.0

Unenroll devices

Unenrollment ends the management of a device by Relution. A device is unenrolled by deleting it: the Delete action is available in the device inventory and on the device details page. After the deletion is confirmed, Relution removes the organization's data from the device and deletes the device from the inventory. The unenrollment is recorded in the audit log, and the device can be enrolled again at any time.

If the selection contains a managed device, the deletion dialog additionally offers the options Keep factory reset protection (FRP) enabled and Also wipe the device's external storage (such as SD cards) under Managed device; both are disabled by default (see Factory Reset Protection →). The Message field that is also shown has no effect on company-owned devices.

> For devices enrolled via Samsung Knox Mobile Enrollment (KME), the profile assignment of the device must be removed in the Samsung Knox Portal before deleting it. Otherwise, the device is automatically re-enrolled.

Effect per enrollment type

What happens on the device depends on how it was enrolled:

ion 26.4.0

Enrollment type	Effect of the deletion
Managed Device →	The device is wiped and reset to factory settings.
Work profile / BYOD →	Only the work profile is removed, including all work apps and data. Private data remains on the device.
Personal profile →	Only the work profile is removed, including all work apps and data. Private data remains on the device.

Trash

Deleted devices are first moved to the Trash (`Devices` → `Trash`). Only deleting a device again from the trash removes it permanently from Relution.

Only devices in the Deleted status are removed permanently. A device in the Deletion pending⋯ status has not yet confirmed the deletion, for example because it is offline. If it is deleted from the trash, it is first only set to Deleted and remains in the trash; only a further deletion removes it permanently.

Delete/Remove organization

It is possible to remove an existing connection between Relution and Android Enterprise

Note

For Android Enterprise enrollments, Android devices communicate directly with Android Enterprise via the Android Enterprise API and not via Relution as in Android Classic/Legacy enrollments. If the connection to Android Enterprise is removed by removing the linked Google account, all existing enrollments are lost and existing devices can no longer be managed in Relution and no new devices can be enrolled via Android Enterprise. Policy configurations that are on enrolled devices at this time can no longer be withdrawn or removed. Subsequent reconnection to regain control of devices is not possible. The consequences of disconnecting in Relution, by contrast, depend on the option selected there (see next section).

Relution-side disconnection of an existing connection

The connection is removed under `Settings` → `Device platform specific` → `Android Enterprise` in the Account settings tab:

- In the Remove Android Enterprise card, the desired option is selected under Enterprise removal options. Remove enterprise and devices known to Relution is preselected.
- Start is clicked.
- The Disassociate organizations dialog is confirmed with Remove.

For version 26.4.0

The Start button is only visible with the permission to edit the Android Enterprise settings.

The options affect the devices differently:

- Remove enterprise and devices known to Relution: The devices managed by Relution are factory reset or have their work profile removed, and they are deleted in Relution. Devices unknown to Relution remain in the Android Enterprise.
- Remove enterprise and devices: In addition to the devices managed by Relution, all other devices of the Android Enterprise are deleted, including those unknown to Relution.

> Even the preselected option factory resets all devices managed by Relution or removes their work profiles. Previously enrolled devices are not restored when the connection is restored.

Google-side disconnection of an existing connection

Disconnecting in Relution does not delete the Google organization. After disconnecting, Relution shows the steps required for deletion under `Settings` → `Device platform specific` → `Android Enterprise`. These steps depend on the enterprise type of the organization.

Managed Google domain

- admin.google.com → is opened, and sign-in takes place with the account used to create or upgrade the organization.
- `Devices` → `Mobile and endpoints` → `Settings` → `Third-party integrations` is opened.
- The third-party integration is selected and Manage EMM providers is clicked.
- In the list of providers, the organization with the Organization ID shown in Relution is removed.

According to the note in Relution, the enterprise can be reactivated within 30 days by signing in with the account used to set up the connection.

GooglePlay Enterprise account

- play.google.com/work → is opened, and sign-in takes place with the account used to create the organization
- In the left menu, Admin Settings is opened
- The ID, which can be seen at the top of the page, is compared with the one in the Relution Portal
- The three dots on the right side of the tile are clicked, followed by Delete organization

A Gmail account can only be associated with a single Google organization and can only be used for a new organization once that organization has been deleted. As long as the Google organization has not been deleted, the connection in Relution can be restored with the same Gmail account; previously enrolled devices are not restored in that case.

For version 26.4.0

Overview

Relution provides a selection of actions to directly control and direct Android Enterprise devices. An outstanding advantage is that these actions can be applied specifically to individual devices.

Available actions

Not every action is available for every enrollment type. Restrictions and minimum versions are noted in the description; actions without a note are available for managed devices, work profiles and devices with a personal profile.

For version 26.4.0

Action	Description
Install app from Google Play Store	Installs a selected app from Google Play Store on the device. Only available for devices enrolled as a managed device or as a work profile.
Install app from the Relution Store	Installs an app stored in the Relution Store on the device: Play Store apps as well as native apps (APK), provided that Relution has determined their signing certificates. Native apps can only be selected if exclusively fully managed devices are selected. Only available for fully managed devices, including those with a personal profile. Details: Manage APK apps →
Remove app	Uninstalls a selected app from the device. Only available for devices enrolled as a managed device or as a work profile.
Clear app data	Deletes all data associated with an app from the device. Available from Android 9.
Send file to device	Transfers a file (e.g. PDF, document, image) securely to the device.
Enterprise wipe	Removes the work profile and all associated policies; apps and data associated with the personal profile are preserved. Only available for devices with a personal profile enabled, from Android 8.
Remove eSIM	Removes an eSIM profile from the device using the ICCID.
Add eSIM	Adds an eSIM profile to the device using the provided activation code.
Wipe device	Resets the device to factory settings and deletes all data. Only available for devices enrolled as a managed device or with a personal profile. Note: Since Relution 5.34.0, it is also possible to remove only the management profile on devices with a work or personal profile (via the trash icon in the device details, or Delete in the device inventory).
Shutdown device	Shuts the device down completely.
Reboot device	Restarts the device. Only available for devices enrolled as a managed device.
Locate device	Determines the current location of the device.
Lock device	Only available for devices enrolled as a managed device or as a work profile. Locks the device with the current password. If no password is set, the device can be unlocked without a password. There is no unlock action; if the password is unknown, a new password can be set via Reset lock passcode (on devices enrolled as a work profile, this only affects the work profile password).
Refresh device info	Updates the device information in the Relution console.
Request device info	Requests the eSIM identifier (EID) of the device. The user must approve the disclosure on the device. Only available for devices enrolled as a work profile, from Android 13.
Enable lost mode	Activates Lost Mode when the device is lost or stolen: lock screen, location tracking and a message on the lock screen. Only available for devices enrolled as a managed device (from Android 11) or with a personal profile (from Android 13).
Disable lost mode	Unlocks the device and turns Lost Mode off again. Same availability as Enable lost mode.

Action	Description
Send message	Displays a text message on the device.
Reset lock passcode	Resets the device password on managed devices. On devices with a work profile or a personal profile, only the work profile password is reset; devices with a personal profile cannot be unlocked with the new password.
Select Play Store app from the Relution Store	Installs a Play Store app pre-approved in the Relution Store on the device. Only available for devices enrolled as a work profile.

For version 26.4.0

Locate Android Device

With Relution it is possible to locate Android Enterprise devices.
The action can be triggered in the Inventory on the Device to be located in the tab `Location` → `Locate device`. If a location is already available, the button is labeled Relocate device. After a request, the button is disabled until the location request triggered this way is completed, but for no longer than about 20 seconds. If the Relution Companion lacks the required permissions, it is disabled as well; while Lost Mode is active, it is not shown. Alternatively, in the tab `Actions` → `Apply action` → `Locate device`.

Each time a device is located, a notification is sent to the device's notification menu. In addition, the process is displayed in the Relution Companion

The successfully located device is displayed on a map in the Location tab under `Devices` → `Inventory` → `the device` → `Location`.

Requirement

The device must have a GPS module and an internet connection, as well as being switched on and basically locatable.

In Relution, locating must be enabled under `Settings` → `Device Management` → `Enrollment` in the Locate device row for the ownership of the device (COD or BYOD). By default, it is enabled for COD and disabled for BYOD. Devices with unknown ownership are locatable by default; this setting cannot be changed in the portal. If locating is disabled, Relution does not offer the Locate device action and hides the Location tab. For Android Enterprise devices in Lost Mode, the Location tab remains visible and updates the position about once a minute; the Locate device action is not available in this case either.

For version 26.4.0

Further requirements are activated location services on the device in the settings or in the quick settings.
Relution grants the location permission of the Companion via the policy: if Locate device is enabled for COD, the permission is granted automatically, otherwise it is denied. This applies regardless of the ownership of the device. This default can be overridden via the Manage apps configuration.
Further Settings →

If these are deactivated, Relution shows the following message in the actions:

```
Unable to determine location; No location available; GPS is disabled; Network location is disabled.
```

If the services are activated, a successful message looks like this:

```
Determined current location, using fused provider, accuracy 13.37 meter, age <1m.
```

Viewing location in the Self-Service Portal

New in 26.4

Authorized users can also view the last known location of their own device directly on a map in the Self-Service Portal, without needing administrator access: View location on a map →

Notes

- Pending actions
  Problems with positioning may occur if actions are still pending in Relution. These must be canceled and the action must be resubmitted.
- Location accuracy
  The option Location accuracy in the device settings has a significant influence on the location accuracy. If this setting is disabled, the location accuracy can be several hundred meters.
  For Samsung devices with Android 13, the setting can be found under `Settings` → `Location` → `Location Services` → `Location Accuracy`.
- Location Permission
  To limit potential misuse, Relution from version 5.31.0 onwards offers the ability to adjust a location permission. Details: Location Services →

For version 26.4.0

Overview

A policy is a collection of one or more configurations. Each policy can be applied to one or more devices at the same time. In addition, one or more policies can be associated with each device.

For version 26.4.0

Available Configurations

Configuration	Description
Always-On VPN →	Manage Always-On VPN settings
Manage apps →	Install, update, and uninstall apps on managed devices
Work profile passcode →	Management of the password policy for the work profile
Conditional Access →	Requires Conditional Access to be set up on the device via the Relution Agent in order to use protected resources
User messages →	Set custom messages
Preferred Activities →	Manages which app is used by default for a specific action
Display →	Manage the display settings for the device
CVTE OEMConfig →	Configure the CVTE OEMConfig app
Compliance enforcement →	Define lock and wipe actions when a device is not compliant
Advanced keyguard feature management →	IT admins can control advanced keyguard (lock screen) features for the device
Advanced security overrides →	Security policies set to secure values by default
Device radio state →	Manage the state of the device's radio settings
Device password →	Management of the password policy for the device
Device connectivity →	Manage the device connectivity settings
Global proxy →	Configures a network-independent global HTTP proxy
Wallpaper →	Manage the wallpaper
Kiosk Mode →	Kiosk mode settings
Knox →	Configure Samsung's Knox Service Plugin (KSP)
Runtime permission management →	Define default responses to permission requests from managed apps
Newline OEMConfig →	Configure the Newline OEMConfig app
Personal Usage →	Configure personal usage for a fully managed device
Play Store Management →	Configuration of Google Play Store features
Relution File Shares →	Sharing configuration for the Relution Files app

Configuration	Description
Relution Decon →	Configuration for the Relution Decon app
Relution Home Screen Layout →	Configure the Relution Home Screen Layout App
Restrictions →	Management of restrictions
Samsung Classroom Management →	Preconfigure the Samsung Classroom Management App
Default Applications →	Define which applications are used as default applications on the device
Location mode →	Configure the settings options of the available location detection
StrongSwan Restrictions →	Configure the StrongSwan app and define a default profile
StrongSwan VPN Profile →	Configure a VPN profile for the StrongSwan app
System updates →	Manage system updates
Wi-Fi →	Management of Wi-Fi settings
Work account setup →	Configure the upgrade of a user account to a managed Google domain
Certificate →	Define a CA certificate or certificate and private key for installation on the device

For version 2

Work profile passcode

This configuration is used to define the password requirements for the work profile of Android Enterprise devices. Requirements for the device lock are defined via the Device password → configuration.

Supported Enrollment Types

The Work profile and Personal profile badges in the form indicate the enrollment types for which the configuration is supported:

- Devices with a work profile →
- Managed devices with a personal profile →

There is no profile selection. In both cases, the password requirements apply to the work profile.

Passcode Quality

Defines the required quality or type of screen lock or password. The selected level is a minimum requirement, passwords of a higher quality level are accepted as well.

The following options are available:

For version 26.4.0

- Complex (strong)
  The password must contain at least one letter, one digit, and one special character. When this option is selected, the following additional mandatory fields are displayed (lowest permitted value in parentheses):

  - Minimum number of letters (1)
  - Minimum number of lower case letters (0)
  - Minimum number of upper case letters (0)
  - Minimum number of non letters (0)
  - Minimum number of numeric characters (1)
  - Minimum number of symbols (1)

  The fields are empty in a new configuration. The configuration can only be saved once all fields have been filled in.

- Alphanumeric
  The password must consist of letters and numbers.

- Alphabetic
  The password must contain at least letters (or symbols).

- Numeric complex
  Requires a numeric password with increased requirements, for example without simple or easy-to-guess number sequences.

- Numeric
  The password must contain at least digits (e.g. a PIN).

- Pattern
  Despite its name, this option does not enforce an unlock pattern. Any lock is sufficient (e.g. pattern, PIN, or password), and there are no requirements regarding its content.

- Biometric (weak)
  A weaker biometric unlock method can be used, if supported by the device. With this selection, the fields Minimum passcode length, Maximum passcode age (in days), Passcode history and Number of failed passcode attempts before all data is erased are hidden and cannot be configured.

> Which options are actually available and enforceable depends on the device, Android version, and manufacturer customizations.

Minimum Passcode Length

Defines the minimum number of characters required for the password. The field is mandatory. The default value and the smallest permitted value is `4`.

Example:

- `4` → The password must be at least 4 characters long.

For version 26.4.0

Maximum Passcode Age (in Days)

Determines after how many days the password must be changed.

Number of days until a new password must be set. If the value is set to `0`, the password never expires.

Example:

- `0` → No password expiration.

Passcode History

Defines how many previously used passwords may not be reused.

Number of stored and previously used passwords that may no longer be used again.

Example:

- `0` → There is no restriction on password reuse.

Number of Failed Passcode Attempts Before All Data Is Erased

For version 26.4.0

Defines after how many incorrect password attempts a reset or wipe is triggered.

If no value is set, no automatic wipe is usually performed.

Disable Work Profile Apps Until User Complies with Password Requirements

If this option is enabled, apps in the work profile remain disabled until the configured password meets the defined requirements. The option is enabled by default.

The period after which blocking and wiping take place if the password requirements are not met is defined in the Compliance enforcement → configuration. By default, only the apps in the work profile are blocked. When wiping, only the work profile is removed on devices with a work profile (BYOD); devices with a personal profile (COPE) are reset to factory settings.

Require Separate Passcode for the Work Profile

If enabled, a separate passcode must be set for the work profile.

If this option is disabled, the same device screen lock may be used in some cases.

> If this option is not enabled, a system-wide timeout of 60 seconds is automatically applied.

Notes

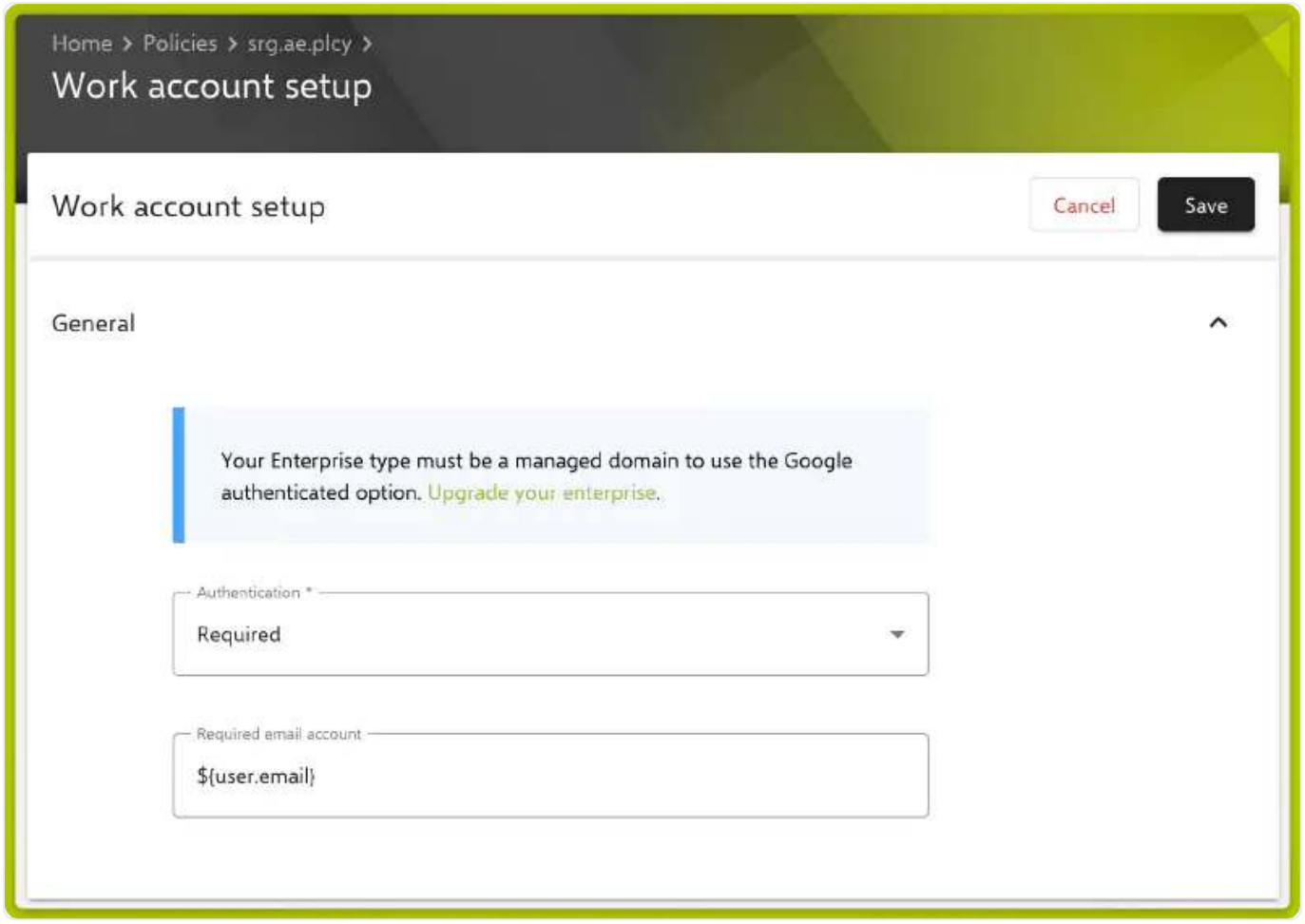
- These settings apply exclusively to the work profile, including on managed devices with a personal profile (COPE).
- Not all options are available to the same extent on every device or Android version.
- Actual enforcement depends on the manufacturer, Android version, and device mode.

For version 26.4.0

Work account setup

The Work Account Setup policy configuration allows administrators to centrally configure Google Work Account settings on fully managed devices.

> The Required option requires the Relution organization to be linked to an enterprise of the managed Google domain type. In addition, user authentication must be enabled for the managed Google domain in the Google Admin console (`admin.google.com`), otherwise the configuration does not take effect. If the organization is still linked to a Google Play Enterprise account, the form shows a hint about upgrading the enterprise (see Upgrade from GooglePlay Enterprise account to managed Google domain →). For more information on setup, see Managed Device →.



Authentication

Defines whether users must authenticate with a Google Work Account during device setup.

Option	Description
Unspecified (default)	No requirement is set. The behavior corresponds to Not required.
Not required	No Google Work Account authentication is required.
Required	Users must authenticate with a Google Work Account.

Required email account

When Required is selected, the Required email account field appears. The managed domain email account the user has to log in with is entered there. Placeholders can be used to create it dynamically.

For version 26.4.0

Advanced security overrides

For devices enrolled in Android Enterprise, the Advanced Security Overrides configuration provides deep control capabilities. Administrators can determine whether the installation of APK files from third-party sources is permitted, whether Google Play Protect verification is enforced, and whether developer mode is available for testing purposes. Settings for the Memory Tagging Extension, content protection, and work profile notifications are also available.

Allow from Unknown Sources

This setting controls whether apps can be installed from sources outside the Google Play Store (side-loading). The following options are available:

- Unspecified (default for new configurations): Relution does not set a value; the Android Enterprise default behavior applies.
- Disallow untrusted app installs on entire device: Side-loading is prohibited across the entire device.
- Allow untrusted app installs in the device's personal profile only: Side-loading is permitted exclusively within the user's private profile.
- Allow untrusted app installs on entire device: Side-loading is permitted across the entire device.

Enforce Google Play Verification

Determines whether security scanning by Google Play Protect is mandatory to identify malicious software.

- Unspecified (default for new configurations): Relution does not set a value; the Android Enterprise default behavior applies.
- Yes: Verification is enforced system-wide and cannot be disabled by the user.
- User Choice: The end user decides whether the verification should be active.

Device Encryption Policy

Defines the security level for data encryption on the physical storage.

Option	Description
No encryption required (default)	No encryption of user data is enforced.
Encryption required, no password required to boot	Data is encrypted, but no password is required during the boot process.
Encryption required, password required to boot	Encryption is active and requires a password to be entered during the startup process.

For version 26.4.0

How devices that do not meet the required encryption are handled is defined in the Advanced security overrides row of the Compliance enforcement → configuration.

Allow Developer Settings

This defines whether Developer Mode can be unlocked on the device. This is primarily relevant for debugging purposes or app testing. For standard production use, this option should remain disabled for security reasons.

Common Criteria Mode

Common Criteria Mode is used to comply with international security standards for information technology.

The setting is only applied to fully managed devices and to managed devices with a personal profile (COPE). Relution does not transfer it to devices with a work profile (BYOD).

> How it works: Enabling this mode strengthens specific security components. This particularly affects the AES-GCM encryption of Bluetooth Long Term Keys and the hardened storage of Wi-Fi configurations.

> Common Criteria Mode enforces an extremely strict security model. This is typically only required for IT infrastructures in national security systems or highly sensitive organizations. The use of standard apps or everyday device functions may be affected. Only activate this mode if explicitly required.

For version 26.4.0

Memory Tagging Extension

Defines the policy for the Memory Tagging Extension (MTE). The setting is marked with the Android 14+, COPE Work profile, and Managed Device badges.

The options Unspecified (default for new configurations), User choice, Enabled, and Disabled are available.

Content Protection

Content protection scans for deceptive apps. The setting is marked with the Android 15+ badge.

The options Unspecified (default for new configurations), User choice, Enabled, and Disabled are available.

Personal Apps That Can Read Work Profile Notifications

Defines which apps in the personal profile may read notifications from the work profile. The setting is marked with the COPE Work profile badge.

Clicking Add opens an app selection in which one or more apps are selected. Their package names are adopted; individual entries can be removed again. If the list remains empty, Relution does not transfer any setting to Google.

For version 26.4.0

Relution Files Android

Relution provides the ability to integrate local file shares —also known as network drives— on Android devices using SMB and WebDAV. By connecting to school or enterprise server environments, users can access relevant documents and content and securely store data and work results on a central server.

Advantages of Relution Files

Data should not be stored in unsecured cloud services with servers outside the EU when GDPR compliance is required. It is also advisable not to store data directly on devices, especially when devices are used by multiple users. Storing documents on on-premise servers via `Relution Files` ensures data security and sovereignty for all users.

Configure Local Network Drives for Relution Files

Local file shares can be configured in Relution in two ways:

Manual setup is described in the documentation of the app itself: Relution Files →

For version 26.4.0

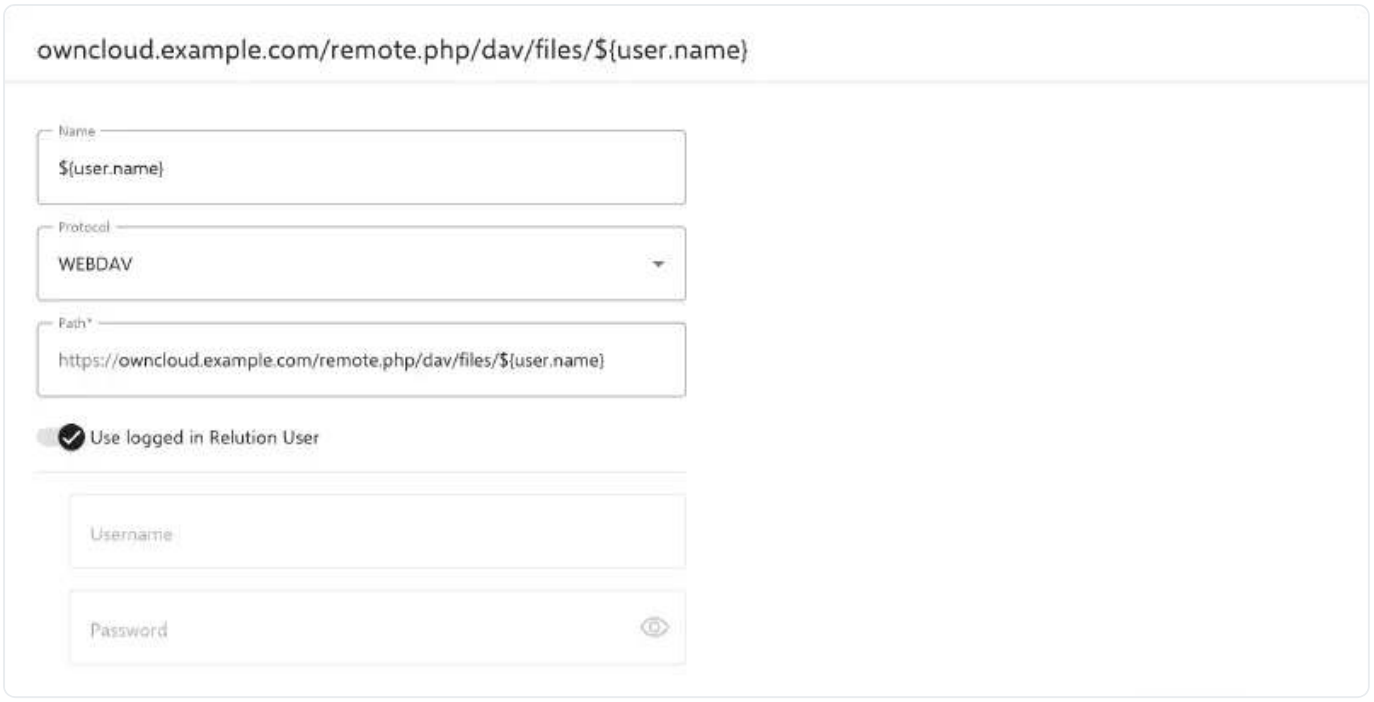
Automatic Configuration of Relution Files via Policies

Using a managed configuration set by an administrator in the Relution Portal removes almost all setup steps for end users. This enables seamless access to the file share.

With the `Relution File Shares` configuration inside a policy, a WebDAV or SMB connection can be prepared for use. On Android, the configuration is only available in Android Enterprise policies and can be added once per policy. If a policy contains the configuration, Relution automatically installs the Relution Files app as a mandatory app and transfers the required managed configuration to it. A separate distribution of the app is not required. If Relution Files is also listed in Manage apps →, the settings made there apply (e.g. installation type).

Add opens the New share dialog. A configuration can contain several shares; at least one is required for saving. For each share, an optional Name, the Protocol (SMB or WEBDAV) and the Path (mandatory) are specified. Without a name, the last path segment is used. For SMB, the path must contain the actual share (e.g. `server/share`; the prefix `smb://` is predefined). WebDAV connections always use HTTPS (the prefix `https://` is predefined). Placeholders such as `${user.name}` can be used in name, path, username and password and simplify the login process.

In addition, the option Use logged in Relution User can be enabled for the share. The credentials of the Relution user logged in on the device are then used. If the option is disabled, a fixed Username and Password can be stored.



Wallpaper

For version 26.4.0

As of Relution 5.33, the Wallpaper configuration is available for Android Enterprise and Android Classic/Legacy. Under Android Enterprise, it is labelled with the Managed Device badge and applies to fully managed devices and to managed devices with a personal profile (COPE), not to devices with a work profile (BYOD). This allows setting an image for the home screen that appears on devices after applying the policy. The policy also enables adding text (including placeholders) to display dynamic text on the wallpaper.

> Android Enterprise requires Relution Companion version 1.18.
>
> Android Classic requires Relution Companion version 5.37.

The Wallpaper configuration sets the image but does not prevent users from changing it on the device.

Relution Decon (content filter)

Starting with version 26.3, Relution enables the setup of a DNS-based content filter for Android Enterprise devices. This feature ensures a secure and focused internet experience by restricting access to selected websites. With AI-powered content categorization, Relution Decon also provides a comprehensive parental control filter with advanced configuration options.

What is Relution Decon?

Relution Decon is an AI-powered add-on for Android Enterprise that filters content in real-time, creating a safe digital environment. Using DNS-based content control, Decon blocks unwanted websites, allowing users to work and learn in a protected, distraction-free space.

Relution Decon uses a DNS proxy to forward all requests to the Decon server. Websites are classified and either allowed or blocked according to policy rules. All data transfers are SSL-encrypted, ensuring user activities remain secure.

Decon App

The Decon app (`io.relution.decon`) is installed on the devices automatically by Relution as soon as a policy containing a Decon configuration is published. Prior distribution via Manage apps → is not required. An entry there only applies additional options such as update behavior, minimum version or permissions, not the install type. Once installed, it acts as the device's Always-On VPN and monitors DNS requests to ensure that only approved content is accessible.

For version 26.4.0

App features:

- Activates a system-wide DNS proxy, which cannot be disabled by the user
- Displays the current status of Relution Decon
- Provides insight into blocked websites and applied filter categories

Preventing manual VPN changes

> Because Relution Decon operates as an always-on VPN, users could otherwise disable or replace it by editing the device's VPN settings. To prevent this, the following two configurations are combined:
>
> - Restrictions →: Disable VPN Configuration enabled
> - Always-On VPN →: **`io.relution.decon`** selected as the always-on VPN app

Decon Policy

In the device policy, `Add` → `Relution Decon` is clicked. This policy automatically configures the Decon app on associated and supported devices and acts as a proxy for all DNS requests.

Policy configuration is completed upon publishing.

Policy configuration hierarchy (highest to lowest priority)

1. Permitted domains
2. Blocked domains
3. Blocked Categories

Decon in Relution Teacher

On Android Enterprise devices, Decon can be selected and managed in class profiles starting with Relution Server 26.3. Prerequisite: the Decon app is installed on the student devices and they have a Decon policy assigned. Relution Teacher only shows a notice about a missing Decon configuration for iOS devices.

More about Relution Teacher →

Filtering

For version 26.4.0

In the Filtering section of the Decon policy, Filter Type determines how websites are filtered:

- Off: No filtering by categories or age level.
- Categories (default): The categories to be blocked are selected individually via toggles. The toggles are only shown for this filter type. Adult content, Advertising and Phishing are blocked by default.
- Age level: Filtering is based on an age level (0+, 6+, 12+ or 16+, default 12+).

Two further toggles are available regardless of the filter type:

- BPJM list: Additionally filters content classified as inadmissible by the BPjM. Entries under Permitted domains can still enable access to such content.
- Safe search: Set independently of the blocked categories and the age level. Blocking the Adult content category does not enable safe search.

If several Decon configurations are used on one device, the strongest filtering automatically takes effect: age-based filters take precedence over category-based filters. Configurations without filtering are ignored.

Category Classification

Relution Decon automatically assigns each website to a category. With the filter type Categories, administrators can define which categories are blocked:

Category	Description	Examples
Adult content	Sites inappropriate for youth	Pornography, Violence, Weapons, Drugs, Gambling, Adult Entertainment, Adult Shopping, Dating
Advertising	Advertising websites	Ad providers
Social media	Social media content	Facebook, Instagram, TikTok, etc.
Entertainment	Entertainment websites like streaming or games	Movies, Games, Videos
Music	Music streaming services	Spotify, Tidal, etc.
News	News and magazines	News, Weather
Shopping	Online shops (excluding adult content)	Amazon, eBay, etc.
Education	Learning websites	Wikipedia, Google Scholar
Generative AI	AI-specific websites	ChatGPT, Perplexity.ai, etc.
Phishing	Potential phishing websites	Potential scams, Data theft
Miscellaneous	Everything else	Remaining sites

For v

Permitted and Blocked Domains

- Permitted domains / Blocked domains (Domains section): Specific domains can be allowed or blocked independently of categories. Only the domain should be specified, not the path. Permitted domains remain accessible even if the filter deems them inappropriate. The number of blocked domains should be limited to about 500.

Privacy

For Android Enterprise, the Privacy section provides the option Auto accept data disclosure (disabled by default). When enabled, the data disclosure is accepted automatically on behalf of the user.

Manage apps

With Relution, Android Enterprise devices can be equipped with configured apps. A Manage Apps configuration can be used to distribute the desired apps to the devices.
Several sources are available for app selection:

- Apps from the Relution App Store
- Apps from the Managed Google Play Store
- Apps added manually.

Apps from the Relution App Store

The Relution App Store provides all apps that have been added from the Managed Google Play Store.
The advantage is the streamlined number of apps, as the entire Managed Google Play Store is not displayed.

> Additionally, starting with Relution Server 26.2 and Relution Client Apps version 26.x, APKs from the Relution App Store can be distributed. This can be done either via the Manage Apps list (installation type Custom) or users can download the APKs directly through the Relution Agent. Alternatively, the Install app from the Relution Store action is available. This only works on fully managed devices, including those with a personal profile. On devices enrolled as a work profile, APK apps are not installed.

For version 26.4.0

Further details: Manage APK apps →

Apps from the Managed Google Play Store

All apps from the Managed Google Play Store are available. This store is similar to the regular Play Store used in personal environments.

Private Apps from the Managed Google Play Store

The Managed Google Play Store also allows uploading private apps. Private apps are also referred to as paid apps, as Google does not offer a payment option in the enterprise environment.
There are three options for this use case:

Installation via Private Play Store

Developers create apps with a Unique Package Name.
These apps are uploaded to the private store at Google using a company-owned Google account and can then be selected in Relution under Managed Google Play Store.

Installation via Public Play Store

Developers make apps available in the public section of the Managed Google Play Store for everyone.
These apps can be added to the Relution App Store as described above or selected directly from the Managed Google Play Store.

Manual Installation via Developer Mode with Manual Distribution (Unsigned App)

For this, developer options must be enabled, and installation from unknown sources must be allowed on all devices receiving these apps.
The `.apk` files are then manually installed on the devices. In this case, the apps are not managed, cannot be managed via Relution, and do not receive app updates.

Add Apps Manually

Apps that are already pre-installed on a device can be managed through this method.
The Package Name of the app is required to uniquely identify apps on the devices.

App Package Names for Samsung Devices

- `com.samsung.android.dialer` | Phone App
- `com.samsung.android.messaging` | Messaging 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 Camera

Installation Types

- Available – Apps are available for users to download and install via the Play Store.
- Pre-installed – Apps are pre-installed on devices. However, users can delete the apps.
- Force-installed – Apps are always automatically downloaded and installed on devices.
- Blocked – App installations are explicitly blocked.
- Custom – set automatically for APK apps from the Relution App Store; it cannot be selected or changed.

Configuration

Some app developers offer a Managed Configuration. Relution displays this if available.
For APK apps from the Relution Store, configurations can be provided in JSON format.

Permissions

App permissions for apps from the Google Play Store can be set here, e.g.:

- Default response to permission requests
- Access to approximate location
- Access to precise location
- Connect via Bluetooth

Advanced

Advanced configurations for Play Store apps, e.g.:

- Share information across profiles
- Automatic update mode
- Install certificates
- Manage configurations
- Prevent uninstallation
- VPN always on lockdown exemption – defines whether the app may communicate without a VPN connection while lockdown mode is enabled (see Always-On VPN →)

These options are also available for manually added apps. For APK apps from the Relution App Store, Advanced only contains the option User app uninstallation mode with the values Unspecified, Allow and Disallow. With Allow, the user may uninstall the app; an app removed this way is not reinstalled by Relution. Unspecified behaves like Disallow.

For version 26.4.0

Restrictions

For Android devices with Android Enterprise enrollment, a variety of restrictions are available in Relution. Basically, it is advisable to be clear about exactly which restrictions are combined. This makes it possible to rule out that devices are configured in such a way that they are no longer usable.

In the portal, the configuration is divided into several sections. The following overview follows this structure. If an option only applies to certain enrollment types or Android versions, this is noted for the option.

Account restrictions

- Disable adding new users and profiles
- Disable removal of other users
- Disable adding and removing accounts
- Disable configuration of user credentials
- Enable selection of a private key if no matching rule is defined: The user can select a private key if no rules are defined to automatically select a private key and certificate for authenticating the device to a server. On devices below Android 9, this setting may leave enterprise keys vulnerable.

For version 26.4.0

Default restrictions

This section is only displayed if the deprecated setting Apps from unknown sources is set to a value other than Disallow untrusted app installs on entire device in an existing configuration.

> The Apps from unknown sources setting is deprecated. The Advanced security overrides configuration is used instead. If it is configured, the deprecated setting is ignored.

Further information: Advanced security overrides →

App restrictions

- Disable app installation
- Disable app uninstallation
- Disable easter egg in settings

Customization restrictions

- Disable user icon customization
- Disable wallpaper customization
- Enable auto date and time zone (Managed Device only): Defines whether automatic date, time and time zone setting is enabled on a company-owned device. The options are Default, User Choice and Enforced.

Device restrictions

This section contains general device restrictions as well as cross-profile settings for devices with a work profile.

General

- Disable keyguard (Managed Device only): Affects the keyguard as a whole. Individual lock screen features are disabled via Advanced keyguard feature management →.
- Enable Factory Reset Protection (FRP) (Managed Device and Personal profile only) and Google account email for FRP: see Factory Reset Protection →.
- Account types for which management is disabled: Account types that the user cannot manage.
- Permitted input methods and Permitted accessibility services: The options are All allowed, System apps only and System and additional specified apps. With the last option, the additionally permitted apps are stored in a list.
- Enterprise display name visibility: Defines whether the enterprise display name is shown on the device (Unspecified, Visible on the device, Hidden on the device). The display name itself is maintained in the Enterprise Display Name field under `Settings` → `Device platform specific` → `Android Enterprise`.
- Assist content policy (Android 15 and later): Controls whether assist content such as screenshots and app information may be sent to a privileged app such as an assistant app (Unspecified, Allowed, Not allowed).
- Autofill policy: Controls the system autofill service (Android 8 and later) with the options Unspecified, User choice and Disabled. To comprehensively restrict credential management, the Credential provider policy default is configured in addition.
- Credential provider policy default (Android 14 and later): Unspecified, Disallowed or Disallowed except system.
- Printing: Unspecified, Allowed or Not allowed.

Cross profile settings

These settings only apply to the Work profile and Personal profile enrollment types. They are not applied on managed devices without a work profile.

- Work profile widgets default value: Defines whether work profile apps may add widgets to the home screen by default if nothing else is specified for the app (Unspecified, Allowed, Not allowed). Unspecified corresponds to Not allowed.
- Copy and paste: Unspecified, Allowed or Disallow from work to personal profile.
- Data sharing: Unspecified, Allowed, Disallow from work to personal profile or Disallowed.
- Show work contacts in personal profile (Contacts section): Unspecified, Disallowed, Allowed or Allow only system apps to access work contacts in the personal profile. In addition, an app list can be maintained: with Unspecified and Allowed, it contains the apps that are not allowed access; with the other options, it contains the apps that are allowed access.

For version 26.4.0

Multimedia restrictions

- Disable screen capture
- Disable adjusting the master volume
- Disable location sharing
- Disable contact sharing over Bluetooth
- Camera access: Default, User choice, Camera disabled or Camera access enforced. Controls the use of the camera and whether the user can use the camera access toggle (Android 12 and later). On fully managed devices, disabling the camera applies to the entire device; on devices with a work profile, it applies only within the work profile.
- Microphone access: Default, User choice, Microphone disabled or Microphone access enforced. Controls the use of the microphone and whether the user can use the microphone access toggle (Android 12 and later). The setting only takes effect on fully managed devices.

Network restrictions

- Disable configuring Bluetooth
- Disable configuring mobile networks
- Disable reset of network settings
- Disable VPN configuration
- Disable editing of Wi-Fi networks (deprecated, see note below): see Disabling Wi-Fi configuration →.
- Disable Android Beam (NFC) to share data between apps
- Disable Bluetooth
- Enable network escape hatch: If no network connection can be established at boot time, the escape hatch prompts the user to temporarily connect to a network in order to refresh the device policy. After the policy has been applied, the temporary network is removed again.
- Preferential Network Service (Work profile only): Controls whether the preferential network service is enabled in the work profile (Unspecified, Disabled, Enabled). The setting has no effect on fully managed devices.

for version 26.4.0

Storage restrictions

- Disable mounting physical external media
- Disable USB file transfer (deprecated, see note below)

Telephony restrictions

- Disable sending and receiving SMS messages
- Disable outgoing calls
- Disable roaming data services
- Disable configuring tethering and portable hotspots (deprecated, see note below)
- Disable configuring cell broadcast

The options Disable editing of Wi-Fi networks, Disable USB file transfer and Disable configuring tethering and portable hotspots are deprecated. The Device connectivity → configuration is used instead. If both configurations are present, these three options are ignored.

Possible pitfalls

The following options can result in devices no longer being usable or reachable as intended.

Factory Reset Protection

With the Enable Factory Reset Protection (FRP) option, resetting to factory settings via the Android device settings can be blocked on managed devices. Resetting via the recovery menu is not affected.

The email addresses of device admins are stored in the Google account email for FRP field. These addresses must be Google accounts. If the device has been reset to factory settings, one of these device admins must sign in with their Google account (email and password) to unlock the device. If no addresses are specified, the device does not provide factory reset protection. This setting should therefore be used with caution.

Disabling Wi-Fi configuration

If Disable editing of Wi-Fi networks is active and no Wi-Fi networks are specified, Wi-Fi is disabled on the device. If devices cannot establish a Wi-Fi connection because the configured networks are unreachable or faulty, there is no way to intervene manually. The setting then cannot be undone either, since the devices are offline.

This option should only be used in conjunction with Enable network escape hatch. If no network connection can be established at boot time, it allows a Wi-Fi network to be configured temporarily in order to refresh the device policy.

For Version 26.4.0

System updates

System updates are a key component of device management in Android Enterprise. They enable the configuration of update policies for managed devices to ensure security and stability.

System Update Type

In the Manage System Updates section, the System Update Type for managed devices can be defined. The available options are:

- Unspecified: Follows the device's default system update behavior. This typically requires manual acceptance of system updates.
- Automatic: Automatically installs system updates as soon as they become available.
- Windowed: Automatically installs system updates within a defined daily maintenance window. This also ensures that Play apps are updated during the window. This option is recommended for kiosk devices to ensure that pinned foreground apps from Play remain updated.
- Postpone: Delays the automatic installation of system updates for up to 30 days.

When Windowed is selected, the required fields Start time and End time appear (preset to 00:00 and 00:30). The times refer to the device's local time. If the end time is earlier than the start time, the maintenance window spans midnight. Start and end time must be at least 30 minutes apart; otherwise, the configuration cannot be saved.

For version 26.4.0

Annual System Update Freeze Period

The Annual system update freeze period defines periods during which no system updates are installed. Start and end date consist only of month and day; the period recurs every year.

Features of the Freeze Period

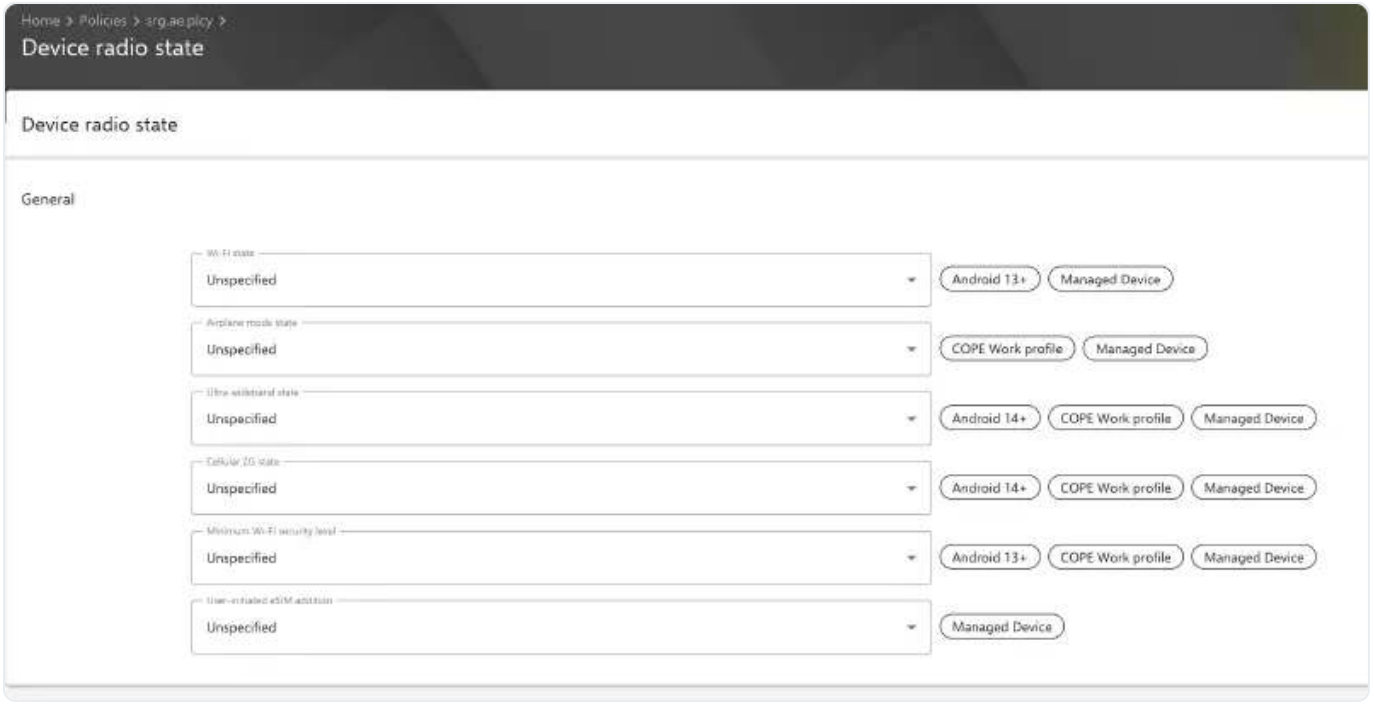
- During the freeze period, all incoming system updates (including security patches) are blocked.
- Outside the freeze period, the normal update behavior applies.
- Freeze periods are created via Add. Multiple periods can be defined and removed individually.
- A period may cover at most 90 days. There must be at least 60 days between two periods.
- If the end date is earlier than the start date, the period spans the turn of the year.

Device radio state

This policy centrally manages the status and usage of wireless technologies on managed Android devices.

The Device radio state policy enables centralized management of various wireless technologies on Android Enterprise devices. Administrators can define whether users are allowed to control certain features themselves or if these are enforced to be enabled or disabled.

Each setting additionally offers the option Unspecified, which is preselected in a new configuration. In this case, the Android Enterprise default behavior defined by Google applies: User choice for Wi-Fi, Airplane Mode, Ultra-Wideband and Cellular 2G, Open network security for the minimum Wi-Fi security level, and Allowed for adding eSIMs.



Wi-Fi State

Defines the state of the Wi-Fi function.

Options:

- User choice – Users can enable or disable Wi-Fi themselves.
- Enabled – Wi-Fi is permanently enabled.
- Disabled – Wi-Fi is permanently disabled.

Support:

- Android 13+
- Managed devices

Airplane Mode State

Controls whether Airplane Mode can be activated.

Options:

- User choice – Users can enable or disable Airplane Mode themselves.
- Disabled – Airplane Mode is permanently disabled.

Support:

- COPE work profile
- Managed devices

Ultra Wideband State (UWB)

Regulates the use of Ultra-Wideband (e.g., for precise location tracking).

Options:

- User choice – Users can enable or disable UWB themselves.
- Disabled – UWB is permanently disabled.

Support:

- Android 14+
- COPE work profile
- Managed devices

For version 26.4.0

Cellular 2G State

Allows restriction of 2G network usage (relevant for security reasons).

Options:

- User choice – Users can control the use of 2G networks themselves.
- Disabled – 2G networks are permanently disabled.

Support:

- Android 14+
- COPE work profile
- Managed devices

Minimum Wi-Fi Security Level

Defines the minimum security standards that Wi-Fi connections must meet.

Options:

- Open network security – No restrictions.
- Personal network security – Minimum requirement of WPA/WPA2.
- Enterprise network security – Requires WPA2-Enterprise.
- Enterprise 192-bit network security – Highest security requirement.

Note: Insecure networks can be blocked if stricter policies are defined.

Support:

- Android 13+
- COPE work profile
- Managed devices

User-Initiated eSIM Addition

Determines whether users are allowed to add eSIM profiles independently.

Options:

- Allowed – Users can add eSIM profiles.
- Disallowed – Users cannot add eSIM profiles.

Support:

- Managed devices

For version 26.4.0

Kiosk Mode

With the policy configuration Kiosk Mode Relution offers the possibility to strongly restrict the operation of Android devices with Android Enterprise enrollment and protect the devices from misoperation.

Relution Home Screen Layout

On fully managed devices (Device Owner), the Relution Home Screen Layout configuration automatically activates Kiosk Mode in the background and sets the Relution Homescreen Layout App as the launcher. For the other Android Enterprise enrollments (managed device with a personal profile and work profile), the app receives the configured layout but is not set as the kiosk launcher. The Relution Home Screen Layout configuration offers the possibility to conveniently drag and drop the app layout on the devices via the Relution Portal. Additionally, there is the possibility to define a background image and add custom static or dynamic texts on the background.

In this configuration, the Relution Homescreen suppresses notifications on the lockscreen.

> The Relution Home Screen Layout and Kiosk Mode configurations are mutually exclusive. If the policy already contains one of them (even a disabled one), the other cannot be added.

For version 26.4.0

Use default launcher

The Kiosk Mode configuration replaces the device's home screen with the Android Enterprise default launcher. It displays only managed apps that have been installed via the Manage apps configuration (e.g. with the installation type Force-installed or Pre-installed) on a single page in alphabetical order. All other apps on the devices are hidden from users and cannot be used.

> Using Kiosk Mode requires a fully managed device or a managed device with a personal profile (COPE); it is not available on devices with a work profile (BYOD). Enabling Kiosk Mode by default prevents the use of the phone feature, which also suppresses making emergency calls.

Settings

In addition to the Customise Kiosk Launcher App section (see below), the Kiosk Mode configuration contains the sections General and Kiosk customization.

General

- Stay on while battery plugged – multiple selection of the charging modes `AC`, `USB` and `WIRELESS` in which the device stays on.
- Maximum time to lock Device – selection between 15 seconds and 20 minutes. Without a selection, the device's default setting applies. A fixed screen timeout from the Display → configuration is only applied if it is shorter than this value.
- Disable toasts and overlays – prevents toasts and overlays from being displayed on the device.

Kiosk customization

The following values are preselected in a new configuration:

Field	Preselection	Further options
Power button actions	Available	Unavailable, Available - (Default)
System error warnings	Mute	Enabled, Muted - (Default)
System navigation	Disabled	Enabled, Home button only, Disabled - (Default)
Status bar	Disabled	Enabled, System info only, Disabled - (Default)
Device settings	Allowed	Blocked, Allowed - (Default)

For ver

The options with the suffix - (Default) apply the Android Enterprise default behavior. The Kiosk customization section is only available in the Kiosk Mode configuration, not in Relution Home Screen Layout.

Use alternative launcher

If additional features and apps other than the apps added in the Manage apps policy configuration are to be available on the Android devices, for example system apps, it is necessary to use an alternative launcher. To do this, the toggle Use a custom kiosk launcher app instead of the default launcher is enabled in the Customise Kiosk Launcher App section. The Select button in the Select custom launcher app field then opens the Select an app dialog. There, Managed Google Play Store App (Android Enterprise) is chosen as the source and the launcher app is added. Alternatively, the sources Relution App Store app and Manually add app are available.

The launcher can then be configured using the available options. Manual configuration is carried out via the function Configure custom launcher app.

Play Store Management

With the policy configuration Play Store Management, Relution offers the possibility to control the operation of Android devices with Android Enterprise enrollment by reducing the available content in the Google Play Store to the content of the Manage apps configuration. It is also possible to configure app updates.

Restricted Google Play Store

Enable the restricted Play Store - Disabled

- When the user opens the Google Play Store on the device, they can see and install all public apps.

Enable the restricted Play Store - Enabled

- When the user opens the Google Play Store on the device, no apps or only the apps from the Manage apps configuration are visible. Depending on the specified installation type from the Manage apps list, the user can install the released apps.

> If the restricted Google Play Store is enabled, apps that are not included in the Manage apps configuration are automatically uninstalled from the device. System apps and apps that Relution adds to the policy itself (e.g. Relution Agent and Companion) are excluded. This also applies if the restricted Google Play Store is enabled via a lesson.

For version 26.4.0

App updates

The Automatic app update field in the Play Store Management configuration offers 4 options:

- User choice
- Never
- Wi-Fi only
- Always

> Kiosk mode can prevent automatic updates.

> The options Disable app installation and Disable app uninstallation (Restrictions configuration, App restrictions section) prevent any installation or uninstallation, including those triggered via MDM.

User messages

Managed Android Enterprise devices can display a message on the lock screen. This makes it easier to identify the device or can be used for a contact option in case of loss. In addition, a short and a long support message can be configured, which are displayed as a pop-up in the system settings, for example, when a locked setting is accessed.

Message	Display location	Trigger
Lock screen message	device's lock screen	always visible
Short support message	pop-up in the system settings	access to a locked setting
Long support message	pop-up in the system settings	access to the device administrator setting

> All messages can also be customized by country: if a device is set to English, for example, the message matching the system language is displayed. Each message consists of a Default message and, optionally, localized messages, which are created in the table below it together with the respective Language. If the system language of the device does not match any localized message, the default message is displayed. As soon as a localized message has been created, the default message is a mandatory field.

For version 26.4.0

All three messages support placeholders, which Relution replaces individually for each device, e.g. `${device.name}`, `${device.serialnumber}`, `${device.uuid}` or user placeholders. The available placeholders are shown in the Available placeholders area below the form.

Lock Screen Message

This message is displayed on the device's lock screen. Useful content includes:

- name of the company/organization
- device name, serial number or device ID (via placeholder)
- contact email or phone number

Short Support Message

This message is displayed as a pop-up within the device's settings whenever access to a locked setting is attempted.

Long Support Message

This message is displayed as a pop-up within the device's settings whenever access to the device administrator setting is attempted.

Runtime permission management

Via the policy configuration Runtime permission management, Default responses to permission requests for managed apps can be set globally.

In the Default response for permission requests section, the field If an app requests permission: offers the options Ask the user (default), Grant the permission or Deny the permission. The preset value is Ask the user (default).

> Be careful with blanket prohibitions. If the approach is too restrictive, some apps may no longer function as desired.

Furthermore, in addition to the defined default behavior, there are exceptions for specific permissions.

Default Android Permissions

The permission requests present in the Android operating system can be configured in the Runtime permission management configuration, along with the desired behavior. When a permission is added, one of the three options is selected in the Behavior field (default: Ask the user (default)).

For version 26.4.0

> Permissions defined here override the setting made above in the Default response for permission requests section. This also applies to custom permissions.

Custom Permissions

App-specific permission requests can be configured if required by an app. The names of these permissions can usually be found in the documentation provided by the respective app manufacturer. Here, too, one of the three options is selected in the Behavior field when a permission is added (default: Ask the user (default)).

Wi-Fi

This policy centrally distributes Wi-Fi network definitions to Android Enterprise devices.

The Wi-Fi policy allows Wi-Fi networks to be centrally set up on Android Enterprise devices without requiring users to enter credentials themselves. Multiple Wi-Fi configurations can be added to a single policy at once.

Tethering is not controlled by this policy but by the Tethering settings option of the Device connectivity → configuration.

Network Definition

- Wi-Fi configuration name – internal name for identification in Relution.
- The network's SSID – network name in plain text. Alternatively Hex representation of the network's SSID, required for SSIDs that cannot be encoded in UTF-8. At least one of the two fields is mandatory. If both are filled in, they must match.
- This network is hidden – enable if the network does not broadcast its SSID.
- Join network automatically – connects the device automatically once the network is in range.

Security Type

- Security type: None / Open, WEP PSK, WPA/WPA2/WPA3 PSK, WEP 802.1x, WPA/WPA2/WPA3 EAP.
- Passphrase: required for PSK-based security types.

For version 26.4.0

EAP Authentication (WEP 802.1x, WPA/WPA2/WPA3 EAP)

- Accept EAP types: PEAP, TLS, TTLS, SIM, AKA or PWD, plus Identity (required field). For PWD, additionally Password.
- For PEAP and TTLS, additionally Anonymous identity, Password and Phase 2 Authentication: PAP or MSCHAPv2.
- For TLS, PEAP and TTLS: Client certificate type or certificate template (see Certificate Management →) and TLS maximum version.
- Server certificate validation: Trusted CA certificates, Domain Suffix Match (required field, Android rejects an empty list as insecure), Subject Alternative Name (SAN) match and optionally Certificate subject name substring of trusted RADIUS services.
- Enable Opportunistic Key Caching for fast roaming

MAC Address Randomization

MAC Address randomization mode (Hardware/Automatic, default: Automatic) – only sent to devices running Android 13 or later.

Proxy

In the Proxy settings section, Proxy type defines the kind of proxy: None, Manual or Automatic configuration (PAC).

- With Manual: Host and Port for HTTP Proxy, HTTPS Proxy, FTP Proxy and/or SOCKS Proxy, with at least one proxy required, plus Bypass proxy for (list of addresses that are not routed through the proxy).
- With Automatic configuration: PAC URL.

A proxy that applies regardless of the connected network is defined via the Global proxy → configuration.

Support

- Managed devices (Device Owner)
- COPE work profile (Personal Profile Enabled)
- Not available for a pure work profile (BYOD/Profile Owner)

For version 26.4.0

Always-On VPN

This policy defines which VPN app stays permanently active on the device.

The Always-On VPN policy determines which already installed VPN app should stay permanently active on an Android Enterprise device. Unlike the StrongSwan configurations →, which equip a specific VPN app with its own profile, this policy only selects which app acts as the always-on VPN – the app itself must be installed separately via Manage apps →, since it is not deployed automatically by this policy.

Settings

> The Always-On VPN settings can be changed by the user on the device, unless the Disable VPN configuration option is enabled in the Restrictions →.

- Select Always-On VPN app (required, Select button) – the app that should remain permanently active as the VPN connection.
- Deny networking when VPN is not connected (lockdown mode) – permits network traffic exclusively through the VPN connection. As long as the VPN is not connected, no network access is available. Even while the VPN is connected, any traffic outside the tunnel remains blocked unless the respective app is exempted as a lockdown exemption →.

> With lockdown mode enabled, the device must be able to connect to the VPN. Otherwise, no Wi-Fi connection is possible and the device cannot communicate with Relution.

For version 26.4.0

Split Tunneling

The Always-On VPN policy only determines which VPN app stays permanently active. Which traffic is routed through the tunnel is determined by the configuration of the VPN app or the VPN gateway. If it does not restrict the tunnel to specific apps or destination networks, Android routes all traffic through the VPN.

Split tunneling is therefore also possible in combination with Always-On VPN, provided the VPN app supports it:

- App configuration of the VPN app – If the vendor offers a managed configuration, it is available in Manage apps → via the Configuration action. Whether and how apps or networks can be defined for the tunnel there depends on the respective VPN client.
- StrongSwan – In the StrongSwan VPN Profile →, the Applications section offers the choice between Only these Apps will use the VPN and These Apps will not use the VPN (default). If the list remains empty with These Apps will not use the VPN, all apps use the VPN. In the Split tunneling section, traffic can additionally be split by destination network: Only route traffic to specific subnets via VPN, everything else is routed as if there was no VPN or Traffic to these subnets will not be routed via VPN. Optionally, Block IPv4 traffic not destined for the VPN and Block IPv6 traffic not destined for the VPN block the remaining traffic of the respective protocol version.
- VPN gateway – Alternatively, the gateway pushes only the internal networks as routes to the device instead of tunneling all traffic.

Lockdown Mode and Exemptions

With lockdown mode enabled, Android blocks any traffic that does not pass through the VPN. Apps excluded from the tunnel via split tunneling have no network connection in this case. The same applies to traffic to destination networks for which the VPN does not provide a route. Split tunneling based solely on destination networks is therefore not usable with lockdown mode enabled. This also applies to splitting by subnets in the Split tunneling section of the StrongSwan VPN Profile.

Individual apps can be exempted from lockdown. To do so, the VPN always on lockdown exemption option is set in Manage apps → via the Advanced action:

- Unspecified / Enforce – the app is subject to lockdown mode.
- Exemption – the app may communicate even without an active VPN connection. This setting is supported as of Android 10.

The option is not available for APK apps from the Relution App Store. For these apps, Advanced only contains the option User app uninstallation mode.

An exempted app continues to use the VPN as long as the VPN app includes it in the tunnel. For an app to communicate outside the tunnel while lockdown mode is enabled, it must therefore be marked as Exemption and also be excluded from the tunnel in the VPN app.

Support

- Managed devices (Device Owner)
- COPE work profile (Personal Profile Enabled)
- Work profile (Profile Owner/BYOD)

For version 26.4.0

StrongSwan

These policies configure the StrongSwan app and its VPN profiles on Android Enterprise devices.

Relution offers two related policies for the StrongSwan → app (`org.strongswan.android`): StrongSwan Restrictions controls the app's behavior and references a default profile, while StrongSwan VPN Profile defines the actual IKEv2 VPN connection. Via Always-On VPN →, the StrongSwan app can additionally be set as the permanently active VPN app. Which profile is connected is determined by the Select a Default VPN Profile setting in the StrongSwan Restrictions.

As soon as a policy contains one of the two configurations, Relution automatically installs the StrongSwan app as a required app, grants it the requested permissions and allows it to install certificates. A separate assignment via Manage apps → is not necessary. Any setting stored there for StrongSwan, e.g. a different install type, is overridden.

StrongSwan Restrictions

- Allow users to create profiles
- Allow users to import profiles
- Allow users to use existing profiles
- Allow users to import certificates
- Allow users to access Settings
- Do not show a warning if the app is not on the device's power whitelist
- Select a Default VPN Profile (Select button) – reference to a StrongSwan VPN Profile configuration of the same policy version

For version 26.4.0

StrongSwan VPN Profile

Multiple VPN profiles can be created and managed in the portal. The form consists of the StrongSwan VPN Profile area with the sections General, User Certificate and CA certificate, and the Advanced settings area.

General

- Name of the profile
- Server – address of the VPN server. The port is set under Advanced settings.
- VPN Type:
  - IKEv2 EAP (Username/Password)
  - IKEv2 Certificate
  - IKEv2 Certificate + EAP (Username/Password)
  - IKEv2 EAP-TLS (Certificate)
  - IKEv2 EAP-TNC (Username/Password)
- Username – only for VPN types with username/password

User Certificate

This section only appears for VPN types with a certificate. The user certificate is specified here (see Certificate Management →).

CA Certificate

CA or server certificate used to verify the VPN server.

Advanced Settings

The Advanced settings area is divided into the following sections.

General

- Server identity and Client identity
- DNS Servers, MTU of the VPN tunnel device, Port and NAT-T keepalive interval
- Send certificate requests
- Certificate validation via OCSP or CRL, plus Use strict revocation checking
- Use RSA/PSS signatures and Use IPv6 transport addresses

Split Tunneling

- Subnets to include or exclude
- Block IPv4/IPv6 traffic not destined for the VPN

Proxy

Host, port and Exclude hosts from proxy.

For version 26.4.0

Applications

- Only these Apps will use the VPN – only the listed apps use the VPN, all other apps communicate outside the tunnel
- These Apps will not use the VPN – the listed apps communicate outside the tunnel, all other apps use the VPN. If the list remains empty, all traffic is routed through the VPN.

With lockdown mode enabled in Always-On VPN →, apps outside the tunnel only have a network connection if they are set as a lockdown exemption.

> Automatic connection on demand is not possible with Android Enterprise. The VPN is connected manually once in the StrongSwan app; after that, the traffic of the specified apps is routed through the tunnel. This also applies with Always-On VPN →: the user establishes the initial connection.

Algorithms

IKEv2 Algorithms and IPsec/ESP Algorithms.

Support

- Managed devices (Device Owner)
- COPE work profile (Personal Profile Enabled)
- Work profile (Profile Owner/BYOD)

Personal Usage

This policy configures personal usage for a fully managed device with a work profile.

The Personal Usage policy restricts the personal profile of a fully managed device with a work profile (COPE).

Settings

- Disable camera – disables the camera in the personal profile.
- Disable screen capture – prevents screenshots in the personal profile.
- Account types for which management is disabled – prevents adding specific account types in the personal profile.
- Maximum amount of days that Work mode can be turned off for – limits how long users may pause Work mode (minimum 3 days, default 90).
- Allow Bluetooth sharing – controls whether content from the personal profile may be shared via Bluetooth. Values: Unspecified (default, behaves like Allowed), Allowed, Disallowed. Disallowed requires Android 8; a compliance violation is reported on older devices.
- Users can create a private space profile – allows or prevents creating an additional Private Space profile. Values: Unspecified (default, behaves like Allowed), Allowed, Disallowed. With Disallowed, existing private spaces are removed.

Personal Play Store

- List type: Blocklist or allowlist
- Blocked apps or Allowed apps – controls which apps may be installed from the Play Store in the personal profile.

Support

- COPE work profile (fully managed device with work profile)

For version 26.4.0

Device password

This configuration defines the password requirements for the lock of the entire device.

The Device password configuration defines the requirements for the device lock of Android Enterprise devices. The requirements apply to the entire device. Requirements for a separate work profile password are defined via the Work profile passcode → configuration instead.

Difference from the Work Profile Password

Both configurations use the same form for the password requirements but differ in scope:

	Device password	Work profile passcode
Scope	Device lock (entire device)	Work profile only
Badges in the form	none	Work profile, Personal profile
Fully managed devices	applied	ignored by the server
Additional options	none	Disable work profile apps until user complies with password requirements, Require separate passcode for the work profile

Both configurations can be part of the same policy. Relution then transfers both requirements to the device: one for the device and one for the work profile.

Fully managed devices → have no work profile. A Work profile passcode configuration is not transferred to them; the device lock is controlled exclusively via Device password.

Supported Enrollment Types

The form shows no badges, so the configuration is not restricted to specific enrollment types. It is available for all Android Enterprise enrollment types:

- Managed device →
- Managed device with a personal profile →
- Device with a work profile →

Passcode Quality

Minimum complexity that has to be fulfilled when a password is set. For a new configuration, Numeric is preselected.

The following options are available:

- Complex (strong)
  The password must contain at least one letter, one digit and one special character. With this selection, the following additional mandatory fields appear (smallest permitted value in brackets):
  - Minimum number of letters (1)
  - Minimum number of lower case letters (0)
  - Minimum number of upper case letters (0)
  - Minimum number of non letters (0)
  - Minimum number of numeric characters (1)
  - Minimum number of symbols (1)

  The fields are empty for a new configuration. The configuration can only be saved once all fields are filled in.
- Alphanumeric
  The password must contain digits and letters (or symbols).
- Alphabetic
  The password must contain letters (or symbols).
- Numeric complex
  The password consists of digits without repeating or ordered sequences. The portal shows the hint: “The user must have entered a password containing at least numeric characters with no repeating (4444) or ordered (1234, 4321, 2468) sequences.”
- Numeric
  The password must contain digits.
- Pattern
  Despite the name, no unlock pattern is enforced. Any kind of lock must be set up (e.g. pattern, PIN or password); there are no requirements regarding its content.
- Biometric (weak)
  The device must at least be secured with a low-security biometric unlock method. With this selection, all other fields are hidden.

> Which options are actually available and enforceable depends on the device, the Android version and manufacturer customizations.

For version 26.4.0

Minimum Passcode Length

Defines the minimum number of characters for the password. The field is mandatory and prefilled with `4`. The smallest permitted value is also `4`.

Maximum Passcode Age (in Days)

The maximum number of days until a new password has to be set. If the value `0` is specified, the password never expires. The field is mandatory and prefilled with `0`.

Passcode History

Number of already used passwords that are saved and cannot be used again. The field is mandatory and prefilled with `0`, meaning there is no restriction on reuse.

Number of Failed Passcode Attempts Before All Data Is Erased

Defines after how many incorrect entries the data is erased. The smallest permitted value is `1`. The field is optional: if no value is set, the data is never erased.

For version 26.4.0

Behavior on Non-Compliance

If the device password does not meet the requirements, the device reports a compliance violation. The period after which the device is blocked and reset as a result is defined in the Device passcode row of the Compliance enforcement → configuration. This row applies to fully managed devices and managed devices with a personal profile. On devices with a work profile, the Work profile passcode row applies instead. Without a custom rule, the default periods apply.

An option to disable apps until the requirements are met is only offered by the Work profile passcode configuration.

Notes

- The Device password configuration can only be added once per policy.
- Not all options are available to the same extent on every device or Android version.
- Actual enforcement depends on the manufacturer, Android version and enrollment type.

Advanced keyguard feature management

This configuration disables selected lock screen features on managed devices.

The Advanced keyguard feature management configuration disables individual features of the lock screen (keyguard) of Android Enterprise devices, such as the camera, notifications or biometric unlock methods. The lock itself remains in place. Requirements for the device lock password are defined via the Device password → configuration.

Supported Enrollment Types

The Managed Device badge in the form indicates that the configuration is intended for company-owned devices:

- Managed device →
- Managed device with a personal profile →

The configuration is not intended for devices with a work profile → (BYOD). It can only be added once per policy.

Disabling Device Keyguard Features

The General section contains one checkbox per feature. None of them is selected for a new configuration. Each selected checkbox disables the respective feature on secure lock screens.

For version 26.4.0

Option	Effect (hint text in the portal)
Disable all	Disables all current and future keyguard customizations
Disable biometrics	Disables all biometric authentication on secure keyguard screens
Disable camera	Disables the camera on secure keyguard screens (e.g. PIN)
Disable fingerprint sensor	Disables the fingerprint sensor on secure keyguard screens
Disable remote input	Disables text entry into notifications on secure keyguard screens
Disable facial recognition	Disables facial recognition for authentication on secure keyguard screens
Disable iris scanner	Disables the iris scanner for authentication on secure keyguard screens
Disable notifications	Disables showing all notifications on secure keyguard screens
Disable trust agents state	Ignores the trust agent state on secure keyguard screens
Hide sensitive content from notifications	Hides sensitive content from notifications on the lock screen

When Disable all is selected, all other checkboxes are cleared and disabled, as they are already included in this selection. The individual features can only be selected again after Disable all is cleared.

> Whether a feature is actually present on the lock screen (e.g. iris scanner or facial recognition) depends on the device.

Difference from Restrictions

The Restrictions → configuration contains the option Disable keyguard. This option affects the keyguard as a whole, whereas Advanced keyguard feature management only switches off individual features on the lock screen.

For version 26.4.0

Compliance enforcement

This configuration defines when non-compliant devices are blocked and wiped.

The Compliance enforcement configuration defines block and wipe actions for Android Enterprise devices that do not meet certain requirements of a policy. For each supported configuration, it can be defined after how many days of non-compliance the device is blocked and subsequently wiped.

The configuration is available for all Android Enterprise enrollment types and can only be added once per policy. Which enrollment type an individual rule applies to depends on its row (see below).

Default Behavior

Without a custom rule, Relution sets default rules for the monitored settings: non-compliant devices are blocked after 20 days and wiped after 30 days.

Custom rules can only shorten the periods: a maximum of 10 days is permitted for blocking and a maximum of 30 days for wiping.

For version 26.4.0

Configuration Overview

The table in the form always contains the same four rows, one per configuration whose non-compliance can be enforced. The columns show the values of the respective rule: Block after days, Block scope, Wipe after days and Preserve factory reset protection.

Row	Monitored settings	Applies to
Advanced security overrides	Device encryption policy from Advanced security overrides →	all enrollment types
Device passcode	Password requirements from Device password → and Work profile passcode →	fully managed devices, managed devices with a personal profile
Work profile passcode	Password requirements from Device password → and Work profile passcode →	devices with a work profile
Restriction	Permitted input methods, Permitted accessibility services and Disable keyguard from Restrictions →	all enrollment types; Disable keyguard only on fully managed devices

The Device passcode and Work profile passcode rows both refer to all password requirements of the device. Which of the two rows applies is determined solely by the enrollment type.

Two actions are available in the context menu of a row:

- Configure opens the Configure rule dialog.
- Reset removes the custom rule of the row. The default rule then applies again.

Configure Rule

Each rule always consists of a block action and a wipe action. A block without a subsequent wipe cannot be configured.

Block Action

- Block after days
  Number of days the device must be non-compliant before the device or the work profile is blocked. The prefilled value is `10`; values from `0` (immediate block) to `10` are permitted. The value must be smaller than Wipe after days. When the block takes effect, a notification is shown on the device that describes, where possible, how to resolve the non-compliance.

- Block scope
  Defines what the block applies to. The setting only takes effect on company-owned devices. Unspecified is preselected.

  - Unspecified – equivalent to Work profile.
  - Work profile – only apps in the work profile are blocked; apps in the personal profile remain usable.
  - Device – the entire device is blocked, including apps in the personal profile.

For version 26.4.0

Wipe Action

- Wipe after days
  Number of days the device must be non-compliant before it is wiped. The prefilled value is `30`; values from `0` to `30` are permitted. Company-owned devices are reset to factory settings; on devices with a work profile (BYOD), the work profile is removed.

- Preserve factory reset protection
  Defines whether the factory reset protection (FRP) data is preserved when the device is reset. Off by default. The setting does not apply to work profiles.

Clicking Confirm adds the rule to the table. It is only saved together with the configuration.

Multiple Policies

If several policies of a device contain the Compliance enforcement configuration, the rule of the policy with the higher priority applies for each monitored setting. Settings without a custom rule keep the default rule.

Global proxy

This configuration defines a network-independent global HTTP proxy for managed devices.

The Global proxy configuration defines an HTTP proxy that applies regardless of the connected network. It is intended for the enrollment types Managed Device → and managed device with a personal profile → (COPE), not for devices with a work profile → (BYOD).

The portal shows the following notice in the form:

> Typically proxies should be configured per-network. However for unusual configurations like general internal filtering a global HTTP proxy may be useful. If the proxy is not accessible, network access may break. The global proxy is only a recommendation and some apps may ignore it.

A per-network proxy is defined in the Proxy settings section of the Wi-Fi → configuration.

Proxy type

The Proxy type field determines how the proxy is defined. Different fields are shown depending on the selection.

- Direct – host, port and exclusions are specified manually. This option is preselected in a new configuration.
- PAC script – the proxy is configured automatically via a PAC script.

For version 26.4.0

Direct

- Proxy host (required) – IPv4 address (e.g. `10.0.0.1`) or URL with `http://` or `https://` and a domain name with a top-level domain in lowercase (e.g. `http://proxy.example.com`), in each case without port and path. A host name without protocol (`proxy.example.com`) or without top-level domain (`http://proxy`) is not accepted. If the input is invalid, the field is marked as erroneous and the configuration cannot be saved.
- Proxy port (required) – port of the proxy; values from `0` to `65535` are accepted.
- Hosts for which the proxy is bypassed – list of hosts whose connections do not go through the proxy. Host names may contain wildcards such as `*.example.com`.

> With proxy port `0`, Relution does not transfer a global proxy to the device, so the configuration has no effect.

PAC script

- PAC script URI (required) – URI of the PAC script used to configure the proxy. The portal expects a valid URL.

Validation

When saving, Relution checks that a Proxy host is specified for proxy type Direct and a PAC script URI for proxy type PAC script. Fields of the other proxy type are not transferred to the device.

For version 26.4.0

Device connectivity

This configuration manages the connectivity settings of Android Enterprise devices.

The Device connectivity configuration combines the settings for USB data access, Wi-Fi, tethering, Bluetooth sharing, private DNS, Wi-Fi roaming, access points (APN) and preferential network services. The portal shows the enrollment types and Android versions a setting applies to as badges on the respective field; they are listed below under Support.

In a new configuration, Unspecified is preselected for the selection fields. The exception is the Wi-Fi SSID restriction, where the denylist is preselected.

The configuration replaces the deprecated options for Wi-Fi configuration, USB file transfer and tethering in the Restrictions configuration. If a policy contains both configurations, the device connectivity settings apply (see Restrictions →).

USB data access

Controls what files and/or data can be transferred via USB. Charging is not affected.

Options:

- Unspecified
- Allow USB data transfer
- Disallow USB data transfer
- Disallow USB file transfer

For version 26.4.0

The effect of Unspecified on USB file transfer is described in File transfer via USB →.

Support:

- COPE Work profile
- Managed Device
- For Disallow USB data transfer additionally Android 12+ and USB HAL 1.3+

Configure Wi-Fi

Controls to what extent users may configure Wi-Fi networks themselves.

Options:

- Unspecified
- Allow configuring Wi-Fi
- Disallow adding Wi-Fi – supported from Android 13 on COPE Work profile and Managed Device.
- Disallow configuring Wi-Fi – supported on COPE Work profile and Managed Device.

With Disallow configuring Wi-Fi, the portal shows the warning “The device can’t use Wi-Fi, unless a Wi-Fi configuration is added!”. In this case, the required networks are distributed via the Wi-Fi → configuration.

Wi-Fi direct settings

Controls the use of Wi-Fi Direct.

Options:

- Unspecified
- Allow Wi-Fi direct
- Disallow Wi-Fi direct

Support:

- COPE Work profile
- Managed Device
- Android 13+

Tethering settings

Controls to what extent users may use tethering such as Wi-Fi or Bluetooth tethering.

Options:

- Unspecified
- Allow all tethering
- Disallow Wi-Fi tethering – supported from Android 13 on COPE Work profile and Managed Device.
- Disallow all tethering – supported on COPE Work profile and Managed Device.

For Version 26.4.0

Bluetooth sharing

Controls whether content may be shared via Bluetooth.

Options:

- Unspecified
- Allowed
- Disallowed

Wi-Fi SSID restriction

Defines which Wi-Fi SSIDs the device may connect to. This does not affect which networks can be configured on the device.

Options:

- Disallow connection to Wi-Fi SSIDs (preselected) – denylist. The SSIDs are entered in the field Wi-Fi SSIDs which cannot be connected to.
- Allow connection only to Wi-Fi SSIDs – allowlist. The SSIDs are entered in the field Wi-Fi SSIDs which can be connected to; at least one entry is required.

> For the allowlist, the portal points out that at least one Wi-Fi SSID needs to be available, otherwise the device will be unable to connect to Google or Relution.

Support:

- COPE Work profile
- Managed Device
- Android 13+

Private DNS

- Private DNS mode – configuration mode for the device's global private DNS settings.
  - Unspecified – defaults to User choice.
  - User choice – users may configure private DNS themselves.
  - Automatic – the device tries to use the network-provided DNS server over an encrypted connection before resorting to cleartext. Users cannot change the setting.
  - Specified host – the device only uses the DNS server specified in the Private DNS host field. Users cannot change the setting.
- Private DNS host – host name of the DNS server. The field can only be edited in Specified host mode and is then required; without a host name, Relution rejects saving.

For version 26.4.0

Support:

- Private DNS mode: Work profile, Managed Device
- Private DNS host: Managed Device

Wi-Fi roaming

In the Wi-Fi roaming area, Add creates one Wi-Fi roaming setting per SSID:

- SSID (required) – network name the setting applies to. Only one setting per SSID is possible.
- Wi-Fi roaming mode – Default (preselected), Disabled or Aggressive.

Support:

- Managed Device
- COPE Work profile
- Android 15+

APN

The Access Point Name (APN) area manages mobile network access points.

Enable override APNs

Options: Unspecified, Disabled, Enabled. Supported on Managed Device from Android 10.

APN settings

Add creates an APN setting. In the dialog, the portal points out that only the APN type Enterprise should be selected to use the setting in a work profile. An APN setting with the same name or the same APN as an existing one is not accepted.

For version 26.4.0

Field	Description
APN types	Required, multiple selection: Enterprise (Android 13+), Bearer Independent Protocol (BIP) (Android 12+), Carrier Branded Services (CBS), Default, Dial-up Networking (DUN), Emergency, Firmware Over-the-Air (FOTA), High-Priority (HiPri), Initial Attach (IA), IP Multimedia Subsystem (IMS), Mission Critical Service (MCX), Multimedia Messaging System (MMS), Rich Communication Services (RCS) (Android 15+), Secure User Plane Location (SUPL), Virtual SIM (VSIM) (Android 12+), XML Configuration Access Protocol (XCAP) (Android 11+)
Name	Required, display name of the APN setting
APN	Required, name of the access point
Numeric operator ID	Optional
Carrier ID	Optional, value from `0`
Authentication type	Unspecified, None, PAP, CHAP, PAP or CHAP
Username, Password	Optional
Proxy address, Proxy port	Optional, port from `0`
Server address (MMSC)	Optional
MMS proxy address, MMS Proxy port	Optional, port from `0`
Protocol, Roaming protocol	Unspecified, IP, IPv4/IPv6, IPv6, Non-IP, Point to point (PPP), Unstructured
Network types	Multiple selection: EDGE, GPRS, GSM, HSDPA, HSPA, HSPAP, HSUPA, IWLAN, LTE, NR (New Radio) 5G, TD_SCDMA, UMTS
Enable Always-on PDU Session	Unspecified, Not always on, Always on (Android 15+)
MVNO type	Unspecified, Group Identifier level 1 (GID), Integrated Circuit Card Identifier (ICCID), International Mobile Subscriber Identity (IMSI), Service Provider Name (SPN)
MTU v4, MTU v6	Optional, value from `0` (Android 13+)

Preferential network services

The Preferential network service settings area assigns apps to dedicated enterprise network slices, such as 5G enterprise slices.

- Default preferential network ID – applies to apps without their own configuration. Options: Unspecified (preselected), No preferential network, Preferential network 1 to Preferential network 5. A preferential network selected here must also be included in the list of configurations.

Under Preferential network service configurations, Add creates one configuration per network ID:

- Preferential network ID (required) – Preferential network 1 to Preferential network 5. Each ID can only be used once.
- Fallback to default connection – whether the app may fall back to the default connection when the preferential network is unavailable. Options: Unspecified, Allowed, Disallowed.
- Use of other networks – whether the app may use networks that do not match the preferential network service criteria. Options: Unspecified, Allowed, Disallowed (Android 14+).

If Use of other networks is set to Disallowed, Fallback to default connection must also be set to Disallowed. If the list contains no configuration, Relution transfers nothing for this area to the device, including no default network ID.

Support:

- Android 13+
- Managed Device
- Work profile

For version 26.4.0

Certificate

This configuration installs a CA certificate or a certificate with private key on the device.

The Certificate configuration distributes a certificate from the Relution certificate management, a certificate issued via a certificate template, or the user certificate of the assigned user to Android Enterprise devices. A policy can contain several certificate configurations.

The installation is carried out by the Relution Companion app, which Relution grants permission to install certificates (see Companion & Daemon →).

General

The General area defines which certificate is installed.

- Selected certificate or template (preselected) – in the Certificate or certificate template field, Select opens the Select a certificate or a certificate template dialog. There, an uploaded certificate is available on the Certificates tab and a certificate template on the Certificate templates tab. Certificates in PKCS#1 and PKCS#12 format are offered. Without a selection, the configuration cannot be saved.
- User's certificate for VPN and apps – instead of a fixed certificate, the certificate stored under VPN and apps in the profile of the user assigned to the device is installed.
    - Certificate name – selects a specific certificate by name when the user has several certificates of this type. The field may contain placeholders resolved per device (see Advanced placeholders →). If left blank, the longest-lived certificate is used.

For version 26.4.0

Certificates in PKCS#1 format are installed as CA certificates, PKCS#12 containers as certificates with private key.

Background on the certificate sources:

- Certificate Management →
- Built-In CA →
- Certificate Pool →

Certificate alias

The alias is generated automatically as soon as a certificate, a template or the option User's certificate for VPN and apps is selected, and cannot be edited. The copy icon copies it to the clipboard.

The portal describes its purpose as follows: when a managed configuration requires a certificate alias, this value is used to refer to this configuration.

To keep the alias unique on the device, Relution passes it to the Companion app extended by the hexadecimal serial number of the certificate in parentheses.

Behavior when a user certificate is missing

If the user assigned to the device has no matching user certificate, Relution still transfers the other configurations of the policy. The certificate is then not installed, and a warning is written to the server log.

For version 26.4.0

Display

This configuration manages the display settings of a managed Android Enterprise device.

The Display configuration determines whether brightness and screen timeout are chosen on the device by the user or enforced. In the portal, the configuration is labelled with the enrollment mode Managed Device; it applies to fully managed devices and to managed devices with a personal profile (COPE), not to devices with a work profile (BYOD). It can be added only once per policy.

Both settings are located in the General section and consist of two levels: a selection field defines the mode, an indented field below it defines the value. The value field can only be edited if the selected mode requires a value.

Brightness

Brightness is controlled by two fields: the mode and the brightness value.

Configure Brightness

Determines how the screen brightness is controlled.

Options:

- User configured – Brightness is set on the device. This option is preselected in a new configuration.
- Adaptive brightness – Brightness is adjusted adaptively; in addition, the value from the Screen brightness field is transmitted.
- Fixed brightness – Brightness is fixed to the value in the Screen brightness field.

For version 26.4.0

Screen brightness

Mandatory as soon as Adaptive brightness or Fixed brightness is selected under Configure Brightness. With User configured, the field is locked and no brightness value is sent to the device.

The hint text in the portal reads: “The screen brightness can be configured on a scale from 1-255, where 255 is the maximum brightness”. Values outside this range are not accepted; no default value is prefilled.

Screen timeout

The screen timeout is also controlled by two fields: the mode and the duration.

Configure screen timeout

Determines whether the time until the screen turns off is enforced.

Options:

- User configured – The timeout is set on the device. This option is preselected in a new configuration.
- Fixed timeout – The timeout is fixed to the value in the Screen timeout field.

Screen timeout duration

The Screen timeout field can only be edited with Fixed timeout. The available values are 15 seconds, 30 seconds, 1 minute, 2 minutes, 5 minutes and 10 minutes; 30 seconds is preselected.

> If the policy also contains a Kiosk Mode → configuration with a value for Maximum time to lock Device, Relution only transmits the fixed screen timeout if it is shorter than the maximum time to lock. Otherwise only the mode is transmitted, without a timeout value.

Support

- Managed device →
- Managed device with a personal profile → (COPE)
- Not available for devices with a work profile → (BYOD)

For version 26.4.0

Preferred Activities

This configuration manages which app should be used as default for a specific operation.

The Preferred Activities configuration assigns a specific app to Android operations (intents). Each entry consists of an app and, optionally, an activity, categories and actions; Android then permanently uses this app for matching operations. In the portal, the configuration is not labelled with a specific enrollment mode. It can be added only once per policy.

The configuration does not install the selected app. Installation is handled separately, e.g. via Manage apps →. A complete use case – the Relution Homescreen as default launcher – is described in the article Homescreen as default launcher →. For typical default apps such as browser or phone, the Default Applications → configuration offers a dedicated selection.

List of apps

The configuration shows a list with the columns Name, Bundle identifier, Activity, Actions and Categories. The Actions and Categories columns only show the last part of each name (e.g. `HOME` for `android.intent.category.HOME`).

A new entry is created via Add. The context menu of an entry offers Edit and Delete; several selected entries are deleted via the context menu of the list. Each app can only appear once in the list: apps already listed are excluded from the selection in the Relution App Store, and if an app already listed is added again by another route, the new entry replaces the previous one. In a policy version that has already been published, the list is read-only.

For version 26.4.0

Selecting the app

The Activity dialog creates an entry in three steps. In the first step, the source of the app is selected:

- Relution App Store app – An app is selected from the Relution App Store. Native and public apps for Android and Android Enterprise are offered.
- Managed Google Play Store App (Android Enterprise) – A free app is searched for in the managed Google Play Store via Android Enterprise. This source is only available if Android Enterprise is set up for the organization.
- Manually add app – The name and bundle identifier of an app are entered manually. The fields Name and Internal name are mandatory; the package name is entered as internal name (example in the portal: `com.mwaysolutions.relution`).

In the second step, the app is selected or the details of the manual app are entered.

Activity, categories and actions

In the third step, the details of the entry are defined. When an entry is edited later via Edit, only these fields are shown; the app itself remains unchanged.

- Activity – optional class name of the activity within the app, e.g. `io.relution.homescreen.MainActivity`. If the field is filled, Relution transmits `package name/activity` as the target; if it is empty, only the package name is transmitted.
- Categories – list of intent categories, e.g. `android.intent.category.HOME`. The input suggests the standard Android categories; custom values are possible.
- Actions – list of intent actions, e.g. `android.intent.action.MAIN`. The standard Android actions are suggested here as well.

Categories and actions are not mandatory. A hint in the dialog refers to the Google documentation → for details on the standard categories and actions.

For version 26.4.0

Location mode

This configuration defines how the location setting is handled on a managed Android Enterprise device.

The Location mode configuration controls the location setting (location services) of the device. In the portal, it is labelled with the enrollment mode Managed Device; it applies to fully managed devices and to managed devices with a personal profile (COPE), not to devices with a work profile (BYOD). It can be added only once per policy.

How the setting interacts with app permissions for location is described in the article Location Services →.

Location setting on the device

The selection field Location setting on the device in the General section is the only setting of the configuration.

Options:

- User choice – The location setting is not restricted. This option is preselected in a new configuration.
- Enable location setting on the device – The location setting is enabled on the device.
- Disabled – The location setting is disabled on the device.

The selected value is also passed to the Relution apps on the device (e.g. the Relution Agent).

For version 26.4.0

Note on work profiles

The portal displays the following hint in the form:

> On Android 11 and above, work profiles on company-owned devices cannot directly enforce location services. Compliance can only be restored once the user manually turns on/off location services through the device's Settings application.

Support

- Managed device →
- Managed device with a personal profile → (COPE), subject to the limitation described in the note on work profiles →
- Not available for devices with a work profile → (BYOD)

Samsung Classroom Management

This configuration deploys and configures the Samsung Classroom Management app for lessons.

The Samsung Classroom Management configuration sets up the app of the same name for lessons on Android Enterprise devices. In the portal, it is not labelled with a specific enrollment mode. It can be added only once per policy. Samsung Classroom Management requires a separate license (see Teacher →).

Behavior on the device

If a policy contains this configuration, Relution automatically extends the device policy:

- The Samsung Classroom Management app (`com.tabnova.classroomapp`) is deployed as a forced installation; its runtime permissions are granted. A managed configuration for the same app from Manage apps → is replaced by the values of this configuration.
- The classes the device user belongs to are passed to the app, including teachers and students. Classes are maintained under `Education` → `Classes` (see Educationfunction →).
- If the device user is registered as a teacher in at least one class, the Relution Teacher app (`io.relution.teacher`) is additionally deployed as a forced installation.
- The country stored in the organization's address is passed as country; if none is set, `Deutschland` is used.

For version 26.4.0

General

- Subscription code – mandatory. Code of the Samsung Classroom subscription that activates the app.
- User name – name under which the device is listed in the app. Prefilled with the placeholder `${user.name}`. The app only shows classes containing a member with exactly this name; the value should therefore match the Relution user name. Below the form, the portal displays the available user and device placeholders (see Advanced placeholders →).
- School name – optional. If the field is left empty, the name of the organization is passed.
- Apply default web filter list (`https://school.tabnova.com/block.list`) – activates the default block list of Samsung Classroom. Switched off by default.
- URL of the custom web filter list – optional. Address of a custom block list.

Clean up after lesson

This section defines what is reset on the device after the lesson.

- Trigger Mode – checkboxes Reboot and Sign out; both can be selected at the same time. Neither is selected in a new configuration.
- Clear cookies – deletes the browser cookies. Switched on in a new configuration.
- Folders and files to delete – list of file and folder names, e.g. `Downloads` or `DCIM`.

Apps to clear

The list contains apps whose data is cleared or which are uninstalled after the lesson. Via Add, free public apps are selected from the Relution App Store or from Managed Google Play; an app already contained in the list is not added twice.

Two checkboxes are available per app:

- Clear data – the app data is deleted.
- Uninstall – the app is uninstalled.

When an app is added, both checkboxes are enabled. Selected apps are removed from the list via Delete.

For version 26.4.0

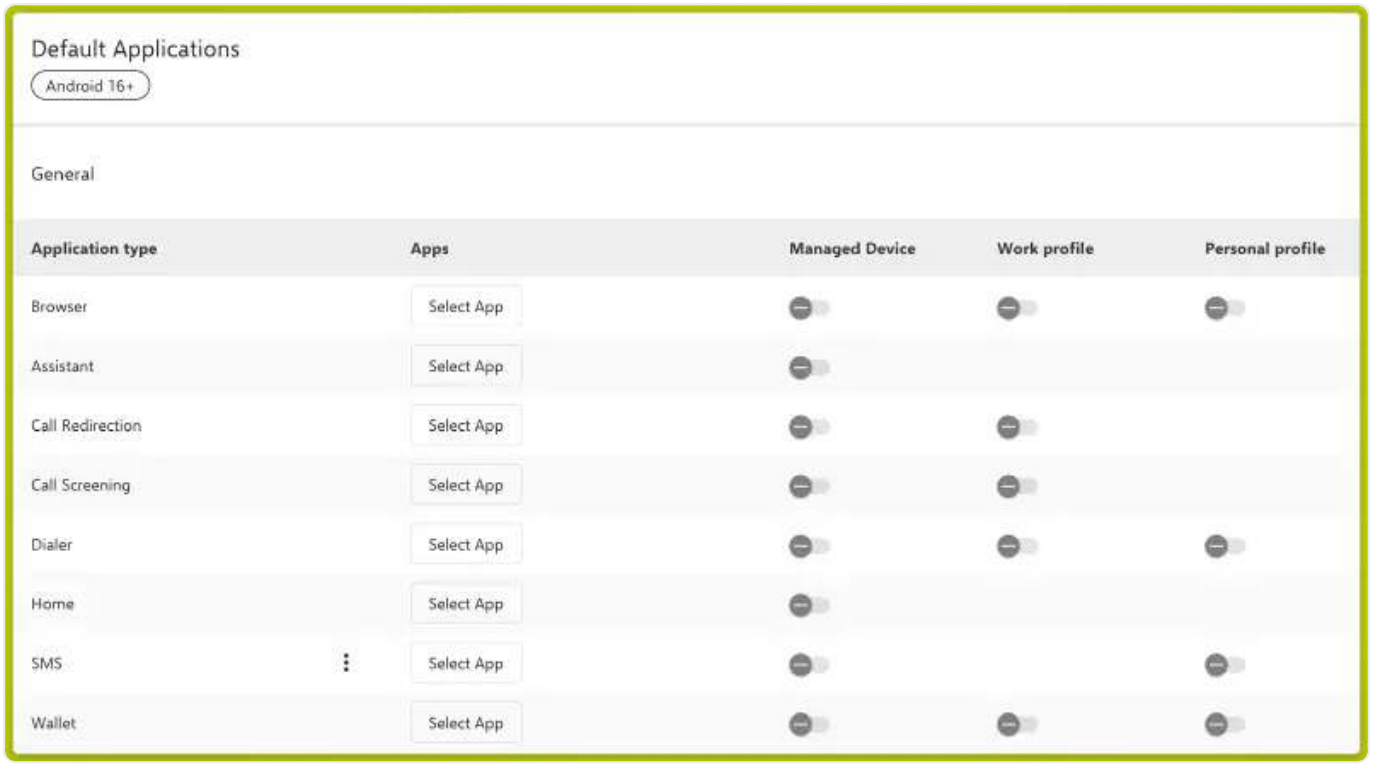
Default Applications

This policy allows administrators to set default apps for specific functions on managed Android devices.

The Default Applications policy allows administrators to configure default apps for various functions on Android devices. These settings are particularly useful for standardizing the user experience and ensuring that only approved applications are used. This feature is available for devices running Android 16+.

Function Overview

Administrators can configure default apps for the following functions in the table below:



Application Type	Apps	Managed Device	Work Profile	Personal Profile
Browser	Brave, Google Chrome	✅		
Assistant	Select App			
Call Redirection	Select App			
Call Screening	Select App			
Dialer	Select App			
Home	Select App			
SMS	Select App			
Wallet	Select App			✅

Configuration Options

- Select App: Administrators can choose the desired default app for each function.
- Managed Device: Enables or disables the configuration for fully managed devices.
- Work Profile: Enables or disables the configuration for the work profile.
- Personal Profile: Enables or disables the configuration for the personal profile.

> Default apps that are set for Managed Device or Work profile and are not included in any app configuration of the policy are automatically provided by Relution with the installation type Available. They are therefore not installed automatically. To ensure that a default app is installed, it is additionally added via the Manage apps configuration, e.g. as Force-installed. If one of the default apps is set to Blocked there, the configuration fails.

Note on Multiple Default Apps

Multiple apps can be selected for the same function, e.g. Brave and Google Chrome as browsers, as shown above. If several of these apps are installed on the device, Android uses the first app in the list. The decisive order is the one displayed after saving and reopening the configuration. It does not necessarily match the order of selection and currently cannot be changed manually.

For version 26.4.0

Samsung Knox

Relution supports Samsung Knox to provide advanced security and management features for Samsung devices.
Knox policies can be applied system-wide or within the work profile, depending on the device mode (Device Owner or Work Profile).
The Samsung Knox Service Plugin is automatically deployed on devices where the Knox policy is applied.
Configuration is done through this plugin and offers the following features:

Overview of Knox Features

The plugin provides the following functional areas:

Profile Settings

- Profile name and version
- Knox license key (e.g., Knox Suite, DualDAR)
- Enable/Disable Debug Mode

App and Policy Management

- Separate app policies (Work Profile vs. Device Owner)
- Device settings (e.g., Camera, Quick Panel, Firmware Updates)
- Work profile policies (Profile Owner)
- App assignments for accessing Knox SDK

For Version 26.4.0

Network & Security

- Advanced Wi-Fi configurations *(Premium)*
- APN profiles
- VPN profiles *(Premium)*
- Firewall profiles
- Proxy profiles (manual or PAC)

Certificates & Keys

- Certificate management *(Premium)*
- Deployment of certificates
- Approved apps for accessing private keys *(Premium)*
- UCM plugin configurations *(Premium)*

Device Configuration & Customization

- Device accounts and policies
- Device and settings customization *(Premium)*
- Key mapping for launching apps
- DeX customizations *(Premium)*
- Peripheral configurations
- USB device whitelisting

Advanced Profiles

- NPA Data Points *(Premium)*
- RCP Data Sync *(Premium)*
- Permission controls for apps

Behavior in Relution

- Configuration is done in the managed app configuration editor of the Knox Service Plugin.
- A Knox configuration takes precedence over a Knox Service Plugin configuration in the Manage Apps configuration and overwrites it.
- If the Manage Apps configuration of the same policy version already contains a Knox Service Plugin configuration, it is adopted when the Knox configuration is created. The form displays a notice to this effect.
- Placeholders for user, device and certificates are supported.
- If the plugin reports errors, the Knox configuration is shown in the device details with the yellow status Notice rather than as a violation (Violated). Without errors, the status is Resolved. The plugin's feedback can be viewed there.
- If the Knox configuration is removed from the policy, the Knox Service Plugin remains force-installed on devices where it is already installed and receives an empty configuration. This also applies if the plugin is blocked in Manage Apps.

For version 26.4.0

Notes

- Many features are only available on Knox-enabled Samsung devices. A list of supported devices is available on the Samsung Knox support page →.
- Some advanced options require a valid Knox Premium License.
- Before rollout, it is recommended to test with pilot devices, as Knox and Android Enterprise policies may overlap.

App distribution

Companies are increasingly deciding to support certain work processes with a mobile app. Among many other conceptual issues, the question of how this app should be distributed to users quickly arises. Often, the use case is that not only employees, but also external people should get the app - this can include for example service providers, partners or customers. In most cases, this app is also explicitly not intended for a broad customer base, but is aimed at selected professional users.

Method	Target audience	Account requirement
Apple App Store	general public	Apple ID
Google Play Store	general public	Google account
Apple TestFlight	selected users (beta)	Apple ID
Google Alpha/Beta Testing	selected users (beta)	Google ID
Internal enterprise app store	known, defined user group (e.g. employees, partners)	none, if distributed via MDM

For version 26.4

Distribution via public app stores

Apple and Google each provide an infrastructure for distributing apps. For Apple, apps are made available to end users through the Apple App Store. Every iOS device has the App Store app pre-installed. For this, the management and publishing of apps is done via the Developer Portal and App Store Connect. At Google, apps are made available to end users via the Play Store. The PlayStore app is preinstalled on every Android device. The administration and publication of apps for this is done via the developer portal. Apple and Google define the framework for publishing apps via their systems.

If a device is managed via an MDM system, the Store app can also be locked for the user and may therefore not be available to the end user.

Distribution via Apple App Store

Advantages

- Apps are available to end users via Apple’s standard mechanism
- Apps do not need to be re-signed and re-provisioned with an updated provisioning profile after one year
- Apps can be selectively enabled or blocked for individual countries
- Apps can be offered for a fee - if desired - in defined structures (Apple charges a percentage commission fee of 15% for this)
- Apple provides the infrastructure for distribution and billing

Disadvantages

- Users need an Apple ID on the device to install apps from the Apple App Store
- For enterprise customers with managed devices, the Apple App Store may be blocked via MDM
- All Apple specifications have to be met, such as support for new device classes like iPhone X
- In a review, Apple reserves the right not to publish the app or to subsequently remove it.
- The review can lead to delays of up to 10 days (currently, the average review duration is about 3 working days).
- Apps can only be made available to selected user groups on a very limited basis

Distribution via Google Play Store

Advantages

- Apps are available to end users via Google's standard mechanism
- Apps can be selectively enabled or blocked for individual countries
- Apps can be offered for a fee in defined structures (Google charges a percentage commission fee of 15% for this)
- Google provides the infrastructure for distribution and billing

Disadvantages

- Users need a Google account to install apps from the Play Store
- For enterprise customers with managed devices, the Play Store may be blocked via MDM
- All Google specifications have to be met
- After automated app scans, Google reserves the right to remove the app from the store at a later date.
- Due to technical scans, the release of apps can be delayed by a few hours.
- Apps can only be made available to selected user groups to a very limited extent

For version 26.4.0

Distribution via beta programs of the public app stores

Apple and Google each offer a beta testing program in addition to the distribution of public apps. At Apple, apps are made available for beta testing to end users via the TestFlight app. On iOS devices, this app can be installed from the Apple Store app.

The administration and publication of apps for this is done via the Developer Portal and App Store Connect in the TestFlight area. On Google, apps are made available for alpha or beta testing via the Play Store. The Play Store is preinstalled on every Android device.

The administration and publication of apps for this is done via the Developer Portal in the Alpha and Beta Testing area. Apple and Google define the framework for publishing apps via their systems.

Distribution via Apple Testflight

Advantages

- Apps are available to users via a mechanism provided by Apple
- Apps can be selectively enabled for individual users
- Apple provides the infrastructure for distribution and billing

Disadvantages

- Users need an Apple ID to install apps from the Apple App Store
- One-time installation of the TestFlight app is required to install the app
- Apple reserves the right not to publish the app in a "reduced" review
- Delays of up to 10 days may occur due to the review (currently, the average review duration is about two working days).
- App signature expires after 90 days

The TestFlight service is primarily intended for a short testing period before publishing an iOS app. It is not suitable for permanent operation due to the short validity of the signature.

Distribution via Google Alpha and Beta Testing

Advantages

- Apps are available to users via a mechanism provided by Google
- Apps can be selectively enabled for individual users
- Google provides the infrastructure for distribution and billing

Disadvantages

- Users need a Google ID to install apps from the Play Store
- Enterprise customers with managed devices may have Play Store blocked via MDM

Distribution via internal enterprise app store

In addition to distributing apps via the respective public stores, Apple and Google also offer mechanisms for distributing apps internally, primarily for enterprises. In the case of Apple, the Apple Enterprise program and an enterprise app store such as Relution is required.

The apps are made available to end users via a separate App Store app or a mobile website. Apps are managed via the developer portal.

Apps are distributed via the respective enterprise app store provider. At Google, apps can be made available for download and installation via a web service.

For special devices, such as Samsung, optimized installation and distribution mechanisms can be used. Apple and Google define the possibilities for distributing apps in parallel to their systems.

For version 26.4.0

Distribution of iOS apps via Enterprise App Store

Advantages

- Apps can be distributed to selected user groups, e.g. as a deep link or after logging in with previously configured user name and password
- Users do not need an Apple ID to install apps from an internal Enterprise App Store
- Not all Apple requirements have to be met
- The release of app updates is not delayed by a review from Apple
- Some enterprise app stores (e.g. Relution) can be used without device management (MDM)
- An existing user management system (ActiveDirectory/LDAP) can be connected so that users do not need new credentials

Disadvantages

- Apps are available to end users via a special mechanism that is approved by Apple, but requires initial configuration by the user (see here →)
- *Apps must be re-signed and re-provisioned with an updated Provisioning Profile after one year. However, this can be automated with Relution, so there is actually no disadvantage here.*
- The infrastructure for distribution can be provided as a cloud service or on-premise.
- According to Apple guidelines, apps may only be distributed to employees, interested parties and partners, but above all to a known group of users.

Distribution of Android Apps via Enterprise App Store

Advantages

- Apps can be distributed to selected user groups, e.g. as a deep link or after logging in with previously configured user name and password
- Users do not need a Google ID to install apps from an internal enterprise app store
- Not all Google requirements have to be met
- Release of app updates is not delayed by Google technical scans
- Some enterprise app stores (e.g. Relution) can be used without device management (MDM)
- An existing user management system (ActiveDirectory/LDAP) can be connected so that users do not need new credentials.

Disadvantages

- Apps are available to end users via a special mechanism that is approved by Google, but requires initial configuration by the user
- The infrastructure for distribution must be provided as a cloud service or on-premise

For version 26.4.0

Manage APK apps

There are three possible ways to deploy self-developed enterprise apps on Android devices enrolled via Android Enterprise. The official way provided by Google and recommended by us is the distribution via the managed Play Store.

Since Relution 26.2, APK apps uploaded to the Relution App Store can also be distributed as custom apps on fully managed devices, including those with a personal profile. Security mechanisms of Android Enterprise do not have to be deactivated for this. This option is not available on devices enrolled as a work profile.

The third way is the direct distribution of an APK file, e.g. via the Relution Legacy app, web or email. Since various security mechanisms of Android Enterprise have to be deactivated, this way is not recommended and only makes sense in exceptional cases.

Distribution via the Play Store

There are two ways to upload apps to the Play Store. In both cases, a developer account is necessary. A Google developer account costs a one-time fee of $25.

Deploy app via the Play Store console (recommended)

The app is regularly uploaded to the Play Store via any developer account (Google Play Console →). We recommend using an official enterprise account for this purpose.

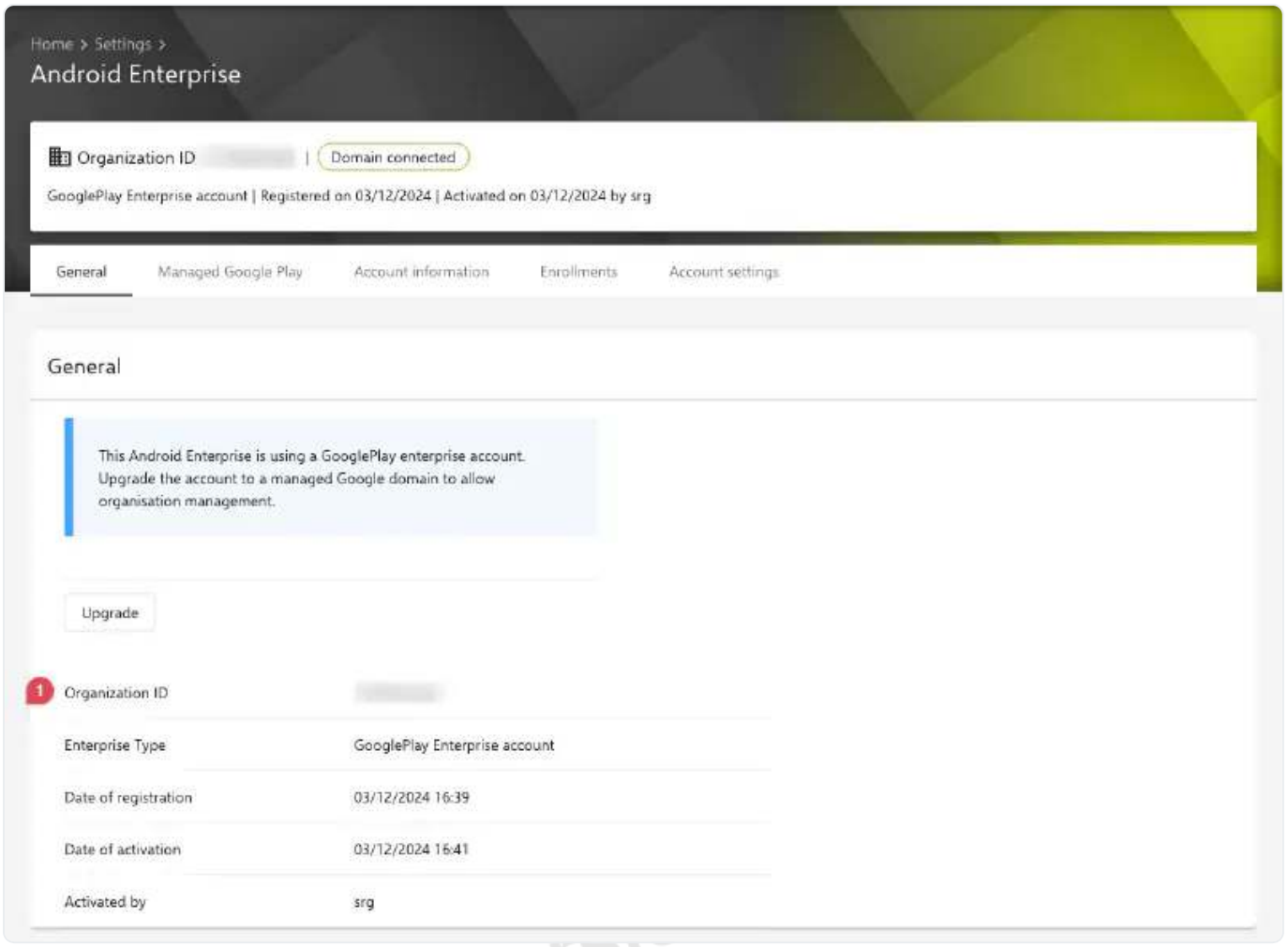
For version 26.4.0

Here, all the setting options of the Play Store are available, such as the possibility to pre-publish development versions of the app only for certain groups of people.

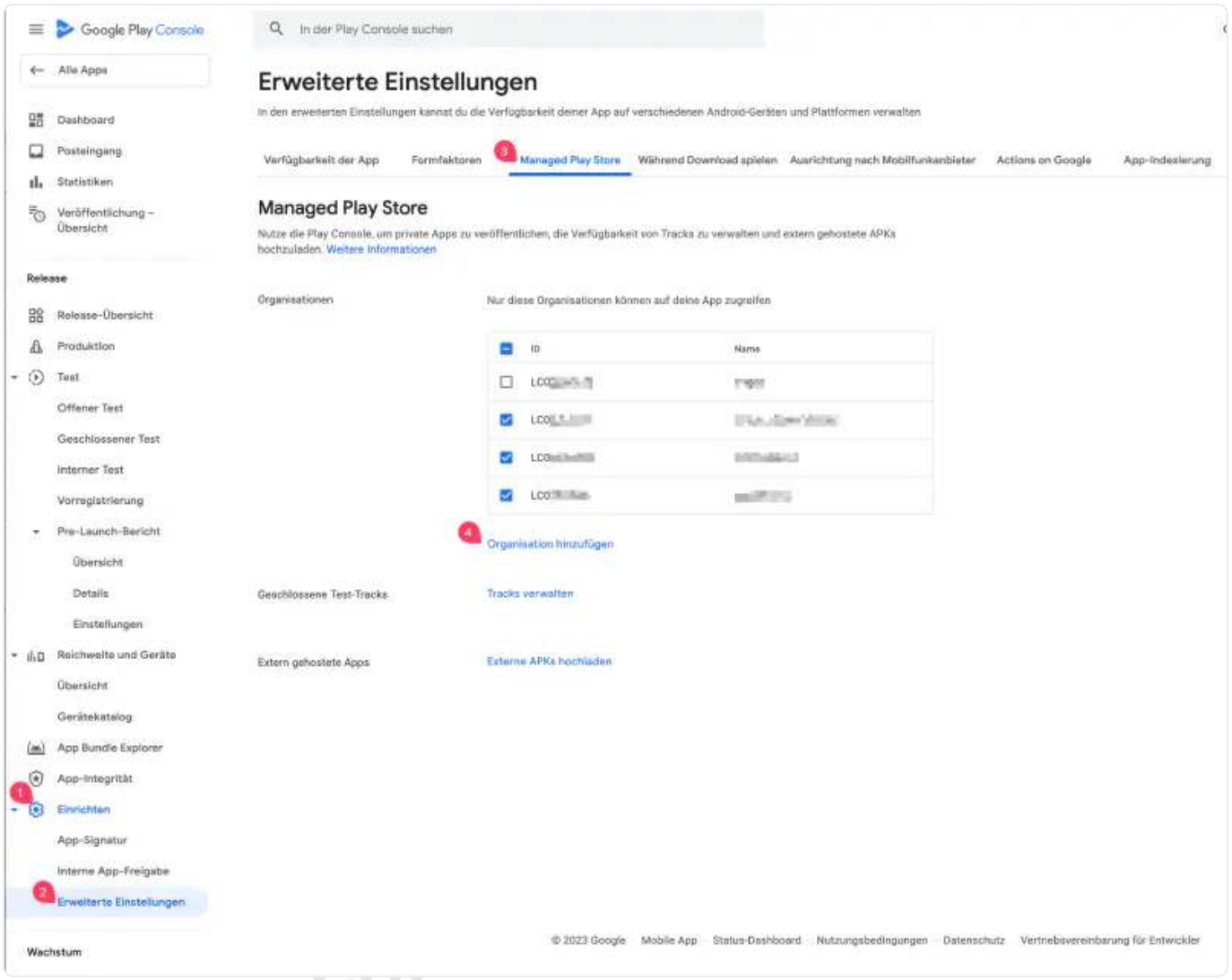
If the app is not to be available to the public, its availability can additionally be restricted to a specific organization. Caution: This setting cannot be reversed afterwards. If the app is to be offered publicly in the future, it must be published again under a different package name.

The big advantage is that the app can then be released for other companies or company accounts. This can be helpful, for example, in the event of a server relocation, but also if the access data to the Google account used for Android Enterprise is lost.

To restrict the app to that organization, its organization ID can be stored under `Setup` → `Advanced settings` → `Managed Play Store`. The ID starts with `LC0...`. This ID is visible e.g. in Relution under `Settings` → `Device platform specific` → `Android Enterprise`.


Home > Settings >
Android Enterprise
Organization ID
Domain connected
GooglePlay Enterprise account | Registered on 03/12/2024 | Activated on 03/12/2024 by srg
General
Managed Google Play
Account information
Enrollments
Account settings
General
This Android Enterprise is using a GooglePlay enterprise account. Upgrade the account to a managed Google domain to allow organisation management.
Upgrade
1
Organization ID
Enterprise Type
GooglePlay Enterprise account
Date of registration
03/12/2024 16:39
Date of activation
03/12/2024 16:41
Activated by
srg

For versi



Upload via the Play Store dialog in Relution

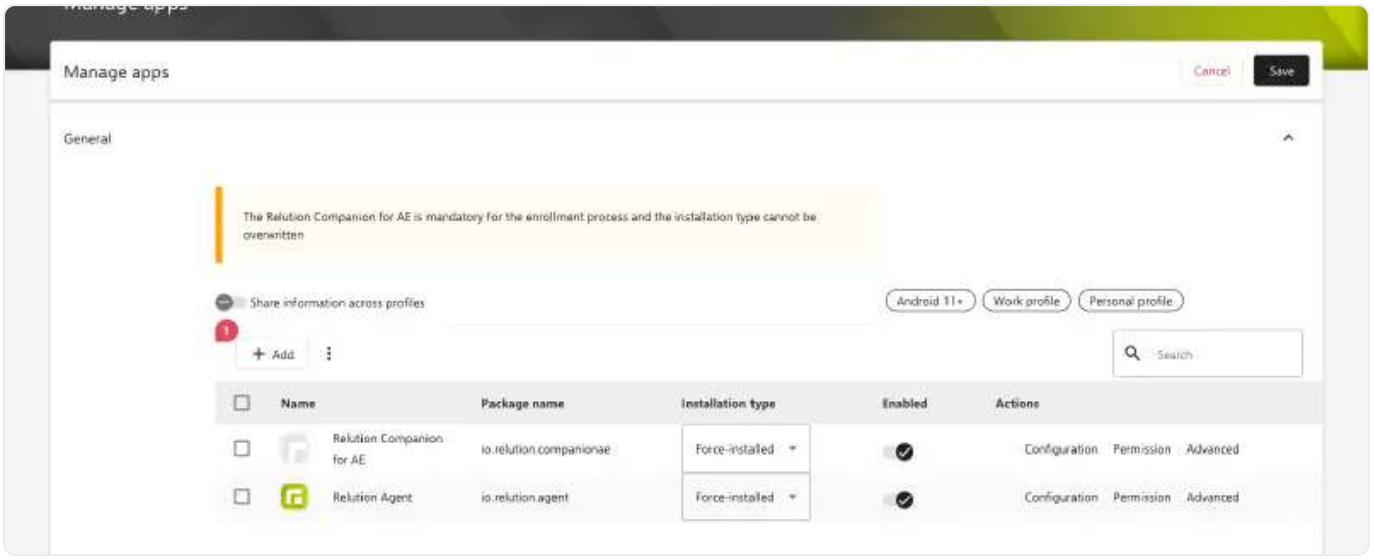
Instead of uploading the app via the Google Play Console, it can also be uploaded directly from Relution. However, the Google account used to set up Android Enterprise must be a corresponding developer account.

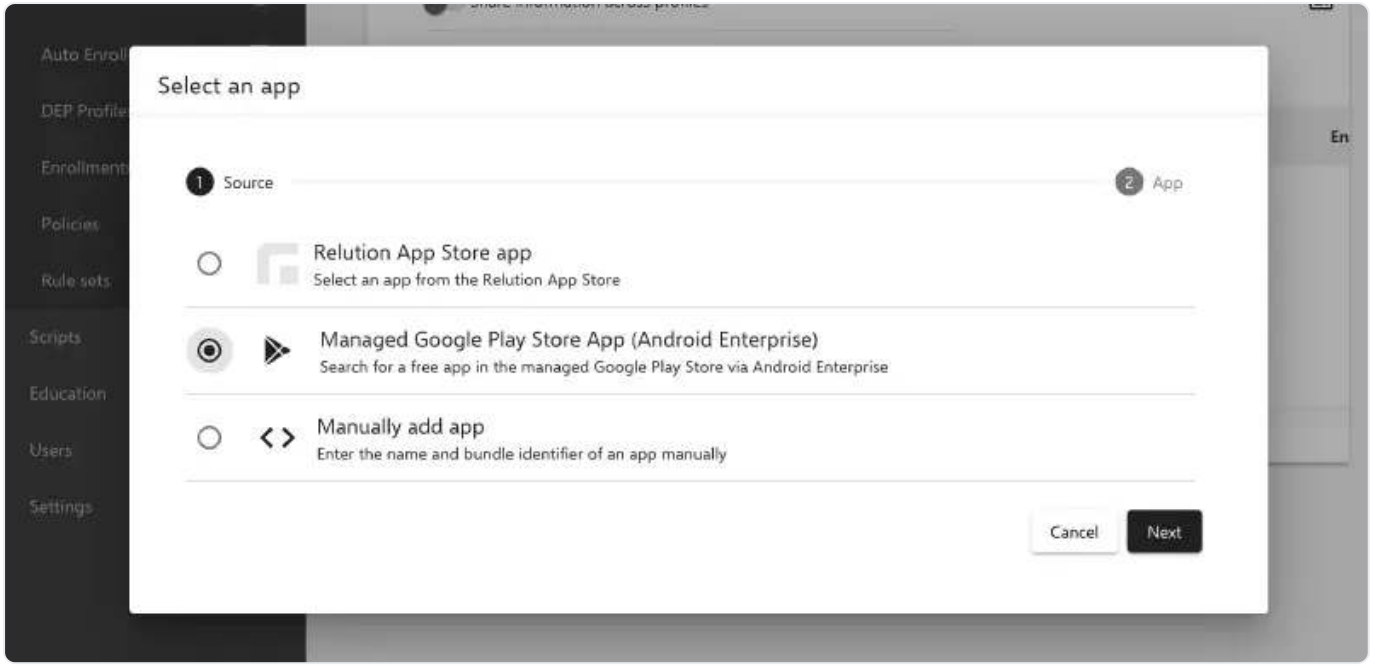
Apart from the name of the app, no other settings can be made here and there is also no possibility to activate the app for other companies or enterprise accounts afterwards. Due to these restrictions, we generally advise against this option.

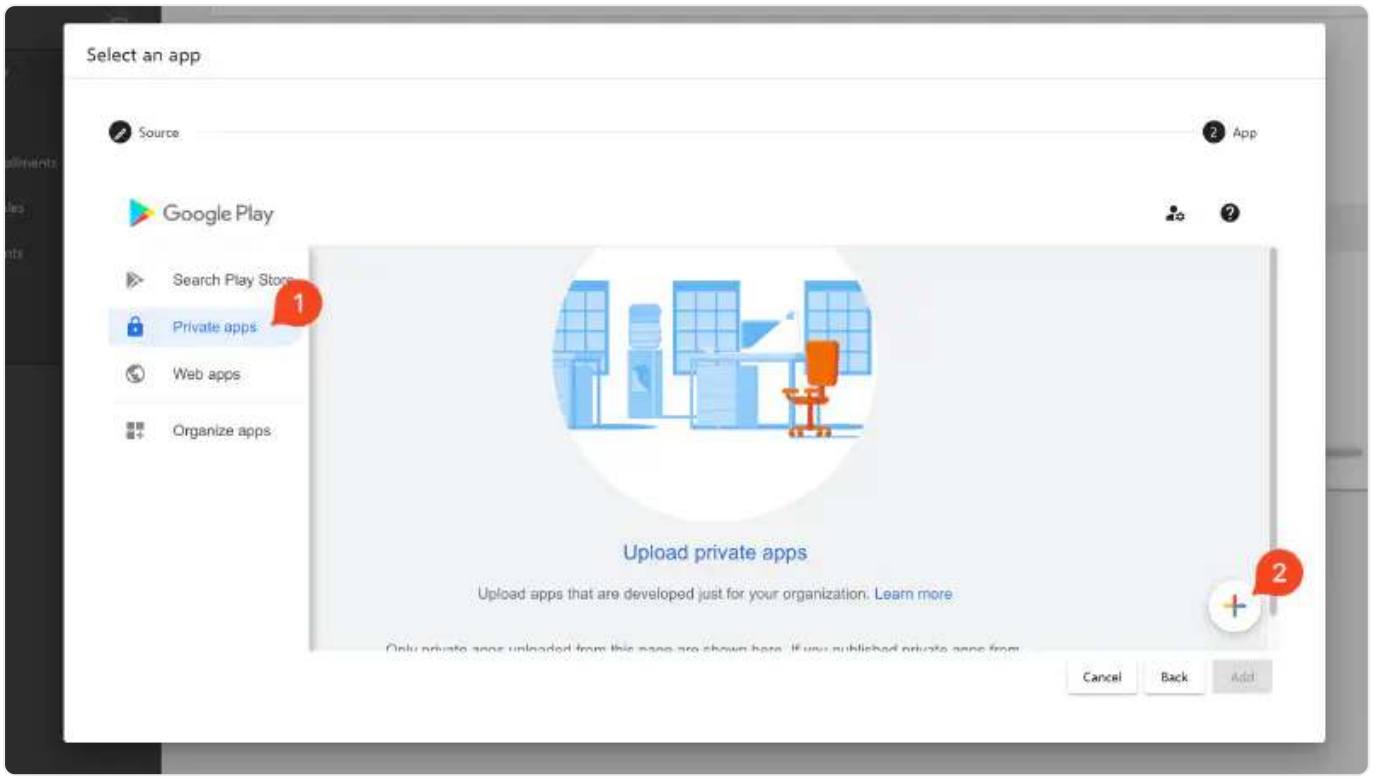
An app is uploaded as a private app as follows:

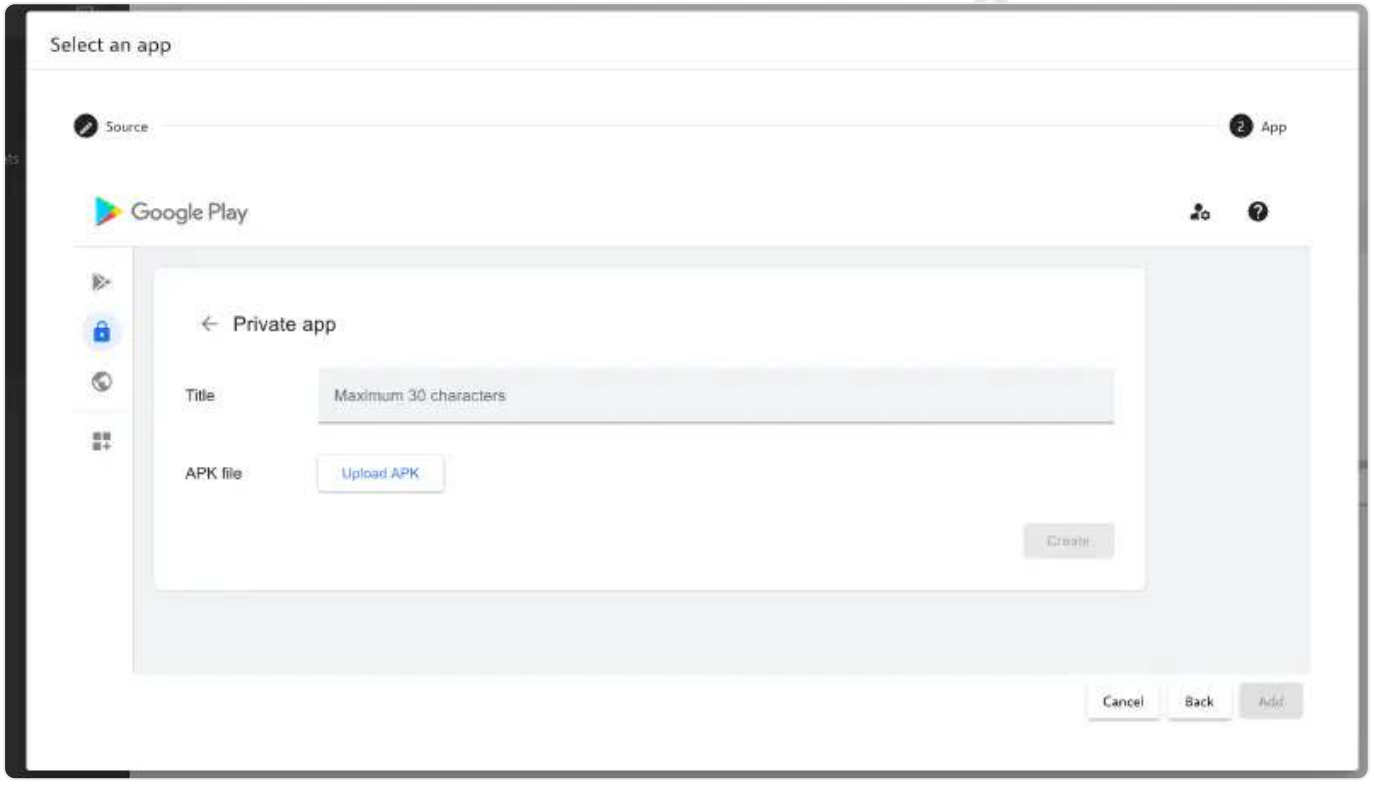
1. In Relution, `Devices` → `Policies` is opened.
2. Any Android Enterprise policy is opened and a Manage apps configuration is added.
3. Add is clicked in the configuration.
4. Managed Google Play Store App (Android Enterprise) is selected.
5. The link Private Apps is opened.
6. + is clicked to add a new app.

Caution: The package name of the app must be unique. If the app is already available in the Play Store, even as a private app from another company, it cannot be uploaded again. We therefore generally recommend uploading via the Play Store, which can then also be used to unlock the app for other organization IDs.


Manage apps
Cancel
Save
General
The Relution Companion for AE is mandatory for the enrollment process and the installation type cannot be overwritten
Share information across profiles
Android 11+
Work profile
Personal profile
+ Add
Search
Name
Package name
Installation type
Enabled
Actions
Relution Companion for AE
io.relution.companionae
Force-installed
Configuration
Permission
Advanced
Relution Agent
io.relution.agent
Force-installed
Configuration
Permission
Advanced


Auto Enroll
DEP Profiles
Enrollment
Policies
Rule sets
Scripts
Education
Users
Settings
Select an app
1 Source
2 App
Relution App Store app
Select an app from the Relution App Store
Managed Google Play Store App (Android Enterprise)
Search for a free app in the managed Google Play Store via Android Enterprise
Manually add app
Enter the name and bundle identifier of an app manually
Cancel
Next





Distribution of an APK file

Since Relution 26.2, native apps uploaded to the Relution App Store in the `.apk` format can be distributed directly on fully managed devices, including those with a personal profile:

- In the Manage apps policy configuration via `Add` → `Relution App Store app`. The app is added with the installation type Custom.
- Via the Install app from the Relution Store action. Native apps can only be selected there if exclusively fully managed devices are selected.

In both cases, Relution must have determined the signing certificates of the APK. The relaxed security settings described below are not required for this option.

On devices enrolled as a work profile, custom apps are not installed. The Select Play Store app from the Relution Store action available there only offers Play Store apps.

For these devices and for installing downloaded APK files (e.g. from email or the web), the following policy settings are required:

1. configuration Advanced security overrides.
    - The option Allow from unknown sources must be set to Allow untrusted app installs on entire device.

      This basically allows users to install APK files from any source on the device!
2. configuration Play Store management
    - The option Enable the restricted Play Store must be deactivated.

      If the restricted Play Store is active, the device will remove apps that have not been installed on the device using the Manage apps configuration or are part of the system after about 10 minutes.

      This allows users to install any apps from the Play Store in the managed profile.

For version 26.4.0

Once these settings are made it is again possible to install any APK files on the device. Since users can install APK files from any source in this mode, we generally advise against enabling these settings. Furthermore, there is no easy way to ensure the up-to-dateness of apps.

Alternatively, the package name of the corresponding app can be manually added in a Manage apps configuration to allow it. This should prevent the app from being automatically removed by the device.

There are various options for distributing APK files, for example:

Installation via the Relution Legacy app.

For this, the Relution Legacy App is installed on the device via a Manage apps configuration. Afterwards, users can log in to the app and get access to all native Android apps that are stored in the Relution Store. Users can download and install these apps via the Legacy app. Depending on the Android version, users must also grant the Relution app the right to request app installations.

If the Companion (Legacy) is additionally enrolled (requires another device license!), administrators can alternatively install apps via action on devices enrolled as a work profile. Depending on the device type, users may still have to agree to the installation manually. On fully managed devices, including those with a personal profile, this is not necessary: the Install app from the Relution Store action is available there without additional enrollment or device license (see above).

Installation via email

Users receive the APK file to be installed from the company via email.

Installation from the web

Users receive the APK file to be installed via a download link that is distributed via email, Messenger or SMS, for example.

Further links

Android Enterprise Help →

For version 26.4.0

Self-hosted apps

Self-hosted Android apps offer companies and organizations control over their data and allow them to increase their privacy and security. By installing and managing these apps on their own servers, they retain full control over their sensitive information while reducing their dependence on external service providers.

This function is available from Relution Server 5.23

Prerequisites

- It is necessary to have an active Android developer license.
- The automatically generated Google Play Managed accounts cannot be used when uploading apps via the Managed Play Store, as these accounts are not linked to an active Android developer account and cannot be linked.
- Self-hosted private apps must be configured in the Google Play account with an active Android developer license.
- A Google account must be linked to Relution `Home` → `Settings` → `Android Enterprise`.

> They cannot be installed remotely by IT administrators on devices with work profiles. Users with a work profile must install these apps manually via Managed Google Play.

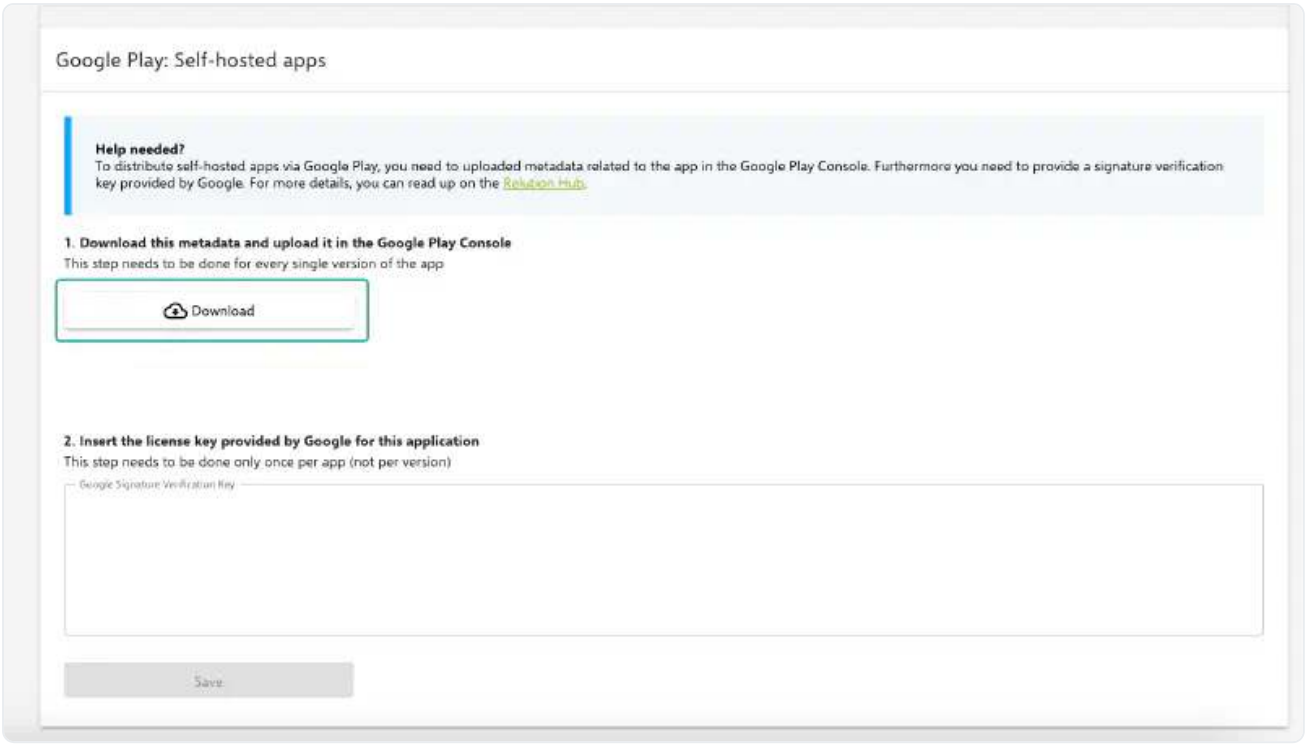
For version 26.4.0

App and metadata

1. the `apk` file must be uploaded in Relution under `Home` → `Apps` → `App Store` → `Add` (dialog Add a new app). An existing app can also be used.

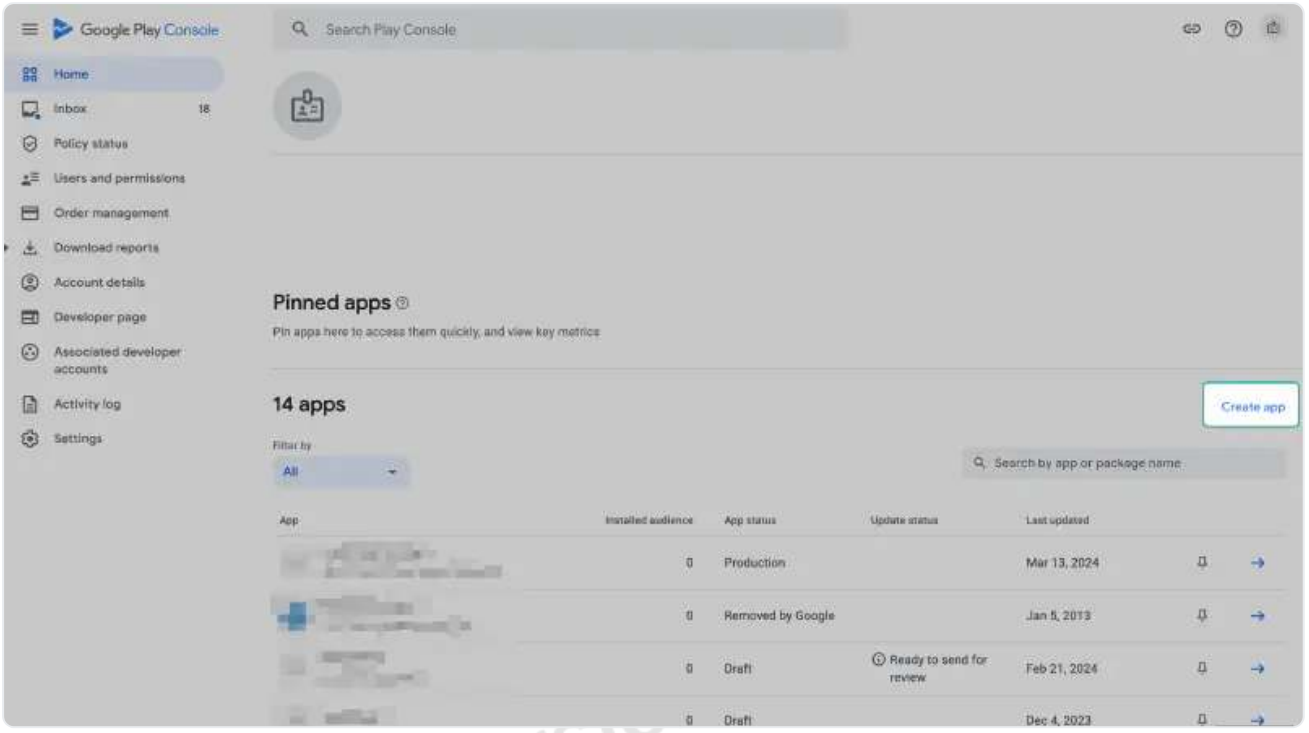
   > The app version must have the Release status in Relution. The Google Play: Self-hosted apps section is only displayed in the Information tab if the version under Release is selected there.

2. the metadata must be loaded in `json` format via the Download button in the Google Play: Self-hosted apps section of the app's Information tab.



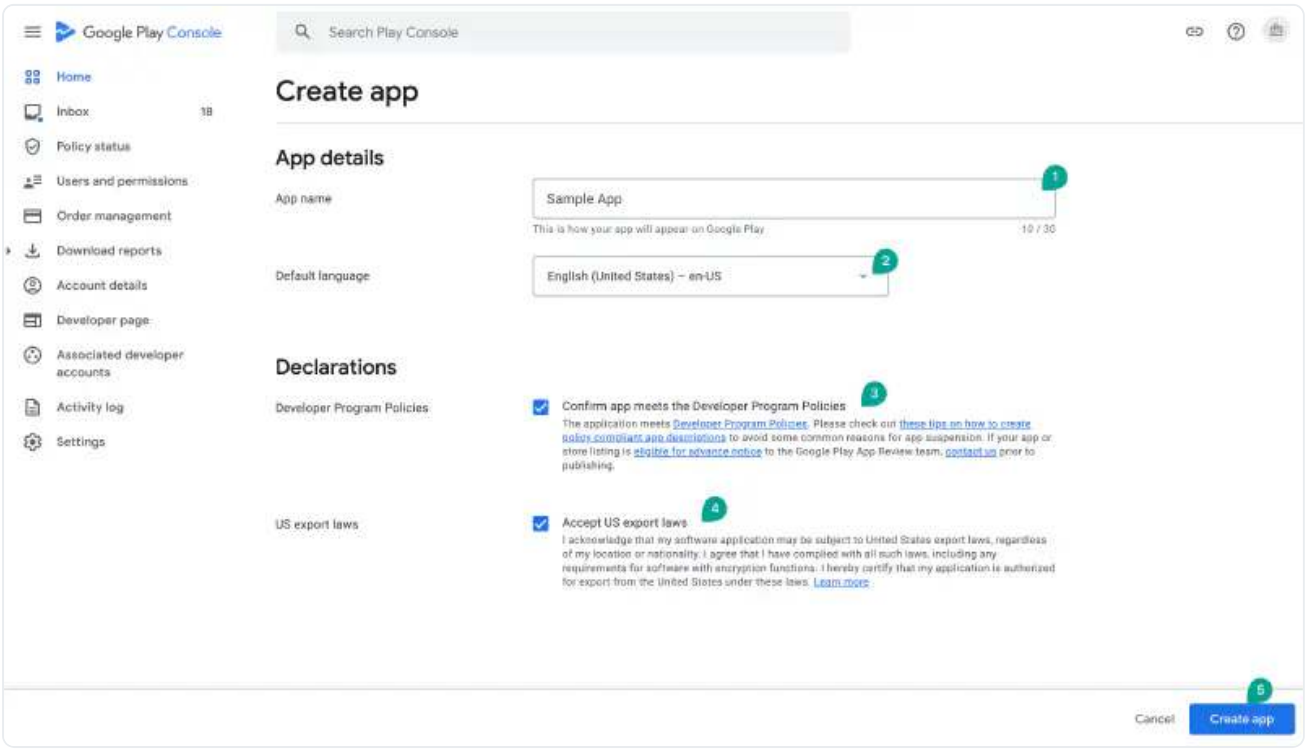
Create app

1. The Google Play Console → is opened.
2. A new app is created under `Create app`



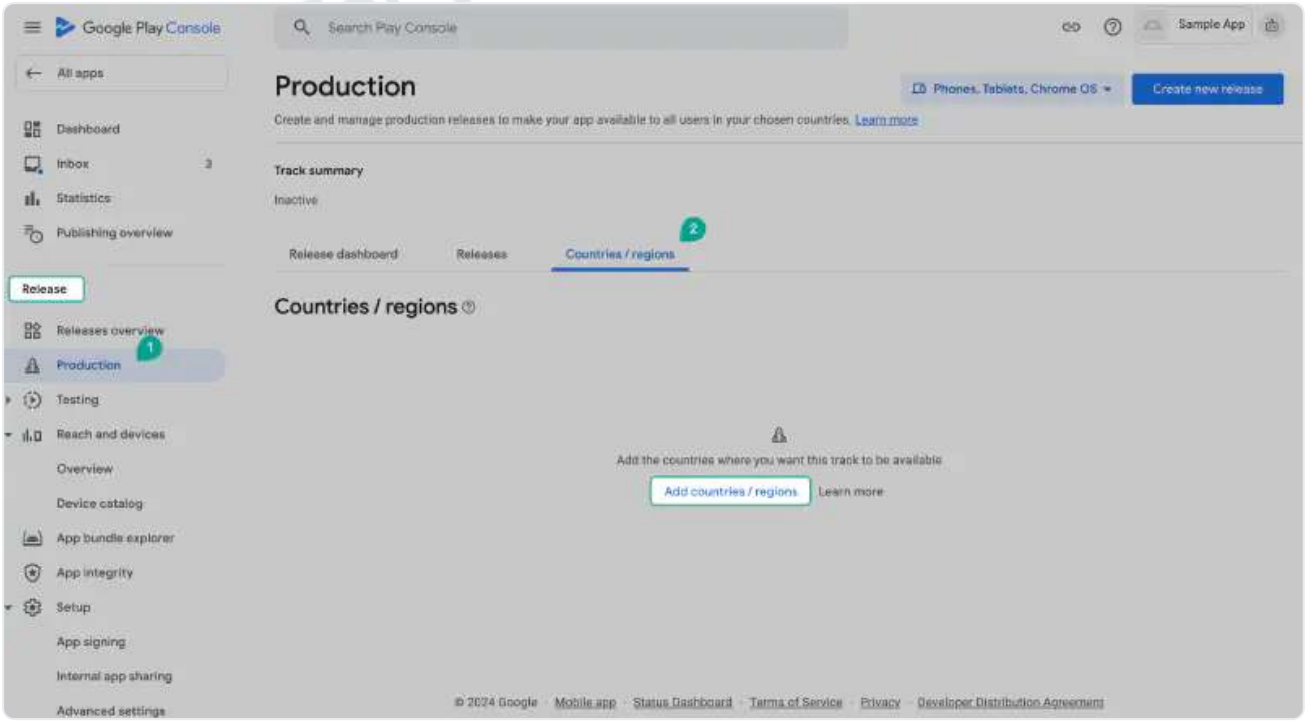
For versi

3. App details are added



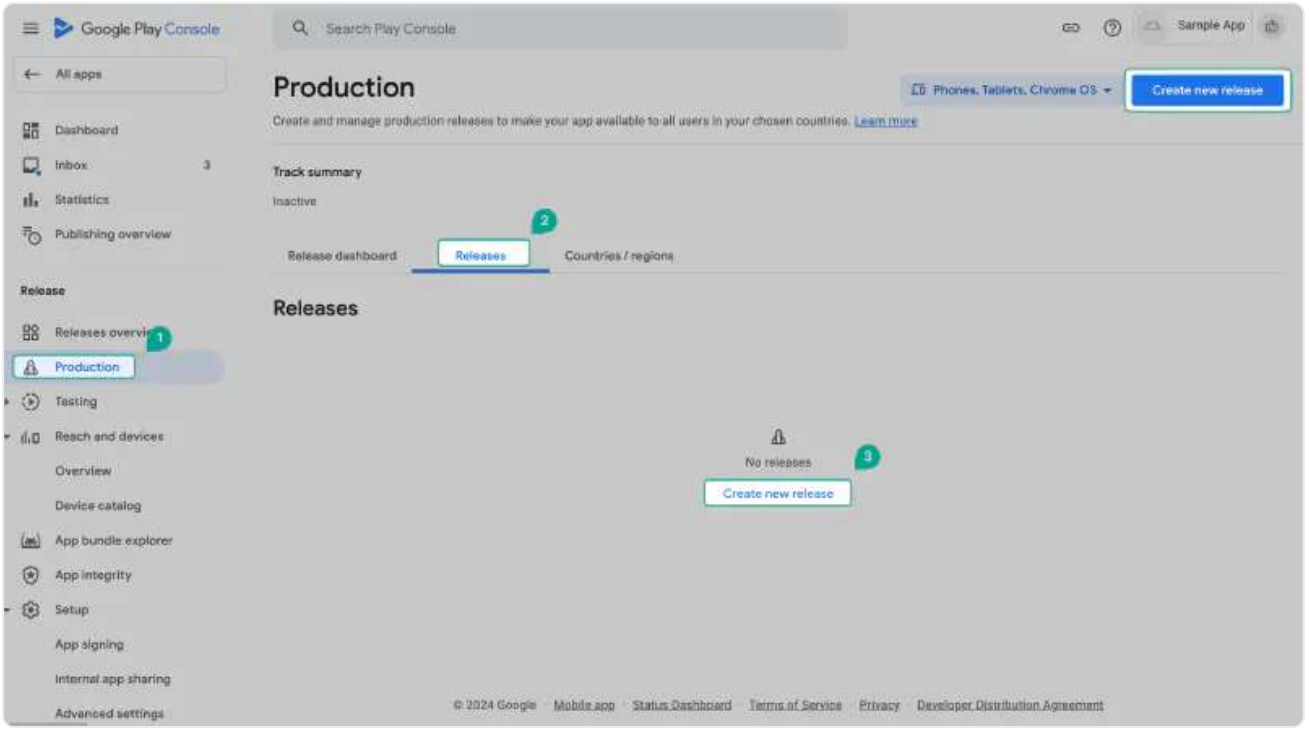
An app icon can be added under Grow > Store presence > Main Store listing in the Graphics section

4. Countries in which the app should be available are added under `Release` → `Production` → `Add countries / regions`



for version 26.4.0

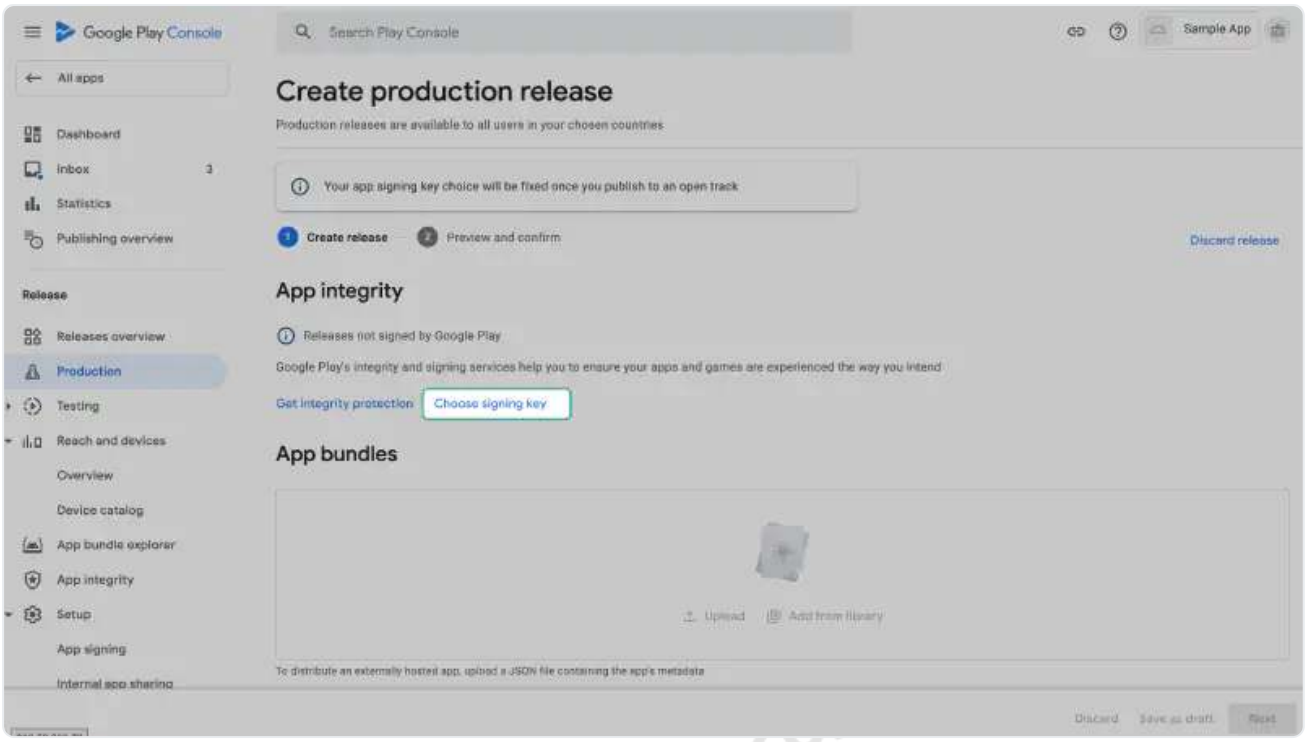
5. A new release is created under `Release` → `Production` → `Releases` → `Create new release`

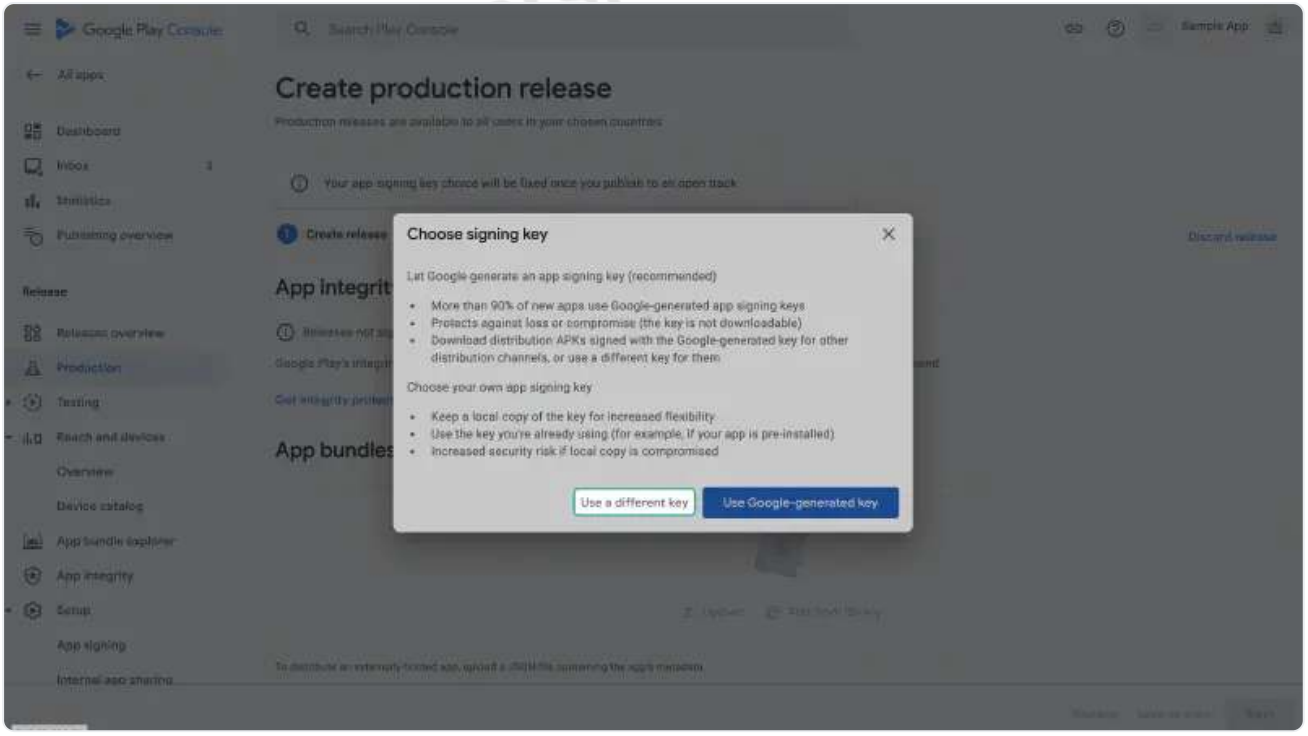


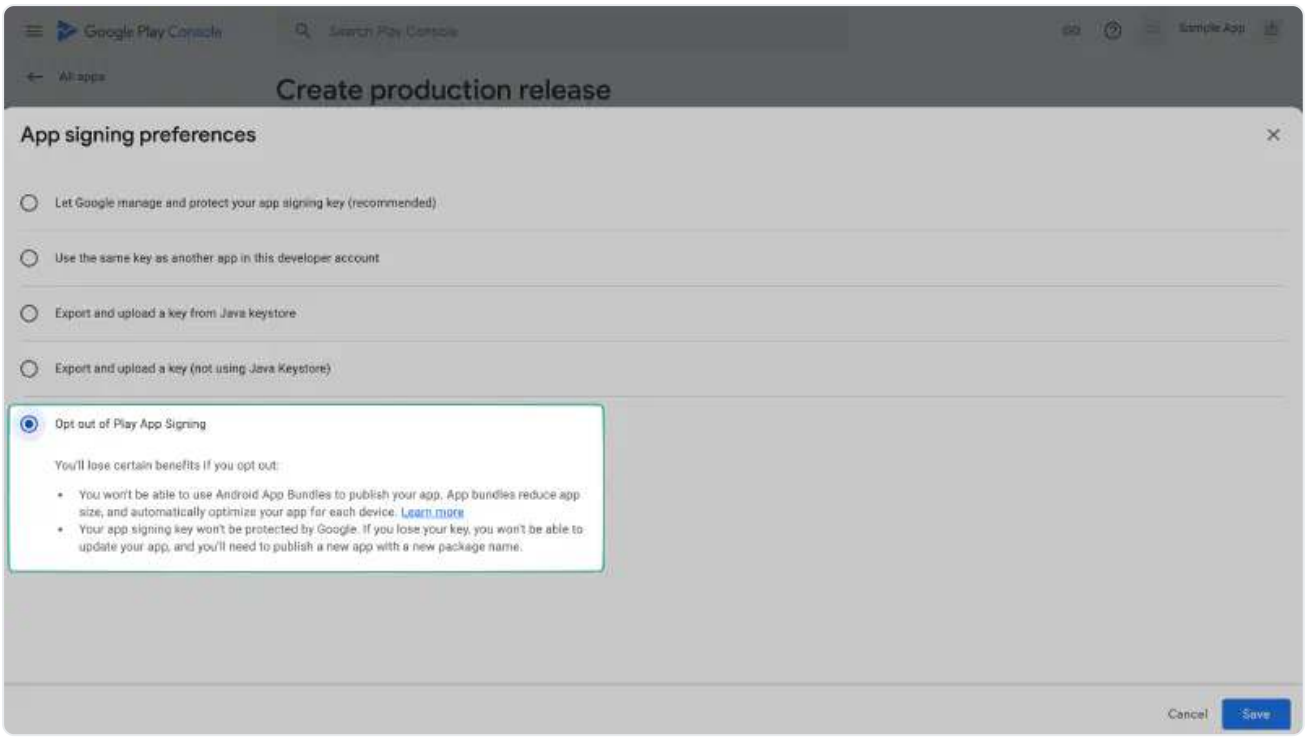
For version 26.4.0

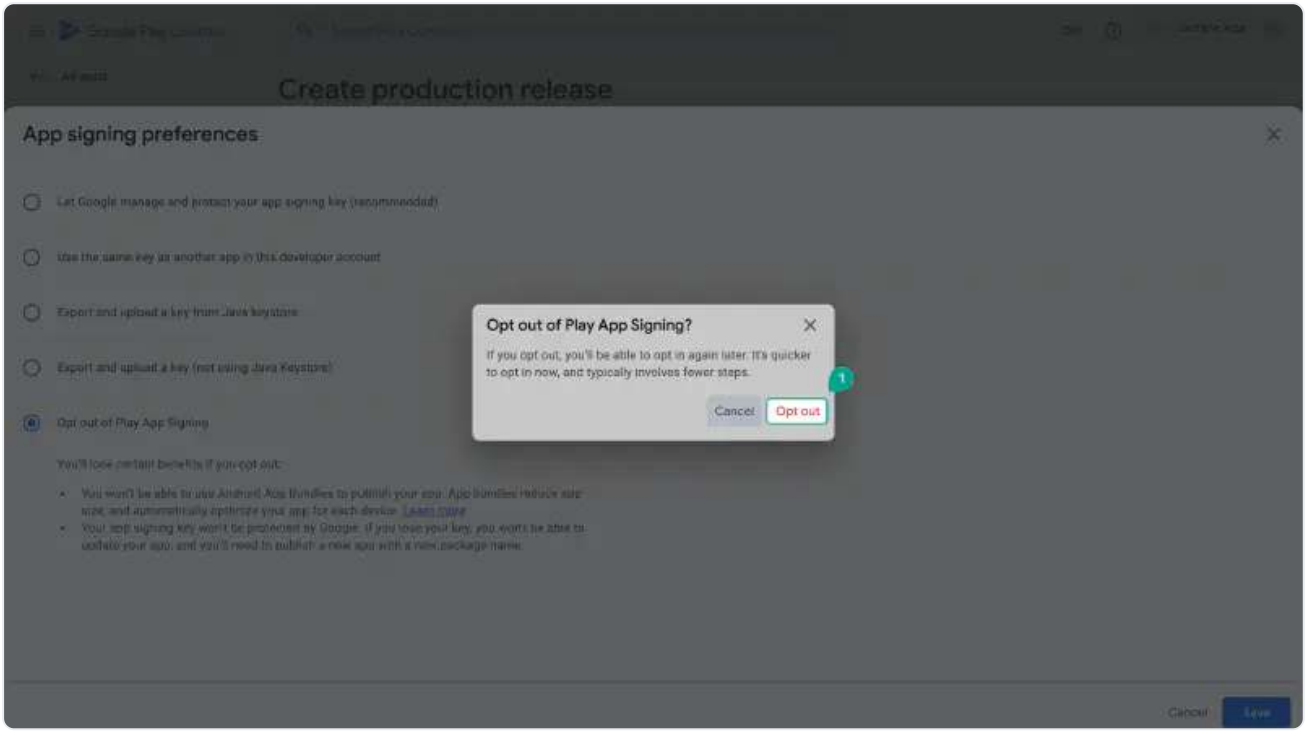
Signing

1. The signing key is selected via `Use a different Key` → `Opt out of Play App Signing` → `Opt out`

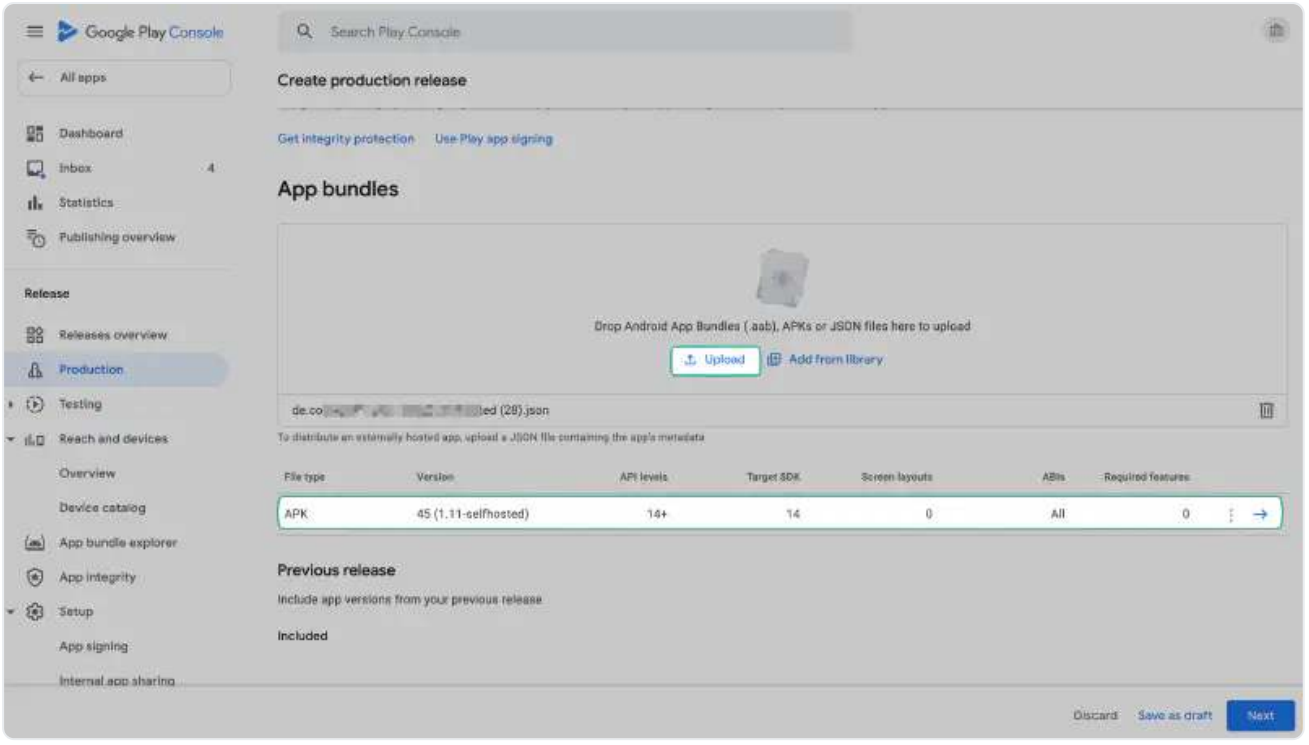




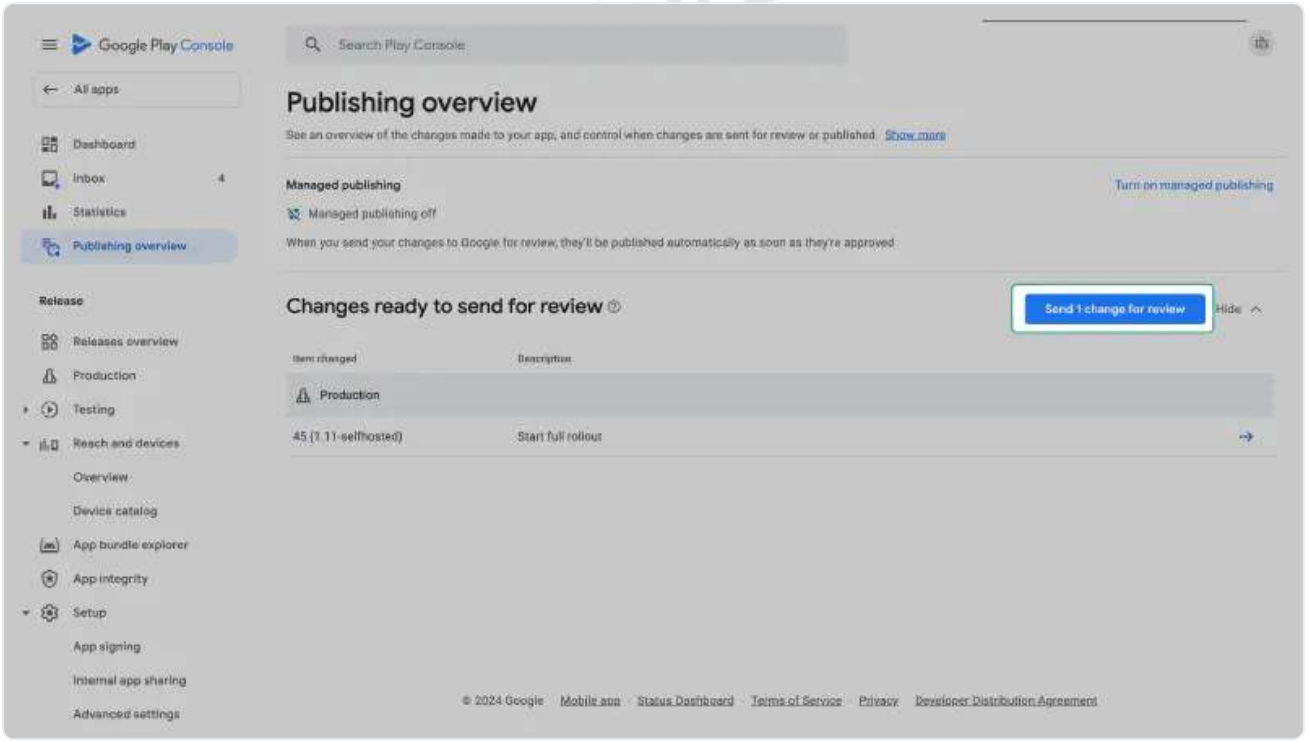

Google Play Console
Search Play Console
Sample App
All apps
Create production release
App signing preferences
Let Google manage and protect your app signing key (recommended)
Use the same key as another app in this developer account
Export and upload a key from Java keystore
Export and upload a key (not 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
1

2. The `json` metadata file from `Relution Portal Step 2` is uploaded, and `Next` and `Save` are clicked

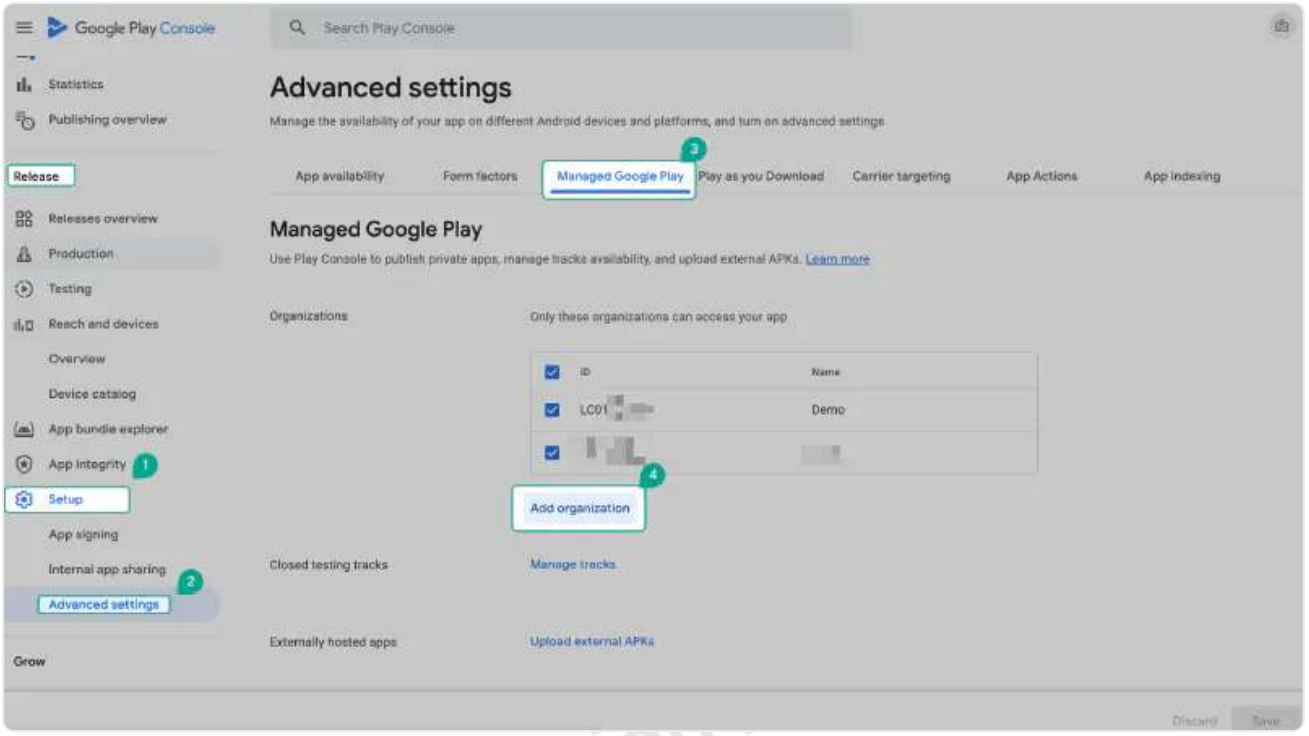


3. The change is submitted for review via `Send 1 change for review`

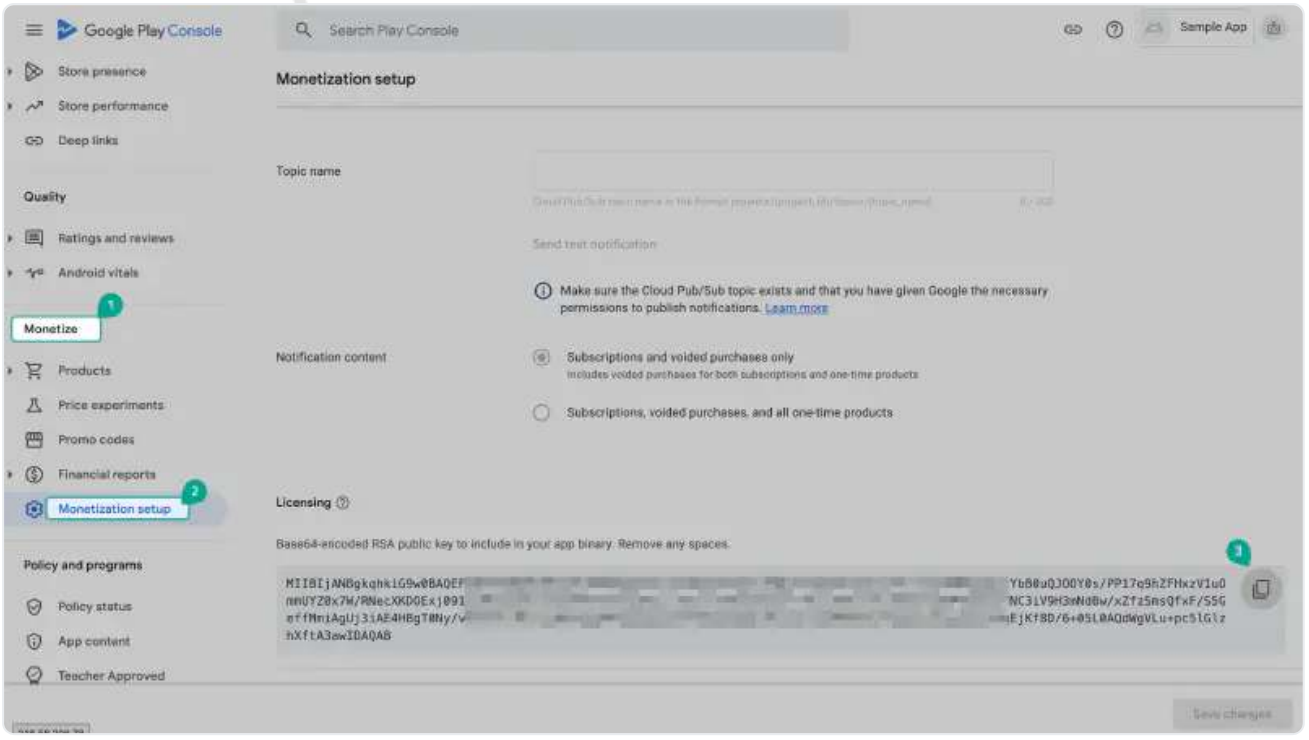


Release app for organization

1. The Google OrganizationID is copied from the Relution Portal under `Home` → `Settings` → `Android Enterprise` and added to the Google Play Console

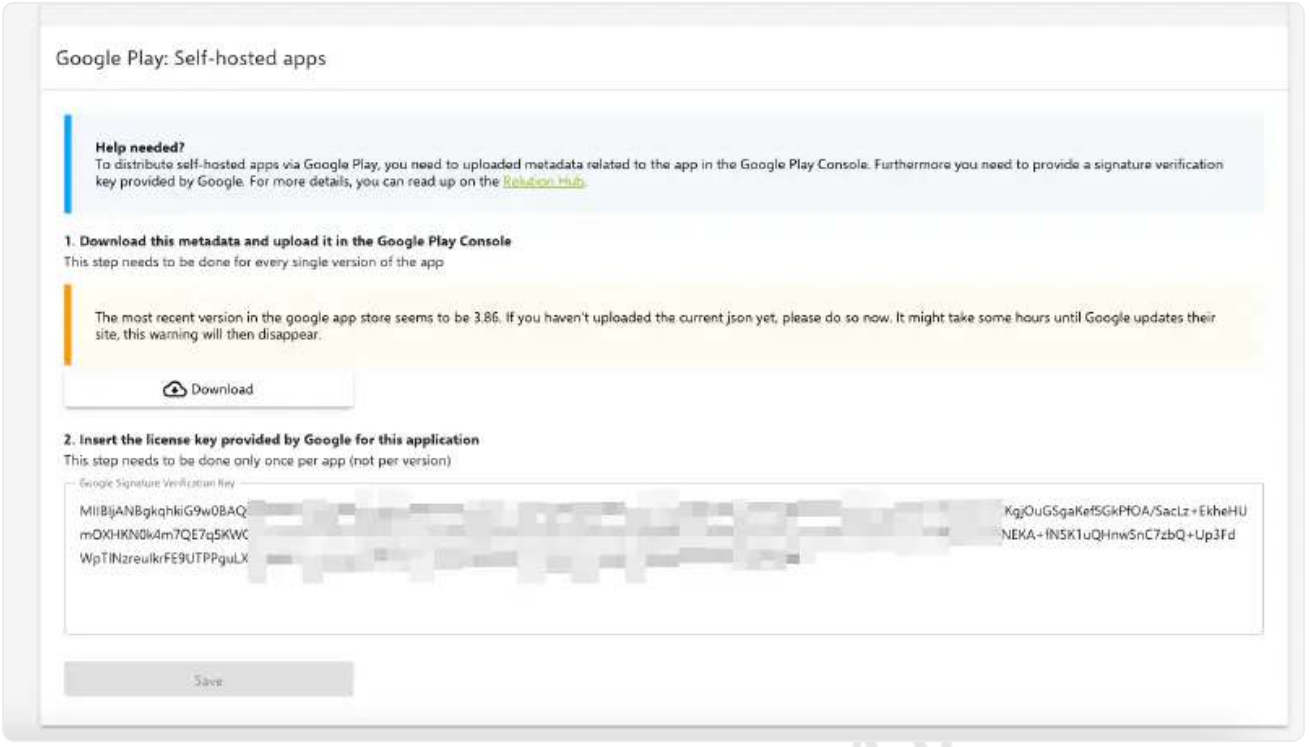


2. The RSA key of the app is copied and added to the app in Relution `Monetize` → `Monetization Setup`



For version

3. The RSA key is pasted in Relution into the Google Signature Verification Key field in the Google Play: Self-hosted apps section of the Information tab of the released app version and saved with Save. This step is only needed once per app, not per version.



For version 26.4.0

Update existing app

1. A new version of the `apk` is uploaded to the Relution App Store under `Home` → `Apps` → `App Store` → `App`
2. The metadata `json` is downloaded

> The most recent version in the google app store seems to be x.xx . If the current json has not been uploaded yet, upload it now. It might take some hours until Google updates their site, this warning will then disappear

3. A new app release is created in the Google Play Console
4. The metadata `json` of the app from Relution is uploaded
5. The change is sent for review

Related topics

- Android Enterprise enrollment → — Setting up Android Enterprise devices.
- MAM app management in Relution → — Basics of app management.

Provide web links

Web links can be provided on Android Enterprise devices. Unlike Apple, web links on devices with `Android Enterprise` enrollment are provided via the `Managed Google Play Store`

Configuration

This requires the `Manage Apps` policy configuration:

1. In the Relution portal, `Devices` → `Policies` is opened and `Add` is clicked
2. An `Android Enterprise` policy is created and a `name` is assigned. `Save` is clicked
3. After clicking `Add`, the `Manage apps` option is selected and the process continues with `Add details`
4. In the next step, Add is clicked again. In the Select an app dialog, the Managed Google Play Store App (Android Enterprise) option is selected under Source and Next is clicked
5. The App step displays the Managed Google Play Store. Web Apps is clicked in its left menu
6. To create a new `Web-App`, the `+` icon in the lower right corner is clicked
7. Weblinks are created and their basic settings are configured in the next dialog
8. The newly created Web App is clicked and confirmed with Select. The dialog closes and the web app appears in the list of the Manage apps configuration
9. The Installation type is adjusted if required and the configuration is applied with Save
10. The policy is published and assigned to the desired devices

With the default installation type Force-installed, the web app is installed automatically on the devices. With Available, it is offered for installation in the Managed Google Play Store on the device.

For version 26.4.0

Play Store shows no apps

On Android Enterprise devices, it may happen that the Google Play Store appears empty or does not display any apps. This typically occurs if certain configurations or approvals in the Managed Google Play Store or Relution are missing. Here's a step-by-step guide to fix this issue:

Find and approve the app in the Managed Google Play Store

Before an app can appear on a device, it needs to be found and approved in the Managed Google Play Store.

1. In a web browser, https://play.google.com/work → is opened.
2. The desired app that is not showing on the device is searched for.
3. Approve the app is used to make the app available within the organization.

Add the approved app to a collection in Relution

After the app has been approved, it needs to be added to an app collection in Relution. Steps in the Relution Portal:

1. Sign-in to the Relution Portal is performed.
2. In the Manage App configuration, add is clicked.
3. Managed Google Play Store App (Android Enterprise) is selected.
4. Manage Apps is selected in the side menu.
5. A collection is created via Create a collection, or an existing one is selected.
6. The app that was just approved in the Managed Google Play Store is selected and added to the collection.

Set the app to available in a policy

To ensure the app is visible on devices, it must be set to available within the appropriate Android Enterprise policy in Relution.. This ensures the app appears on assigned devices. Steps:

1. In the Relution Portal, the Android Enterprise Policy is opened.
2. Manage Apps is selected.
3. The app is located in the list, and Available is selected in the Installation type column. Apps newly added from Managed Google Play are set to Force-installed by default. The Enabled toggle must also be switched on.

Once all steps are completed, the app should appear in the Google Play Store on the device and be available for installation.

For version 26.4.0

Managed Config Chrome

Managed app configurations can be created and applied for Google Chrome within Relution.

Blocklist

`Portal` → `the AE Policy` → `Manage Apps` → `Google Chrome (add if not present)` → `Configuration`

A pop-up window will open here. In the Block access to a list of URLs field, the list below must be entered. Multiple websites are separated by commas.

Blocklist →

```
[
  "example.com",
  "https://ssl.server.com",
  "hosting.com/bad_path",
  "https://server:8080/path",
  ".exact.hostname.com",
  "file://*",
  "custom_scheme:*",
  "*"
]
```

Bookmarks

`Portal` → `the AE Policy` → `Manage Apps` → `Google Chrome (add if not present)` → `Configuration`

Bookmarks →

A pop-up window will open here. In the Bookmarks field, the list below must be entered. Multiple websites are separated by commas.

```
[
  {
    "toplevel_name": "Company bookmarks"
  },
  {
    "name": "Relution",
    "url": "relution.io"
  },
  {
    "children": [
      {
        "name": "Training",
        "url": "relution.io/schulungen/"
      },
      {
        "name": "Helpdesk",
        "url": "helpdesk.relution.io"
      }
    ],
    "name": "Internal URLs"
  },
  {
    "name": "Android resources",
    "url": "google.com"
  }
]
```

For ve

Managed Mail Client

With Relution Mobile Device Management (MDM), it is possible to centrally configure common email clients like Google Mail or Samsung Mail and subsequently distribute these settings to all assigned devices using a policy.

This guide describes how to add the respective email application to the policy and then set it up with dynamic variables for automatic, user-specific configuration.

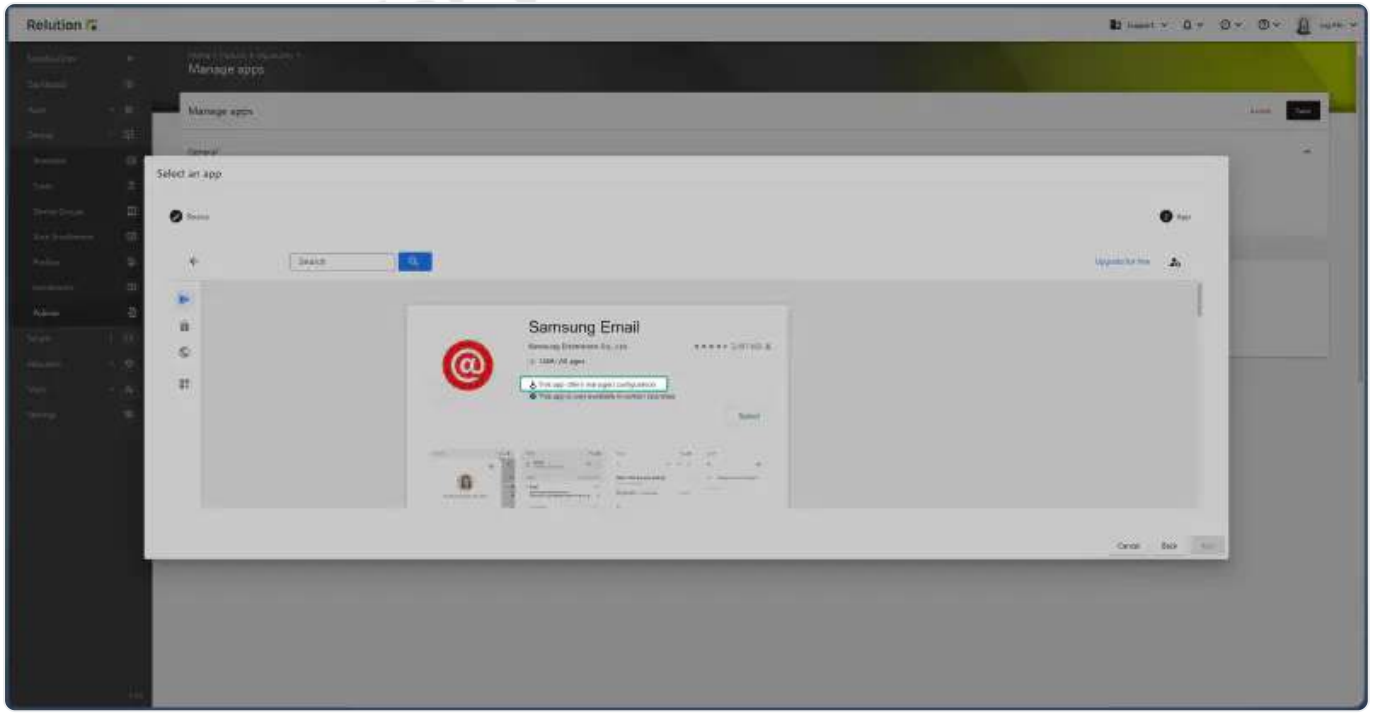
Add the Email Client App to the Policy

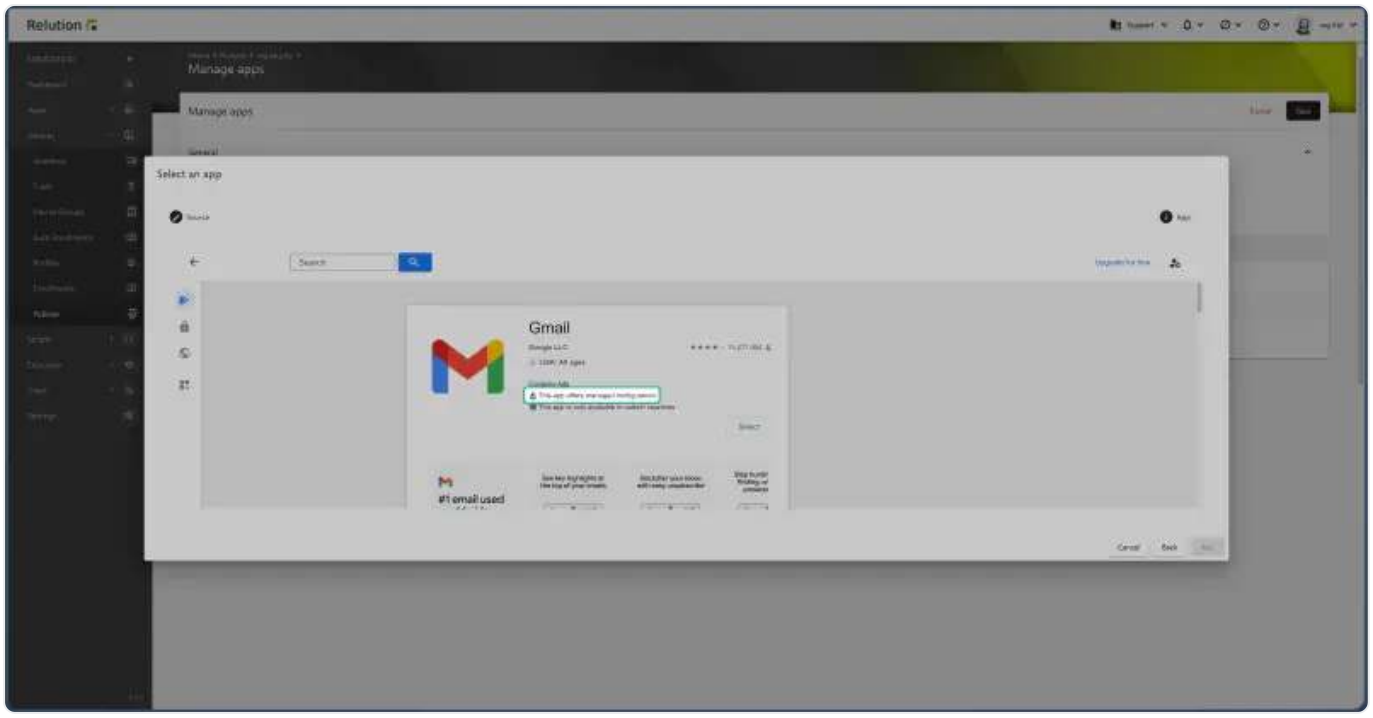
Before this configuration can be performed, the desired email app (Google Mail or Samsung Mail) must be added to the Android Enterprise (AE) policy.

Add App

1. In the Relution Portal, an existing or new Android Enterprise Policy is opened.
2. The Manage apps configuration is selected.
3. The desired email app (e.g., Google Mail or Samsung Mail) is added from the Google Play Store if it is not already included in the list.

- Path: `Portal` → `the AE Policy` → `Manage apps` → `Add` → `Managed Google Play Store App (Android Enterprise)` → `Google Mail/Samsung Mail (add if not present)`





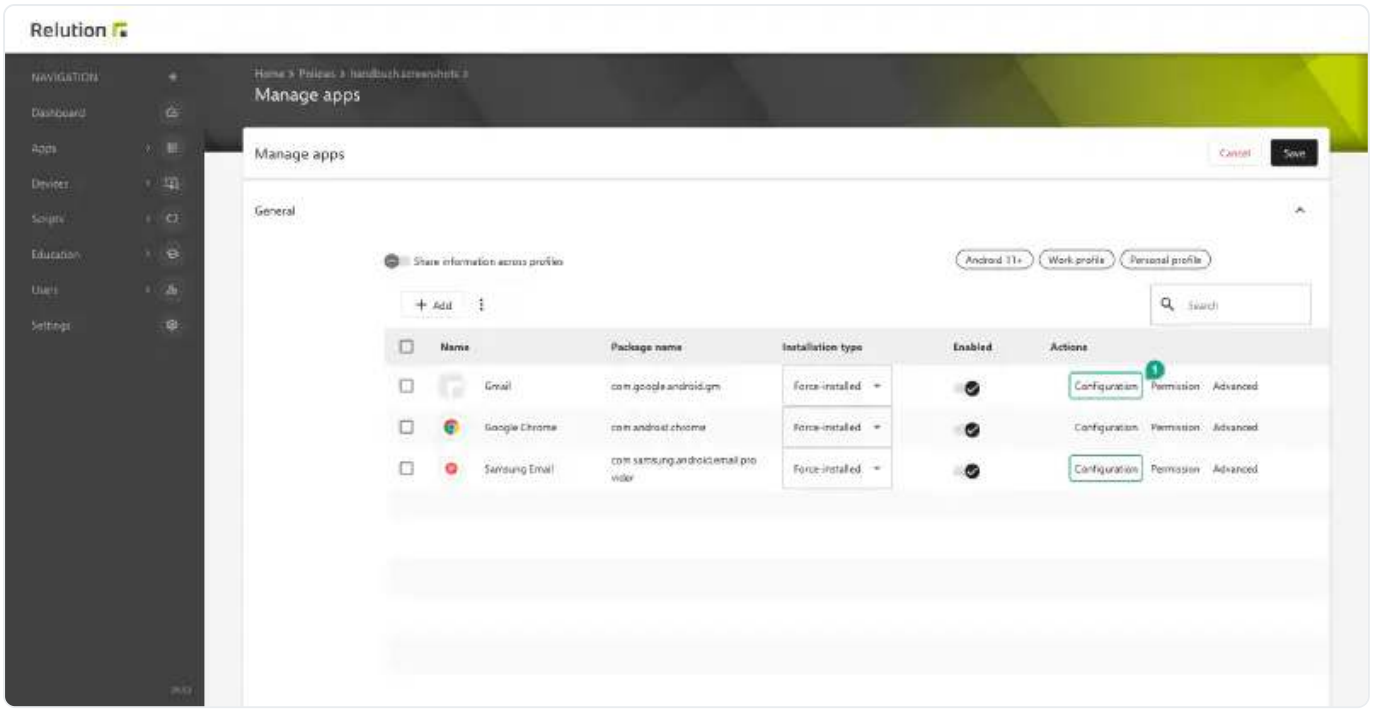
Note on App Configuration: Apps for which managed configuration options (Managed Configs) are available are directly identifiable in the selection (as shown in the screenshots). To be noted: The scope of these configurations is determined exclusively by the respective app manufacturer. Relution has no influence on the options provided.

For version 26.4.0

Start Configuration

1. For the added email app, Configuration is clicked.
2. In the dialog, the desired values (see below) are entered and applied with Confirm.
3. The Manage apps configuration is then saved with Save. Confirm only applies the values to the open configuration; without Save, they are lost when leaving the page.

Changes are only possible in the latest, not yet published policy version. If it has already been published, a new version is created first.



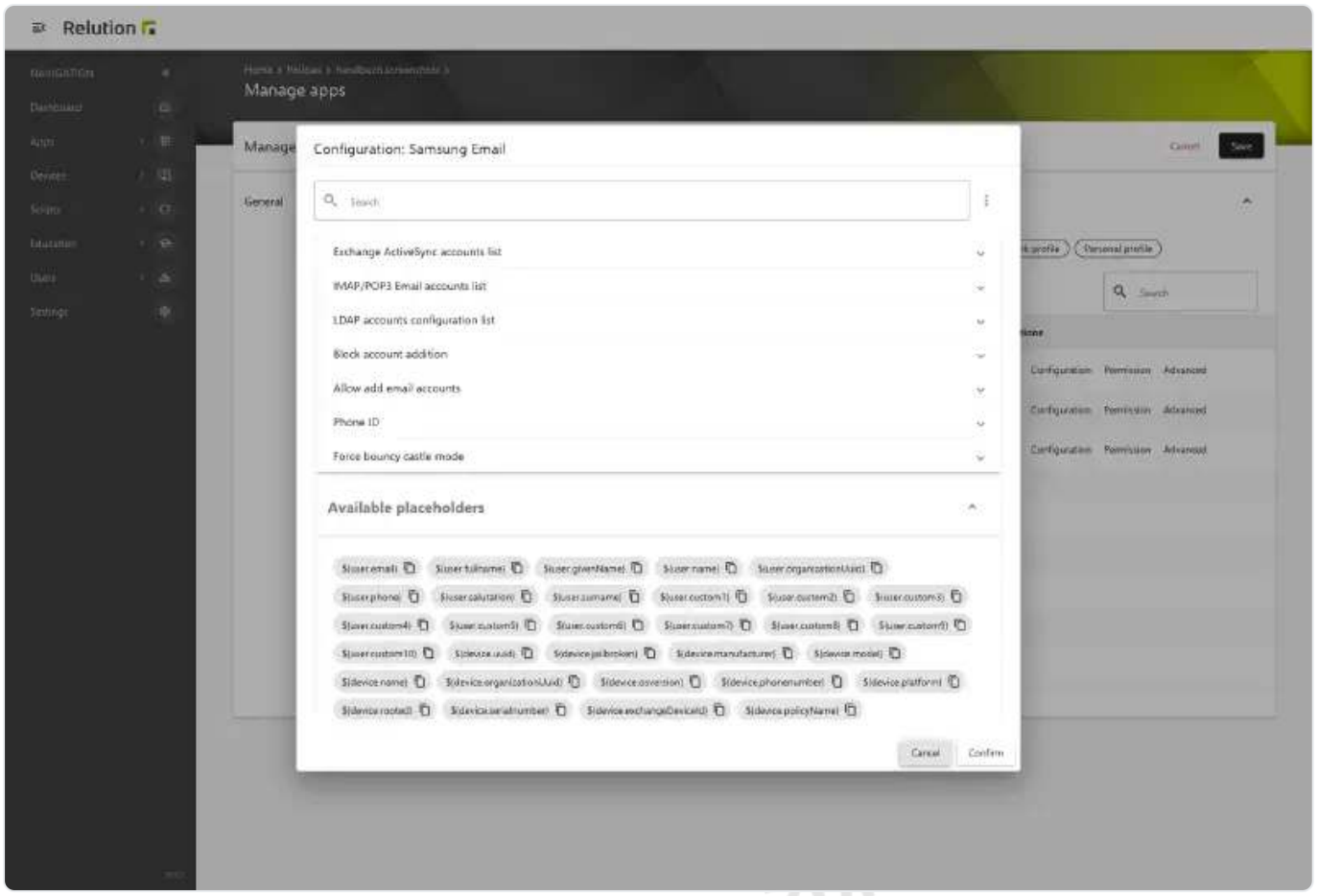
App Configuration with Variables (Managed Configuration)

The configuration of the email client takes place via the so-called Managed Configuration (Verwaltete Konfigurationen). Here, user data and server information are stored, whereby Variables (Platzhalter) can be used to automatically adapt the settings to the respective user.

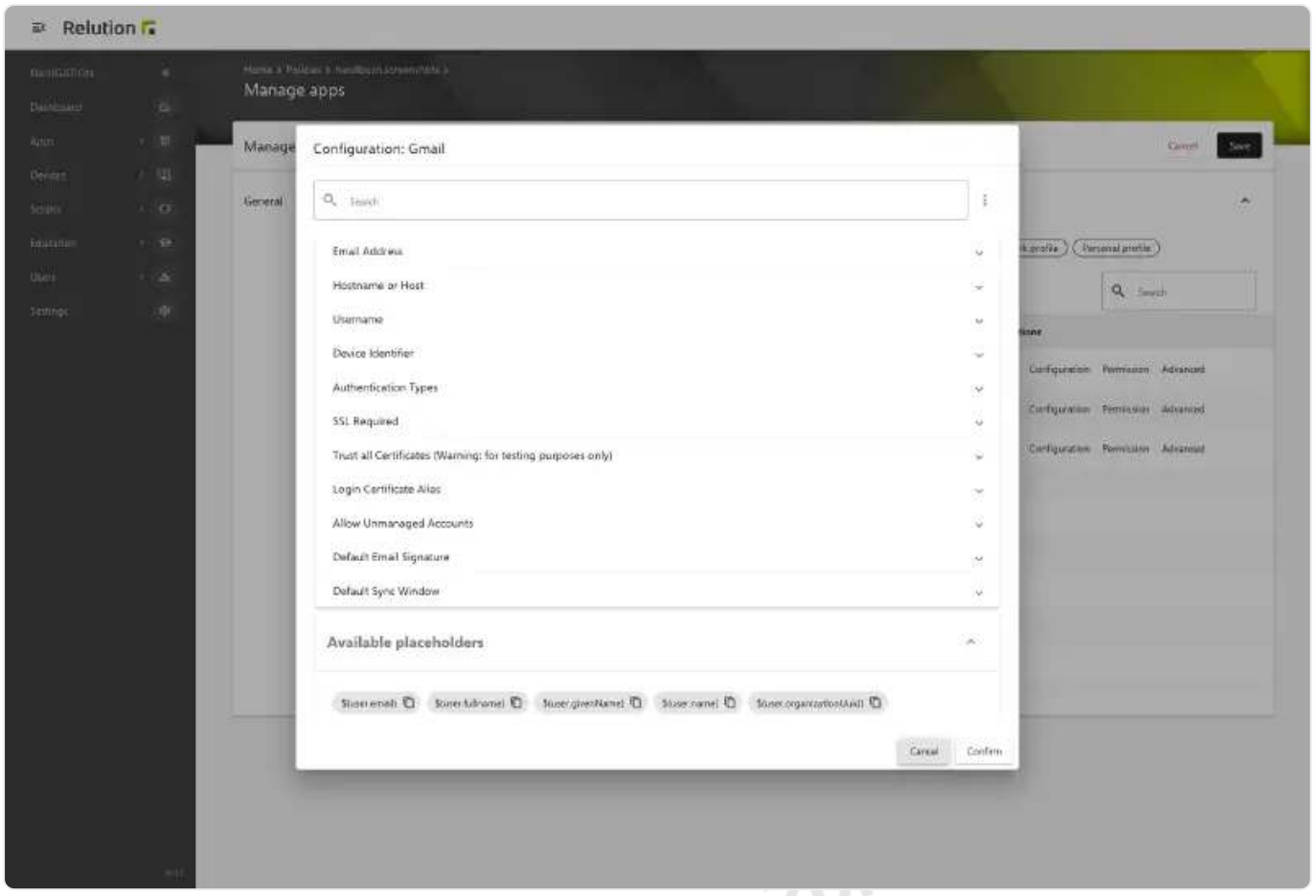
For version 26.4.0

Important Note on Configuration with Variables: For a flexible and generally valid configuration, the Relution variables can be used (e.g., `${user.email}`).

- Display: The available variables are shown in the respective configuration view.
- Prerequisites for Functionality: For these variables to be correctly resolved, the following conditions must be met in the Relution system:
    1. Valid Data: The required information (e.g., an email address for `${user.email}`) must be validly stored with the user.
    2. Device Assignment: The user must be assigned to the device in question.



For version 26.4.0



For version 26.4.0

Summary and Distribution

After the Managed Configuration is saved, the email app will be automatically configured and distributed upon publishing to all devices the policy is assigned to (e.g., via device groups). The variables are filled with the data of the user assigned to the respective device. Users only have to open the app, enter their password, and can immediately retrieve their emails without having to make manual server settings.

> Should the data in the configuration be adjusted in Relution but not applied on the end device, the corresponding app must be deleted and the new configuration applied again.

> The configuration should initially be tested with a small group of devices to ensure that all variables and server settings are adopted correctly.

Configuration of Google Mail and Samsung Mail with Secure Mail Gateway (SMG)

Specific configuration adjustments for the mail applications are required when using a Secure Mail Gateway (SMG). A detailed guide for implementing this integration and these adjustments can be found in the Knowledge Base: SMG Integration for Gmail →

Configure Gmail for SMG

To use the Secure Mail Gateway with Gmail, some configurations are necessary under Android Enterprise. Below is an overview of the parameters that need to be configured. It is important that there have been no previous attempts to configure Gmail on the device, as otherwise fragments of these configurations can lead to errors.

‘Gmail’ from Google is particularly suitable as a mail client and as an example for this article, as the app is generally available for all Android versions and device models.

The app cannot be configured manually on the device if the Secure Mail Gateway is to be used.

These instructions require a functioning and configured Secure Mail Gateway.

Configuration

The following configuration parameters are required.

Email address

Which e-mail address should be configured? Either a fixed address or the variable `${user.email}` can be used here.

Hostname or Host

The host name of the SMG Service URL configured in the Secure Mail Gateway → settings must be entered as the host name. Depending on the setup, this is the host name of the Relution server or a separate subdomain of the SMG service.

> `https://` must not be specified.

Username

The username must be specified in the spelling `unique-name-of-relution-organization\username`. The unique name of the organization can be viewed under `Settings` → `General Organization Settings`.

Device Identifier

The variable `${device.exchangeDeviceId}` must be used here.

Authentication Types

Allow basic authentication must be activated and Allow modern authentication must be deactivated.

For version 26.4.0

Configure Outlook

In Relution, Microsoft Outlook for Android Enterprise can be preconfigured through a managed app configuration. The email account is populated automatically using variables (e.g. `${user.email}`), so that only the password has to be entered when the app is first launched.

The following describes a minimal configuration for a Microsoft 365 account.

Configuration

`Portal` → `the AE Policy` → `Manage Apps` → `Microsoft Outlook (add if not present)` → `Configuration`

In the configuration pop-up, the following fields are filled in. All keys share the common prefix `com.microsoft.outlook.EmailProfile.`.

Key	Value	Description
`ServerHostName`	`outlook.office365.com`	Address of the Microsoft 365 / Exchange server
`EmailUPN`	`${user.email}`	User principal name (account sign-in name)
`EmailAddress`	`${user.email}`	Email address of the account
`EmailAccountName`	`${user.fullname}`	Display name of the account
`AccountType`	`ModernAuth`	Authentication method (modern authentication)

> The variables `${user.email}` and `${user.fullname}` are resolved automatically per user. Further placeholders and functions are described under Advanced placeholders →.

data separation

Three basic approaches are available for separating business and private data on Android devices: full device management of an organization-owned device, the managed device with a personal profile (COPE) as an organization-owned device with a separate private area, or the Work Profile as a separate container on a private device.

Full device management (Device Owner, from Android 9)

Since Relution 5 at the latest, Android Enterprise enrollment as a fully managed device (Device Owner) has become increasingly common for managing Android devices in Relution. The MDM functions are integrated into the operating system and standardized. This enables a largely vendor-independent, uniform MDM functionality on the Android platform. The Android Enterprise functions are only available for certified devices. Samsung devices can be managed and secured even more extensively with the KNOX functions. The Relution Client App is no longer mandatory for Android Enterprise Enrollment.

Additionally, the classic enrollment as `device administrator` is still available. In this case, the Relution Client App is provided with special rights on the device to be able to execute the MDM functions. However, with this type of enrollment, the options for MDM intervention are highly dependent on the Android device used.

A wide range of configurations and functions are available when managing Android devices:

- Installation and configuration of apps (e.g. Exchange client)
- Managed Google Play Store
- WiFi and VPN configuration
- Fully automated device enrollment (KNOX Mobile Enrollment)

For version 26.4.0

Managed device with a personal profile (COPE)

With the enrollment type Set up managed device with a personal profile (Company Owned, Personally Enabled – COPE), an organization-owned device is issued to users who may also use it privately. In addition to the managed area, a personal profile is available to which administrators have neither insight nor access. Relution manages the entire device and can, for example, perform a factory reset, which also deletes all private data.

Personal profile →

Work Profile Enrollment

Android Enterprise additionally offers the so-called Work Profile, which is intended for private devices and sets up a container Work on the device that can be managed by Relution. This container contains a Managed Play Store, which only makes approved apps available for installation. Installing apps from the Managed Google Play Store is possible without a local Google account. Additionally, the apps can be configured via Relution if a Managed App Configuration is supported by the respective app (e.g. an email app with a predefined server address and user ID). The container can also contain its own address book to separate business and private contacts.

Relution cannot affect anything outside the container (Personal), e.g. the device cannot be reset to factory settings. However, the container can be removed via Relution, which deletes all the data it contains. The Lock device action is also available for devices with a work profile. Whether only the work profile or the entire device is locked depends on Android and the lock settings on the device.

Relution supports the work profile in an organization in parallel with the full device management of Android Enterprise and the classic enrollment as Device Administrator. Thus, mixed operation with different devices is possible in Relution.

Functional limitations

In addition, the following functions in the Work container can also be disabled by restriction:

- App Block/Allowlisting
- Creation of new users and profiles
- Adding and removing accounts
- Install apps
- Uninstalling apps
- Using the camera
- Taking screenshots
- Configuring and using Bluetooth
- Sharing contacts via Bluetooth
- Configure mobile network
- Configure VPN
- Using Android Beam (NFC) to share app data
- Mount external physical media

Configuring Wi-Fi networks and transferring files via USB can only be restricted on managed devices and devices with a personal profile (COPE), not in the work profile of private devices.

For version 26.4.0

Homescreen as default launcher

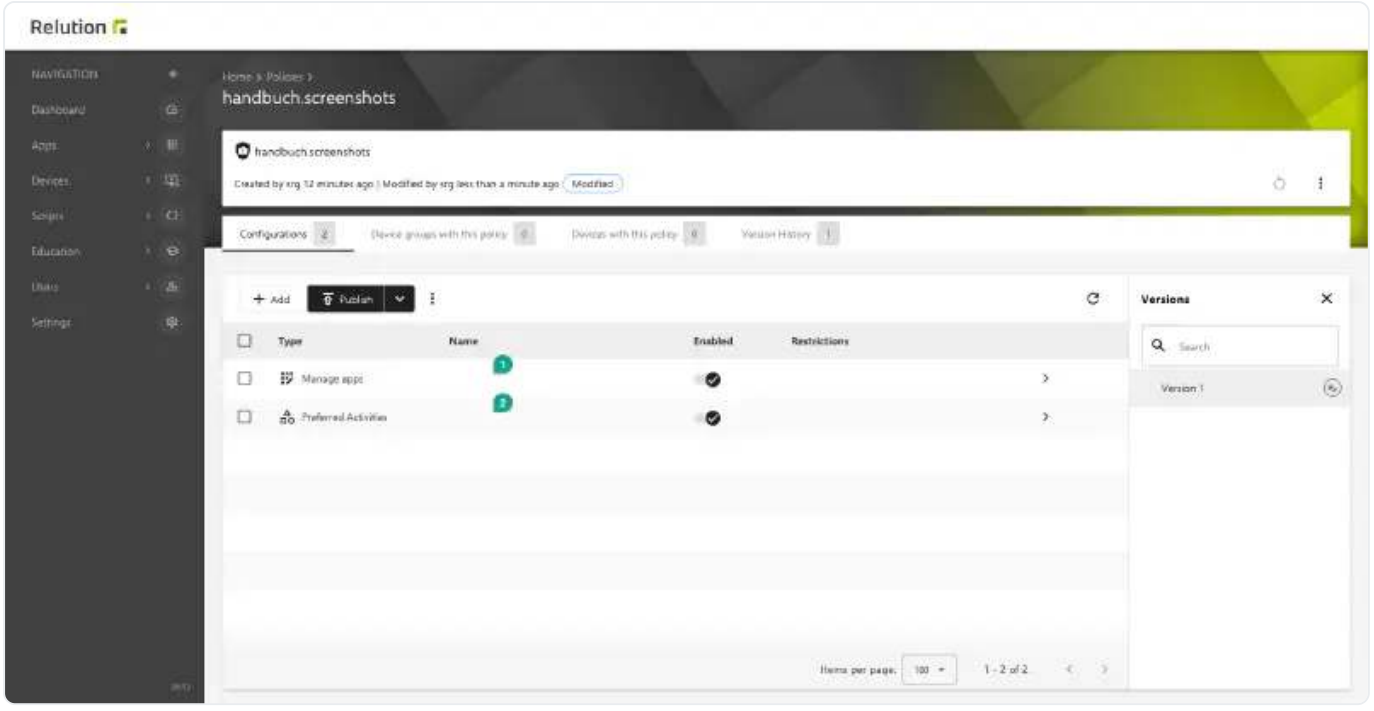
The Relution Homescreen can be used in two ways:

1. Kiosk Mode →: Via the dedicated Relution Homescreen configuration (strictly locked down).
2. Separate Launcher: By setting it as the default app.

Using it as a default launcher offers the advantage that notifications remain visible on the lock screen, the system menu can be accessed from the top of the screen, and system apps can be displayed if required.

Policy with Configurations

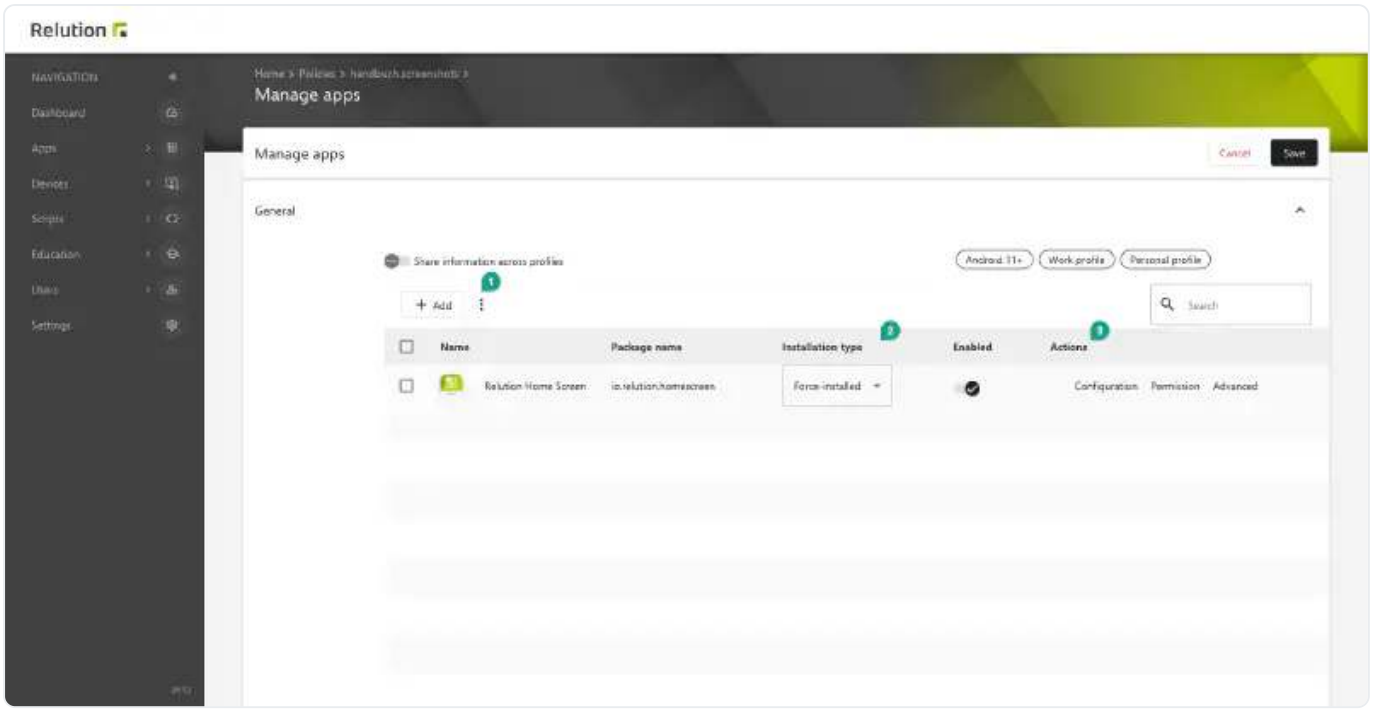
To have the Relution Homescreen act as the default launcher without enforcing the restrictive Kiosk Mode, two specific configurations must be combined within one policy: Manage Apps and Preferred Activities.

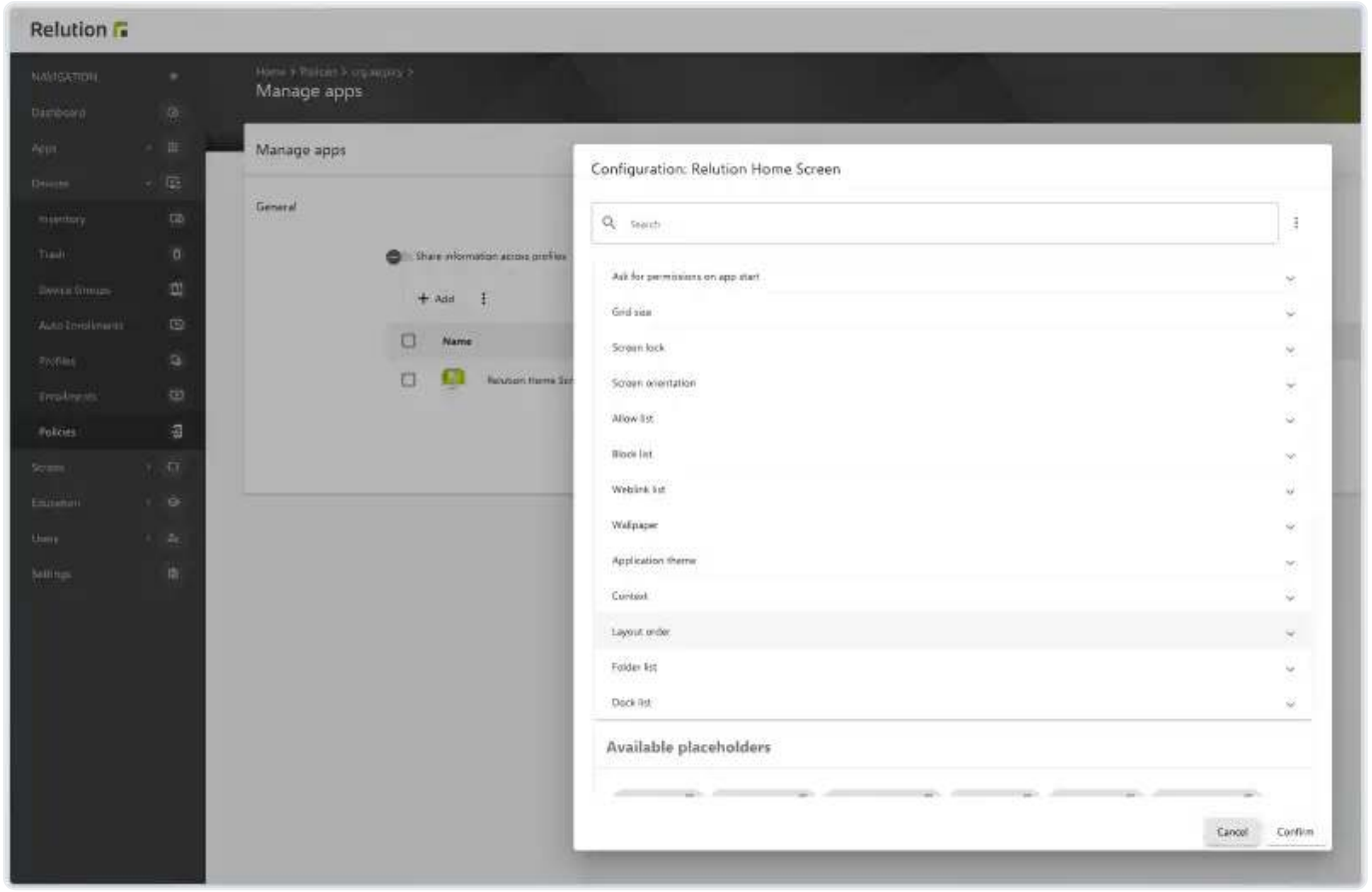


Manage Apps

This configuration ensures that the app is present on the device and correctly set up.

- The Relution Homescreen app (`io.relution.homescreen`) is added to the Manage Apps list using the “Add” button from the Google Play Store (1).
- The Installation type is set to Force-installed (2).
- Via the Configuration link in the Actions column, the desired settings for the layout and functions of the homescreen can be manually defined (3).

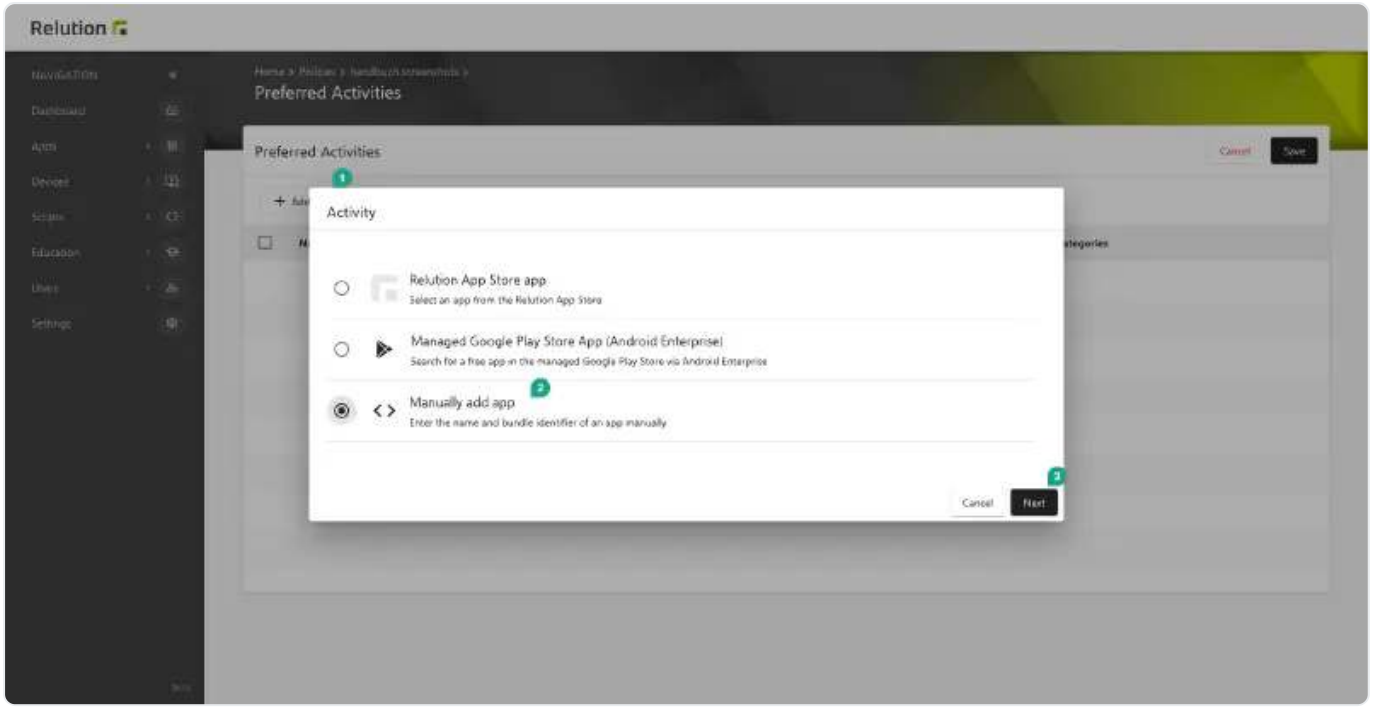




Preferred Activities

This configuration changes the default behavior of Android and defines the Relution Homescreen as the primary user interface (Home). All fields are described in the article Preferred Activities →.

In the configuration, Add is clicked and Manually add app is selected.



The following identifiers are entered:

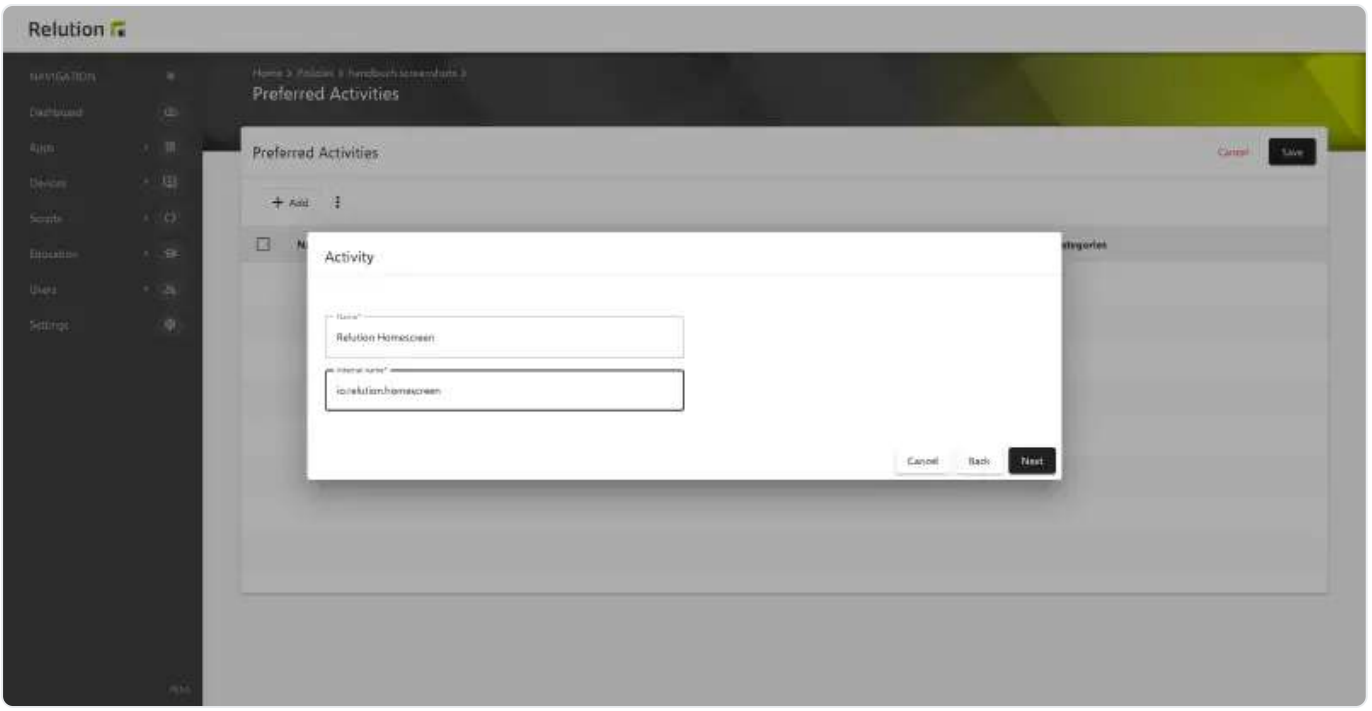
- Name:

```
Relution Homescreen
```

- Internal Name (Package Name):

```
io.relution.homescreen
```

ersion 26.4.0



The parameters are filled in exactly as follows:

- Activity:

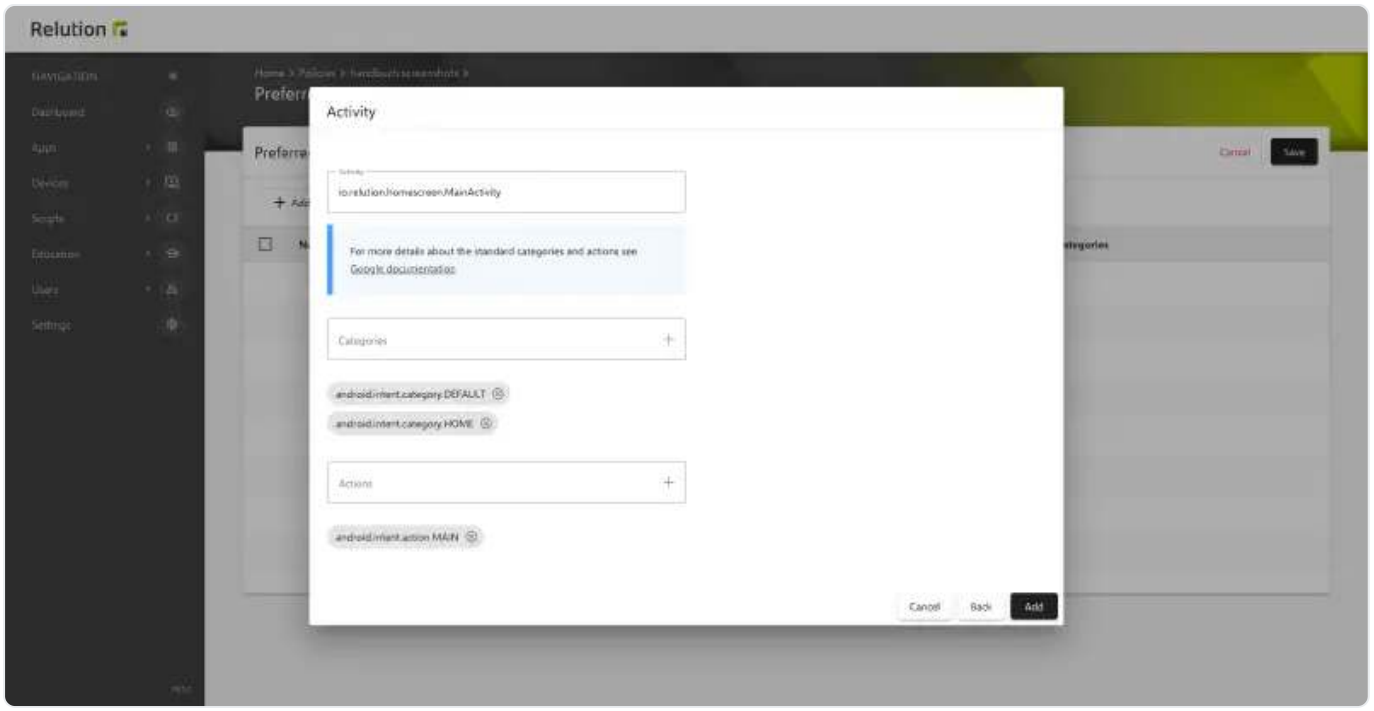
```
io.relution.homescreen.MainActivity
```

- Categories:

```
android.intent.category.DEFAULT
android.intent.category.HOME
```

- Actions:

```
android.intent.action.MAIN
```



Assignment

Once both configurations have been saved in the policy, it must be assigned to an appropriate Device Group. After the policy is pushed, the Relution Homescreen will be automatically activated as the default launcher.

For version 26.4.0

Location Services

With Relution it is possible to configure location services for Android Enterprise devices. The administrator can specify the location services of the device and location permissions for individual apps or leave it to the user.

Location services

Via the Location mode → configuration, administrators use the Location setting on the device field to specify whether users can turn location services on or off. To do this, the field must be set to User choice. If no configuration is given, User choice is the default.

If location services are disabled, apps will not be able to locate the device, regardless of what permissions have been assigned. This affects all apps, including Google Maps or Waze, for example.

- The Enable location setting on the device option enables the location setting on the device. As of Android 11, work profiles on company-owned devices cannot directly enforce location services; in this case, the user must enable location services manually in the device settings.
- The Disabled option deactivates and prohibits changes to the location setting.

Default app permissions

Whether the Relution Agent and Companion Apps get the permission to locate depends on what is set under `Portal` → `Settings` → `Device Management` → `Enrollment` in the Locate device row. If here the tracking is disabled for `COD` both apps will not get permission to track.

> Companion since server version 5.18.0, Agent since server version 5.19.3

Individual app permissions

This default can additionally be overridden individually by adding an app to the Manage apps configuration. If Agent and/or Companion is added here, the app permissions can be set individually. For example, the user can be given the right to set all permissions of the app.

> Companion since server version 5.18.0, Agent since server version 5.19.3

Without permission for the Agent, for example, policy assignment depending on geofences and iBeacons cannot be used. Without permission for the Companion, the Locate device action cannot be used.

The default response for permission requests is set as follows: `Portal` → `the AE Policy` → `Manage apps` → `Relution Companion for AE` (add if not present) → `Permission` A popup will open here with the item Default response for permission requests.

For version 26.4.0

If Google Location Services were deactivated during device setup, they must be subsequently activated for localization in Relution Companion

Factory Reset Protection

For Android Enterprise devices, Relution offers two settings related to factory reset in the restrictions of a policy. Both work independently of each other and can be combined:

- The Enable Factory Reset Protection (FRP) toggle blocks factory reset via the Android settings on managed devices. A reset via the recovery menu remains possible.
- Google accounts are stored in the Google account email for FRP field. After a reset, a prompt to log in with one of these accounts is displayed during the device setup process to make the device operational again. If no account is entered, FRP is not active.

Configure FRP

1. In the Relution portal, the menu item `Devices` → `Policies` is opened and Add is clicked.
2. An Android Enterprise policy is created and a name is assigned. Save is clicked.
3. After clicking on Add, the Restrictions option is selected and the process continues with Add details.
4. Optionally, the Enable Factory Reset Protection (FRP) toggle is activated to block factory reset via the Android settings. A reset via the recovery menu remains possible.
5. Optionally, one or more Google accounts are entered in the Google account email for FRP field. After a reset, one of these accounts must sign in to unlock the device. If the field remains empty, FRP is not active.
6. The configuration is saved and the current version of the policy is published.
7. To apply the policy to Android Enterprise devices, the desired devices are added via the Devices with this policy tab. The selected settings are then automatically applied to the devices.

For version 26.4.0

Show Captive Portal

To establish a connection with a WLAN, a package name must be enabled for Android Enterprise. This is `com.android.captiveportallogin` and must be added manually as Available in the Manage apps configuration. The app is added via Add with the source Manually add app, entering the package name in the Internal name field. Manually added apps initially receive the installation type Force-installed, so the value in the Installation type column is then changed to Available.

It is then possible to establish a connection with a Wifi that displays a captive portal.

Calls are not displayed

In Kiosk or Homescreen Layout mode, Android Enterprise does not display incoming or outgoing calls: the device rings or vibrates, but no call overlay appears on the screen. This is because Android blocks all apps and overlays in this mode that are not explicitly permitted by the policy—the call UI is controlled by manufacturer-specific system packages that must be included in the whitelist. The following policy changes fix this:

Adjust Policy Restrictions

For the incoming call window to function as a system overlay, Kiosk Mode must be used instead of the Homescreen Layout.

Additionally, the following parameters must be configured in the Kiosk Mode configuration:

- Disable toasts and overlays (General section): Must be disabled (to allow required system overlays).
- Status bar (Kiosk customization section): Must be set to Enabled (as the call banner relies on system notifications to drop down).

If the native Kiosk Mode does not offer enough flexibility for the use case, an alternative launcher such as the Microsoft Managed Homescreen can be implemented by enabling the option Use a custom kiosk launcher app instead of the default launcher. This provides advanced configuration capabilities for complex deployment scenarios.

> When using the Relution Homescreen—in both Kiosk and Layout configurations—these system overlays cannot be enforced and notification sounds cannot be played due to technical platform limitations.

For version 26.4.0

If the Relution homescreen is to be used, it must be configured via Preferred Activities →

Whitelist Required Package Names by Manufacturer

The mandatory system applications required for telephony functionality must be added to the Manage apps configuration with Available selected in the Installation type column.

Samsung Devices

- `com.samsung.android.incallui` — Responsible for the visual call window and interface controls during an active call.
- `com.android.systemui` — Enables head-up notifications (call banners) when the screen is active.
- `com.samsung.android.dialer` — The native Samsung Phone application (dial pad).
- `com.samsung.android.smartcall` — Samsung Smart Call features for caller ID and system-level spam protection.

Google Pixel Devices

- `com.google.android.dialer` — The Google Phone application, including its native, integrated InCall UI.
- `com.android.systemui` — Manages the notification bar and the deployment of the upper incoming call banner.
- `com.google.android.as` — Android System Intelligence (required for AI-assisted call processing on Pixel hardware).

Notification Sounds

Besides the call UI, notification sound playback also depends on the launcher in use.

On the other launchers, notification sounds are played as long as the `com.android.systemui` package is added to the Manage apps configuration with Available selected in the Installation type column:

- Native Kiosk Mode (default launcher of the Android Enterprise configuration)
- Microsoft Managed Homescreen (via the option Use a custom kiosk launcher app instead of the default launcher)

File transfer via USB

USB data transfer (files/pictures) is no longer selectable on Android devices; the corresponding menu item is missing on the device. This is because Google no longer accounts for a field in the API that controls USB access—the function has since been disabled by default.

For version 26.4.0

Restoring the function

As of Relution 5.22.4, a new default value is set server-side for fully managed devices and managed devices with a personal profile (COPE) that re-enables the function:

1. Updating Relution to at least version 5.22.4 (see changelog →).
2. Checking the policy: the default value only applies if the policy does not regulate USB file transfer itself.
    - In the Restrictions configuration, the option Disable USB file transfer must not be enabled (see Restrictions →).
    - If the policy contains a Device connectivity → configuration (as of Relution 5.24.0), its USB data access setting applies instead of the default value. Allow USB data transfer must be selected there. With the preselection Unspecified, USB file transfer remains blocked.
3. Reapplying policies on the affected devices: Under `Devices` → `Inventory`, a filter is set for all Android devices, all devices are selected, and the policies are reapplied via the three-dot menu.

Manual enrollment

In order to manage devices in Relution, they must be enrolled. To do this, the administrator creates an enrollment (registration), which must then be performed on the device. The creation of an enrollment in Relution is the same for all platforms. The subsequent enrollment process on the devices is platform specific `Android Classic / Legacy`.

> As of January 1, 2025, Relution only supports Android 10 and later for both Android Enterprise and Android Classic / Legacy. Support for earlier Android versions has been discontinued.

> Relution will discontinue support for Samsung devices running Android 15+ if they are managed via Android Classic. We recommend switching to Android Enterprise.
>
> Samsung devices running Android 15 can still be managed via Android Classic. However, basic functions such as installing or updating native apps will no longer be available. With Android 16, Samsung will also remove KIOSK mode.

Pre-requisites for enrollments

For version 26.4.0

- To create enrollments, users must be assigned to the organization's `Administrator` or `Device Manager` user group.
- To perform enrollment on the devices, end users must be assigned to at least the organization's `User` group.
- Enrollments are created in the organization in which the device is to be managed. Devices cannot be enrolled in the global organization.
- Background knowledge of which enrollment is used for which Android platform `Android Classic / Legacy` as opposed to `Android Enterprise`.

Create manual enrollments

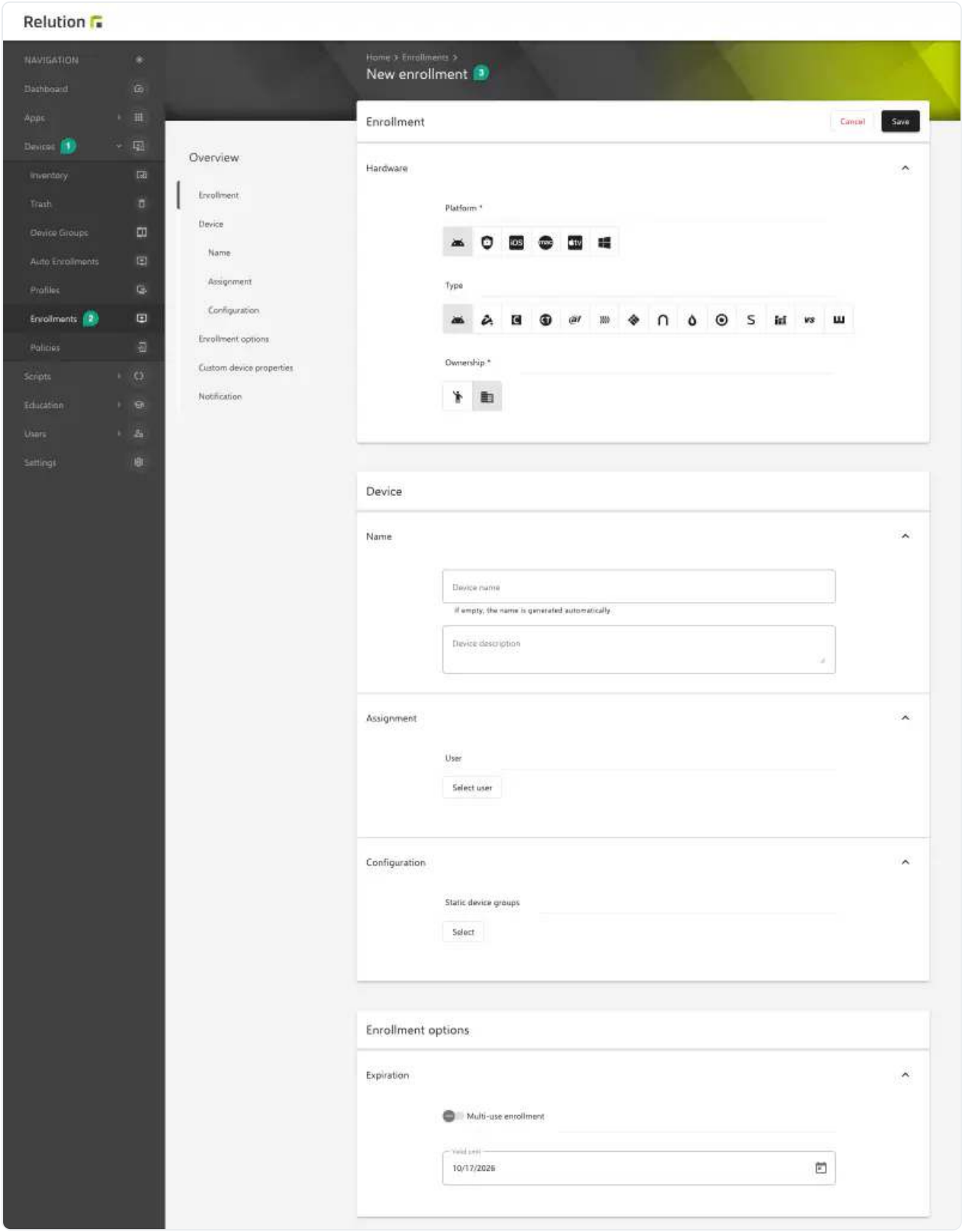
1. In `Devices` → `Inventory`, the Enroll button is clicked (alternatively Add in `Devices` → `Enrollments`).
2. Android is selected as Platform, together with the Ownership (e.g. COD - Company Owned Device). Android remains selected under Type. The other types are intended for enrolling interactive displays, see Whiteboards →.
3. Clicking Save creates the enrollment.

Optional

- Device name and Device description: The device and the enrollment will be named. The description is displayed with the device in the inventory. Both fields can contain user placeholders such as `${user.givenName}`, which are replaced based on the assigned user during enrollment, see Advanced placeholders →.
- User: Relution users can be assigned to devices e.g. for a 1:1-equipment. Only one user can be assigned to a device at a time.
- Static device groups: After successful enrollment, the device is added to the selected device groups →. The policies assigned to these groups are then applied to the device. The field is only visible with the permission to edit device groups.
- Multi-use enrollment: If activated, multiple devices can be enrolled with one enrollment.
- Valid until: Date after which the enrollment can no longer be used. The end of the seventh day after creation is preset, and the date can be changed as required. If the field is left empty, the enrollment does not expire.
- Custom device properties: Customizable fields for additional information.

For version 26.4.0

- Notification: Selection whether the user should be notified about the enrollment by email or SMS. The section is only shown if email or SMS notification is enabled in `Settings` → `Notifications`. Email requires an assigned user with an email address. SMS requires a Phone number; if the assigned user has a phone number on file, it is filled in automatically.



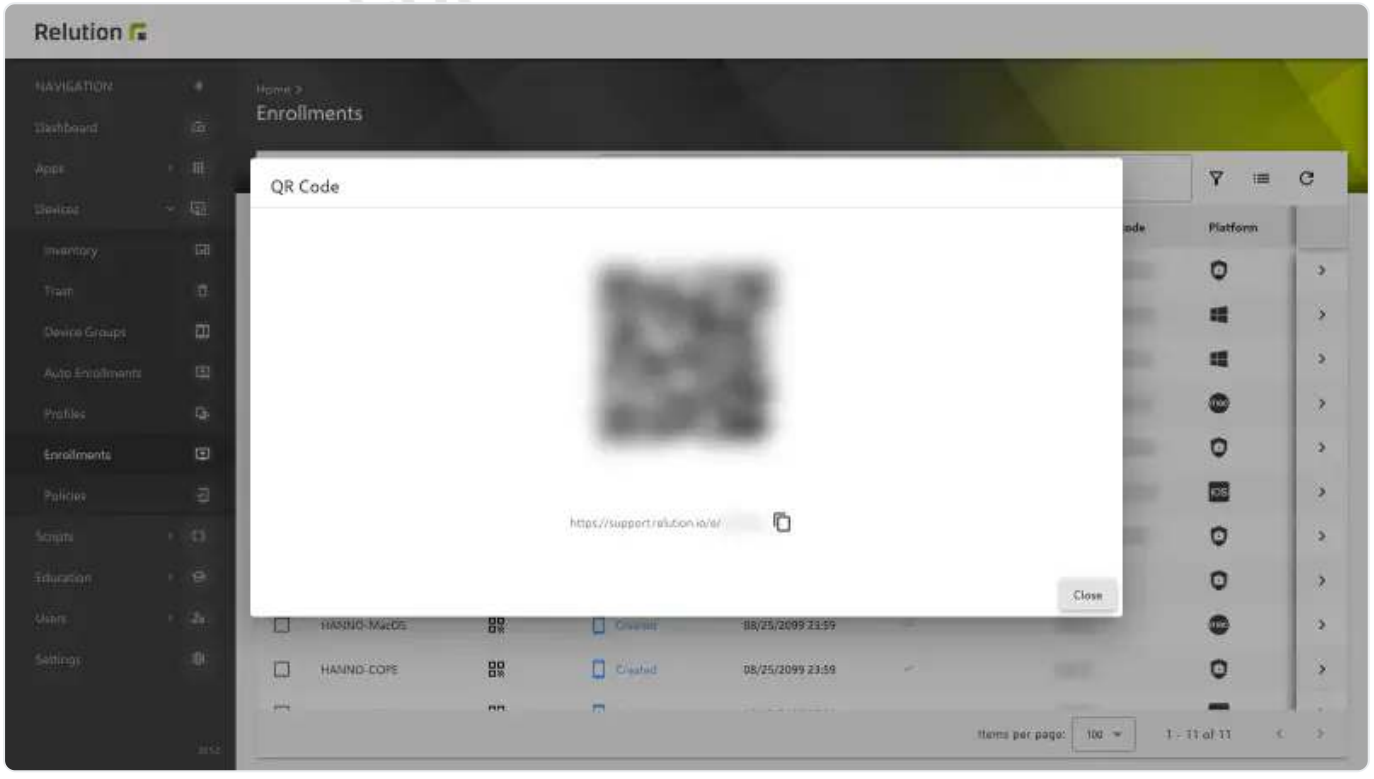
Additional notes

- If no device name has been specified, the device name is generated from the manufacturer and model after the device has been enrolled successfully.
- After saving, the details of the enrollment show the Enrollment code and the Link to the enrollment. Both can be copied to the clipboard, for example to pass on the enrollment without a notification.
- By default, the Enrollment code is 16 characters long (since Relution 26.5.2, previously 6). The length can be set between 12 and 32 characters with the following global configuration property (requires restarting the instance); values outside this range are set to the respective limit:

```
relution:
  enrollment:
    passcodeLength: 24
```

Perform manual enrollment

The following steps must be performed by the Android device user. Based on the notification option selected, the device user will be notified via email or SMS. If the device user is also a member of the `Device Manager` user group, the QR code for the enrollment can also be scanned directly in the organization. It is opened by clicking the icon in the QR Code column under `Devices` → `Enrollments` in the Relution portal (the QR code is also shown in the enrollment details). This is usually the preferred method for enrolling an Android device.



The following steps should then be performed:

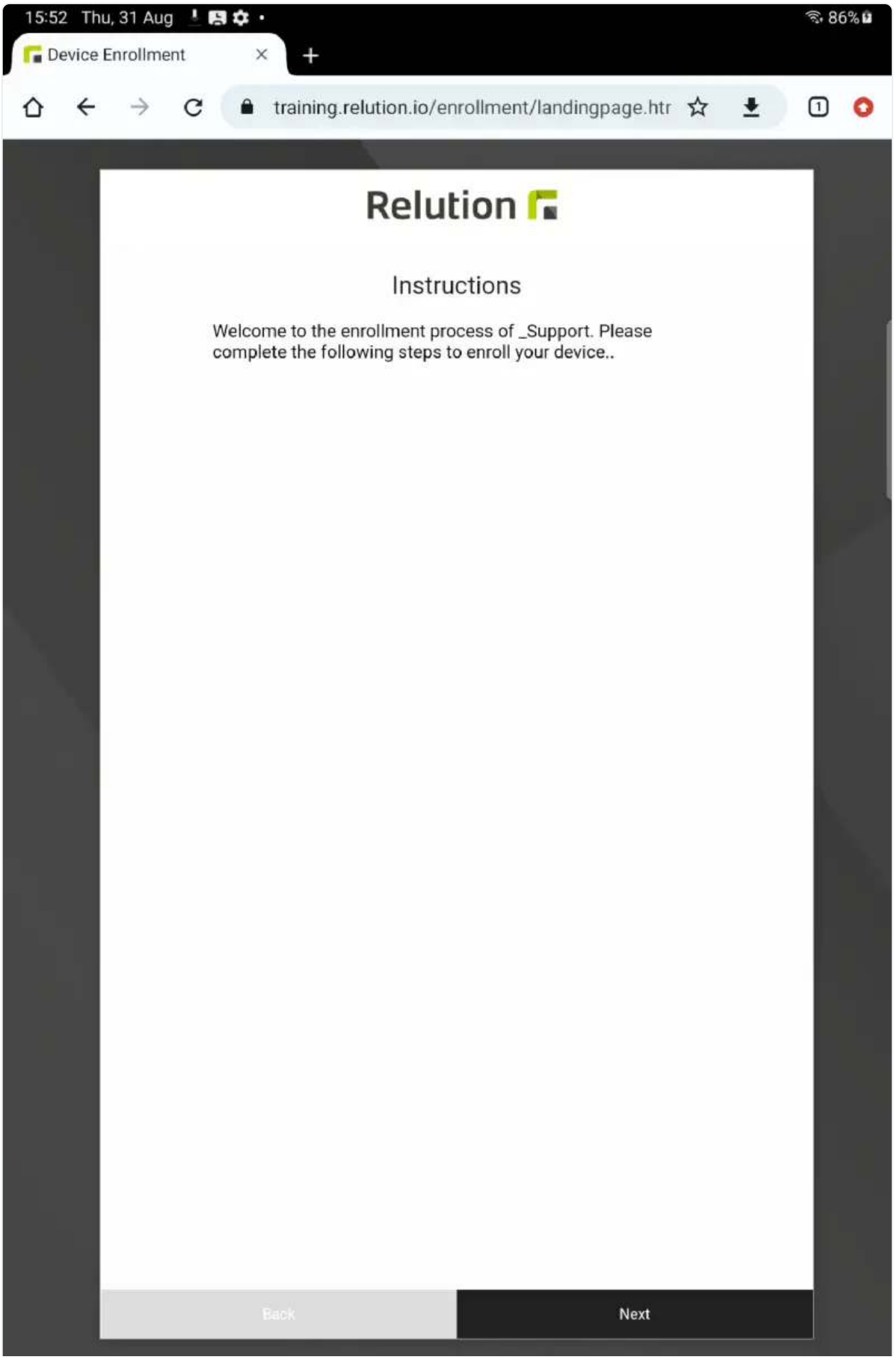
1. It should be made sure that the Android device is connected to the Internet (WiFi or mobile network).

For version 26.4.0

2. The registration link is opened:

    - If a registration email was received: the email is opened on the Android device and the link is tapped, or the email is opened on another device and the QR code is scanned with the Android device.
    - If an SMS was received: the link in the SMS is tapped.
    - If neither was received: the URL from the enrollment should be entered manually in the browser, or the responsible administrator should be contacted.

For version 26.4.0

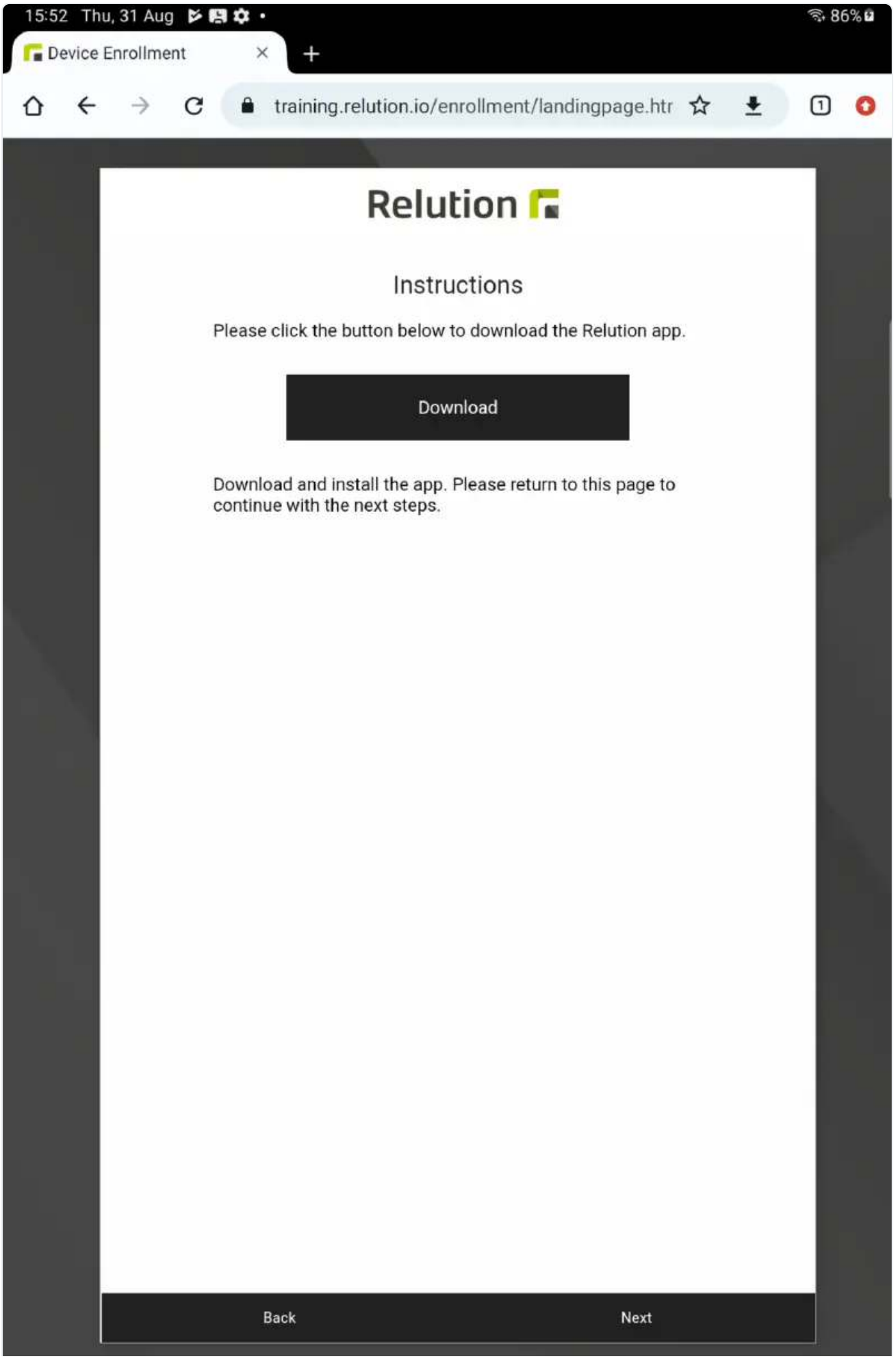

15:52 Thu, 31 Aug
86%
Device Enrollment
training.relution.io/enrollment/landingpage.htr
Relution
Instructions
Welcome to the enrollment process of _Support. Please complete the following steps to enroll your device..
Back
Next



For version 26.4.0

3. The browser on the Android device shows this welcome screen. Tapping Next continues.

For version 26.4.0


15:52 Thu, 31 Aug
86%
Device Enrollment
training.relution.io/enrollment/landingpage.htr
Relution
Instructions
Please click the button below to download the Relution app.
Download
Download and install the app. Please return to this page to continue with the next steps.
Back
Next

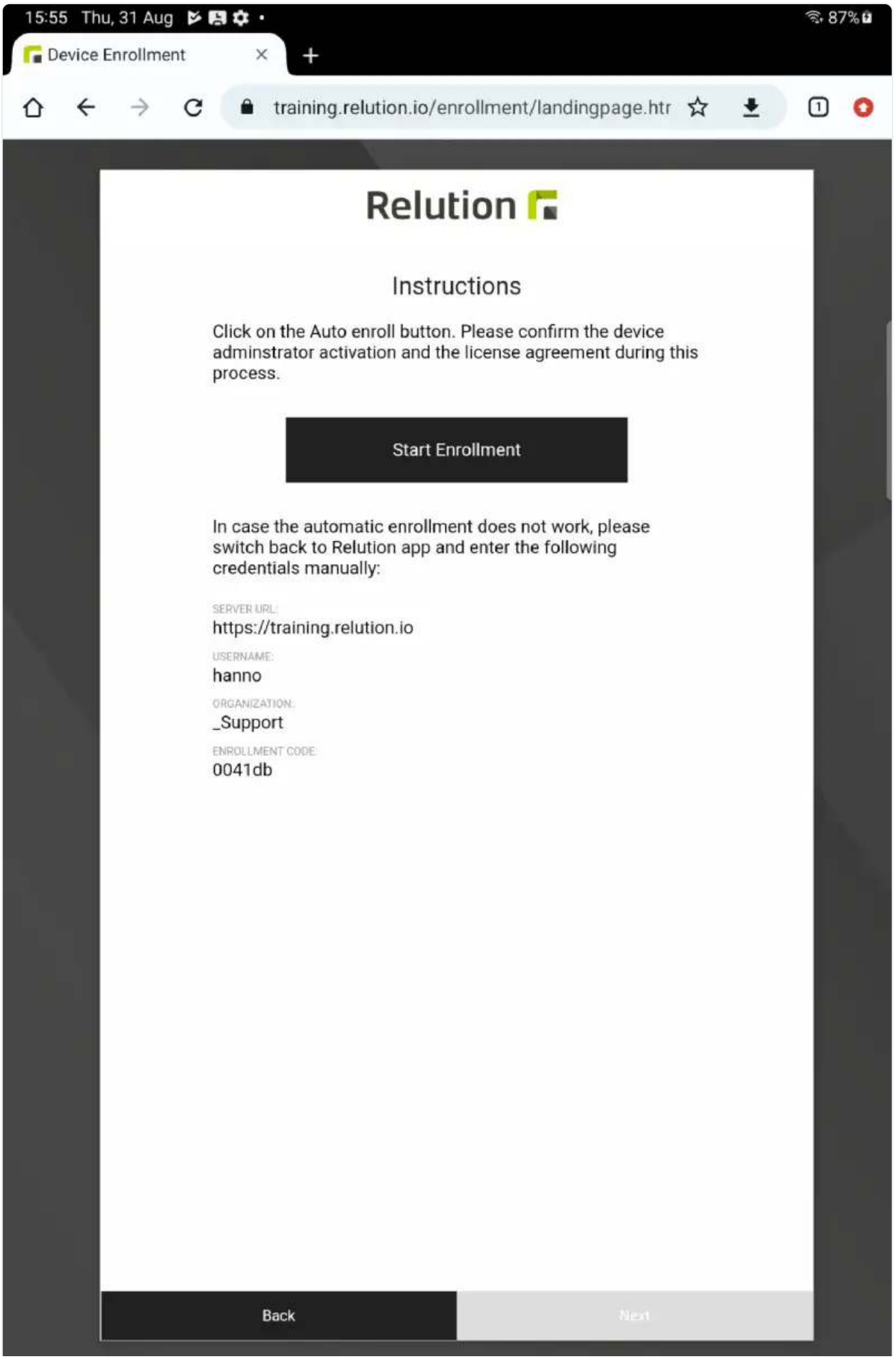


For version 26.4.0

4. A prompt to download and install the `Relution Companion` for Android appears (alternatively available as *.apk from our server Relution Companion APK →).

   After the installation is complete, one should return to the browser to continue with the log in. If the installation fails, installing apps from unknown sources is not allowed on the Android device. As of Android 8, this permission is granted per app, namely for the app used to download the Relution app, for example the browser (Install unknown apps, depending on the manufacturer under `Settings` → `Apps` → `Special app access`). Up to Android 7, the setting is located under `Settings` → `Security` → `Unknown sources`.

For version 26.4.0

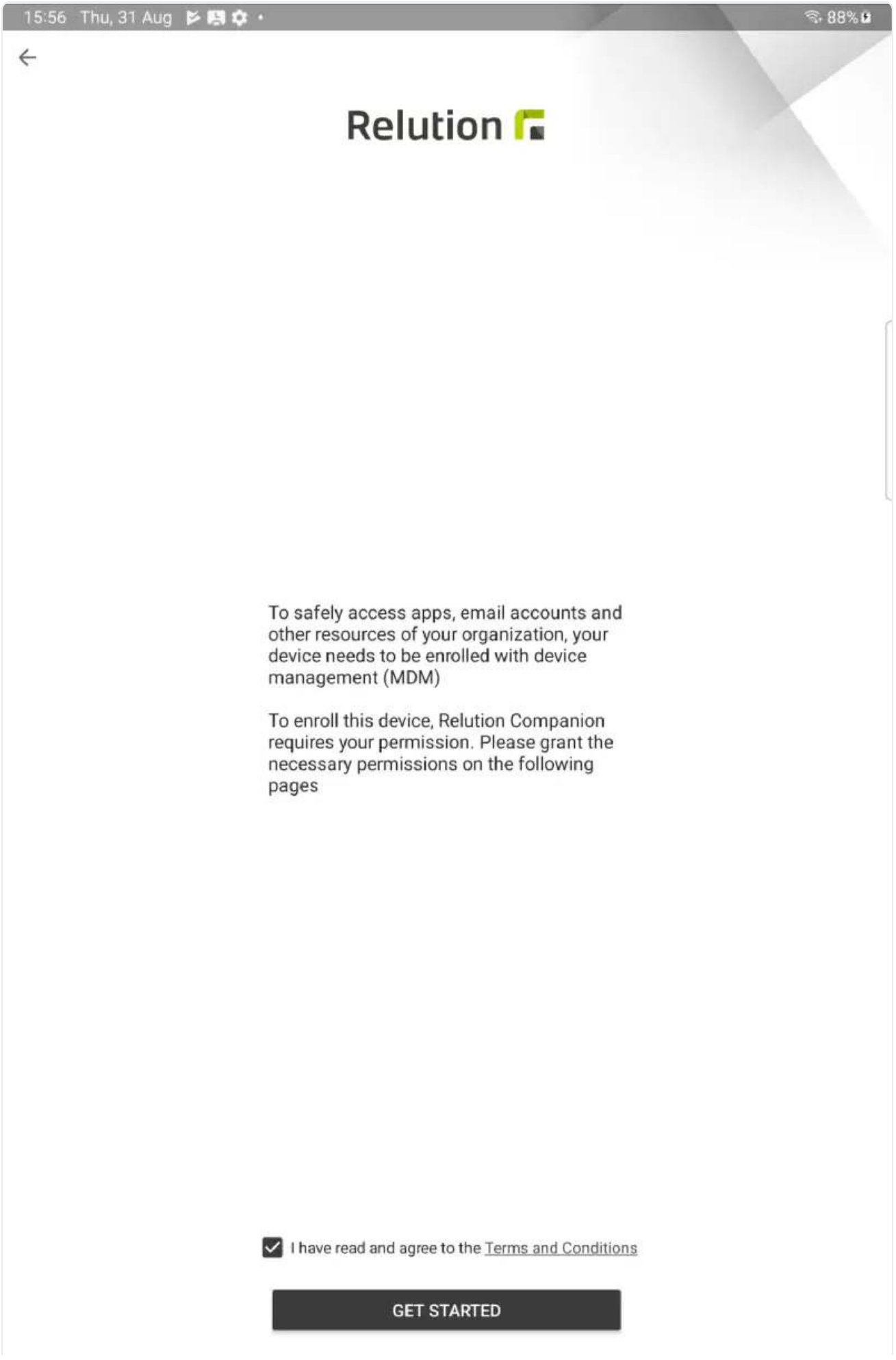

15:55 Thu, 31 Aug
87%
Device Enrollment
training.relution.io/enrollment/landingpage.htr
Relution
Instructions
Click on the Auto enroll button. Please confirm the device adminstrator activation and the license agreement during this process.
Start Enrollment
In case the automatic enrollment does not work, please switch back to Relution app and enter the following credentials manually:
SERVER URL:
https://training.relution.io
USERNAME:
hanno
ORGANIZATION:
_Support
ENROLLMENT CODE:
0041db
Back
Next



For version 26.4.0

5. Tapping Start Enrollment opens the `Relution Companion` for Android.

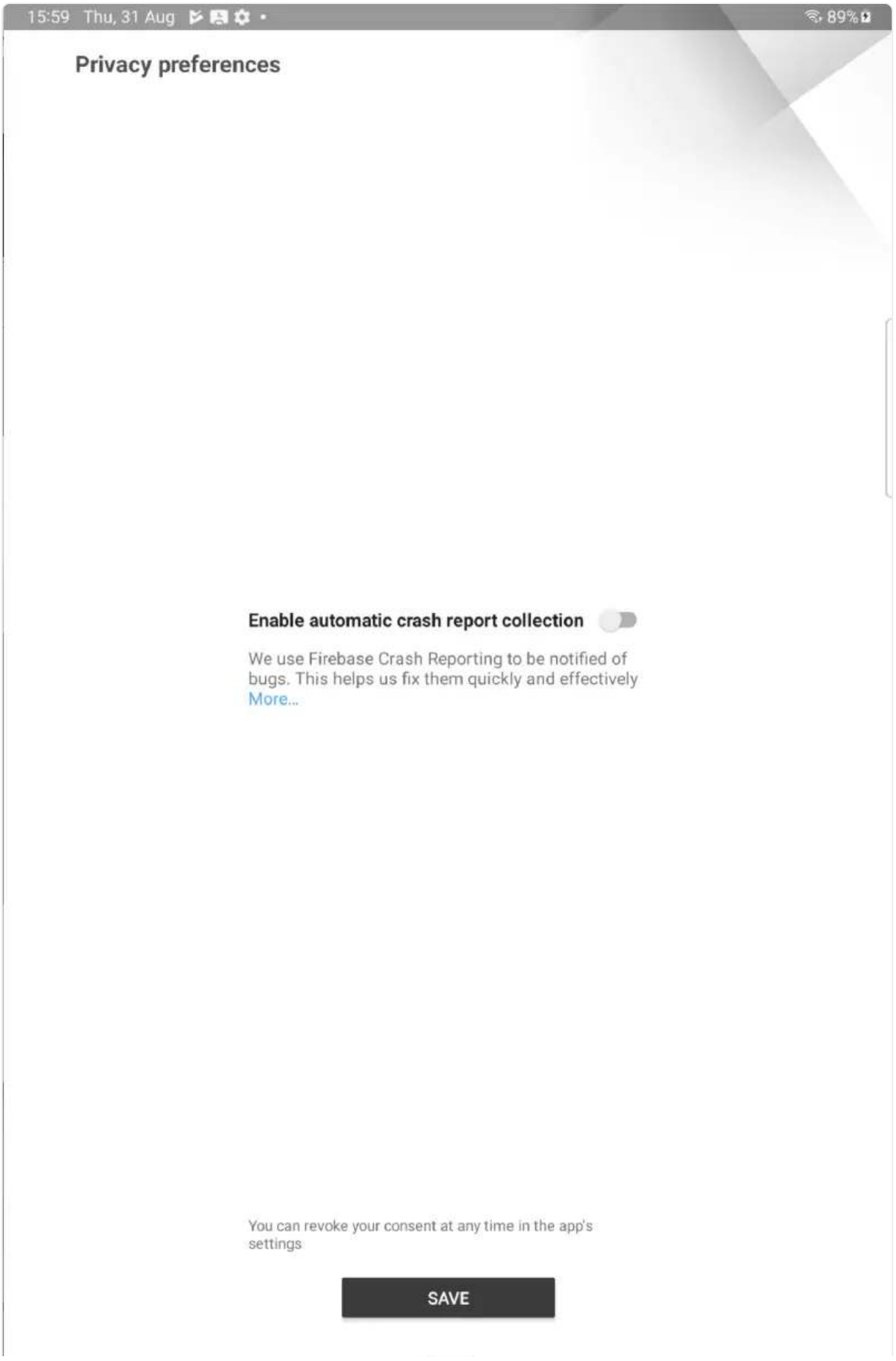
For version 26.4.0

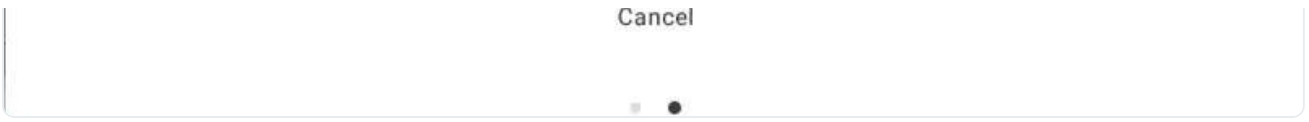

15:56 Thu, 31 Aug
88%
Relution
To safely access apps, email accounts and other resources of your organization, your device needs to be enrolled with device management (MDM)
To enroll this device, Relution Companion requires your permission. Please grant the necessary permissions on the following pages
I have read and agree to the Terms and Conditions
GET STARTED

For version 26.4.0

6. After the terms and conditions have been accepted, Get started is tapped.

For version 26.4.0


15:59 Thu, 31 Aug
89%
Privacy preferences
Enable automatic crash report collection
We use Firebase Crash Reporting to be notified of bugs. This helps us fix them quickly and effectively
More...
You can revoke your consent at any time in the app's settings
SAVE

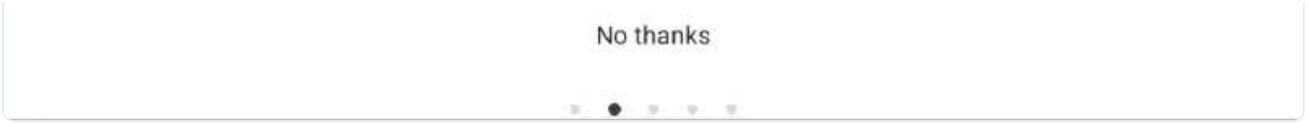


For version 26.4.0

7. The Privacy preferences screen determines which optional data the `Relution Companion` may transmit, e.g. automatic crash reports. Save applies the selection, which can later be revoked in the app’s settings.

For version 26.4.0


16:01 Thu, 31 Aug
90%
Locate device
In case your device gets stolen or is lost, Companion can be used to find it again. Your permission is required so that your IT can determine its location. This data is sent to a secure Relution server and is never shared with anyone, except your IT department.
If you do not grant permission at this time, you will be asked again once your IT attempts to locate the device
GRANT PERMISSION



8. Permission to locate the device can then be granted. If permission is not granted, the administrator will not be able to locate the Android device if it is stolen or lost.

For version 26.4.0

9. Relution can also be allowed to read the device status to share the phone number and IMEI with the administrator. This information is transmitted encrypted and never shared with third parties.

For version 26.4.0

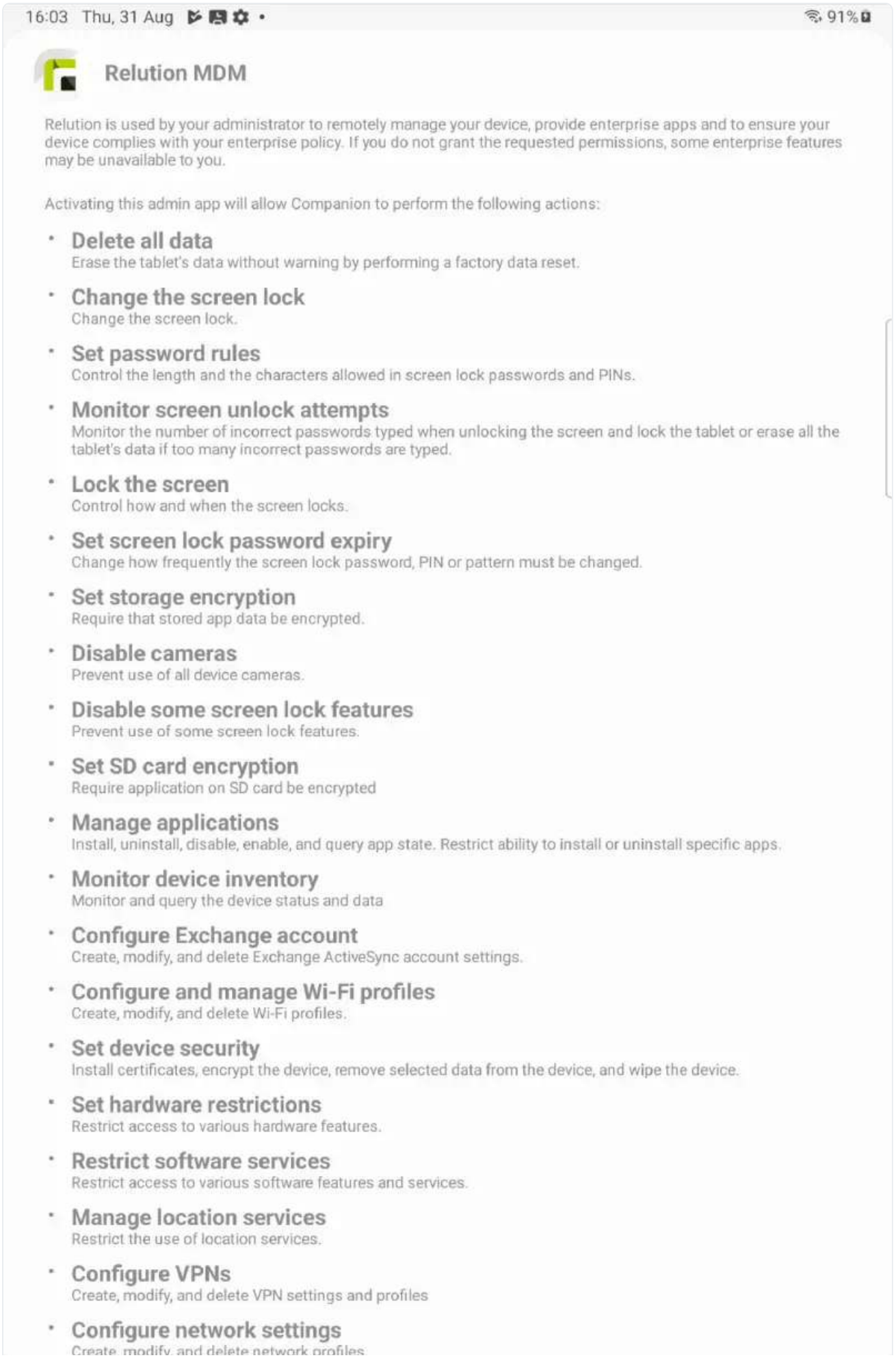

16:02 Thu, 31 Aug
90%
Device admin must be enabled
To access organization resources your device must comply with enterprise policy. To ensure your device is compliant, your IT must be able to manage some aspects of your device including but not limited to device wipe, lock device, etc. Please enable the device admin to continue.
On Samsung devices it may also be necessary to accept Samsung's privacy policy. Please confirm this dialog as well.
ENABLE DEVICE ADMIN



For version 26.4.0

10. A prompt then appears to grant administrative rights to Relution. This is necessary to ensure that the Android device complies with the organization's requirements, such as password policies. If the option Withdraw Android legacy devices in case the device administrator permission is not granted is enabled in `Settings` → `Device Management`, the device is withdrawn from management if the permission is not granted or is revoked later.

For version 26.4.0

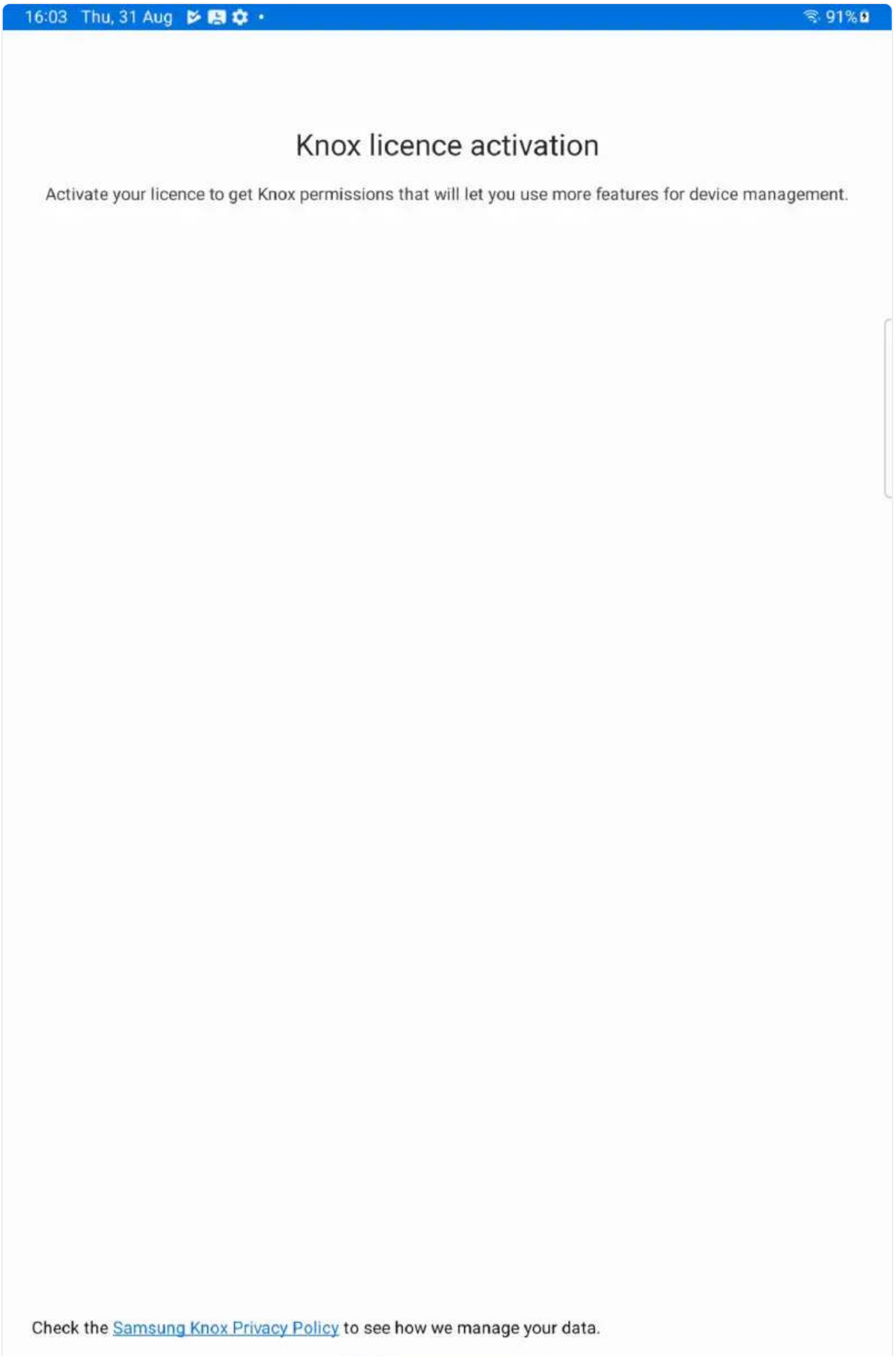

16:03 Thu, 31 Aug
91%
Relution MDM
Relution is used by your administrator to remotely manage your device, provide enterprise apps and to ensure your device complies with your enterprise policy. If you do not grant the requested permissions, some enterprise features may be unavailable to you.
Activating this admin app will allow Companion to perform the following actions:
Delete all data
Erase the tablet's data without warning by performing a factory data reset.
Change the screen lock
Change the screen lock.
Set password rules
Control the length and the characters allowed in screen lock passwords and PINs.
Monitor screen unlock attempts
Monitor the number of incorrect passwords typed when unlocking the screen and lock the tablet or erase all the tablet's data if too many incorrect passwords are typed.
Lock the screen
Control how and when the screen locks.
Set screen lock password expiry
Change how frequently the screen lock password, PIN or pattern must be changed.
Set storage encryption
Require that stored app data be encrypted.
Disable cameras
Prevent use of all device cameras.
Disable some screen lock features
Prevent use of some screen lock features.
Set SD card encryption
Require application on SD card be encrypted
Manage applications
Install, uninstall, disable, enable, and query app state. Restrict ability to install or uninstall specific apps.
Monitor device inventory
Monitor and query the device status and data
Configure Exchange account
Create, modify, and delete Exchange ActiveSync account settings.
Configure and manage Wi-Fi profiles
Create, modify, and delete Wi-Fi profiles.
Set device security
Install certificates, encrypt the device, remove selected data from the device, and wipe the device.
Set hardware restrictions
Restrict access to various hardware features.
Restrict software services
Restrict access to various software features and services.
Manage location services
Restrict the use of location services.
Configure VPNs
Create, modify, and delete VPN settings and profiles
Configure network settings
Create, modify, and delete network profiles

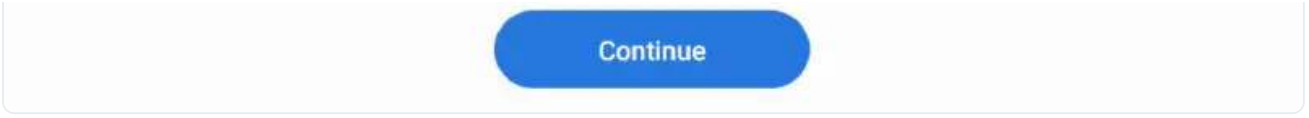


For version 26.4.0

11. Tapping Activate grants the administrative permissions. Depending on the manufacturer and Android version of the device, the screen layout and the button label may differ from the screenshot above.

For version 26.4.0

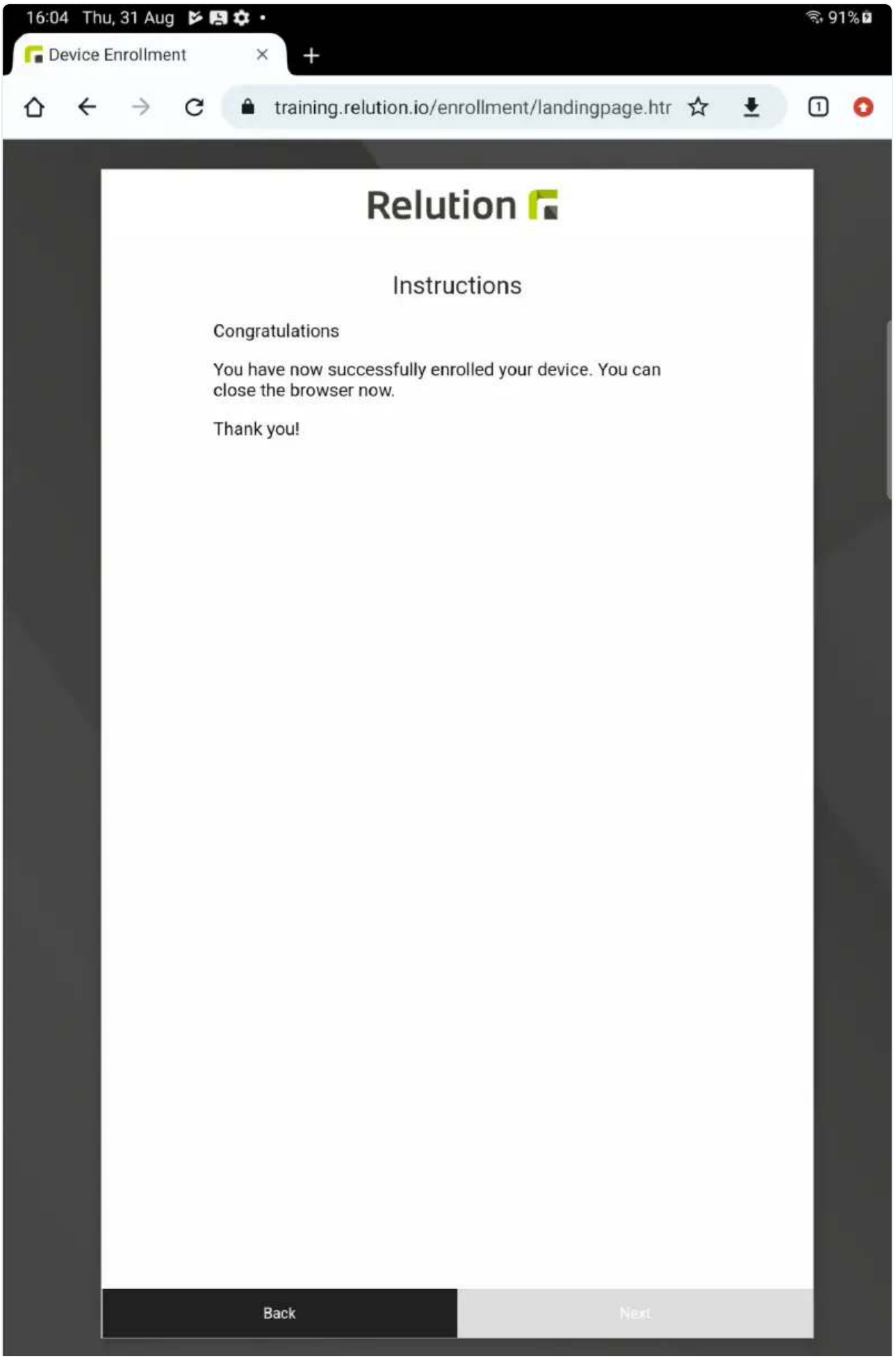

16:03 Thu, 31 Aug
91%
Knox licence activation
Activate your licence to get Knox permissions that will let you use more features for device management.
Check the Samsung Knox Privacy Policy to see how we manage your data.



For version 26.4.0

12. On Samsung devices, a Knox license activation dialog with a reference to the Samsung Knox privacy policy also appears. This dialog is confirmed with Continue as well.

For version 26.4.0


16:04 Thu, 31 Aug
91%
Device Enrollment
training.relution.io/enrollment/landingpage.htr
Relution
Instructions
Congratulations
You have now successfully enrolled your device. You can close the browser now.
Thank you!
Back
Next



13. The Android device will now complete the enrollment process and then show up in the device inventory of the appropriate Relution organization for management.

For version 26.4.0

Overview

Relution provides a selection of actions to directly control and direct Android Legacy/Classic devices. An outstanding advantage is that these actions can be applied specifically to individual devices.

Some of these actions are also available for Android Classic whiteboards. Which actions are offered depends on the manufacturer and is listed on the respective manufacturer page →. For example, Add Shortcut, Remove Shortcut and Locate Device are only available on a few whiteboards, and Reset Lock Passcode on none. Actions developed specifically for interactive whiteboards can be found under Actions (Whiteboards) →.

For version 26.4.0

Available actions

Action	Description
Alert →	Triggers an alarm on the device, even if the device is silent
Install App from Prowise App Store →	Select an app from the Prowise App Store to install (Prowise whiteboards only)
Remove App →	Uninstalls an app from the device
Send File to Device →	Upload a file to a directory on the device
Wipe Device →	Resets the device to its factory state and deletes all data from the device
Reboot Device →	Restarts the device
Locate Device	Requests the current location of the device. May fail if the location permission has not been granted on the device
Lock Device →	The device will be locked with the currently set password. If no password is set, the device can be unlocked without a password
Refresh Device Info →	Updates all available information about the device, listed in the Information tab
Send Message →	Displays a text message on the device
Reset Lock Passcode	Sets a new device password. Only available up to Android 10; on Android 7–10 only if no password is currently set on the device
Install Prowise Update →	Installs the latest Prowise firmware update (Prowise whiteboards only)
Deploy Relution Store App →	Search for an app in the Relution Store and distribute it to the devices
Remove Shortcut →	Removes a shortcut from the home screen
Add Shortcut →	Adds a shortcut to a website on the home screen
Install Update →	Installs a desired update on the selected device

Trigger Alarm

The Alert action triggers an alarm on the selected device, even if the device is set to silent. This makes it easier to locate the device in a room, for example. The Duration (in seconds) parameter defines how long the alarm sounds; the default is 30 seconds, the maximum is 60 seconds.

The action can also be triggered via device groups, either event-based or on a schedule: Device group actions →

Remove App

The Remove app action uninstalls a selected app from the device. The app can be selected from four sources: Relution App Store app, Google Play Store app, Installed app or Internal name of an app (entering the package name). Several apps can be selected at once in the lists.

The Installed app list only contains apps that the device last reported as installed; system apps, the Relution app and apps currently being installed are hidden there. If several devices are selected, only apps installed on all of these devices are shown.

If immediate removal is not possible, the user is prompted again every 1440 minutes (once a day) to remove the app.

Alternatively, apps can be removed in the device details on the Installed apps tab via Uninstall.

For version 26.4.0

Send File to Device

The Send file to device action uploads a selected file to a directory on the device. The target directory is specified in the Directory field relative to the device's external storage (`/sdcard/`); the default is `Download/` . ZIP archives are automatically unpacked unless the Don't decompress ZIP archives option is enabled – APK, JAR, and OBB files, however, are never unpacked automatically. Since Android 6.0, receipt of the file must also be confirmed on the device.

The action can also be triggered via device groups, either event-based or on a schedule: Device group actions →

Wipe Device

The Wipe device action resets the device to its factory state and deletes all data from the device.

The action is selected in the details of a device under `Devices` → `Inventory` on the `Actions` tab via Apply action. Before execution, the dialog points out that all stored content is permanently deleted and cannot be restored after the reset. For Android Classic devices, the dialog offers no further options.

Prerequisite

The action must be enabled under `Settings` → `Device Management` → `Enrollment` in the Wipe device row for the device's ownership (COD or BYOD). By default, it is enabled for COD and disabled for BYOD. For devices with unknown ownership, it is always available; this setting cannot be changed in the portal. If the action is disabled for the ownership, Relution does not offer it.

The action is not available for Prowise and SMART whiteboards.

Status and Cancellation

Android Classic devices only confirm receipt of the action. Relution therefore sets the status to Executed as soon as the action is delivered; this does not indicate whether the device was actually reset. Once created, the action cannot be cancelled.

For version 26.4.0

Reboot Device

The Reboot device action restarts or shuts down the device. In the portal, the action is marked with the Interactive Whiteboard badge for Android Classic devices.

The action is selected in the details of a device under `Devices` → `Inventory` on the `Actions` tab via Apply action. The following options are available in the next step:

- Reason for rebooting: optional information on why the device is restarted.
- Power off (also marked with the Interactive Whiteboard badge): The device is shut down instead of restarted.

For KION and Newline devices, neither the reason nor the Power off option is available.

Lock Device

The Lock device action locks the device with the currently set password. If no password is set, the device can be unlocked without a password.

For Android Classic devices, this is the only lock action. No further input is required when sending it.

Whiteboards

On whiteboards from ADVANTouch, CTOUCH, i3-Technologies, Newline, Promethean, Prowise and VS, a password or PIN must be set before locking, either locally on the device or, if available, via configuration.

The action is not available on whiteboards from Clevertouch, heinekingmedia, SMART and ViewSonic.

Unlocking

An unlock action only exists for whiteboards from CTOUCH, i3-Technologies and Newline, see Unlock Device →. All other devices are unlocked on the device itself with the password.

From Android 7, an unknown device password cannot be replaced via the Reset lock passcode action either: on Android 7 to 10, it only sets a new password if no password is currently set on the device; from Android 11, it is no longer available.

For version 26.4.0

Availability by ownership

The action is only offered if it is enabled under `Settings` → `Device Management` → `Enrollment` in the Lock device row for the ownership of the device (COD or BYOD). By default, it is enabled for both.

Refresh Device Info

The Refresh device info action updates all available information about the device shown on the Information tab of the device details.

In the details of a device under `Devices` → `Inventory`, the action is triggered directly via the Refresh device information icon in the header area; no dialog opens. Alternatively, it is available on the `Actions` tab under Apply action.

Relution sends the action to the Relution Companion on the device via push notification. If push delivery is not possible, the action remains in the Pending status until the device fetches it itself the next time it connects. The displayed information is only updated once the device has responded.

Send Message

The Send message action displays a text message on the device. A title and the message text (Content) are required.

On smartphones and tablets, the message is delivered to the Relution app via push. If sending succeeds, the action immediately receives the status Executed, with the title and content of the delivered message as a comment. The status confirms delivery, not that the message has been read on the device. If the push fails, the action remains Pending until the device fetches it itself. Interactive displays (whiteboards) do not receive the message via push to the Relution app but, like other actions, via the device channel.

Completed message actions are automatically removed from the action history after 10 days by default.

Deploy Relution Store App

The Deploy Relution store app action allows searching for an app in the Relution Store and distributing it to the device. Native Android apps from the Relution Store are available for selection; one app is selected per action and distributed in its released version. Installation from unknown sources must be enabled on the device for this.

For version 26.4.0

The dialog offers two toggles, both enabled by default:

- Deploy silent if possible: Installation is attempted in the background. If this does not succeed automatically, the user is prompted on the device to install the app.
- Remove app on Enterprise Wipe: The app is removed from the device again during an Enterprise Wipe.

The action is not available for Prowise whiteboards; apps are installed there via Install App from Prowise App Store →.

Add Shortcut

The Add Shortcut action adds a shortcut to a website on the home screen of the device. The required fields are Label (caption of the shortcut) and URL (valid target URL). Optionally, a custom image in JPEG or PNG format with a maximum size of 1 MB can be set via Icon.

Label and URL are also needed to remove the shortcut later using the Remove Shortcut → action.

The action is available for Android Classic devices; among whiteboards, only for Promethean → and wende.interaktiv → (Wende 8 and Wende 9).

Remove Shortcut

The Remove Shortcut action removes a shortcut from the home screen of the device. The shortcut to be removed is specified using the required fields Label and URL; there is no selection list of existing shortcuts. The values to enter are those with which the shortcut was created using the Add Shortcut → action.

The action is available for Android Classic devices; among whiteboards, only for Promethean →.

For version 26.4.0

Overview

A policy is a collection of one or more configurations. Each policy can be applied to one or more devices at the same time. In addition, one or more policies can be associated with each device.

For version 26.4.0

Available Configurations

Configuration	Description
ADVANTouch →	Manages ADVANTouch interactive whiteboards
App compliance →	Manages app-specific restrictions
Clevertouch →	Manages Clevertouch interactive whiteboards
CTOUCH →	Manages CTOUCH interactive whiteboards
Dahua →	Manages Dahua interactive whiteboards
EShare →	Configures the EShare app
Exchange	Manages Exchange accounts
Scheduled OTA update →	Installs firmware updates on Clevertouch, i3 and Newline interactive whiteboards at scheduled times
Wallpaper →	Sets the wallpaper
Hotspot →	Manages the hotspot configuration
i3 →	Manages i3 interactive whiteboards
Interactive Board Configuration	Manages restrictions for interactive whiteboards
Kiosk Mode →	Manages kiosk mode settings
Access Point Name configuration	Manages an Access Point Name
Newline	Manages Newline interactive whiteboards
Passcode	Manages password policies for Android devices
Promethean →	Manages Promethean settings
Restrictions →	Manages device restrictions
Wireless network restrictions	Manages Wi-Fi restrictions
SMART →	Manages SMART interactive whiteboards
VPN	Manages VPN settings
ViewSonic →	Manages ViewSonic interactive whiteboards
VS →	Manages VS interactive whiteboards

Configuration	Description
WiFi →	Manages Wi-Fi settings
Certificate →	Selects a certificate that is installed on the device by default

Wallpaper

As of Relution 5.33, the Wallpaper configuration is available for Android Enterprise and Android Classic/Legacy. This allows setting an image for the home screen that appears on devices after applying the policy. The policy also enables adding text (including placeholders) to display dynamic text on the wallpaper.

> Android Enterprise requires Relution Companion version 1.18.
>
> Android Classic requires Relution Companion version 5.37.

The Wallpaper configuration sets the image but does not prevent users from changing it on the device.

For version 26.4.0

Configuration

The General section contains the following fields:

- Text on wallpaper – optional text placed on the image. Placeholders are resolved per device; the supported placeholders are listed in the form below the input fields.
- Text color – hex color code, e.g. `#ffffff` (default), optionally via the color picker.
- Wallpaper – the image itself (mandatory). The maximum file size is 3 MB by default; on self-hosted servers, it can be adjusted via the parameter `relution.wallpaper.max-file-size.android`. If the image is larger, the portal displays an error message and the configuration cannot be saved.

App Compliance

Android Classic / Legacy allows Native Apps to be uploaded as `.apk` files to the Relution App Store and distributed to enrolled Android devices via action or policy. Distribution via action is described under Deploy Relution Store App →.

> Google Play apps cannot be installed automatically in Android Classic. Google Play Store apps entered under Required apps must be installed by the user; the Auto install option is only available for native apps from the Relution App Store. For managed distribution of Google Play apps, Android Enterprise (Managed Google Play) is required.

Native apk via a policy

This method does not provide automatic updates for new app versions.

First, the app is deployed to the Relution App Store, then distributed via a policy with the App compliance configuration.

> Only one policy with the App compliance configuration can be applied per device. If another configuration of this type is assigned to a device, it is skipped and not applied.

For version 26.4.0

1. In the Relution portal, the menu item `Apps` → `App Store` is opened and a new app is added via Add.
2. The option Native app is selected, followed by Next.
3. Under Choose file, the desired `.apk` file is selected via Select.
4. On the following page, the release status of the app must be changed from Development (blue icon) to Release (green icon). The change is confirmed with Save.
5. Under `Devices` → `Policies`, a new policy is created via Add. An Android policy is created and given a Name. The policy is saved via Save.
6. Via Add, the App compliance option is selected, followed by Add details.
7. The List Type is preselected as Blocklist — The apps below are not allowed by default. Regardless of this, the desired apps from the Relution App Store are added under Required apps.
8. The configuration is saved and the current version of the policy is published.
9. To apply the policy to Android devices, the desired devices are added via the Devices with this policy tab. The devices are assigned to an existing static device group with this policy or to a newly created static device group. The selected settings and apps are then automatically applied or installed on the devices.

Selecting Auto install installs the respective apps automatically on the Android devices. For the installation, the devices must be assigned to users who are members of the AppStore User user group.

Configuration settings

The App compliance configuration is divided into three sections.

General

- Enforce block / allowlist only while roaming – the blocklist or allowlist is only applied while the device is roaming. If the option is switched off, the list applies regardless of the roaming state.
- Ignore block / allowlist while on a wireless network – only available if the previous option is enabled. While the device is connected via Wi-Fi, apps are allowed even when roaming.
- List Type – Blocklist — The apps below are not allowed (default) or Allowlist — The apps below are allowed.

For an allowlist, Non-allowed apps defines how all other apps are handled:

- Uninstall – the user is prompted to uninstall the app from the device. The option is not available if Enforce block / allowlist only while roaming is enabled.
- Disable – the app remains installed but can no longer be started by the user.
- Block internet access – revokes the app's internet access. The option has no effect on pre-installed apps, and some apps may crash as a result; in that case, Disable is preferable.

Blocked or allowed apps

Depending on the List Type, the section is called Blocked apps or Allowed apps. Apps can be added from the Relution App Store, from the Google Play Store or manually via their package name.

The Disable system apps option attempts to block all system and pre-installed apps. This includes the phone app, so emergency calls can no longer be made. If telephony is required, the phone app has to be put on the allowlist.

For version 26.4.0

Required apps

The apps entered here must be installed on the device, otherwise the device is considered noncompliant. Google Play Store apps must be installed by the user; Auto install is only possible for native apps from the Relution App Store.

The configuration is rejected on saving if

- an app is on the blocklist and under Required apps at the same time, or
- a weblink is entered as a required app.

Restrictions

Targeted restriction of device and app features increases security when using Android devices and can optimize device usage by providing more focus. Controlling device settings and restricting access also prevents third-party apps from accessing corporate data and resources. Restriction availability may vary, depending on device manufacturer and existing OS version. Some of the restrictions are only available on Samsung Knox devices (group Knox specific restrictions).

Applying restrictions to Android devices

1. In the Relution portal, a new policy is created under `Devices` → `Policies` via Add.
2. An Android policy is created and given a Name. The policy is saved via Save.
3. Via Add, the Restrictions option is selected, followed by Add details.
4. After selecting the desired options, the configuration is saved and the current version of the policy is published.

   If Enforce Device Encryption or Enforce SD Card Encryption is enabled, the policy must also contain an enabled Passcode configuration. Otherwise, the version can neither be published nor tested. For effective encryption, a passcode quality should also be set in the passcode configuration.
5. To apply the policy to Android devices, the desired devices are added via the Devices with this policy tab. The devices are assigned to an existing static device group with this policy or to a newly created static device group. The selected restrictions are then automatically applied on the devices.

For version 26.4.0

Many options in the restrictions offer explanations and extended information via a mouse-over. Options that require a Samsung Knox device are grouped under Knox specific restrictions.

Available restrictions

The Restrictions configuration is divided into three groups. Via the download icon (Export restrictions as CSV file) above the groups, all restrictions and their current values can be exported as a CSV file.

General restrictions

- Enforce Device Encryption – encrypts accounts, settings, apps and their data, media and other files. Afterwards, a PIN or password has to be entered each time the device is switched on. The encryption can only be removed by a factory reset, which erases all data. The process takes an hour or more; the device should be charged and plugged in, as an interruption can lead to data loss.
- Deny Camera
- Deny Camera/Widgets on lock screen – the lock screen must be secured with a PIN, pattern or password.
- Disable root detection – rooted devices are no longer reported as noncompliant. The device details continue to show the device as rooted.

Roaming

- Activate restrictions only while roaming – the restrictions are only applied while the device is roaming.
- Allow on WiFi – only available if the previous option is enabled. The restrictions are then only applied while roaming and not connected to a Wi-Fi network.

Knox specific restrictions

These options are only available on Samsung Knox devices.

Section	Options
General	Deny Screen Capture, Deny Clipboard, Deny to switch GPS on or off, Deny to change date and time, Deny widgets on Lockscreen, Deny shortcuts on Lockscreen
Storage	Enforce SD Card Encryption, Deny SD Card Access, Deny SD Card Write
Debugging	Deny USB Debugging, Deny Google crash reporting
USB restrictions	Deny Media Transfer Protocol (MTP), Deny USB Tethering, Deny USB Host Storage
Backup & reset	Deny Google Backup, Deny factory reset, Deny OTA upgrade, Deny safe boot
App restrictions	Deny Installation of non Play Store Apps, Deny Google Play, Deny Youtube, Deny Browser, Deny Settings, Deny Voice Dialer

Notes on individual options:

- Enforce SD Card Encryption requires an alphanumeric device password. The passcode policy can only be changed while the encryption is deactivated.
- Deny Media Transfer Protocol (MTP) blocks any file transfer via USB, since Android only transfers files via MTP. PTP (Picture Transfer Protocol) is affected as well.
- Deny USB Host Storage prevents USB sticks, external hard drives or SD card readers from being mounted as storage via USB OTG.
- Deny safe boot prevents booting into safe mode, which could otherwise be used to leave kiosk mode.
- Deny Installation of non Play Store Apps blocks the installation of apps from outside Google Play; the user cannot allow it in the Android settings. If the option is disabled, the user can allow the installation in the Android settings; it is not enabled by the option itself.

Kiosk Mode

The Kiosk Mode turns Android devices into purpose-built devices suitable for work-related applications. End users can therefore only use the app approved by the organization and use approved device functions on provided devices with Kiosk Mode activated.

For this purpose, there are two modes that can be applied to Android devices - one is Single App Mode and the other is Multi App Mode.

When kiosk mode is active, the device shows the Relution Launcher, whose activation the user has to confirm; on Samsung devices with SAFE, this confirmation is not required. The user has no access to the system settings.

> In kiosk mode, emergency calls are only possible if the phone app is among the permitted apps or an Emergency Phone # is set under Device settings.

Kiosk in Single App Mode

The Single App Mode is a locking mechanism that restricts device access to a single application. Devices running in Single App Mode serve only one purpose: running a specific application with minimal device functionality. The application starts itself, runs in the foreground, and is restarted even when the devices are shut down or rebooted. In this way, Kiosk Mode ensures proper use of the devices while avoiding unnecessary distractions for users.

For version 26.4.0

1. In the Relution portal, the menu item `Devices` → `Policies` is opened and Add is clicked.
2. An Android policy is created and given a Name, then saved with Save.
3. After clicking Add, the Kiosk Mode option is selected, followed by Add details.
4. The On/Off switch remains enabled (default). The mandatory Password field holds the password used to leave kiosk mode on the device (Exiting kiosk mode →). Without a password, the configuration cannot be saved.
5. Enable Single App Mode is turned on and exactly one app is selected. The selected app must already be installed on the device, e.g. via the Deploy Relution Store App → action.
6. After selecting additional options and restrictions (Additional settings →), the configuration is saved and the current version of the policy is published.
7. To apply the policy to Android devices, the desired devices are added in the Devices with this policy tab. The selected settings will then be automatically applied to the devices.

Kiosk in multi-app mode

The Multi App Mode restricts devices to a specific selection of applications relevant to the work requirements of the organization. Users can access and use the approved applications. The Kiosk Mode allows complete control over device usage and ensures that devices are only accessed and used for specific purposes.

1. In the Relution portal, the menu item `Devices` → `Policies` is opened and Add is clicked.
2. An Android policy is created and given a Name, then saved with Save.
3. After clicking Add, the Kiosk Mode option is selected, followed by Add details.
4. The On/Off switch remains enabled (default). The mandatory Password field holds the password used to leave kiosk mode on the device (Exiting kiosk mode →). Without a password, the configuration cannot be saved.
5. If the option Enable Single App Mode is turned off, an app selection can be added. The selected apps must already be installed on the device. As soon as more than one app is selected, Single App Mode can no longer be turned on.
6. Furthermore, additional options are available, of which the following are relevant:
    - Enable all native apps from Relution App Store - enabled by default. The kiosk then shows all native apps from the Relution App Store in addition to the app selection; apps that are not installed are offered for download. To show only the selected apps, the option is disabled.
    - App store refresh interval - only while the previous option is enabled; defines how often the device refreshes the Relution App Store list (1, 2, 4, 6, 12 or 24 hours; default 12 hours). A shorter interval makes new apps appear sooner but increases battery consumption and data usage.
    - Only display installed Apps - if disabled, all available apps will be displayed and offered for download.
    - Show apps installed by an administrator - apps that have been installed on the devices via the Deploy Relution store app action automatically appear in kiosk mode, even if they are no longer available in the store.
    - Group apps by category - arranges the apps on the launcher in folders by category. An app with several categories appears in each of these folders.
    - App arrangement type - with Dynamic (default), the grid is calculated automatically. With Fixed and Fixed and centered (grid starting from the center of the screen), Number of app icons per row and Number of app icons per column are defined (1 to 12 each).
7. After selecting additional options and restrictions (Additional settings →), the configuration is saved.
8. If required, the Kiosk Mode configuration is supplemented with the App compliance configuration.
9. The current version of the policy is published.
10. To apply the policy to Android devices, the desired devices are added in the Devices with this policy tab. The selected settings will then be automatically applied to the devices.

For version 26.4.0

Additional settings

Regardless of the selected mode, the configuration offers the following settings:

- Show device name - shows a name on the launcher. If the Device name field is empty, the name of the device is shown. Changes to the device name may take several hours to appear on the device.
- Device settings - Keep screen on while charging, Emergency Phone # as well as Homescreen Wallpaper and Lockscreen Wallpaper (PNG or JPEG each). The emergency phone number and the lock screen wallpaper appear on the lock screen and therefore require a lock screen, which can be enforced with a passcode configuration. The emergency phone number can be used to make an emergency call even if the device is locked or kiosk mode is active.
- Device restrictions - among others, navigation bar, status bar, system bar, task manager and home key, as well as Samsung features such as Airview, S-Voice, edge screen, multi-window and smart clip. Navigation bar, status bar and its expansion, system bar, task manager, home key and edge screen are allowed by default. If the navigation bar or system bar is disabled, the app itself is responsible for navigation. Clear notifications and Wipe recent tasks remove notifications and the list of recently used apps respectively.
- Hardware Restrictions - under Disable hardware keys, the on/off button, the volume buttons as well as the home, back and menu buttons can be blocked.

Exiting kiosk mode

The password prompt appears on the device when the screen is tapped quickly 2 times, 4 times, 1 time and 3 times, with a pause of more than 0.5 seconds between the groups. After entering the Password stored in the configuration, kiosk mode can be exited.

For version 26.4.0

WiFi

The WiFi policy allows managing the WiFi settings on Android Classic devices. A policy can contain several WiFi configurations, e.g. for different networks. Placeholders can be used in the configuration and are resolved per device during transfer; the available placeholders are shown in the form below the input fields.

Restrictions on WiFi usage, e.g. allowed or blocked SSIDs and a minimum security level, are not defined here but via the separate Wireless network restrictions configuration.

General

- The network's SSID – name of the network (mandatory).
- Priority – integer from 0. If multiple networks are available, the device first connects to the network with the highest priority. By default, all networks have priority 0.
- This network is hidden – for networks that do not broadcast their SSID.
- Encryption type – None / Open (default), WEP, WPA/WPA2 PSK or 802.1x EAP (EAP). For WEP and WPA/WPA2 PSK, the Password field is mandatory; for WPA/WPA2 PSK, it must be 8 to 63 characters long.

802.1x EAP (EAP)

For version 26.4.0

This section only appears for the encryption type 802.1x EAP (EAP). Under Accept EAP types, PEAP (default), TLS, TTLS and PWD are available. Depending on the type, the following fields are shown:

- PEAP and TTLS: Phase 2 Authentication (None, MSCHAP, MSCHAPv2, GTC or PAP, default: None), CA certificate, Identity, Anonymous identity and Password. For PEAP, PAP and MSCHAP are rejected when saving.
- TLS: CA certificate, User authentication certificate and Identity. Two options are available for the user authentication certificate:
  - Select certificate – a certificate with a private key (PKCS#12) from Certificate management →.
  - Use user certificate – the Wi-Fi certificate from the profile of the user assigned to the device (see User certificates →). The optional Certificate name field selects a specific certificate by name if the user has several Wi-Fi certificates and may contain placeholders. If left blank, the longest-lived certificate is used.
- PWD: Identity and Password.

Certificates without a private key (PKCS1) from certificate management are available as CA certificate.

> On Samsung Knox devices, a configuration with the EAP type PEAP, TLS or TTLS is only applied if the policy also contains an enabled Passcode configuration. If it is missing or disabled, the form displays a corresponding notice.

Proxy type

- None (default) – no proxy.
- Manual – Host (without protocol) and Port (1 to 65535) of the proxy server are mandatory. Bypass proxy for takes a list of addresses that are not routed through the proxy.
- Automatic configuration – PAC URL with the address of the PAC file (mandatory).

Certificate

The Certificate policy allows selecting a certificate to be installed by default on the device. A policy can contain several certificate configurations, but each certificate only once.

Prerequisites

- The certificate has previously been uploaded under `Settings` → `Certificates` (see Certificate management →).
- Only certificates of type PKCS1, i.e. certificates without a private key (e.g. `crt`, `cer`), can be selected. PKCS#12 files (`pfx` / `p12`) are not listed.
- On Samsung Knox devices, the certificate is only installed if the policy also contains an enabled Passcode configuration. If it is missing or disabled, the form displays a corresponding notice.

For version 26.4.0

Configuration

In the Add Certificate dialog, Select next to the Certificate field in the General section opens the Select a certificate dialog. Certificates already used in another certificate configuration of the same policy are hidden there. The field is mandatory; Save only becomes active once a certificate has been selected. The name of the configuration is taken automatically from the name of the certificate.

Factory Reset Protection

Organizations need to ensure the security and compliance of Android devices used for service delivery. Relution can be used to minimize effort and increase security by remotely setting up, managing, and monitoring work-related devices and promptly fixing any errors that occur. A Relution Companion for Android installed on the devices enables Android Classic / Legacy enrollment of the devices into Relution. Additionally, a factory reset can be forbidden on the devices.

Denying the factory reset is a Knox-specific restriction of the Restrictions configuration and is only available on Samsung devices with Knox. On devices from other manufacturers, the option has no effect.

FRP configuration

1. In the Relution portal, the menu item `Devices` → `Policies` is opened and Add is clicked.
2. An Android policy is created and given a Name, followed by a click on Save.
3. After clicking Add, the Restrictions option is selected, followed by Add details.
4. Under Knox specific restrictions, in the Backup & reset section, the option Deny factory reset must be enabled. In new restrictions configurations, the option is enabled by default.
5. The configuration is saved and the current version of the policy is published.
6. To apply the policy to Android devices, the desired devices are added via the Devices with this policy tab. Alternatively, the policy is assigned to entire device groups via the Device groups with this policy tab. The selected settings are then automatically applied to the devices.

> On Samsung devices with Knox, the Reset device to factory settings button is then grayed out. Resetting via Recovery Mode is also no longer possible.

For version 26.1.0

Since the option is enabled by default, every restrictions configuration denies the factory reset as long as the option is not disabled. If a device is to be reset deliberately, the option Deny factory reset is disabled and a new version of the policy is published.

All other options of the configuration are described under Restrictions →.

ADVANTouch

Relution makes it possible to manage interactive whiteboards from the ADVANTouch brand.

Supported product ranges and models

Relution supports the following ADVANTouch product series:

- ADVANTouch PRO 1, 2.0, 2.1, and 3
- ADVANTouch vGAP 2, 3, 4, and 5

Support is generally available from Android API 24 (equivalent to Android 7.0 or higher).

Enrollment

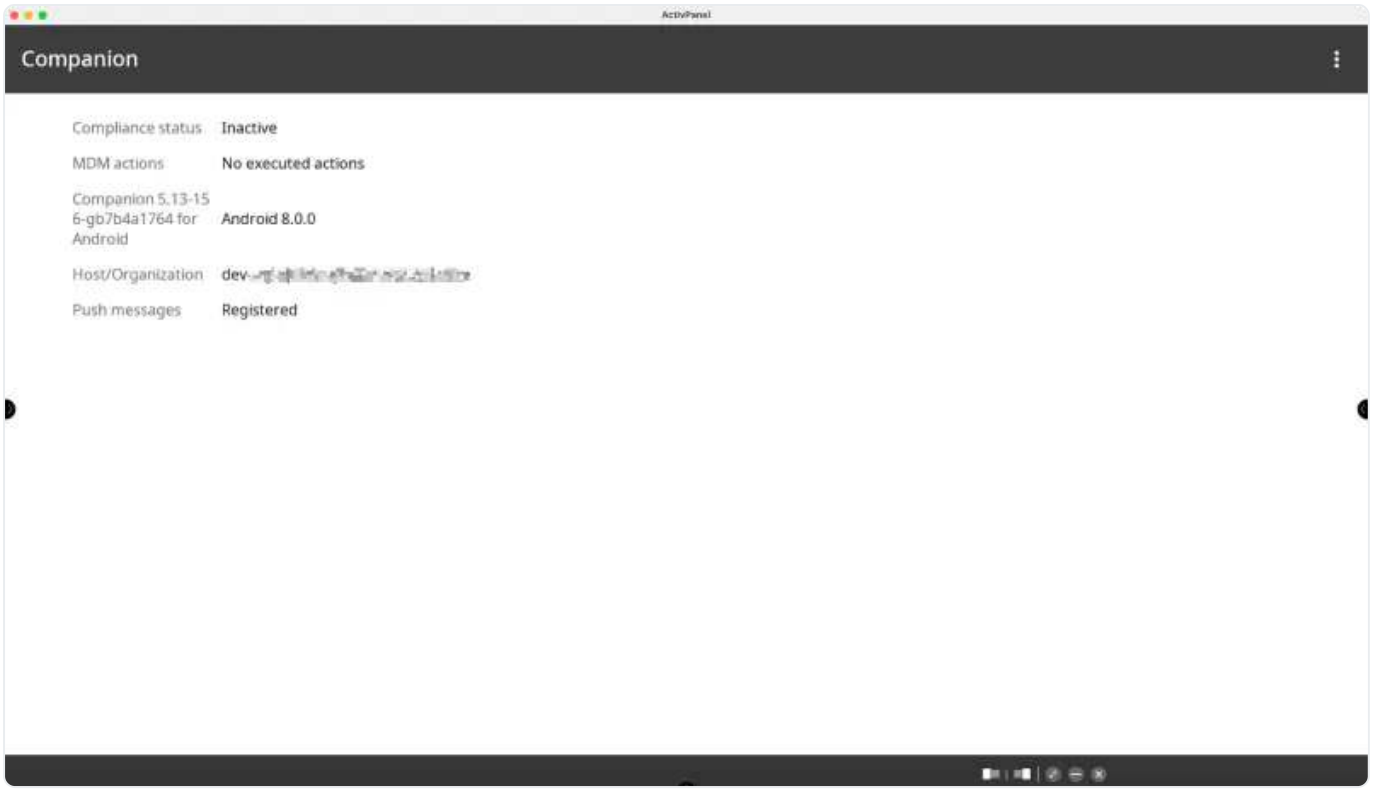
For Version 26.4.0

An enrollment is created for the platform Android with ADVANTouch selected as the type.

The Relution Companion for ADVANTouch (package name `com.mwaysolutions.relution.advantouch`) must be installed before enrollment. The standard Relution Companion cannot enroll with an enrollment of type ADVANTouch; the server rejects the enrollment.

In the Relution Companion, the server address and the enrollment code are entered.

The Companion then asks for several confirmations, and the displayed notifications and authorization requests are confirmed. After successful enrollment, a corresponding confirmation screen will appear.



The device should now be visible in the Relution Portal inventory.

For version 26.4.0

Supported Actions

The following actions can be performed on ADVANTouch interactive whiteboards via Relution:

Action	Description
Trigger Alarm →	
Remove App →	
Send File to Device →	
Wipe Device →	
Reboot Device →	Restart or shut down (Power off option)
Lock Device →	Prerequisite: a password or PIN is set locally on the device or via the manufacturer-specific policy (Enable LockScreen Pin)
Refresh Device Info →	
Send Message →	
Deploy Relution Store App →	
Update Operating System →	

For version

Supported Policies

The following policies are supported on ADVANTouch interactive whiteboards:

Policy	Restrictions
Hotspot →	
App Compliance →	
Certificate →	Device Owner

Manufacturer-specific policy

The manufacturer-specific policy ADVANTouch offers the following settings:

For version 26.4.0

Setting	Description
Brightness	Set brightness to a fixed value from 0 to 100
Enable Eye Care	
Lock touch input	
Boot Source	Set the active source after the display powers on (Do Not Change, Android, HDMI 1–3, USB-C 1–2, or VGA)
Current Source	Set the currently active source (same options as Boot Source)
No signal power off	Power off when no signal is received after the set time
No signal power off time	Time from 1 minute to 1 hour until power-off without a signal; only available when No signal power off is enabled
Wake on source plugged in	
Allow source alias	Once enabled, set aliases for Android, HDMI1, HDMI2, HDMI3, and USB-C1
Enable Ethernet	
Wake on LAN	Enable the Wake-on-LAN feature
Mute	
Volume	Set volume to a fixed value from 0 to 100
Enable LockScreen Pin	Set a lock screen PIN (exactly 4 digits)
Enable administrator lock	Set a password for the administrator lock (exactly 4 digits)
Enable settings lock	Only available when the administrator lock is enabled
Language	Set the device language (English, German, or Spanish)
Enable Automatic OTA Update	
Enable installation from unknown sources	Allows installation from unknown sources, including USB drives
Power on automatically	Set weekdays and time for automatic display power-on
Power off automatically	Set weekdays and time for automatic display power-off
Time until panel goes into standby mode	Don’t change, Never, 15 or 30 minutes, 1, 1.5, or 2 hours

A new configuration is preset with the following values: brightness 100, volume 33, language German, standby Never; Enable Ethernet, Enable installation from unknown sources, and Wake on source plugged in are enabled. Brightness, volume, and language have no “Don’t change” option, so these values are always set by the policy.

After changing the lock screen PIN or the administrator lock, a restart of the device might be required for the changes to take effect.

Enable Device Owner

To enable device owner specific functions, the device is first connected as described in Android Debug Bridge setup and connection →.

Once the device is connected, device owner mode is enabled by executing the following command:

```
adb shell dpm set-device-owner
com.mwaysolutions.relution.advantouch/com.mwaysolutions.relution.receiver.MdmDeviceAdmi
nReceiver
```

For version 26.4.0

Clevertouch

Relution makes it possible to manage interactive whiteboards from the Clevertouch brand.

Supported product ranges and models

The following product series are supported:

- IMPACT Lux

Enrollment

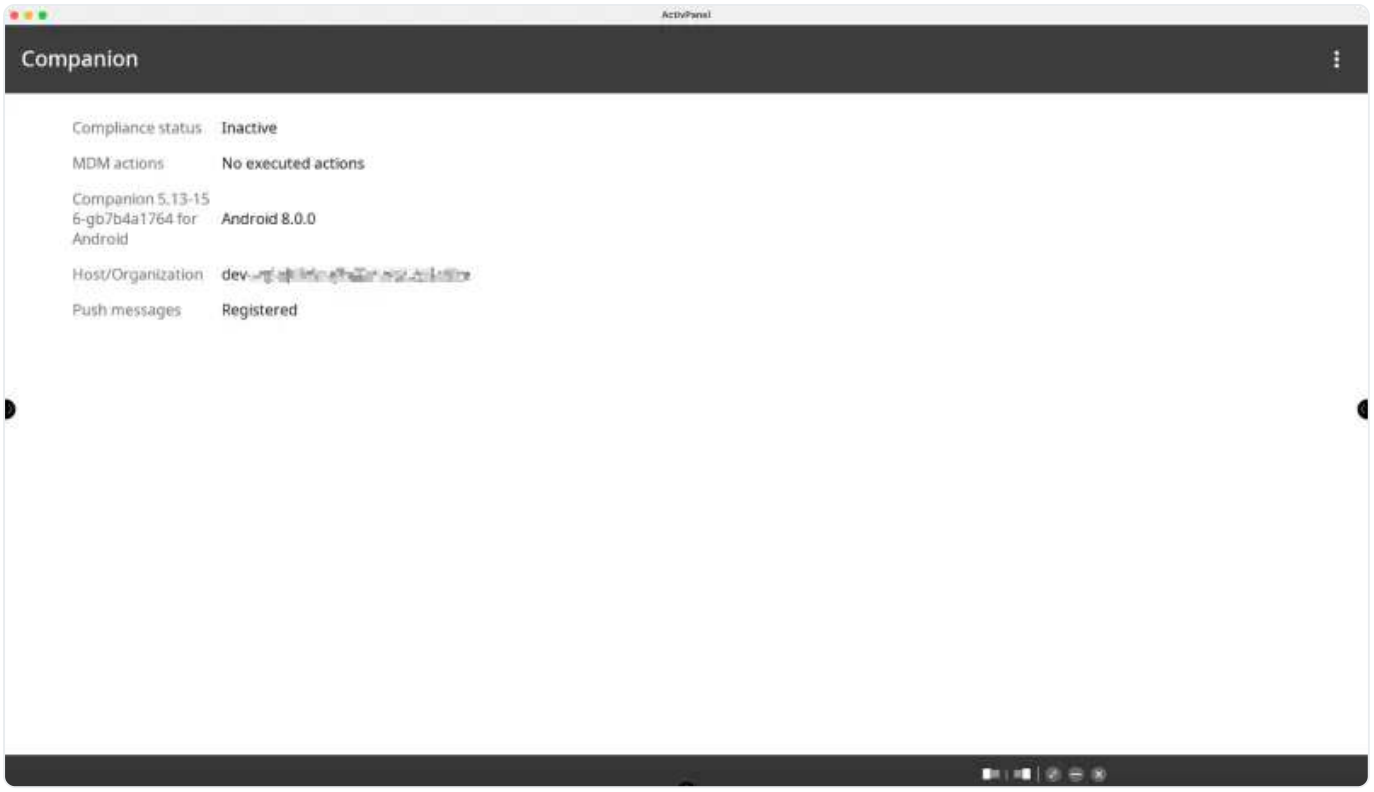
An enrollment is created for the platform Android with Clevertouch selected as the type. The enrollment link is then opened on the device, and the instructions on the webpage are followed.

The Relution Companion for Clevertouch can be downloaded and installed via the displayed download button.

After the Companion has been installed successfully, the enrollment is started from the enrollment page.

The Companion then opens automatically and prompts confirmation of several notes and authorizations. After successful enrollment, a corresponding confirmation screen will appear.

For version 26.4.0



The device should now be visible in the Relution Portal inventory.

For version 26.4.0

Supported Actions

The following actions can be performed on Clevertouch interactive whiteboards via Relution:

Action	Description
Trigger Alarm →	
Remove App →	
Send File to Device →	
Wipe Device →	
Reboot Device →	Restart or shut down (Power off option)
Refresh Device Info →	
Send Message →	
Deploy Relution Store App →	
Update Operating System →	

Supported Policies

The following policies are supported on Clevertouch interactive whiteboards:

Policy	Restrictions
Scheduled OTA Update →	
Hotspot →	
WiFi →	
App Compliance →	

Manufacturer-specific policy

The manufacturer-specific policy Clevertouch offers the following settings:

For version 26.4.0

Setting	Description
Brightness	Set brightness to a fixed value from 0 to 100
Enable Eye Care	
Lock touch input	
Boot Source	Set the active source after the display powers on (Do Not Change, Android, HDMI 1–3, USB-C 1–2, or VGA)
Current Source	Set the currently active source (same options as Boot Source)
No signal power off	Power off when no signal is received after the set time
No signal power off time	Time from 1 minute to 1 hour until power-off without a signal; only available when No signal power off is enabled
Allow source alias	Once enabled, set aliases for Android, HDMI1, HDMI2, HDMI3, and USB-C1
Enable Ethernet	
Mute	
Volume	Set volume to a fixed value from 0 to 100
Enable LockScreen Pin	Set a lock screen PIN (exactly 4 digits)
Language	Set the device language (English, German, or Spanish)
Enable Automatic OTA Update	
Enable installation from unknown sources	Allows installation from unknown sources, including USB drives
Power on automatically	Set weekdays and time for automatic display power-on
Power off automatically	Set weekdays and time for automatic display power-off
Time until panel goes into standby mode	Don’t change, Never, 15 or 30 minutes, 1, 1.5, or 2 hours

A new configuration is preset with the following values: brightness 100, volume 33, language German, standby Never; Enable Ethernet and Enable installation from unknown sources are enabled. Brightness, volume, and language have no “Don’t change” option, so these values are always set by the policy.

After changing the lock screen PIN, a restart of the device might be required for the change to take effect.

CTOUCH

Relution makes it possible to manage interactive whiteboards from the CTOUCH brand.

Supported product ranges and models

The following product series are supported:

- Riva D2

Enrollment

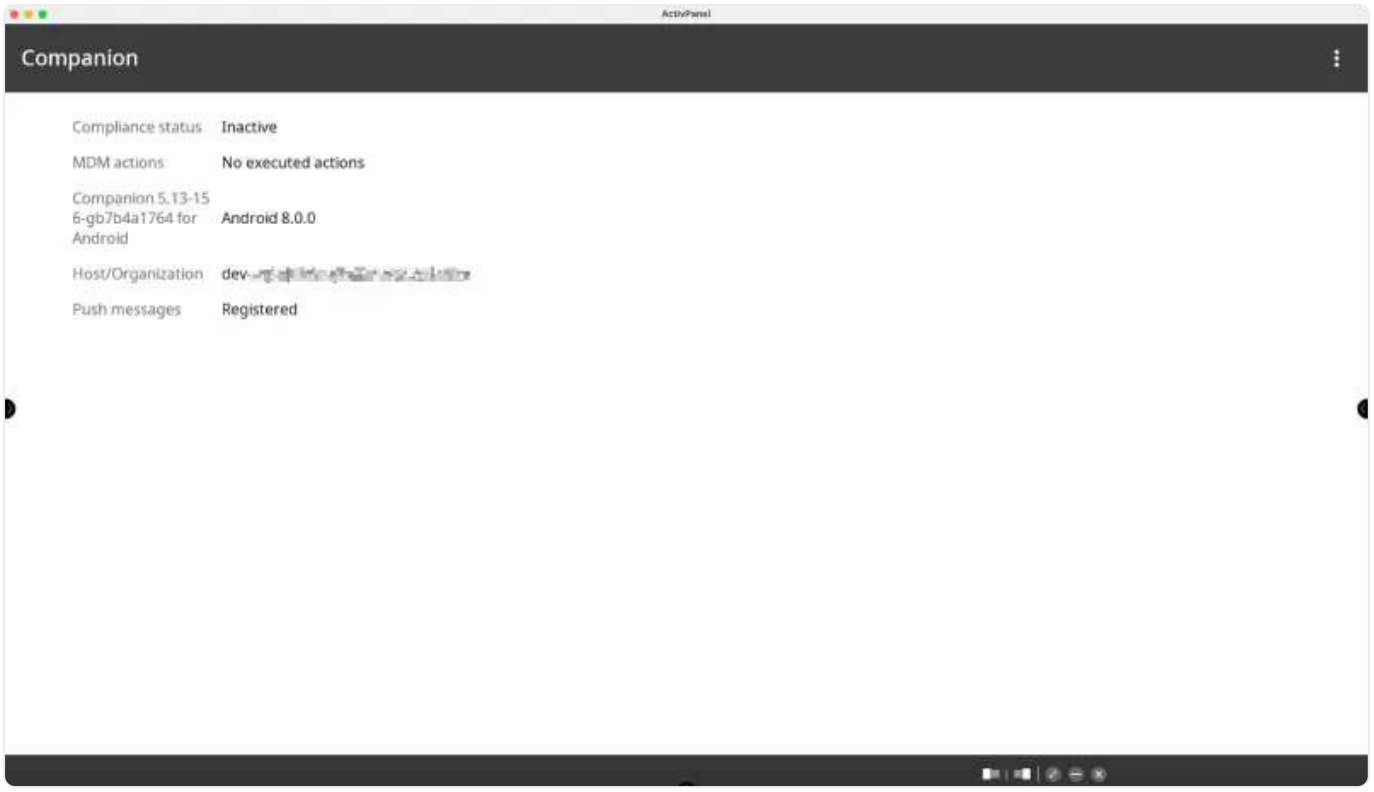
An enrollment is created for the platform Android with CTOUCH selected as the type. The enrollment link is then opened on the device, and the instructions on the webpage are followed.

The Relution Companion for CTOUCH can be downloaded and installed via the displayed download button.

After the Companion has been installed successfully, the enrollment is started from the enrollment page.

The Companion then opens automatically and prompts confirmation of several notes and authorizations. After successful enrollment, a corresponding confirmation screen will appear.

For version 26.4.0



The device should now be visible in the Relution Portal inventory.

For version 26.4.0

Supported Actions

The following actions can be performed on CTOUCH interactive whiteboards via Relution:

Action	Description
Trigger Alarm →	
Remove App →	
Send File to Device →	
Wipe Device →	
Unlock Device →	
Reboot Device →	Restart or shut down (Power off option)
Lock Device →	Prerequisite: a password or PIN is set locally on the device or via the manufacturer-specific policy (Enable LockScreen Password)
Refresh Device Info →	
Send Message →	
Deploy Relution Store App →	Deploy native apps via Relution. Enable installation from unknown sources must be enabled

For version 2

Supported Policies

The following policies are supported on CTOUCH interactive whiteboards:

Policy	Restrictions
WiFi →	
App Compliance →	
Certificate →	Only installation supported

Manufacturer-specific policy

The manufacturer-specific policy CTOUCH offers the following settings:

Setting	Description
Enable LockScreen Password	Set the password of the lock screen; when enabled, the Lockscreen password field is required (at least 6 characters)
Wake on LAN	Enable the Wake-on-LAN feature (preset in new configurations)
Enable installation from unknown sources	Allows installation of apps from unknown sources; required for Deploy Relution Store App
Power on automatically	Set weekdays and time for automatic display power-on
Power off automatically	Set weekdays and time for automatic display power-off
Enable OTA Update	Enable automatic search for OTA updates

For version 26.4.0

Dahua

Relution makes it possible to manage interactive whiteboards from the Dahua brand.

Supported product ranges and models

The following product series are supported:

- LPHXX-ST420

Enrollment

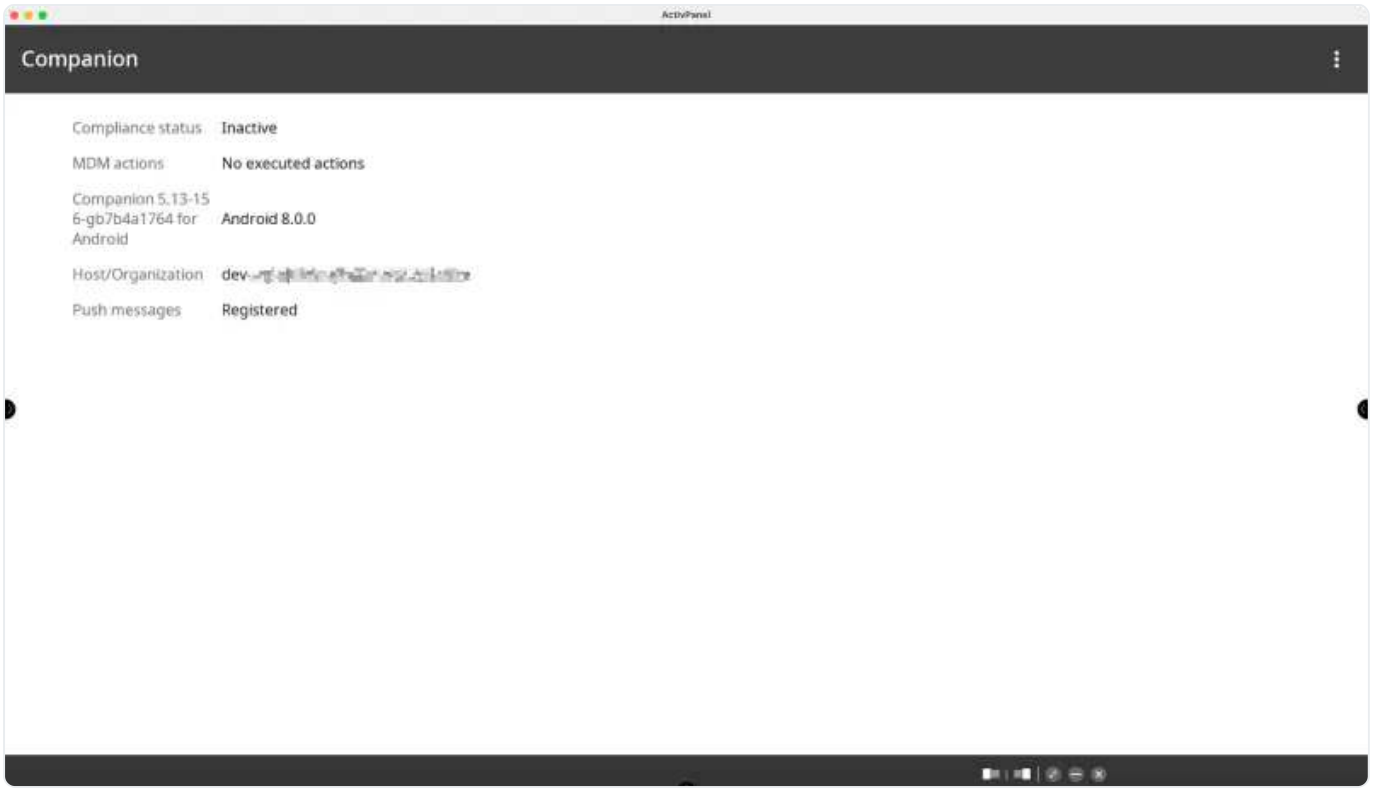
An enrollment is created for the platform Android with the type Dahua. The enrollment link is then opened on the device, and the instructions on the webpage are followed.

The displayed Download button allows the Relution Companion for Dahua to be downloaded and installed.

After the Companion has been installed successfully, the enrollment process is started from the enrollment page.

The Companion then opens automatically and prompts confirmation of several notes and authorizations. After successful enrollment, a corresponding confirmation screen will appear.

For version 26.4.0



The on-screen instructions are then followed until the enrollment is completed.

The device should now be visible in the Relution Portal inventory.

For version 26.4.0

Supported Actions

The following actions can be performed on Dahua interactive whiteboards via Relution:

Action	Description
Trigger Alarm →	
Remove App →	
Send File to Device →	
Wipe Device →	
Reboot Device →	Restart or shut down (Power off option)
Lock Device →	
Refresh Device Info →	
Send Message →	
Deploy Relution Store App →	
Update Operating System →	

For version 26.4.0

Supported Policies

The following policies are supported on Dahua interactive whiteboards:

Policy	Restrictions
EShare →	
App Compliance →	
Ethernet	

Manufacturer-specific policy

The manufacturer-specific policy Dahua offers the following settings:

Setting	Description
Brightness	Set brightness to a fixed value (0–100, default 100)
Enable automatic brightness	Adjust brightness automatically (default: off)
No signal power off time in minutes	Time in minutes without an input signal after which the whiteboard powers off (minimum 1, default 5)
Boot Source	Set the active source after the display powers on
Current Source	Set the currently active source
USB availability	Make the USB ports available (default: on)
Wake on LAN	Enable the Wake-on-LAN function (default: on)
Mute	Mute the sound (default: off)
Volume	Set volume to a fixed value (0–100, default 33)
Language	Set the device language: English, German or Spanish (default German)
Time zone	Set the device time zone (default Europe/Paris)
Power on/off schedules	Up to 5 schedules for automatic power on and off

For ve

Boot Source and Current Source offer Do Not Change (default), Android, HDMI 1–3, USB-C 1–2, VGA, OPS, DisplayPort, Component (YPbPr), AV and Last Source.

heinekingmedia

Relution makes it possible to manage interactive whiteboards from the heinekingmedia brand.

Supported product ranges and models

The following product series are supported:

- Digitale Tafel (DT-86A80-L20HM)
- Digitale Tafel Gen3 (DT-65A11-L30HM)

Enrollment

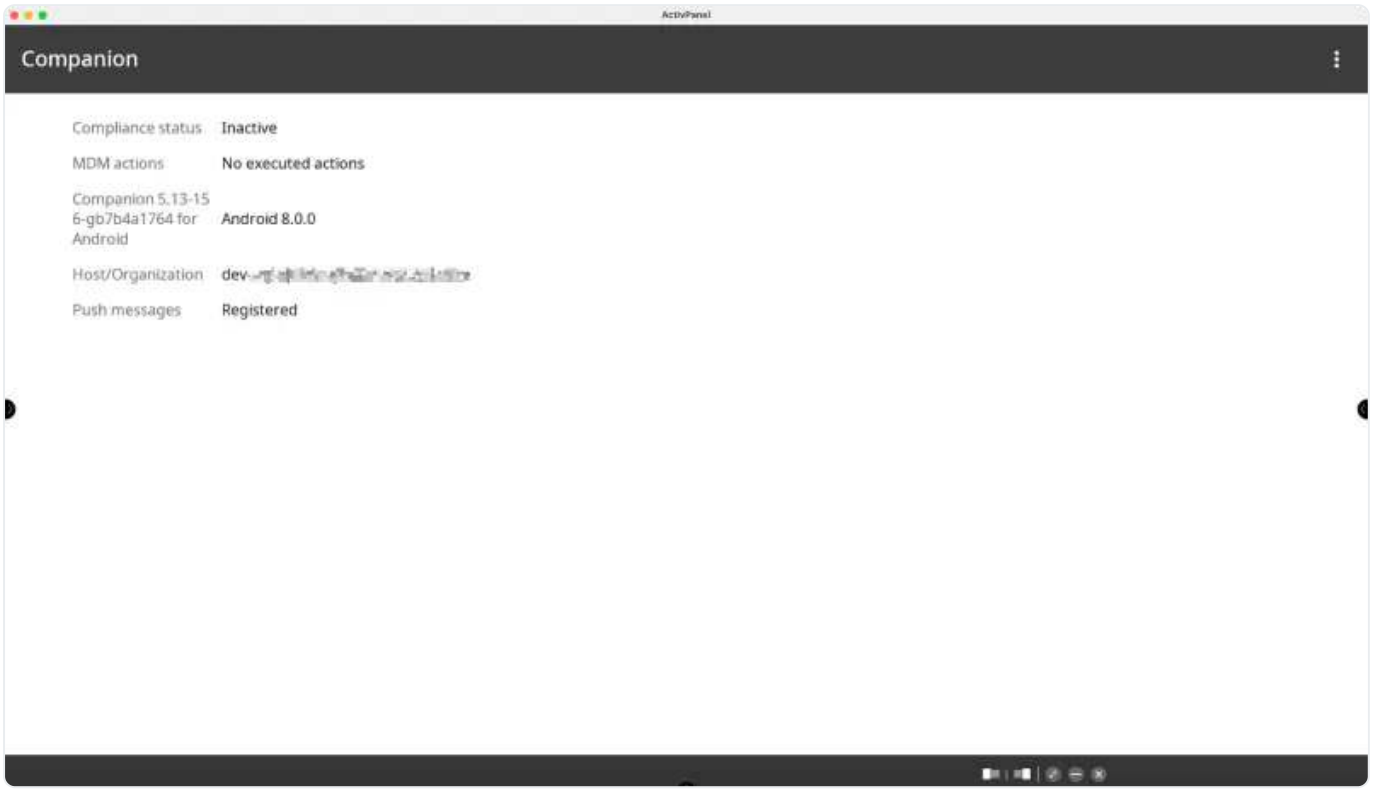
An enrollment is created for the platform Android with the type heinekingmedia. The enrollment link is then opened on the device, and the instructions on the webpage are followed.

The displayed Download button allows the Relution Companion for heinekingmedia to be downloaded and installed.

After the Companion has been installed successfully, the enrollment process is started from the enrollment page.

The Companion then opens automatically and prompts confirmation of several notes and authorizations. After successful enrollment, a corresponding confirmation screen will appear.

For version 26.4.0



The on-screen instructions are then followed until the enrollment is completed.

The device should now be visible in the Relution Portal inventory.

For version 26.4.0

Supported Actions

The following actions can be performed on heinekingmedia interactive whiteboards via Relution:

Action	Description
Trigger Alarm →	
Remove App →	
Send File to Device →	
Wipe Device →	
Reboot Device →	Restart or shut down (Power off option)
Refresh Device Info →	
Send Message →	
Deploy Relution Store App →	
Update Operating System →	

For version 26.4.0

Supported Policies

The following policies are supported on heinekingmedia interactive whiteboards:

Policy	Restrictions
Kiosk Mode →	
Hotspot →	
EShare →	
App Compliance →	

Interactive Board Configuration

The policy Interactive Board Configuration offers the following settings to manage heinekingmedia interactive whiteboards:

Setting	Description
Lock hardware buttons	
Lock remote control	
Lock settings	Lock the device settings. When enabled, the Pin to unlock settings field (digits only) must be filled in. The portal marks this field for Prowise and wende.interaktiv only, but the configuration cannot be saved without it.
Lockscreen	Only available if Lock settings is enabled. Activate the lock screen and set a numeric PIN (required field Lockscreen pin). Disabling Lock settings also disables the lock screen.
Lock touch input	
Lock USB ports	
Block App Installation	
Block App Uninstallation	
Limit maximum volume	Set a value for the maximum volume (field Maximum volume, in percent, 0–100, default 100)
Brightness	Set brightness to a fixed value (0–100, default 100). There is no separate switch; the value is always transferred.
Language	Set the device language: English, German, Spanish or Chinese (default German)
Time zone	Set the device time zone (default Europe/Paris)
Boot Source	Set the active source after booting up the display: Android, AV, DisplayPort, HDMI 1–3, OPS, USB-C, VGA or Last Source (default)
HDMI Output	Set resolution and frame rate: Auto (default), 2k 60Hz, 4k 30Hz or 4k 60Hz
Over the air update URL	Address for over-the-air updates; only HTTPS URLs are accepted
Power on automatically	After enabling the Off/On switch, set weekdays and time for the display to switch on automatically
Power off automatically	After enabling the Off/On switch, set weekdays and time for the display to switch off automatically
Lock selected apps	After enabling the Off/On switch, lock apps by their package names and set a numeric PIN to unlock these apps (required field Pin to unlock apps)

Setting	Description
System utils	Configure the utils: Mem clear, Hardware detect, App Lock, Lock screen, Home, Back, Menu, Screen off, Spotlight, WIFI, Source, White board, Mute, Volume, Brightness and More. When the Off/On switch is enabled, exactly five utils must be selected; otherwise the configuration cannot be saved.
Side Navigation Bar	Configure elements of the side navigation bar: Recent, Source, Control, Settings, Freeze, Screenshot, Time, Camera, Folder, Brightness, Dark. When the Off/On switch is enabled, exactly four elements must be selected; otherwise the configuration cannot be saved.

For version 26.4.0

i3-Technologies

Relution makes it possible to manage interactive whiteboards from the i3-Technologies brand.

Supported product ranges and models

The following product series are supported:

- i3TOUCH E-ONE

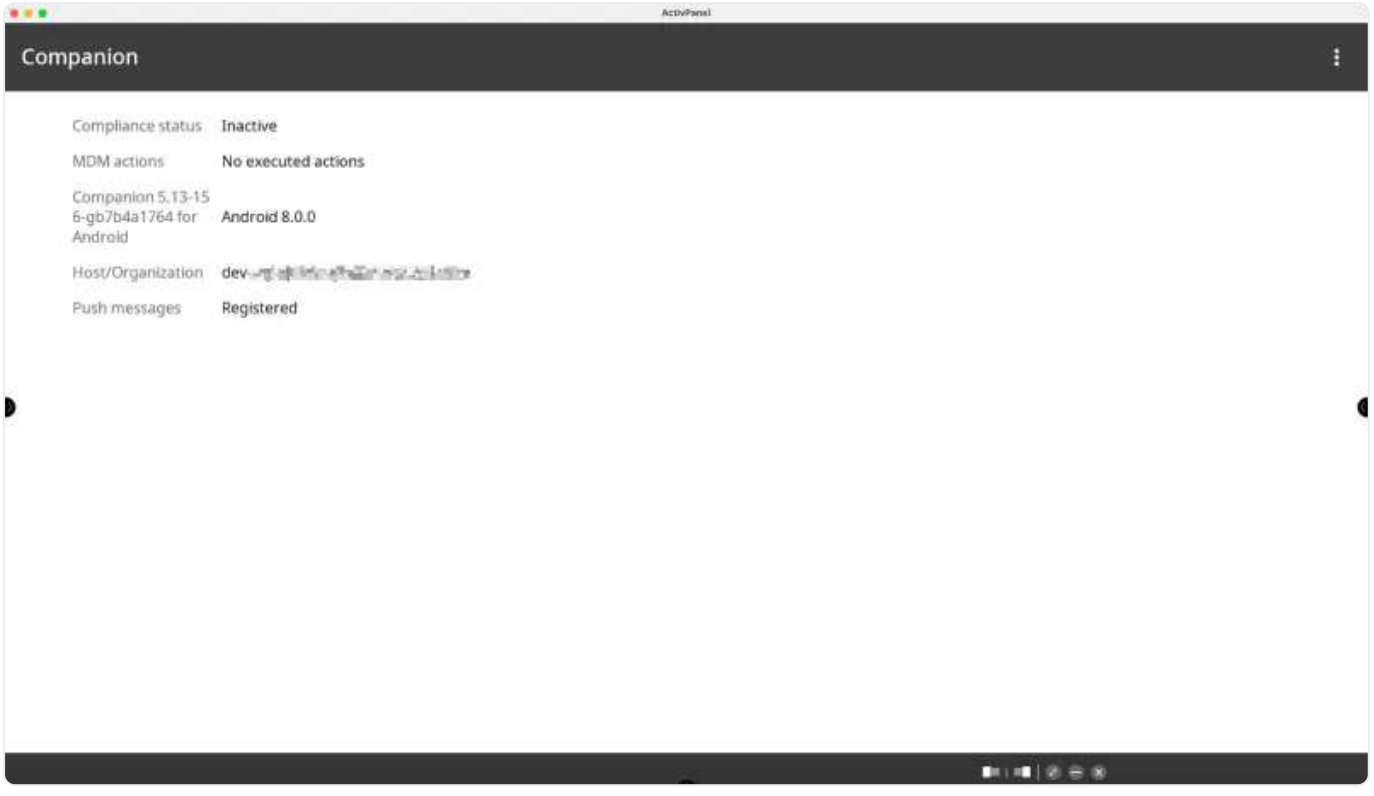
Enrollment

An enrollment is created for the platform Android with the type i3.

The Relution Companion must already be installed via the i3 Store before enrollment.

The Relution Companion is opened, and the server address and enrollment code are entered.

The Companion requests several confirmations. The displayed notifications and authorization requests must be confirmed. After successful enrollment, a corresponding confirmation screen will appear.



For version 26.4.0

The on-screen instructions are then followed until the enrollment is completed.

The device should now be visible in the Relution Portal inventory.

Enable Device Owner

The integration needs Device Owner permissions on the device. To enable Device Owner, the instructions for Android Debug Bridge setup and connection → apply.

After the device has been connected, the device owner mode is enabled by executing the following command:

```
adb shell dpm set-device-owner
com.mwaysolutions.relution.i3/com.mwaysolutions.relution.receiver.MdmDeviceAdminReceive
r
```

Supported Actions

For version 26.4.0

The following actions can be performed on i3-Technologies interactive whiteboards via Relution:

Action	Description
Trigger Alarm →	
Remove App →	
Send File to Device →	
Wipe Device →	
Unlock Device →	
Reboot Device →	Restart or shut down (Power off option)
Lock Device →	
Refresh Device Info →	
Send Message →	
Deploy Relution Store App →	
Update Operating System →	

Supported Policies

The following policies are supported on i3-Technologies interactive whiteboards:

Policy	Restrictions
Kiosk Mode →	
Scheduled OTA Update →	
Hotspot →	
App Compliance →	

Manufacturer-Specific policy

The manufacturer-specific policy i3 offers the following settings:

For version 26.4.0

Setting	Description
Enable automatic brightness	Adjust brightness automatically
Set brightness	Set brightness to a fixed value. Enabling this option unlocks the Brightness field (0–100).
Set volume	Set volume to a fixed value. Enabling this option unlocks the Volume field (0–100).
Enable lock screen PIN	Set a lock screen PIN in the Lockscreen pin field (required, 4–8 digits)
Power on/off schedules	Up to 10 schedules for automatic power on and off

Promethean

Relution makes it possible to manage interactive whiteboards from the Promethean brand.

Supported product ranges and models

The following product series are supported:

- Active Panel 7 and Active Panel 7 Premium
- Active Panel 9 and Active Panel 9 Premium

Enrollment

An enrollment is created for the platform Android with Promethean selected as the type.

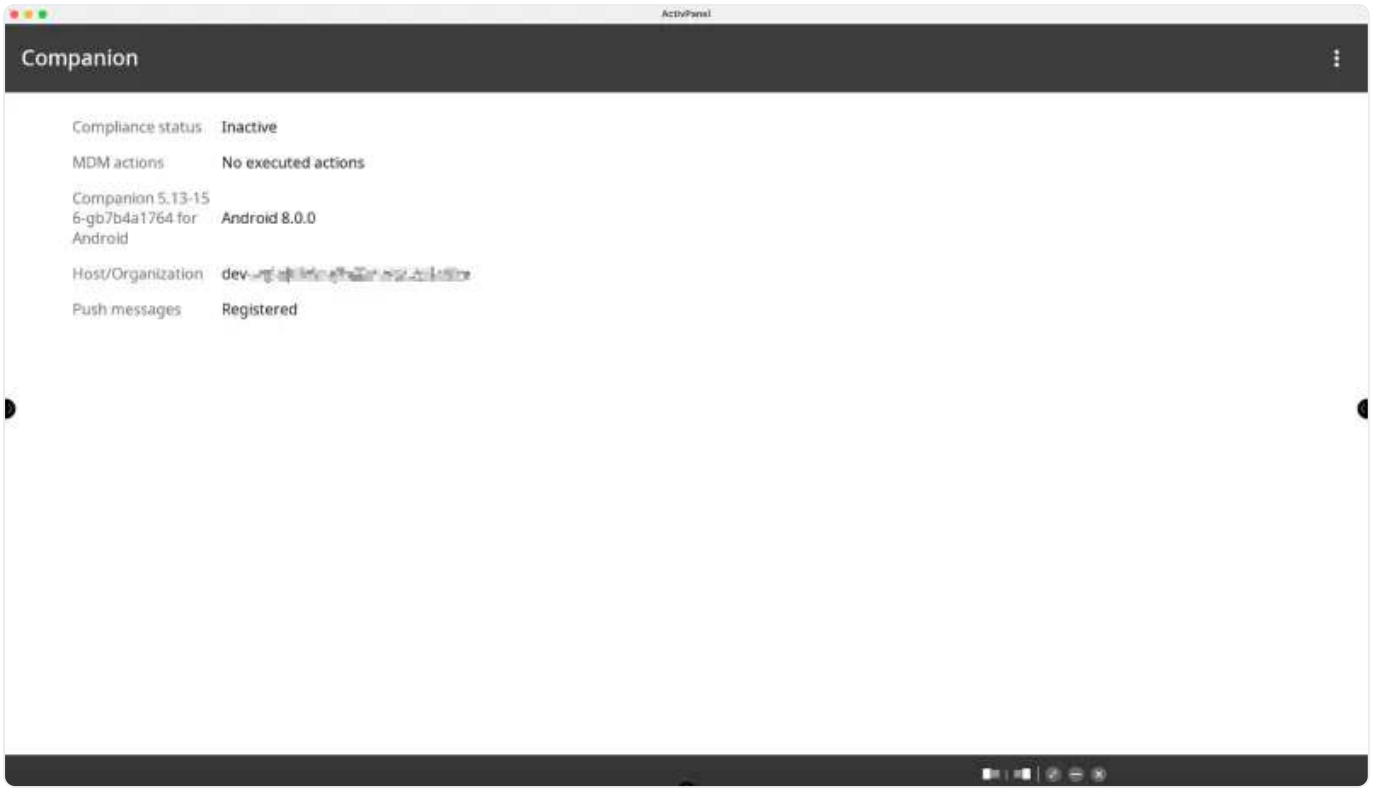
The Relution Companion must already be installed via Promethean World before enrolling.

If Promethean World or the Relution Companion is not available, contacting the personal Promethean representative is recommended.

The server address and the enrollment code are entered in the Relution Companion.

The Companion requests several confirmations; the displayed notifications and authorization requests are confirmed. After successful enrollment, a corresponding confirmation screen will appear.

For version 26.4.0



The on-screen instructions then lead through the remaining steps until the enrollment is completed.

The device should now be visible in the Relution Portal inventory.

Supported Actions

The following actions can be performed on Promethean interactive whiteboards via Relution:

For version 26.4.0

Action	Description
Trigger Alarm →	
Remove App →	
Send File to Device →	
Wipe Device →	
Reboot Device →	Restart or shut down (Power off option)
Lock Device →	Requires a PIN set on the device or via the Activ Panel Pin setting of the manufacturer-specific policy
Refresh Device Info →	
Send Message →	
Deploy Relution Store App →	
Remove Shortcut →	
Add Shortcut →	
Update Operating System →	

Supported Policies

The following policies are supported on Promethean interactive whiteboards:

Policy	Restrictions
Kiosk Mode →	
WiFi →	
Hotspot →	Only available for Active Panel 9 and Active Panel 9 Premium

Manufacturer-specific policy

The manufacturer-specific policy Promethean offers the following settings. They are listed in the same order as in the portal. Selection fields are set to Don’t change when the policy is created; in that case, the value on the whiteboard remains unchanged.

For version 26.4.0

Setting	Description
Brightness	Set brightness to a fixed value between 0 and 100
Brightness Mode	Possible values: Don’t change, Auto, Energy Saving, Eye Protection, Normal
Pencil end	Define the mode of the pencil end: Pen (default) or Eraser
Contrast	Set contrast to a fixed value between 0 and 100. Only available for Active Panel 7
Time until panel goes into standby mode	Automatic transition into standby mode after 3 minutes to 4 hours
Time until panel goes to sleep	Automatic transition into sleep mode after 3 minutes to 8 hours
Enable Proximity Sensor	Enable/disable wake on proximity. Only available for Active Panel 7 and Active Panel 9 Premium
Enable Proximity Sensor Delay Timer	Enables / Disables the delay timer for the proximity sensor
Proximity Sensor Delay Time	Possible values: Don’t change, 1 min, 5 min, 10 min
Enable Proximity Illuminate Screen	Enables / Disables Illuminate Screen when motion is detected
Enable Proximity Reset Standby And Sleep Timer	Enables / Disables Reset standby and sleep timer when motion is detected
Reduce blue light	Enable/disable the blue light filter
Source Detection	Configure automatic source detection. Possible values: Don’t change, Automatic, Manual, Off
Default Source	Set the default source, e.g. the last used source, Home, HDMI 1–3, AV, DP, OPS, USB-C or VGA
HDMI EDID Mode	Set the HDMI EDID mode to EDID 1.4 or EDID 2.0
Show Network Settings	Show or hide the network settings on the device
Wake on LAN	Enable Wake on LAN function
Enable Network Discovery using AirPlay	Enable/disable the AirPlay discovery protocol
Enable Network Discovery using Promethean	Enable/disable the proprietary Promethean discovery protocol
Enable Network Discovery using WebRTC	Enable/disable the WebRTC discovery protocol

Setting	Description
Enable Network Discovery using Wi-Fi Direct	Enable/disable the use of the Wi-Fi Direct discovery protocol
Enable miracast over infrastructure	Enable/disable the miracast over infrastructure protocol. Disable this when Enable Network Discovery using Wi-Fi Direct is off.
Enable IPv6	Enable/disable IPv6. Not available on OPS
Volume	Set volume to a fixed value between 0 and 100. Cannot be changed while Enable Mute is enabled
Enable Mute	Mute the volume
Enable Panel Speakers	Enables / Disables the panel speakers
Enable Include Panel Speakers	Include panel speakers or not. Only enable it when Line Out Mode is set to Line out and Enable Panel Speakers is enabled.
Bass	Bass level between 0 and 100
Balance	Balance level between 0 and 100
Treble	Treble level between 0 and 100
Midrange	Midrange level between 0 and 100
Line Out Mode	Possible values: Don’t change, Earphone, Line out
Enable Subwoofer	Enable/disable the use of the Subwoofer. Only enable when Enable Panel Speakers is enabled.
Panel Mode	Possible values: Don’t change, Full display, No display, Limited display
Enable Users and Profiles	Enable/disable the management of local users on the device. Only available for Active Panel 7
Enable Unified Menu	Show or hide the Unified Menu
Enable Display Menu Tab	Show or hide the Menu tab
Enable Home Source	Enable/disable the home source feature
Enable Apps	Show or hide non-system apps in the launcher
Show App Settings	Show or hide the app settings on the device
Enable Side Loading	Allow or prevent the installation of apps from other sources (side loading)
Enable Google Play	Enable/disable Google Play on the device. Only available for Active Panel 7
Enable Factory Reset	Allow or prevent a factory reset on the device
Lock down settings	Prevent access to and changes of the panel settings on the device

Setting	Description
Enable OTA Update	Allow or prevent over-the-air firmware updates
Enable Local Update	Allow or prevent local firmware updates
Restart Screen Share on update	If enabled, Screen Share restarts whenever network discovery using AirPlay, Promethean or WebRTC changes. Otherwise, Screen Share applies the changes the next time it starts
Apply Activ Panel Pin	Enables management of the PIN. Only available for Active Panel 9 and Active Panel 9 Premium. If the Activ Panel Pin field is left empty while this option is enabled, the PIN on the whiteboard is cleared
Activ Panel Pin	PIN with 4 to 16 digits (only 0–9). Can only be edited if Apply Activ Panel Pin is enabled
Show Passwords Enabled	Enable/disable showing passwords. Enabled by default
Hide System Lock	Show or hide the system lock
Identity requires user logging in to belong to the panel’s enrolled org	

For version 26.4.0

Prowise

Relution makes it possible to manage interactive whiteboards from the Prowise brand.

Supported product ranges and models

The following product series are supported:

- Touchscreen
- Touchscreen Ultra

Enrollment

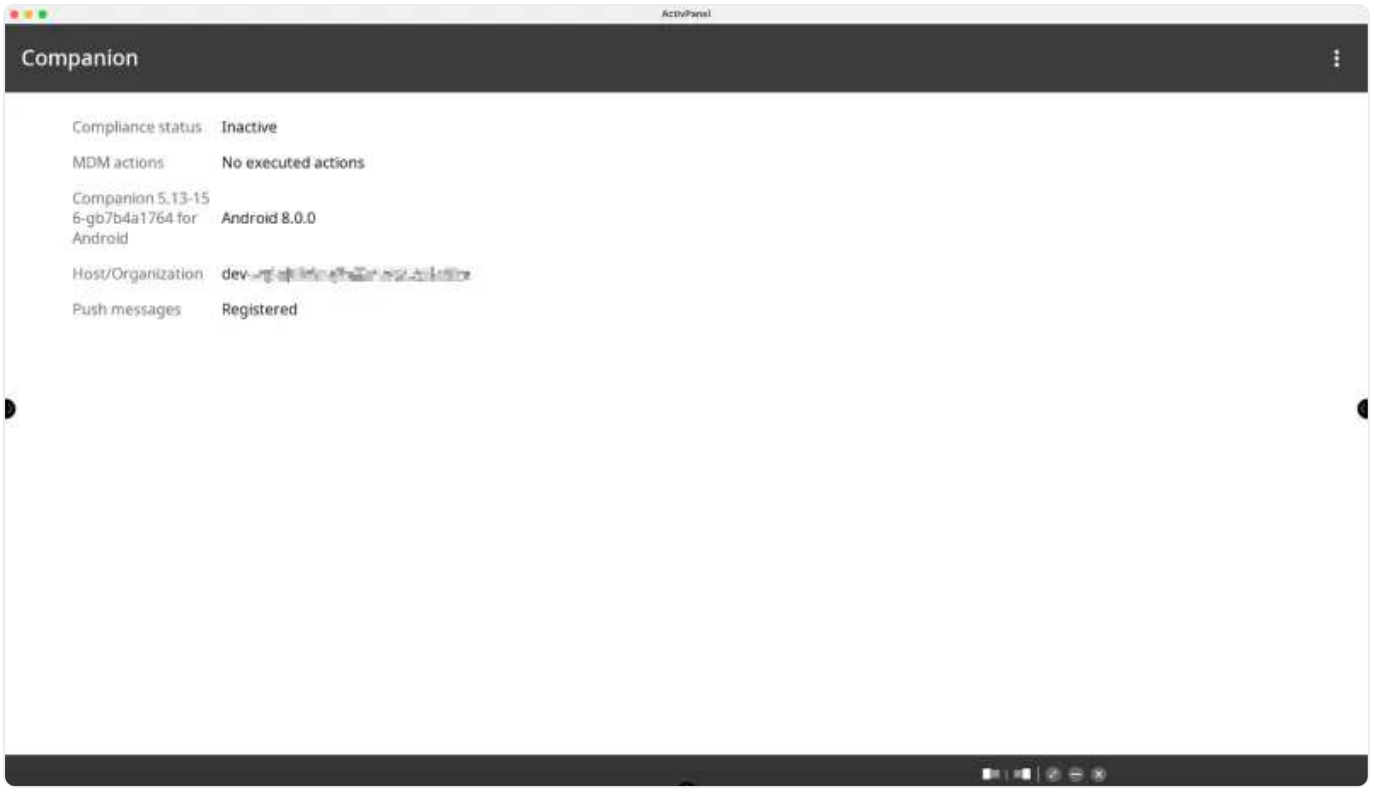
An enrollment is created for the platform Android with Prowise selected as the type.

The Relution Companion must already be installed via the Prowise Store before enrolling.

The server address and the enrollment code are entered in the Relution Companion.

The Companion requests several confirmations; the displayed notifications and authorization requests are confirmed. After successful enrollment, a corresponding confirmation screen will appear.

For version 26.4.0



The on-screen instructions then lead through the remaining steps until the enrollment is completed.

The device should now be visible in the Relution Portal inventory.

Supported Actions

The following actions can be performed on Prowise interactive whiteboards via Relution:

For version 26.4.0

Action	Description
Trigger Alarm →	
Install App from Prowise App Store →	
Remove App →	
Send File to Device →	
Reboot Device →	Restart or shut down (Power off option)
Lock Device →	Requires a password or PIN set locally on the device or, if available, via configuration
Refresh Device Info →	
Send Message →	
Install Prowise Update →	

Among others, Wipe Device, Deploy Relution Store App, Update Operating System and adding or removing shortcuts are not available on Prowise whiteboards. Apps and updates are installed via the two Prowise actions.

For version 26.4.0

Supported Policies

The following policies are supported on Prowise interactive whiteboards:

Policy	Restrictions
Kiosk Mode →	
App Compliance →	

Interactive Board Configuration

The policy Interactive Board Configuration offers the following settings to manage Prowise interactive whiteboards:

Setting	Description
Disable screen sharing services	Disable Reflect, AirPlay, Chromecast and Miracast. The toggle selects all four services; individual services can then be deselected via checkboxes
Lock settings	Locks the settings on the whiteboard. If enabled, Pin to unlock settings is a required field that only accepts digits
Lockscreen	Only available if Lock settings is enabled
Lock USB ports	
Brightness	Set brightness to a fixed value between 0 and 100 (default: 100). The value is sent with every configuration
Lock selected apps	The Off/On toggle locks a list of apps
Disabled input channels	List of video inputs that are disabled on the whiteboard

For version 26.4.0

SMART

Relution makes it possible to manage interactive whiteboards from the SMART brand.

Supported product ranges and models

The following product series are supported:

- MX (IDX55-4)

Enrollment

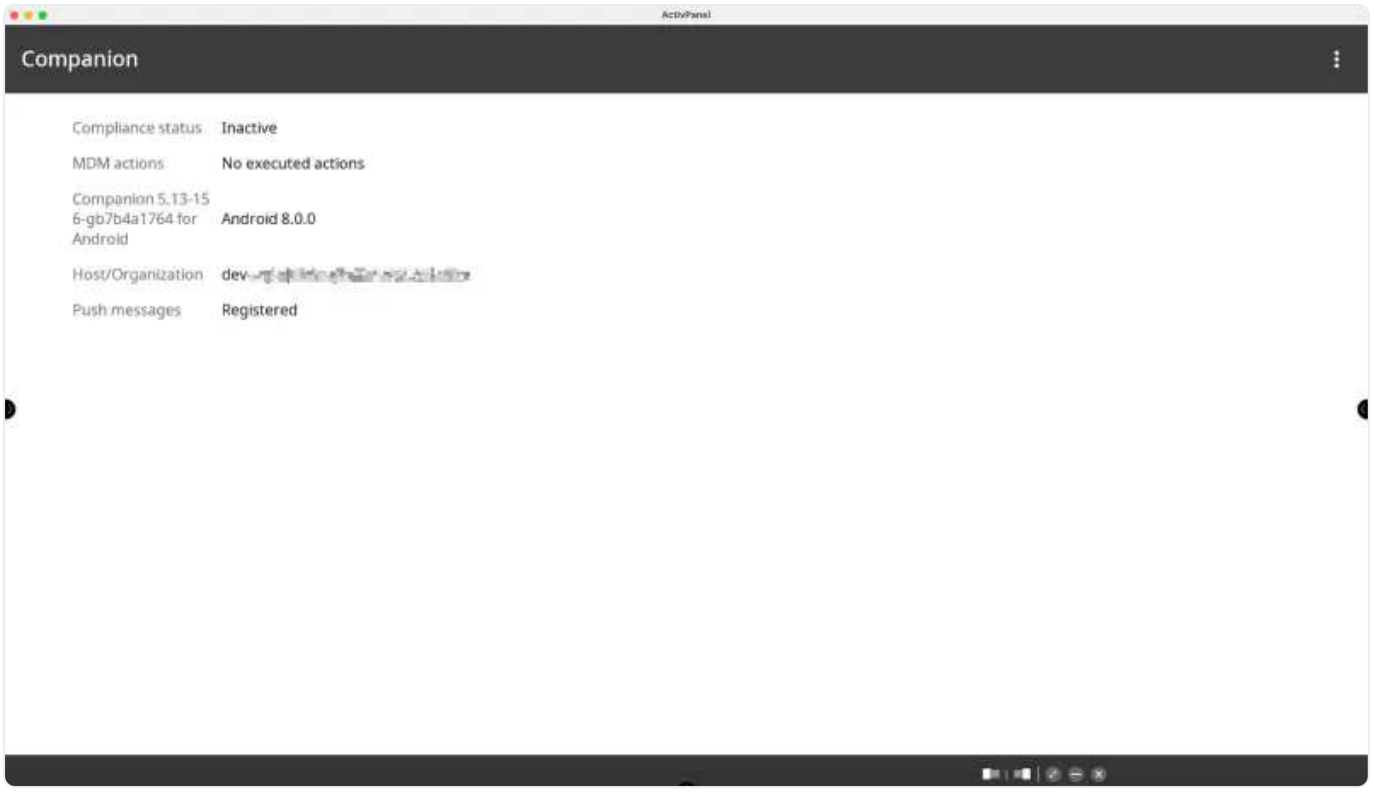
An enrollment is created for the platform Android with SMART selected as the type. The enrollment link is then opened on the device, and the instructions on the webpage lead through the process.

The Relution Companion for SMART can be downloaded and installed via the displayed Download button.

After the Companion has been installed successfully, the enrollment is started from the enrollment page.

The Companion then opens automatically and prompts confirmation of several notes and authorizations. After successful enrollment, a corresponding confirmation screen will appear.

For version 26.4.0



The on-screen instructions then lead through the remaining steps until the enrollment is completed.

The device should now be visible in the Relution Portal inventory.

For version 26.4.0

Supported Actions

The following actions can be performed on SMART interactive whiteboards via Relution:

Action	Description
Trigger Alarm →	
Remove App →	
Send File to Device →	
Reboot Device →	Restart or shut down (Power off option)
Refresh Device Info →	
Send Message →	
Deploy Relution Store App →	

Supported Policies

The following policies are supported on SMART interactive whiteboards:

Policy	Restrictions
App Compliance →	

Manufacturer-Specific policy

The manufacturer-specific policy SMART offers the following settings:

26.4.0

Setting	Description
Boot Source	Set the active source after the display powers on: Android, AV, DP, HDMI 1–3, USB-C 1–2, PC or VGA. Default: Do Not Change
Enable automatic brightness	Enable/disable automatic brightness
Brightness	Set brightness to a fixed value between 0 and 100 (default: 100). The value is sent with every configuration
Time until panel goes into standby mode	Automatic switch to standby after 1, 5 or 30 minutes or 1, 1.5, 2, 5 or 10 hours; alternatively Never
Mute	Mute the volume
Volume	Set volume to a fixed value between 0 and 100 (default: 33). The value is sent with every configuration
Language	System language: English, German (default) or Spanish
Enable App store	Enable/disable the app store. Enabled by default
Enable automatic date & time	Enable/disable automatic date and time
Enable Bluetooth	Enable/disable Bluetooth

ViewSonic

Relution makes it possible to manage interactive whiteboards from the ViewSonic brand.

Supported product ranges and models

The following product series are supported:

- CDExx30
- IFP6550-5
- IFP6552-1ANEP

Enrollment

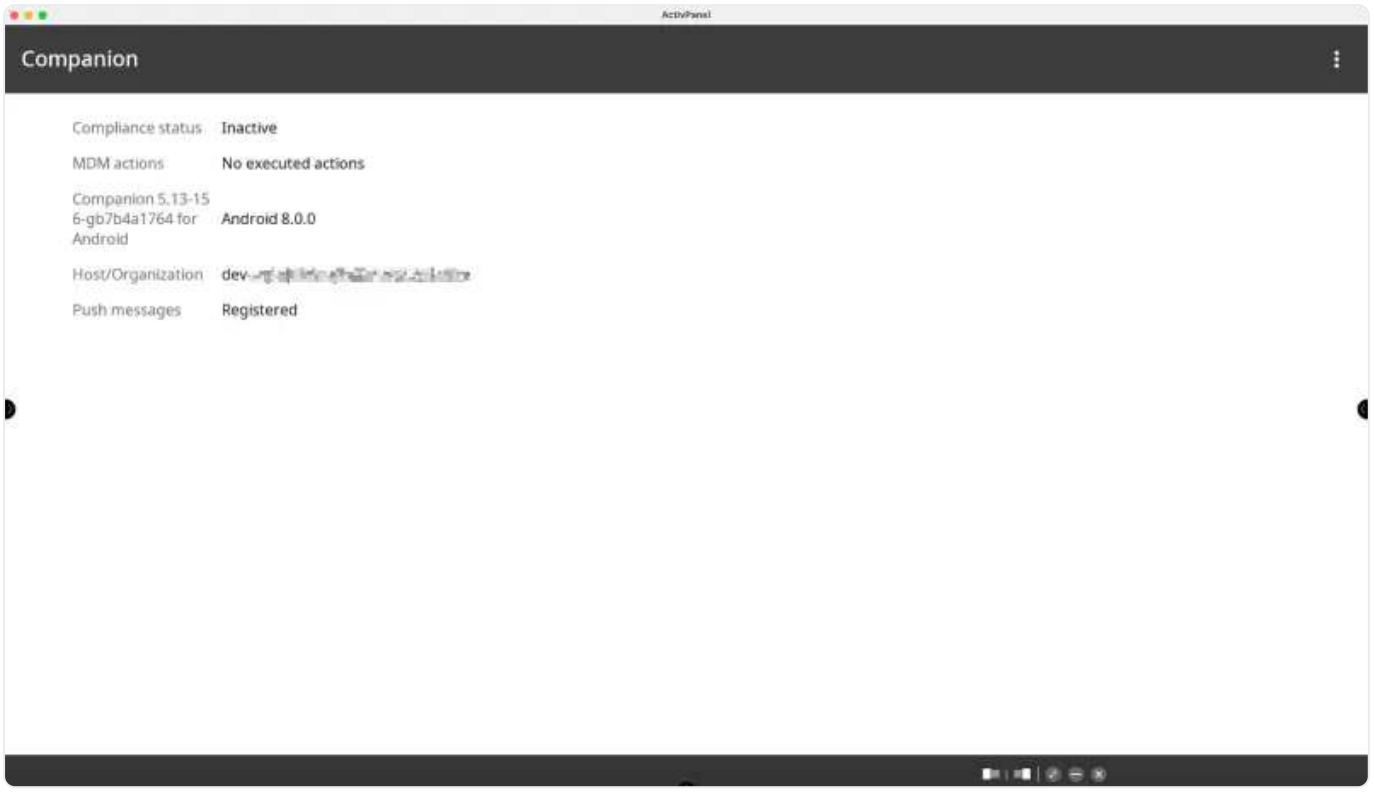
An enrollment is created for the platform Android with the type ViewSonic. The enrollment link is then opened on the device, and the instructions on the webpage are followed.

The Relution Companion for ViewSonic can be downloaded and installed via the displayed Download button.

After the Companion has been installed successfully, the enrollment is started from the enrollment page.

The Companion then opens automatically and prompts confirmation of several notes and authorizations. After successful enrollment, a corresponding confirmation screen will appear.

For version 26.4.0



The on-screen instructions are then followed until the enrollment is completed.

The device should now be visible in the Relution Portal inventory.

For version 26.4.0

Supported Actions

The following actions can be performed on ViewSonic interactive whiteboards via Relution:

Action	Description
Trigger Alarm →	
Remove App →	
Send File to Device →	
Wipe Device →	
Reboot Device →	Restart or shut down (Power off option)
Refresh Device Info →	
Send Message →	
Deploy Relution Store App →	
Update Operating System →	

For version 26.4.0

Supported Policies

The following policies are supported on ViewSonic interactive whiteboards:

Policy	Restrictions
App Compliance →	

Manufacturer-specific policy

The manufacturer-specific policy ViewSonic offers the following settings:

Setting	Description
Current source	Set the currently active source: Do Not Change (default), Android, HDMI 1–3, USB-C 1–2 or VGA
Enable brightness	Set brightness to a fixed value (0–100) (CDExx30 only)
Automatic backlight	Control the backlight automatically (IFP6550, IFP6552 only)
Enable backlight	Set the backlight to a fixed value (0–100) (IFP6550, IFP6552 only)
Enable Eye Care	
Mute	
Volume	Set volume to a fixed value (0–100), default 33
Enable lock screen PIN	Set a lock screen PIN of exactly 4 digits (required when the option is enabled)
Lock the menu	
Lock hardware buttons	
Lock touch input	
Lock settings	Set a password to unlock the settings (field Password to unlock settings, required when the option is enabled)
Enable automatic date and time	
Time zone	
Language	
Power on automatically	Set weekdays and time for automatic display power-on
Power off automatically	Set weekdays and time for automatic display power-off
Eco Mode	Enables or disables the display’s energy-saving mode (Enabled, Disabled). When Eco Mode is disabled, the display defaults to power-save level 1.
Energy Star	Enables or disables the display’s Energy Star mode (Enabled, Disabled)
Standby mode	Defines the display’s standby behavior: Hibernate or Sleep
No signal standby	Time after which the display switches to standby without an input signal: Off, 5, 15 or 30 minutes

Settings that only apply to certain models are marked with a model badge in the portal.

For Eco Mode, Energy Star, Standby mode and No signal standby, Do Not Change is selected by default. The respective setting on the display then remains unchanged.

For version 26.4.0

VS

Relution makes it possible to manage interactive whiteboards from the VS brand.

Supported product ranges and models

The following product series are supported:

- VS-S-E1
- VS-S-E3

Enrollment

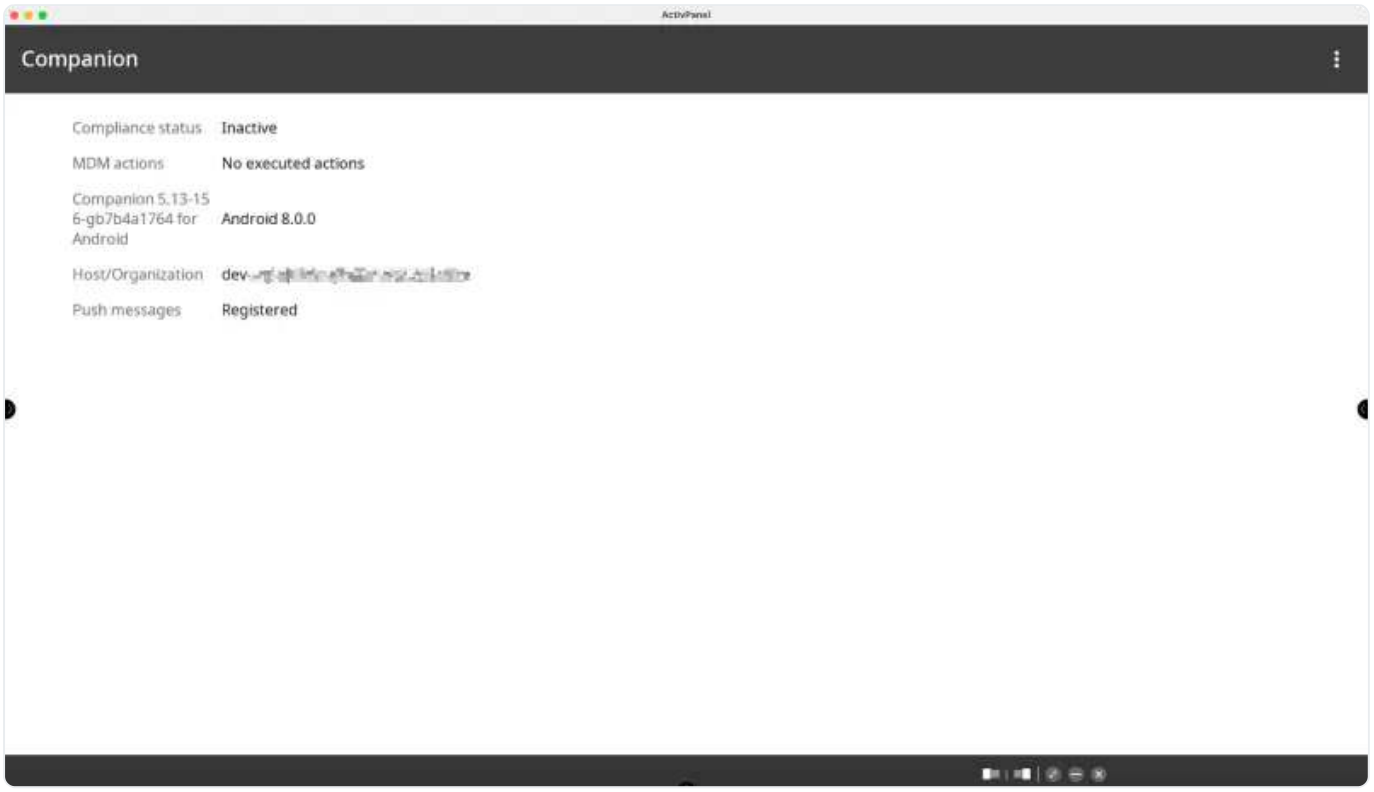
An enrollment is created for the platform Android with the type VS. An individual enrollment link is generated for each enrollment. The link is then opened on the device, and the instructions on the webpage are followed.

The Relution Companion for VS can be downloaded and installed via the displayed Download button.

After the Companion has been installed successfully, the enrollment is started from the enrollment page.

The Companion then opens automatically and prompts confirmation of several notes and authorizations. After successful enrollment, a corresponding confirmation screen will appear.

For version 26.4.0



The on-screen instructions are then followed until the enrollment is completed.

The device should now be visible in the Relution Portal inventory.

For version 26.4.0

Supported Actions

The following actions can be performed on VS interactive whiteboards via Relution:

Action	Description
Trigger Alarm →	
Remove App →	
Send File to Device →	
Wipe Device →	
Reboot Device →	Restart or shut down (Power off option)
Lock Device →	
Refresh Device Info →	
Send Message →	
Deploy Relution Store App →	
Update Operating System →	

For version 26.4.0

Supported Policies

The following policies are supported on VS interactive whiteboards:

Policy	Restrictions
App Compliance →	

Manufacturer-specific policy

The manufacturer-specific policy VS offers the following settings:

Setting	Description
Brightness	Set brightness to a fixed value (0–100), default 100
Enable Eye Care	
Lock touch input	
Boot source	Set the active source after the display powers on: Do Not Change (default), Android, HDMI 1–3, USB-C 1–2 or VGA
Current source	Set the currently active source, same options as Boot source
No signal power off	Powers off the display when no signal is received for the set time
No signal power off time	Time without signal until power-off (1 minute to 1 hour, default 5 minutes); only when No signal power off is enabled
Wake on source plugged in	Enabled by default
Allow source alias	Once enabled, aliases can be assigned for Android, HDMI1–HDMI4, PC and VGA1
Enable Ethernet	Enabled by default
Wake on LAN	
Mute	
Volume	Set volume to a fixed value (0–100), default 33
Enable lock screen PIN	Set a lock screen PIN with exactly 4 characters (required when the option is enabled); a restart of the device might be required for the change to take effect
Language	Set the device language, default German
Enable automatic OTA update	
Enable installation from unknown sources	Allows installation from unknown sources, including USB drives; enabled by default
Power on automatically	Set weekdays and time for automatic display power-on
Power off automatically	Set weekdays and time for automatic display power-off
Time until panel goes into standby mode	Don’t change, Never (default), 15 minutes, 30 minutes, 1 hour, 1.5 hours or 2 hours

wende.interaktiv

Relution enables the management of interactive whiteboards from the wende.interaktiv brand.

Supported product ranges and models

The galneoscreen product series is supported by Relution:

- galneoscreen V2
- galneoscreen V3
- galneoscreen V4
- galneoscreen V5

These models are supported only in combination with the following Android versions:

- Android 8
- Android 9
- Android 11
- Android 14 (limited range of functions)

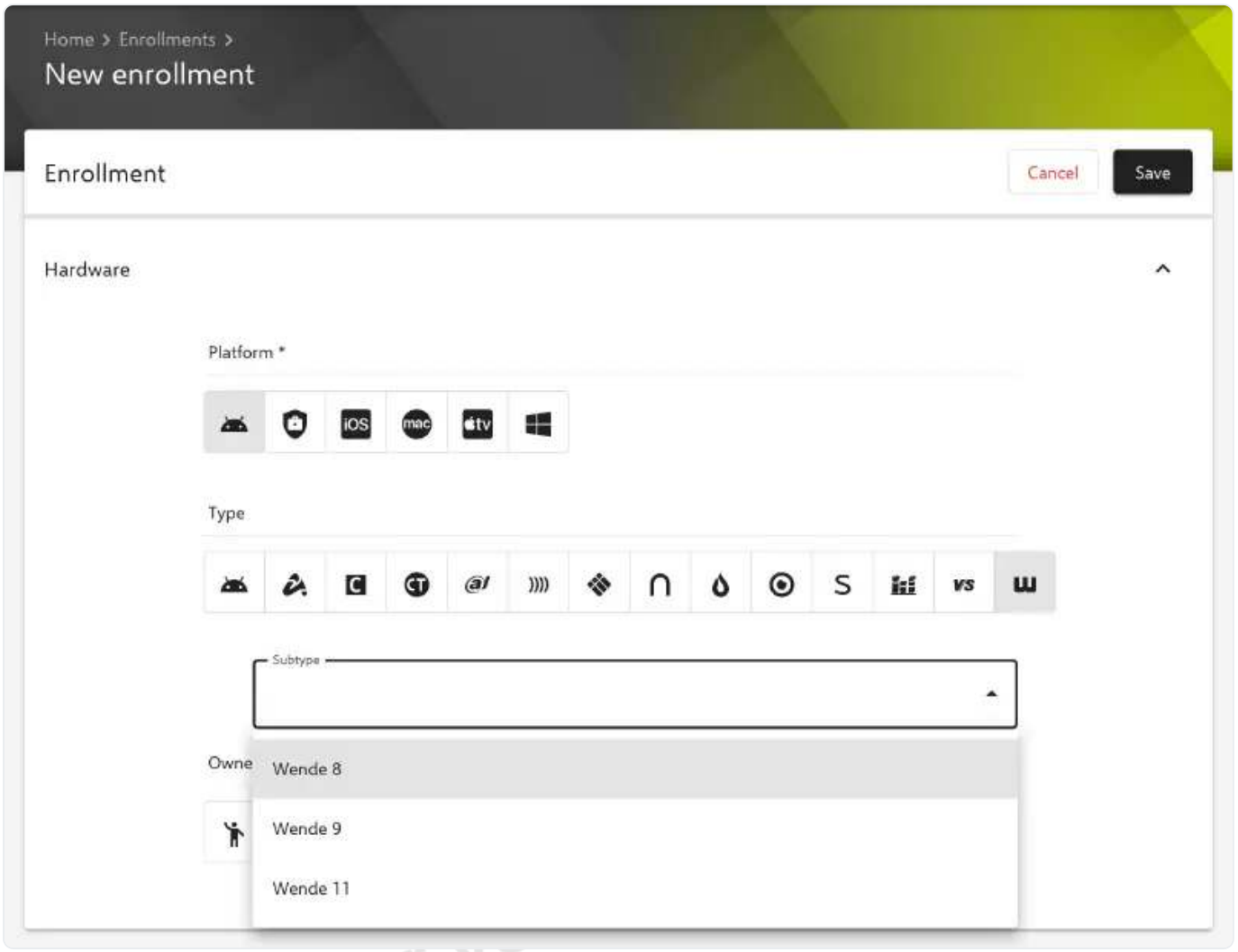
For version 26.4.0

Create enrollment

To enroll a device, an enrollment is created for the Android platform with the enrollment type Wende. Depending on the Android version of the model to be enrolled, the appropriate subtype is then selected: Wende 8, Wende 9, or Wende 11.

The following table provides an overview of which subtype is to be used for which Android version:

Android version	Enrollment subtype	Provision of the Relution Companion
Android 8	Wende 8	Relution
Android 9	Wende 9	Relution
Android 11	Wende 11	Relution
Android 14	Wende 11	wende.interaktiv



Enroll interactive whiteboard

An individual enrollment link is generated for each enrollment. The link is opened on the device, and the on-screen instructions are followed from there.

Devices with Android version 8, 9 or 11: For devices with Android version 8, 9 or 11, Relution automatically provides the appropriate Companion version based on the previously selected enrollment subtype.

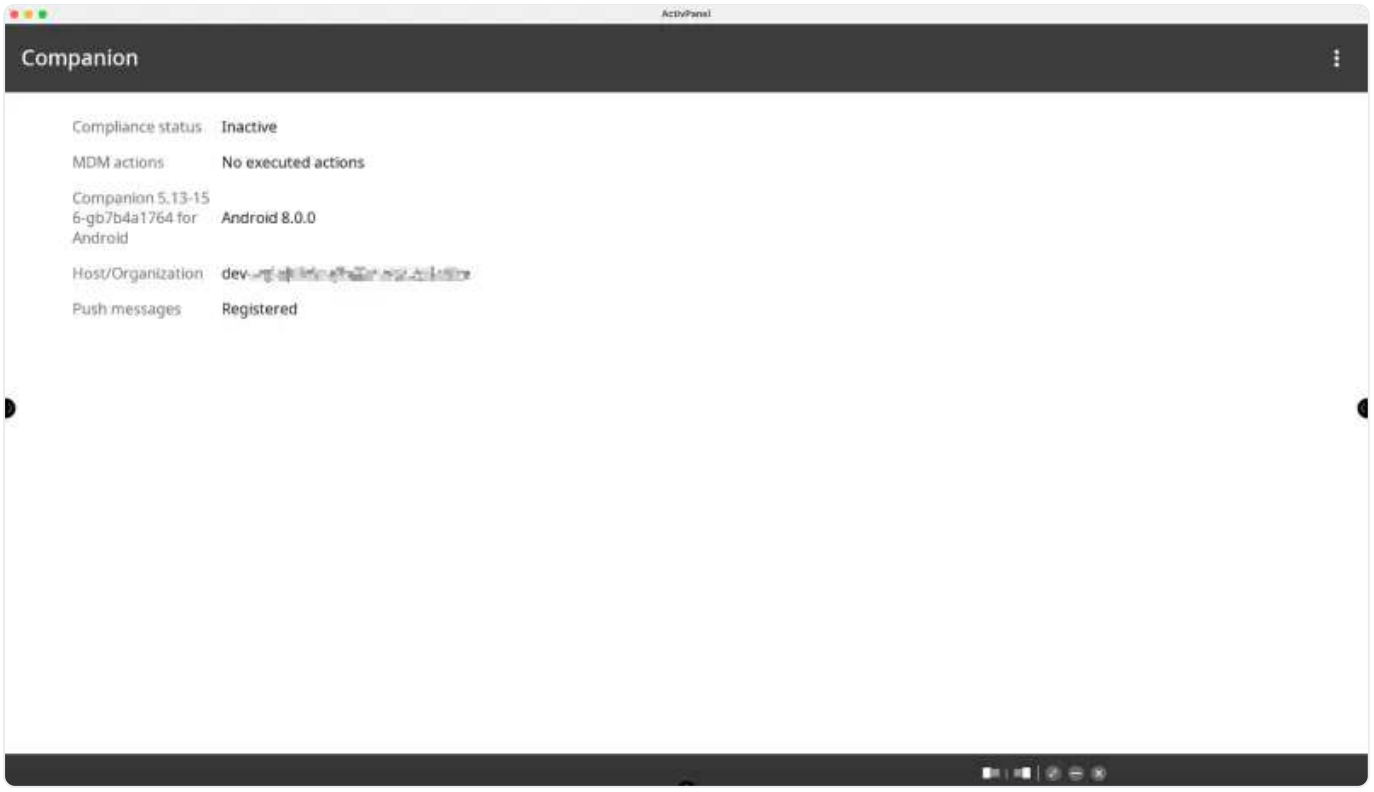
The Download button downloads the Relution Companion for the corresponding whiteboard model and installs it directly on the device.

Devices with Android version 14: Enrolling devices with Android 14 requires the installation of a special version of the Relution Companion for Wende 11.

> This version must be actively requested from wende.interaktiv before enrollment.

After the Companion has been installed successfully, the enrollment process is started from the enrollment page.

The Relution Companion will then start automatically and prompt confirmation of several instructions and authorizations. Once the enrollment is complete, a confirmation screen will appear - similar to the one shown below:



The remaining on-screen instructions are then followed until the enrollment process is completed.

The device should now appear in the Relution Portal inventory.

For version 26.4.0

Update of the Relution Companion

Depending on the enrollment type and Android version, the Relution Companion is either updated automatically via Relution or must be updated manually. Manual updates can be requested from wende.interaktiv.

The following overview shows which method applies:

Enrollment subtype	Android version	Update type
Wende 8	Android 8	automatically
Wende 9	Android 9	automatically
Wende 11	Android 11	automatically
Wende 11	Android 14	manually (provided by wende.interaktiv)

The Companion version that Relution currently provides for Wende 8, Wende 9 and Wende 11 is shown under `Settings` → `Relution Client Apps` → `Wende companion`.

Supported Actions

The following actions can be performed on wende.interaktiv interactive whiteboards via Relution:

Action	Description
Trigger Alarm →	
Remove App →	
Send File to Device →	
Wipe Device →	
Reboot Device →	Restart or shut down (Power off option)
Locate device	
Lock Device →	
Refresh Device Info →	
Send Message →	
Deploy Relution Store App →	
Add Shortcut →	Available on Wende 8 and Wende 9
Update Operating System →	

Supported Policies

The following policies are supported on wende.interaktiv interactive whiteboards:

Policy	Restrictions
Kiosk Mode →	Available on Wende 11
EShare →	
App Compliance →	

Interactive Board Configuration

The Interactive Board Configuration policy provides the following settings for managing wende.interaktiv interactive whiteboards:

Setting	Description
Lock hardware buttons	
Lock remote control	
Lock settings	Set a PIN (digits only) to unlock the settings (field Pin to unlock settings, required when the option is enabled)
Lock touch input	
Brightness	Set brightness to a fixed value
Power on automatically	Set weekdays and time for the display to switch on automatically
Power off automatically	Set weekdays and time for the display to switch off automatically
Lock selected apps	

Update Operating System

The Install Update action (dialog title Update Operating System) installs a specific software update on a selected device.

The action is available for Android Classic whiteboards from all manufacturers except CTOUCH, Newline, Prowise and SMART. For Prowise whiteboards, the Install Prowise Update → action is available instead.

In the dialog, only the version is selected from the Following updates are available for this device: list. Only updates that have been reported as available by the device itself can be selected. If the device does not report any updates, the list remains empty and the action cannot be executed.

If configurations that delay operating system updates are active, the device installs the latest version available to it, which may be older than the selected version. If a passcode is enabled, it must be entered before the update can begin.



Unlock Device

The Unlock device action remotely unlocks the device without entering a PIN. It is typically used to lift a lock set by the Lock Device → action.

The action is only available for whiteboards from CTOUCH, i3-Technologies and Newline. All other devices are unlocked on the device itself with the password.

Install Prowise Update

The Install Prowise update action (dialog title Update Prowise Operating System) installs the latest update on a selected Prowise interactive whiteboard →. The action is only available for Prowise whiteboards and replaces the Install Update action there.

Optionally, a date and time for the update can be selected in the Update on field. If the field is left blank, the update is triggered immediately.

If the action is sent again while an earlier action of this type has not yet been delivered to the device, the earlier action is cancelled. The action can also be configured as a device group action.



For version

Install App from Prowise App Store

The Install app from Prowise app store action installs an app from the Prowise App Store on a Prowise whiteboard →. The action is only available for Prowise whiteboards and replaces the Deploy Relution store app action there.

The app is identified by its package name. The source is chosen in the first step, and exactly one app in the second step:

- Relution App Store app: selection of a native Android app from the Relution App Store.
- Google Play Store app: search in the public Google Play Store.
- Internal name of an app: manual entry of the package name in the Internal name field.

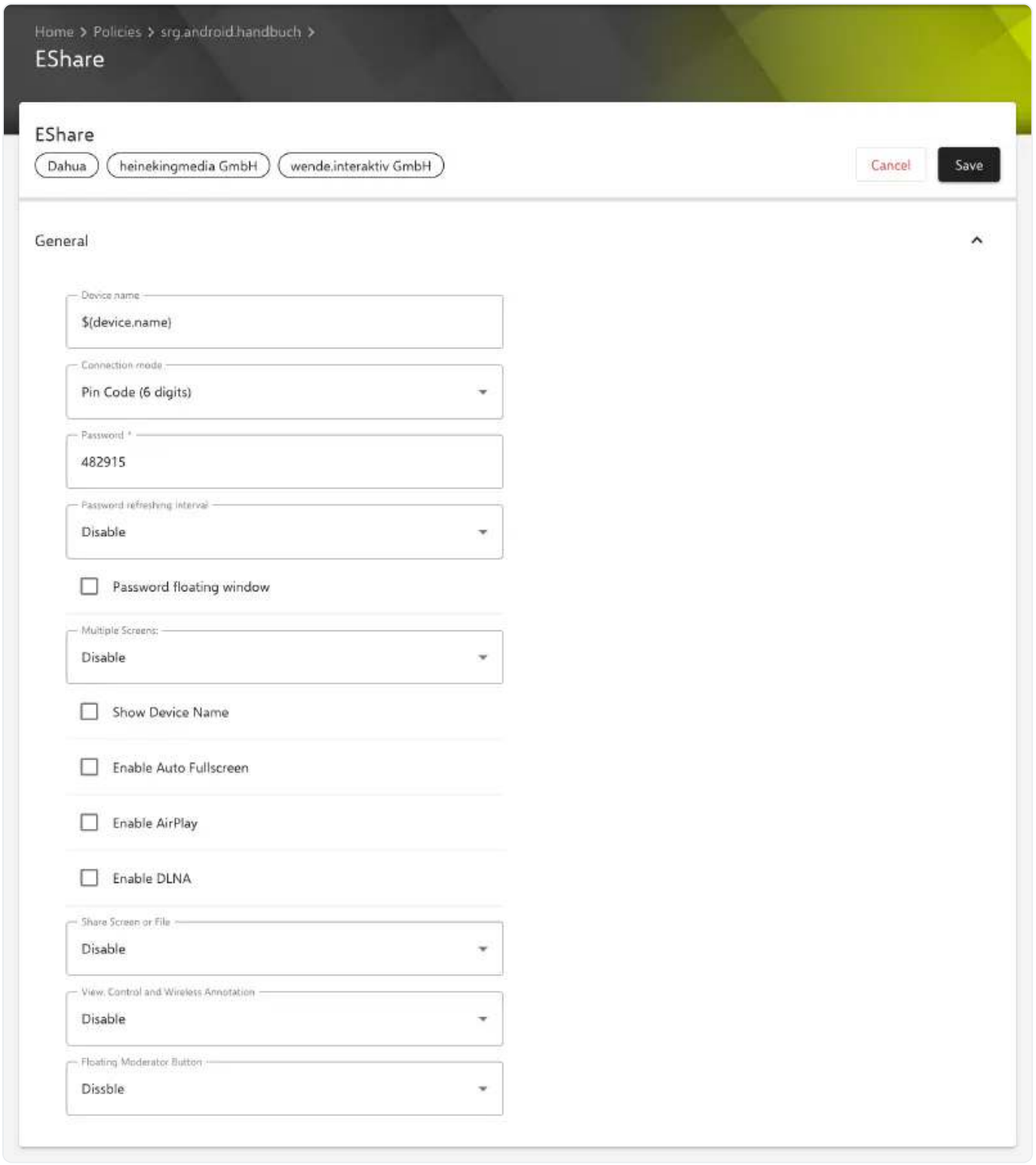
Relution only passes the package name to the Relution Companion on the whiteboard. The whiteboard then installs the matching app from the Prowise App Store, provided it is available there. If the app does not exist in the Prowise App Store, it is not installed.

EShare

EShare is a cross-platform software for wireless screen sharing and collaboration between different devices. Among other things, it enables screen mirroring, file transfer and remote control.

The EShare policy allows the settings for EShare on interactive whiteboards to be configured and managed. In the portal, it is marked for whiteboards from Dahua →, heinekingmedia → and wende.interaktiv →.

For version 26.4.0



Configuration

The following options are available for configuring EShare:

- Device name: Set the name of the device. The placeholder `${device.name}` is preset, so the device name from Relution is used unless it is changed.
- Connection mode: Choose Device Name, Pin Code (6 digits) or Letters (8 characters). With Pin Code (6 digits) and Letters (8 characters), the following options are also available:
  - Password: Required; without a password, the configuration cannot be saved.
  - Password refreshing interval: Disable, 10 Minutes, 30 Minutes, 1 Hour or 1 Day.
  - Password floating window
- Multiple screens: Disable or select 2, 4, 6 or 9 screens.
- Show device name: Enable/disable the display of the device name.
- Enable auto fullscreen
- Enable AirPlay
- Enable DLNA
- Share screen or file: Disable sharing screen or file, allow all or allow only with approval.
- View, control and wireless annotation: Disable all options, allow all options, allow only viewing or allow only with approval.
- Floating moderator button: Choose display option: Disable, always display, only on the home screen or auto.

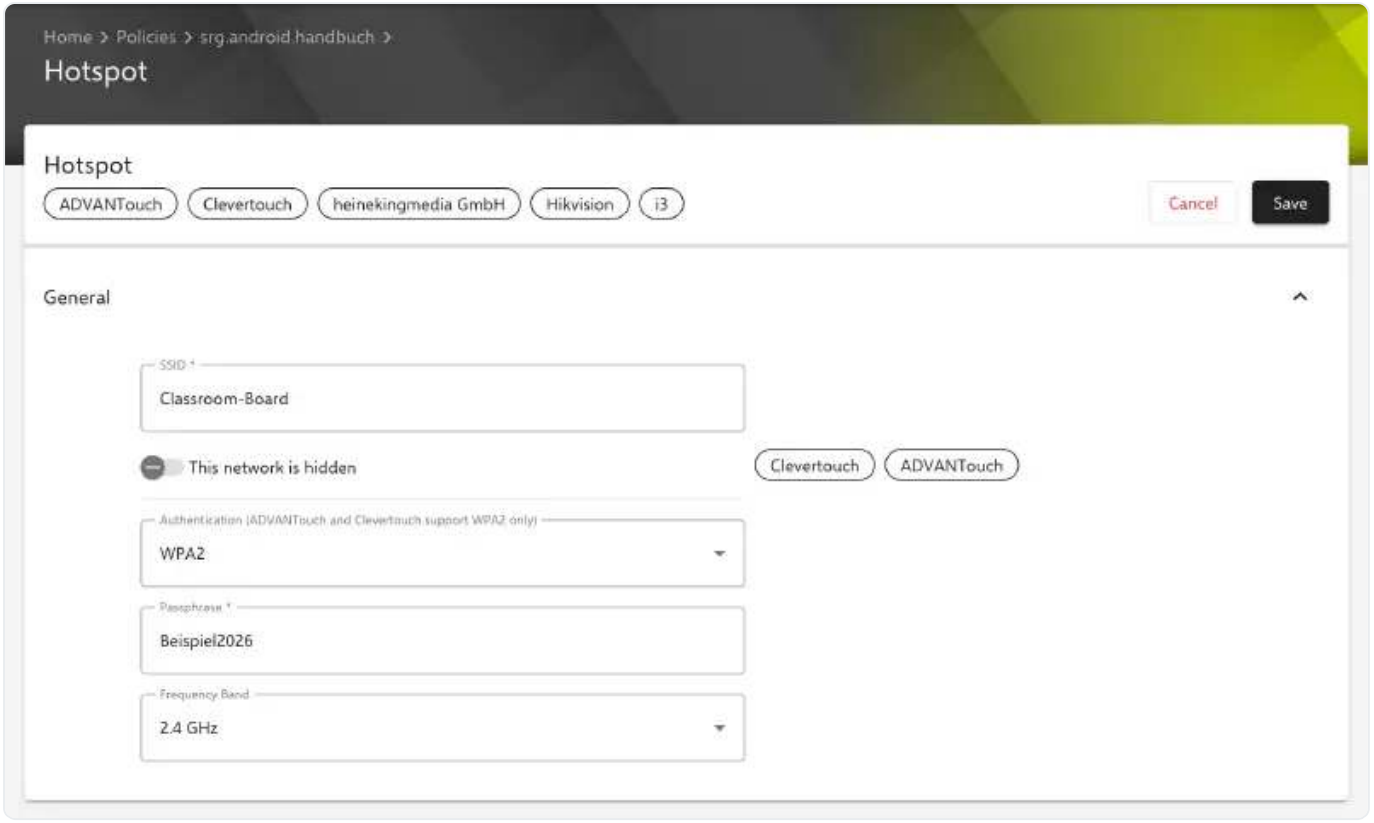
In a new configuration, the connection mode Device Name is preset, all checkboxes are cleared, and Multiple Screens, Share Screen or File, View, Control and Wireless Annotation and Floating Moderator Button are set to Disable.

If the configuration cannot be applied on the device, the compliance violation EShare configuration is shown for the device.

For version 26.4.0

Hotspot

The Hotspot policy allows the configuration and management of Wi-Fi hotspot settings on devices remotely. In the portal, it is marked for whiteboards from ADVANTouch →, Clevertouch →, heinekingmedia →, i3-Technologies → and Hikvision.



Configuration

The following options are available for configuring the Wi-Fi hotspot:

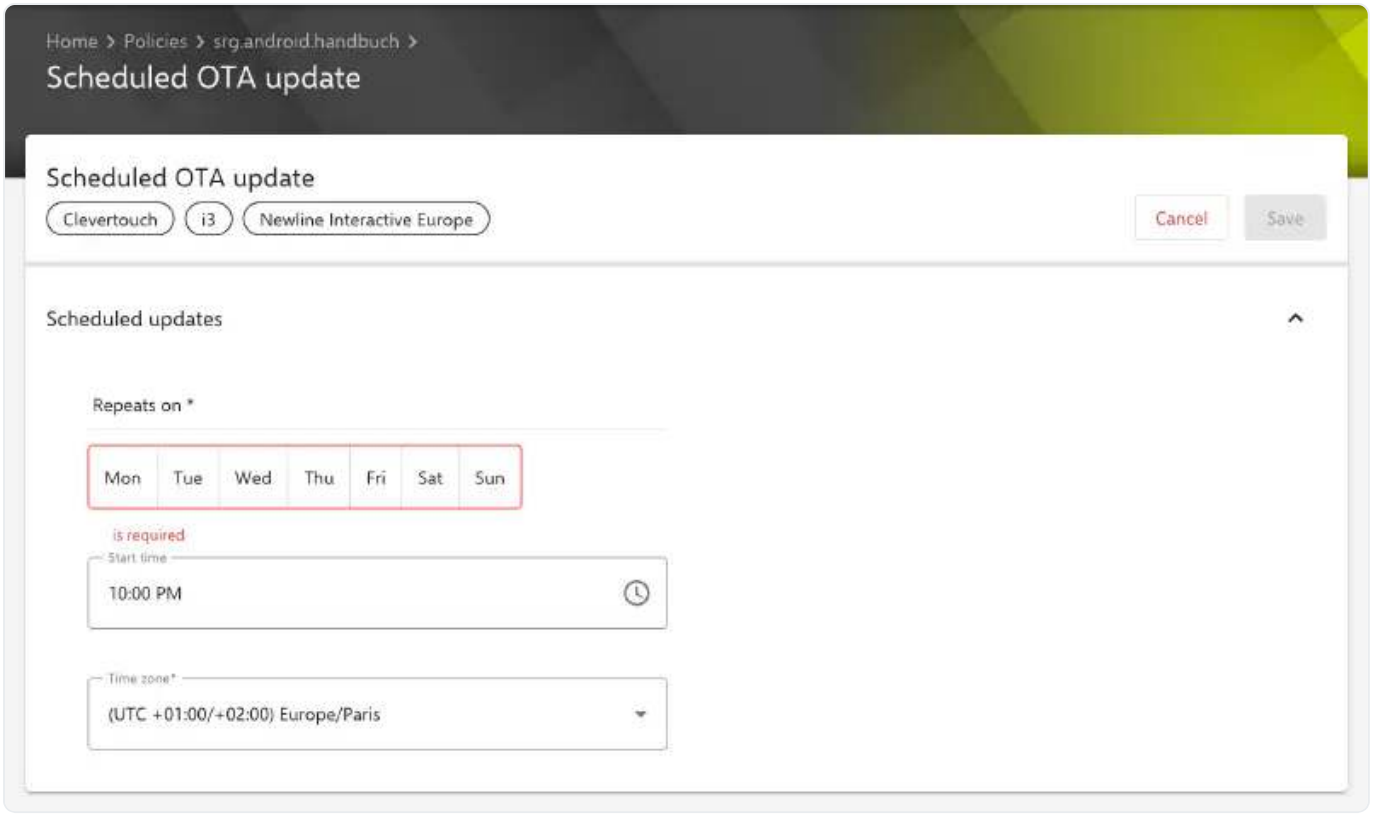
- SSID: The visible name of the Wi-Fi hotspot used for identification by other devices (required).
- This network is hidden: Disables the visible broadcast of the SSID, preventing the hotspot from appearing in the list of available networks. In the portal, this option is marked for Clevertouch and ADVANTouch only and is disabled by default.
- Authentication: None (open network) or WPA2 (default). ADVANTouch and Clevertouch support WPA2 only.
- Passphrase: Password required to access the hotspot. The field is shown only for WPA2, is then required and must be 8 to 63 characters long.
- Frequency Band: The frequency range of the hotspot, 2.4 GHz (default) or 5 GHz.

If the configuration cannot be applied on the device, the compliance violation Hotspot configuration is shown for the device.

Scheduled OTA Update

The Scheduled OTA update policy enables firmware updates on interactive whiteboards to be carried out automatically outside of usage times.

The configuration is supported on whiteboards from Clevertouch →, i3-Technologies → and Newline. Each policy can contain one configuration of this type.



How it works

The start of the update window is defined in the Scheduled updates section:

- Repeats on: Days of the week on which the update window starts (multiple selection, at least one day required). No day is preselected in a new configuration.
- Start time: Time at which the update window starts on the selected days (default 22:00 / 10:00 PM). The start time applies to all selected days.
- Time zone: Time zone in which the start time applies (default Europe/Paris). This time zone is decisive, not the local time of the device; this needs to be taken into account for sites in several time zones.

At the specified time, the Relution Companion checks whether a firmware update is available for the device. If an update is available, it is installed automatically and without user interaction.

When updates are not installed

Firmware updates are not installed if the device is switched off at the scheduled time. For example, if the device is not switched on until the next morning and the update window has been missed, Relution Companion waits until the next defined time window to carry out the update. This ensures that updates are only carried out at the scheduled times.

For version 26.4.0

Device Owner (Companion)

The Device Owner function for the Relution Companion provides the possibilities for advanced management of Android devices. This includes the following functions:

- Install and disable apps without user interaction (policy configuration App compliance →).
- Enable kiosk mode without user interaction (policy configuration Kiosk Mode →).
- Reboot device → action.

Instructions for setting up and connecting the Android Debug Bridge are available here: Android Debug Bridge Setup →

Download Relution Companion

Relution Companion →

Install Relution Companion App on the device

This can be done either manually or via the Android Debug Bridge (ADB).

rsion 26.4.0

```
adb install Relution-normal-release.apk
```

Activate device owner after installation

```
adb shell dpm set-device-owner
com.mwaysolutions.relution/com.mwaysolutions.relution.receiver.MdmDeviceAdminReceiver
```

This command applies to the general Relution Companion with the package name `com.mwaysolutions.relution`. Manufacturer-specific Companion variants use their own package name (e.g. `com.mwaysolutions.relution.i3` or `com.mwaysolutions.relution.advantouch`); the matching command is listed in the respective manufacturer article, for example i3-Technologies → or ADVANTouch →.

Re-enroll device

The device is then re-enrolled in Relution. For this, an enrollment for the platform Android with the type of the respective manufacturer is created and used in the Relution Companion on the device. The procedure is described in the enrollment section of the respective manufacturer article, see Manufacturers →.

For version 26.4.0

Android Debug Bridge Setup

Enable developer mode on the device

This may need to be requested from the manufacturer.

- Settings is opened.
- About phone is opened (the name may vary by manufacturer).
- Build number is tapped seven times until a notification appears (this enables the developer options).
- Back in Settings, Developer options is opened.
- The USB debugging option is located and enabled.

If the policy assigned to the device contains the Restrictions → configuration with the Deny USB Debugging option enabled (preselected for new configurations), USB debugging may be blocked on the device.

Download and install Android Debug Bridge (ADB)

Mac →
Windows →
Linux →

For version 26.4.0

Start Android Debug Bridge (ADB)

```
adb start-server
```

Connect to the device

```
adb connect <IP address>
```

Any trust prompt shown on the device has to be confirmed.

Enroll EDLA devices

With Relution, it is possible to manage EDLA-certified interactive whiteboards via Android Enterprise.

Enrollment

The device is enrolled as a fully managed device →. The enrollment variant using the DPC identifier → is used for this.

> As of Relution 5.33, the enrollment defines whether non-vital pre-installed system apps are disabled during setup or remain enabled. For this, the switch Keep system apps enabled is available under Enrollment options in the Compliance section when the enrollment is created. It is disabled by default. For the enrollment of whiteboards, this switch must be enabled.

Relution includes the switch exclusively in the QR code of the enrollment. The DPC identifier does not contain it; with an enrollment via DPC identifier, the switch therefore has no effect, see Enrollment options →. Pre-installed apps that are disabled after enrollment can be enabled afterwards, see Pre-installed Apps →.

EDLA extensions

For certain interactive whiteboards, extensions are available that supplement the general range of functions with whiteboard-specific features. An overview of these extensions is available under EDLA extensions →.

For version 26.4.0

CVTE hardware platform

Relution makes it possible to centrally manage interactive whiteboards of the CVTE hardware platform.

Supported product ranges and models of the base configuration

The following vendors and product series are supported:

- Heinekingmedia DT-75-C10HM

Supported product ranges and models with Bytello Share

The following vendors and product series support the configuration of Bytello Share screen sharing services:

- Heinekingmedia DT-75-C10HM

For version 26.4.0

Enrollment

Enrollment is performed as described in Enroll EDLA devices →.

Supported Actions

The Android Enterprise Actions → are available, including Shutdown device. This action shuts the whiteboard down completely. With Android Enterprise, it is only supported by certain whiteboards; the portal marks it with the supported vendors, including heinekingmedia (HKM).

Supported Policies

In addition to the CVTE OEMConfig configuration, all Android Enterprise configurations are supported.

Relution CVTE OEMConfig App

To make the additional functions of the whiteboards available via Android Enterprise, the Relution CVTE OEMConfig app must be installed and configured on the device.

Configuration

The Relution CVTE OEMConfig app is configured via a policy with a CVTE OEMConfig configuration.

The configuration installs the Relution CVTE OEMConfig app on the device with the installation type Force-installed, updates it with high priority and grants it the required permissions. Users cannot remove the app. A separate distribution via the Manage apps configuration is neither required nor possible: if the app is listed there, the configuration cannot be saved, and the portal refers to the CVTE OEMConfig configuration.

Placeholders can be used in the configuration values; the form shows the available placeholders.

The app also reports additional device information to Relution, such as IP and MAC address, firmware and system version, and the status of Ethernet, hotspot and Wake-on-LAN.

Configuration of Bytello Share screen sharing services

The following apps are added to the Manage apps → configuration:

Version 26.4.0

Name	Internal Name	Installation type
ScreenSharePro	com.seewo.screensharepro.server	Pre-installed
Bytello ScreenSharePro	com.bytello.screensharepro.server	Pre-installed

Setting options

The Relution CVTE OEMConfig app offers the following configuration options:

Setting	Description
Volume	Set system volume (0-100)
Mute	Enable/disable audio output mute
Sound Mode	Select from Standard, Movie, Classroom, Meeting, Custom modes
Audio Balance	Adjust left/right channel balance (0-100)
Bass	Adjust low frequencies (0-100)
Treble	Adjust high frequencies (0-100)
Brightness	Set display brightness (0-100)
Picture Mode	Standard, Dynamic, Vivid, Soft, Custom, Retail
Sharpness	Adjust image clarity (0-100)
Contrast	Set image contrast levels (0-100)
Hue	Adjust color temperature (0-100)
Saturation	Set color intensity (0-100)
Auto Light Sensor	Enable ambient light adaptation
Blue Light Filter	Reduce eye strain in low-light conditions
Touch Enable	Configure touchscreen functionality
Toolbar Type	Select between Floating Bar, Slide Bar, or System Bottom Bar
Auto Sleep	Set inactivity timeout (0-240 minutes)
No Signal Sleep	Configure automatic shutdown when no input detected (0-7200 seconds)
Eye Care Mode	Enable blue light reduction
Wake on Source	Auto-power on when input connected
Wake-on-LAN	Configure network wake capabilities
Touch Input	Enable/disable touch functionality
OEM Lock	Restrict unauthorized settings changes
Ethernet	Manage wired network connection
Hotspot	Configure wireless access point

Setting	Description
Device Visibility	Control network discovery when sharing
Require Permission	Require approval for sharing sessions
Chromecast	Enable Google casting protocol
AirPlay	Enable Apple screen mirroring
Miracast	Enable Windows wireless display
Webcast	Enable browser-based sharing
Auto Start	Launch sharing service on boot
HID Touch	Enable USB touch control
DLNA	Configure media server capabilities
Device Name	Set custom network name
Code Refresh	Set PIN update frequency
Window Size	Control floating control panel size
Automatic Updates	Configure automatic firmware updates
Update Verification	Enable update authenticity checks
Debug Mode	Enable developer diagnostics
Language	Set system language (English, French, German, Italian, Spanish, Turkish)
Power Schedule	Create automated power on/off schedules with: Daily/Weekly recurrence, Specific time settings, Multiple task support
Source Aliasing	Rename input sources (HDMI/DP/VGA)
Force Input Source	Set startup input channel

Bytello Share options

The Relution CVTE OEMConfig app also offers the following configuration options if Bytello Share is also available:

Setting	Description
Device network visibility	Enable or disable device visibility in network when sharing.
Require permission	All device share screens will need permission
Enable Chromecast	Enable/disable Chromecast support
Enable Airplay	Enable/disable Airplay support
Enable Miracast	Enable/disable Miracast support
Enable Webcast	Enable/disable Webcast support
Auto Start on Boot	Automatically start sharing service on device boot
HID Touch Control	Enable/disable HID touch control support
Enable DLNA	Enable/disable DLNA support
Device Name	Set name for this device
Code Refresh Time	Set time interval for code refresh (minutes)
Floating Window Size	Set size of floating control window (Normal, Mini, Closed)
System bar	Set System bar visible/hidden.

Newline

Relution makes it possible to centrally manage interactive whiteboards of Newline.

Supported product ranges and models

- TT-7523QA (Lyra Pro)
- TT-6523QCA+ (Elara Pro)

Enrollment

Enrollment is performed as described in Enroll EDLA devices →.

Supported Actions

The Android Enterprise Actions → are available, including Shutdown device. This action shuts the whiteboard down completely. With Android Enterprise, it is only supported by certain whiteboards; the portal marks it with the supported vendors, including Newline.

For version 26.4.0

Relution Newline OEMConfig App

To make the additional functions of the whiteboards available via Android Enterprise, the Relution Newline OEMConfig app must be installed and configured on the device.

Configuration

The Relution Newline OEMConfig app is configured via a policy with a Newline OEMConfig configuration.

The configuration is available from Relution 5.34.0 onwards.

The configuration installs the Relution Newline OEMConfig app on the device with the installation type Force-installed, updates it with high priority and grants it the required permissions. Users cannot remove the app. A separate distribution via the Manage apps configuration is neither required nor possible: if the app is listed there, the configuration cannot be saved, and the portal refers to the Newline OEMConfig configuration.

Placeholders can be used in the configuration values; the form shows the available placeholders.

Settings Options

The Relution Newline OEMConfig app offers the following configuration options:

For version 26.4.0

Setting	Description
Sound output	Set the current sound output
Volume	Set the volume of the system. (0–100)
Mute	Set system mute/unmute.
Wake on lan	Enable or disable wake on lan
Wake on Wireless	Enable or disable Wake on Wireless (WoWLAN)
Wi-Fi	Enable or disable Wi-Fi connectivity.
Ethernet	Enable or disable Ethernet
Hotspot	Enable or disable hotspot
Ethernet tethering	Enable or disable Ethernet tethering.
Proxy configuration	Configure network proxy settings including host, Port, and ExclusionList parameters.
Proxy Host	Proxy server hostname or IP address
Proxy Port	Proxy server port number (1–65535)
Proxy Exclusion List	Comma-separated list of hosts to bypass proxy
Brightness	Set brightness value. (0–100). Picture mode must be set to CUSTOM/USER.
Picture mode	Set picture mode.
Font size	Set font size.
Starting source	Set startup source configuration
Auto source switching	Enable or disable automatic source switching.
CEC auto power on	Enable or disable CEC auto power on.
CEC auto power off	Enable or disable CEC auto power off.
HDMI/DP EDID type	Set HDMI/DisplayPort EDID version
Signal source wake up	Enable or disable wake up on new signal source detection.
Debug mode	Enable or disable debug mode
24-hour time format	Enable or disable 24-hour time format

Setting	Description
Left toolbar	Enable or disable the left toolbar
Right toolbar	Enable or disable the right toolbar
Quick settings	Enable or disable quick settings access
Power On Date/Time	Configure scheduled power-on time
Power Off Date/Time	Configure scheduled power-off time
Energy saving time	Enable to set energy saving time. Disable to set to never.
Energy Saving Time (minutes)	Energy saving time in minutes. Common values are 30, 60, 90, 120
Power Button Behavior	Configure power button action (Sleep vs Power Off)
Tap Wake	Enable or disable wake screen by tapping
Eye Protection Writing	Enable or disable writing-oriented eye protection mode
Adaptive Brightness	Enable or disable automatic brightness adjustment for eye comfort
Filter blue light	Enable or disable blue light
Blue Light Filter level	Set blue light filter intensity level (0-100)
Device Logo	Show/hide manufacturer logo
UI Theme	Select between Newline Q or Z theme variants
Auto-clean Files	Set automatic file cleanup interval
Android OS (warning: can only be re-enabled in dealer menu)	Enable or disable Android OS (warning: can only be re-enabled in dealer menu)
USB Lock	Enable or disable USB port locking
Menu Lock	Enable or disable system menu access
Settings Lock	Enable or disable settings modification
Disable App Installation	Enable or disable application installation
Front Power Button Lock	Enable or disable front power button functionality
Front Panel Buttons Lock	Enable or disable front control panel buttons
Touch Lock	Enable or disable touch lock
Signal Source Touch Lock	Set signal source touch lock
Wi-Fi Settings Lock	Enable or disable Wi-Fi configuration changes

Setting	Description
Ethernet Settings Lock	Enable or disable Ethernet configuration changes
Launcher Icons Lock	Enable or disable launcher icon modifications
Admin mode password	Set admin mode password (min 6 characters)
Theme & Wallpaper Lock	Prevent changes to device theme and wallpaper settings
Blocked URLs	Block urls
Local OTA	Enable or disable local firmware updates.
OTA background download	Enable or disable background OTA downloads.
OTA notifications	Enable or disable OTA update notifications.

For version 26.4.0

Pre-installed Apps

To selectively enable pre-installed apps, the respective package name of the app is required. A complete list of all pre-installed apps that are no longer available after enrollment in Android Enterprise can be obtained by resetting the device to factory settings and completing the full device setup process without enrolling the device in Android Enterprise.

> Whether non-vital pre-installed system apps are disabled during enrollment is defined by the enrollment switch Keep system apps enabled. Relution only includes it in the QR code, not in the DPC identifier, see Enroll EDLA devices →.

Once the device is fully set up and ready to use, a connection to the device is established via Android Debug Bridge →. The following command then exports a list of all installed packages:

```
adb shell cmd package list packages > list1.txt
```

The device is then reset to factory settings again and enrolled in Android Enterprise.

After successful enrollment, the device is connected via ADB again and the following command is run:

```
adb shell cmd package list packages > list2.txt
```

Both files can now be compared.

All apps that appear in the file `list1.txt` but are missing from `list2.txt` need to be added with the installation type Pre-installed in the Manage apps configuration.

In the Manage apps configuration, Add opens the Select an app dialog. There, Manually add app is selected as the Source. In the next step, Name (display name of the app) and Internal name (package name) are entered. The internal name corresponds to the entry from the file `list1.txt` to be added – but without the `package:` prefix. Example: If the entry `package:io.relution.files` is to be added, `io.relution.files` is entered as the internal name.

The app is then listed with the installation type Force-installed. In the Installation type column, Pre-installed is selected.

Manual enrollment

Starting with Relution version 5, Windows 10/11 devices can be enrolled and managed without a Microsoft or `Azure AD` account. Enrollment requires a local user. This user must have administrative privileges and must not be deleted after enrollment.

Devices should be equipped with a unique ID. During enrollment, Relution identifies a device by its Windows device ID and treats an enrollment with an already known ID as a re-enrollment of the same device. Especially when preconfiguring via an image, care should therefore be taken to ensure that the devices can be distinguished by the MDM.

In addition to manual enrollment, Windows devices can be enrolled via Autopilot → and via Bulk Enrollment → with a provisioning package.

> The Windows 10/11 Home edition has various limitations when it comes to management. Not all management features are available. Limitations of Windows Home Edition →

Supported Windows versions

- Windows 10/11 Home
- Windows 10/11 Professional
- Windows 10/11 Education
- Windows 10/11 Enterprise

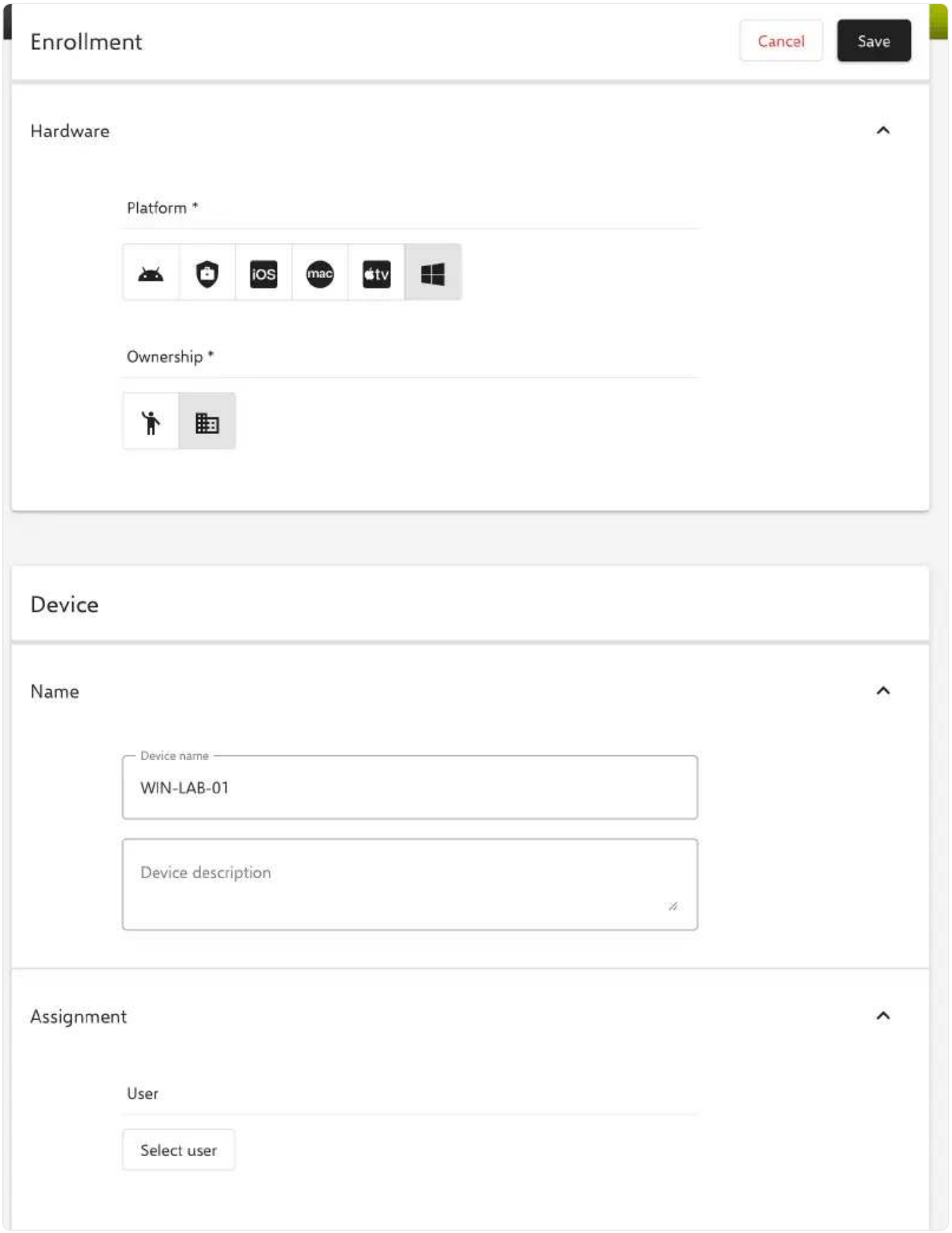
For version 26.4.0

Non-supported Windows versions

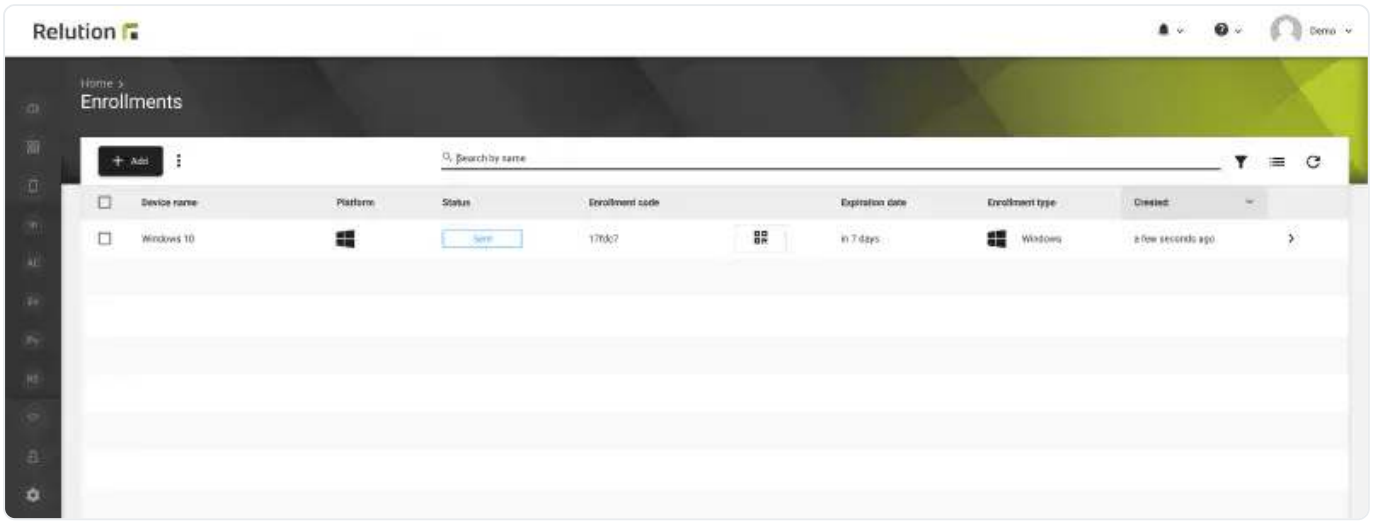
- Windows 10/11 Enterprise LTSC
- Windows 10/11 IoT Enterprise
- Windows 10/11 IoT Enterprise LTSC

Manually enroll Windows devices

To enroll a Windows 10/11 device, a new enrollment must be created in Relution. The enrollment is created under `Devices` → `Enrollments` via Add; the menu item is not available in the global organization. In the Hardware section, Windows is selected under Platform and the Ownership is defined. Optionally, a name is specified under Device name (letters, digits and hyphens only); if the field is left empty, the name is generated automatically. A user can be selected under Assignment, and an expiration date via Valid until.

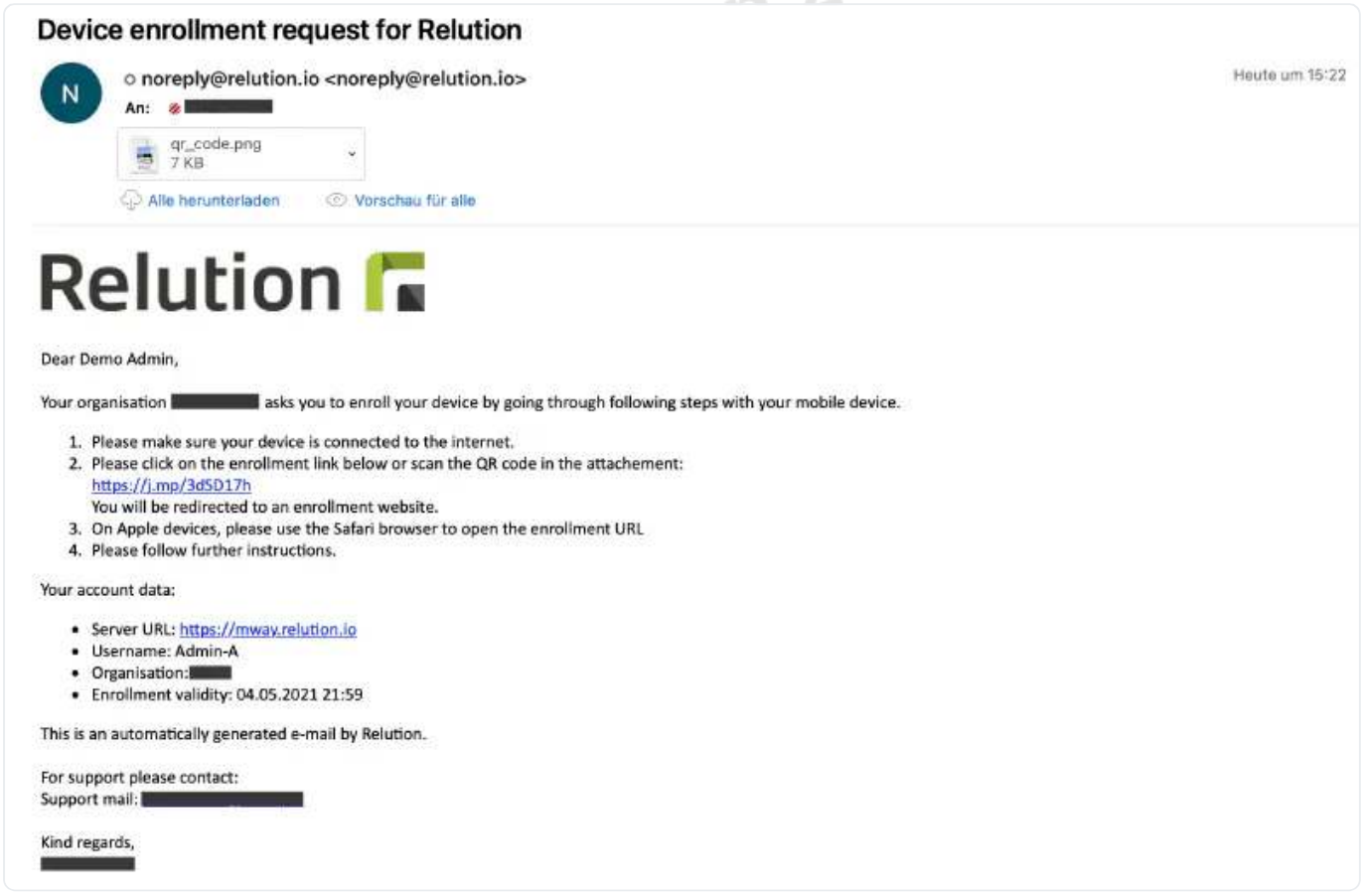


Afterwards, the enrollment is listed under Enrollments – with the status Sent if the enrollment information was sent by email or SMS, otherwise with the status Created. Once a device has been enrolled, an enrollment that is not multi-use changes to the status Enrolled and cannot be used again.



Get enrollment information

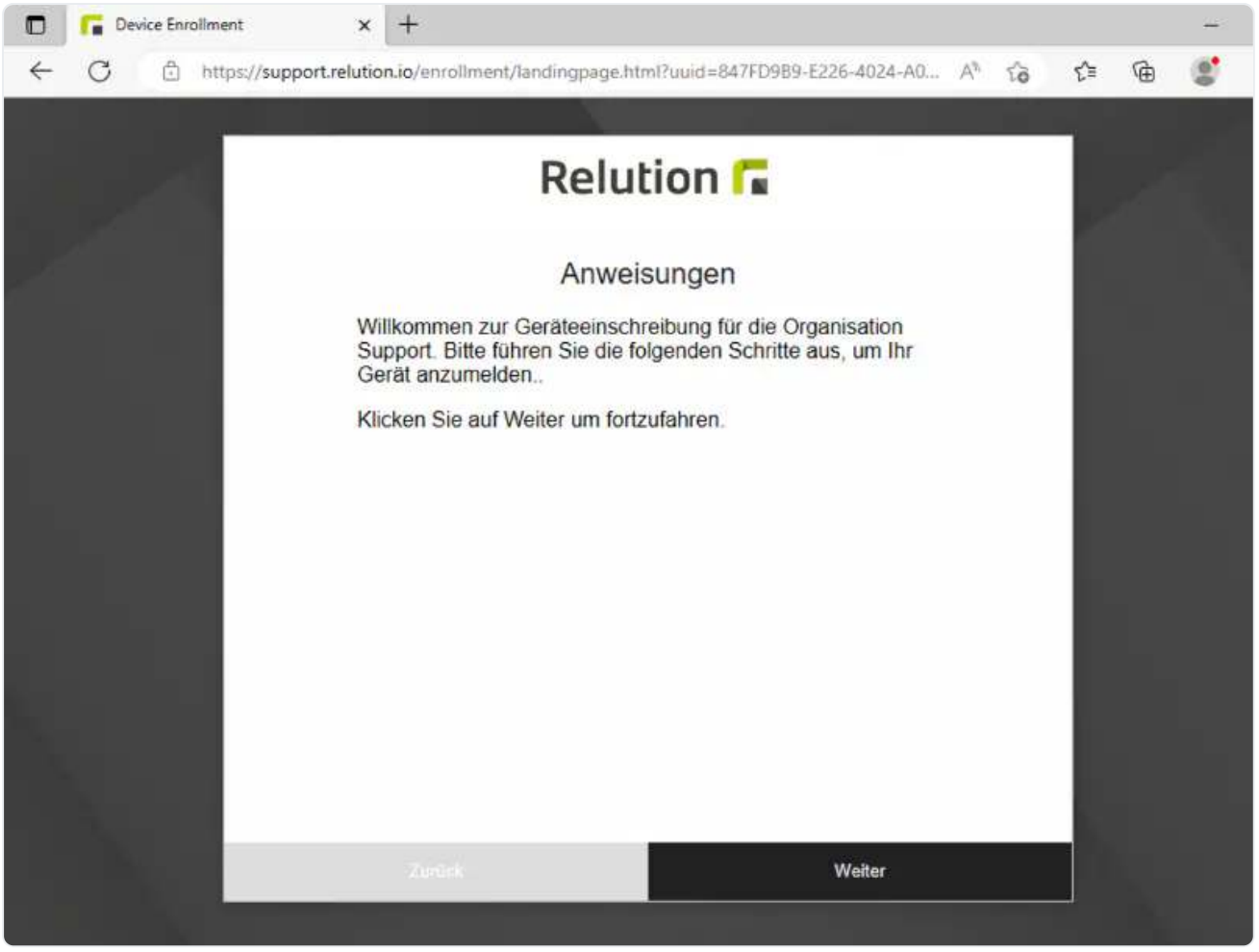
When the enrollment is created, the required enrollment information can be sent in the Notification area by email, by SMS or via both channels. The respective channel must be enabled under `Settings` → `Notifications`. Sending by email requires a user with an email address to be assigned to the enrollment; sending by SMS requires a phone number. For example, users assigned to the devices to be enrolled receive the following email with all relevant information:



The enrollment link in the email automatically opens the enrollment process on the Windows 10/11 device.

Perform enrollment on Windows 10/11 devices

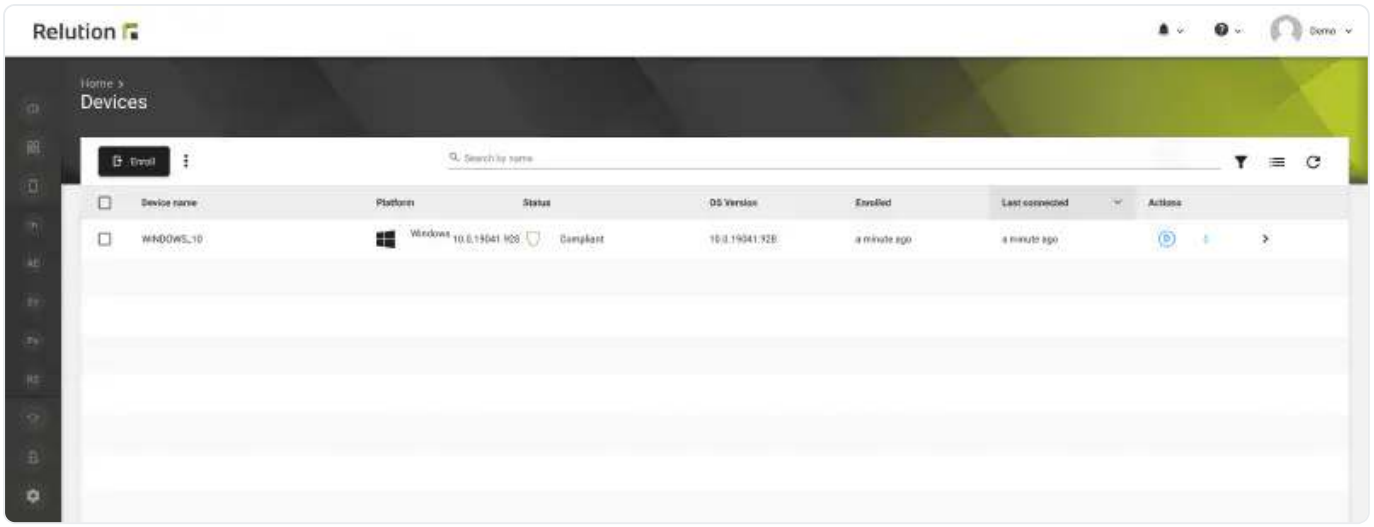
1. The link shown in the enrollment is opened in the browser of the device to be enrolled.

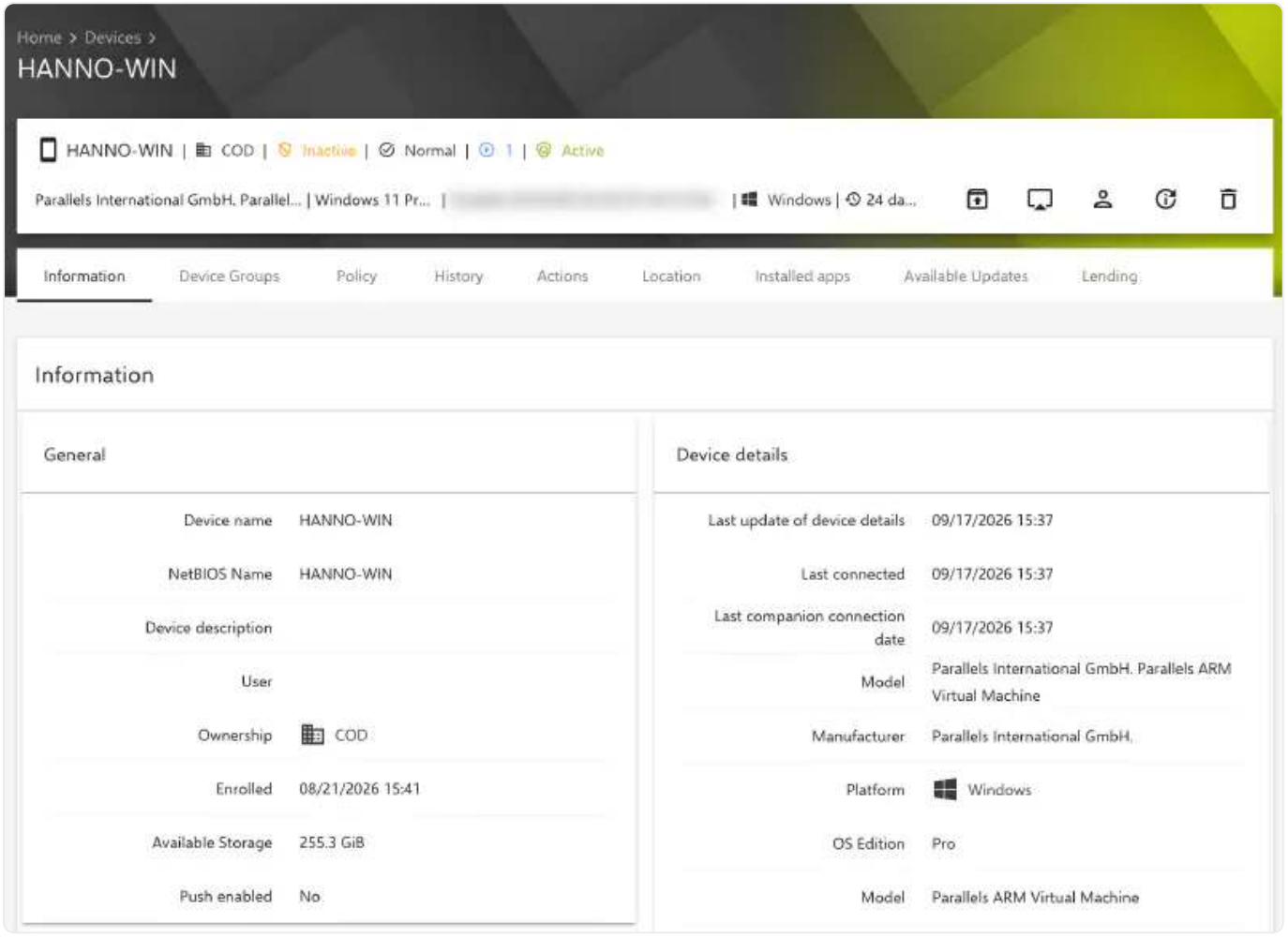


2. Next and then Enrollment are clicked. The browser then tries to open the Settings app; this is confirmed with Open.



3. All further dialogs are confirmed. The device is then enrolled and can be managed with Relution.



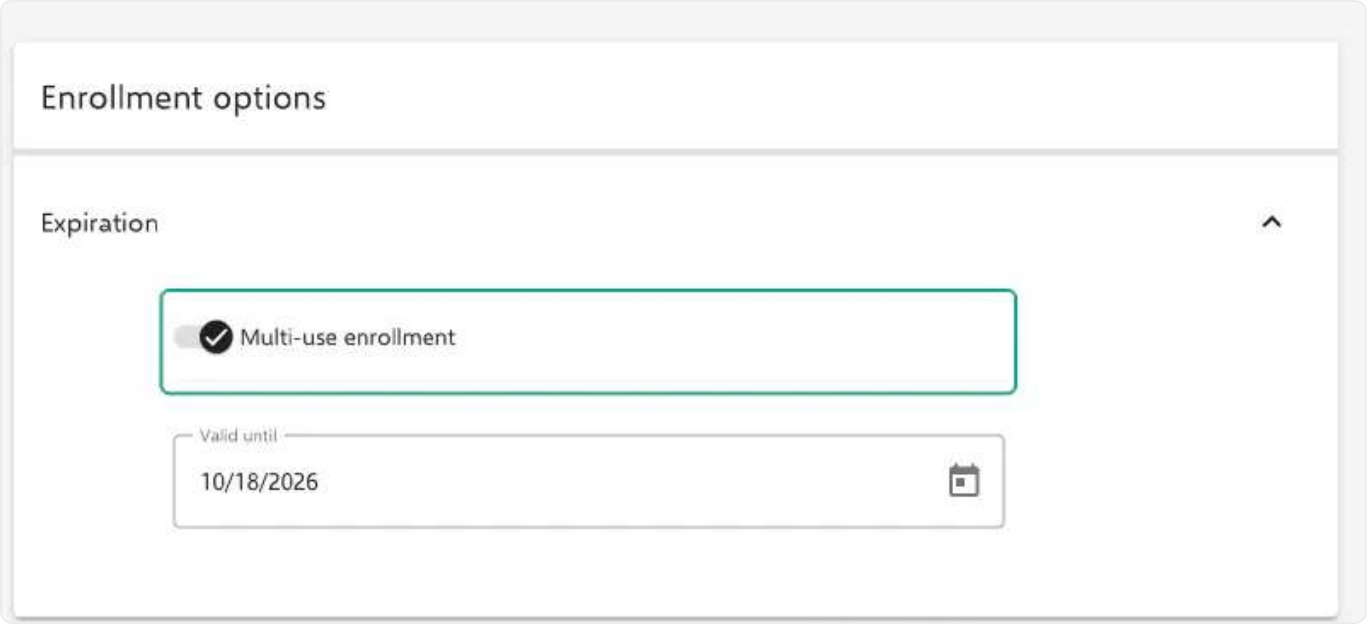


Multiple enrollment of Windows 10/11 devices

Relution supports `bulk enrollment` as an efficient way to enroll a large number of Windows 10/11 devices to be managed by an MDM server without the need to re-image the devices.

For this purpose, the Multi-use enrollment toggle is enabled in the Expiration section of the Enrollment options area when the enrollment is created. The enrollment can then be used for multiple devices. The toggle alone does not perform a bulk enrollment, however: the generated enrollment code is then embedded in a provisioning package (`ppkg`) using Windows Configuration Designer. Bulk enrollment is available for Windows 10/11 Professional, Enterprise and Education. Bulk Enrollment →

The Bulk Enrollment action in the context menu of the enrollment list, on the other hand, creates several individual enrollments for selected users at once and is not intended for this purpose.



For version 26.4

Further details are available in the Microsoft documentation on bulk enrollment:

Windows Provisioning Tool →

> The account on the device that was used to enroll the device must not be deleted.

Bulk Enrollment

When registering and setting up a large number of Windows 10/11 devices, a manual enrollment process creates a not inconsiderable amount of work. The `Windows Bulk Enrollment`, also called mass enrollment, provides an efficient way to enroll many Windows 10/11 devices quickly without having to complete the enrollment through the system settings on each individual device. Mass enrollment of Windows 10/11 devices is available for Professional, Enterprise and Education versions. The enrollment of individual devices is described under Manual enrollment →.

Windows Configuration Designer (WCD)

`Windows Bulk Enrollment` requires the `Windows Configuration Designer (WCD)` tool, which can be downloaded from the Microsoft Store →. Alternatively, the WCD tool can be downloaded via the Windows Assessment and Deployment Kit (ADK) → and is then also available in other languages.

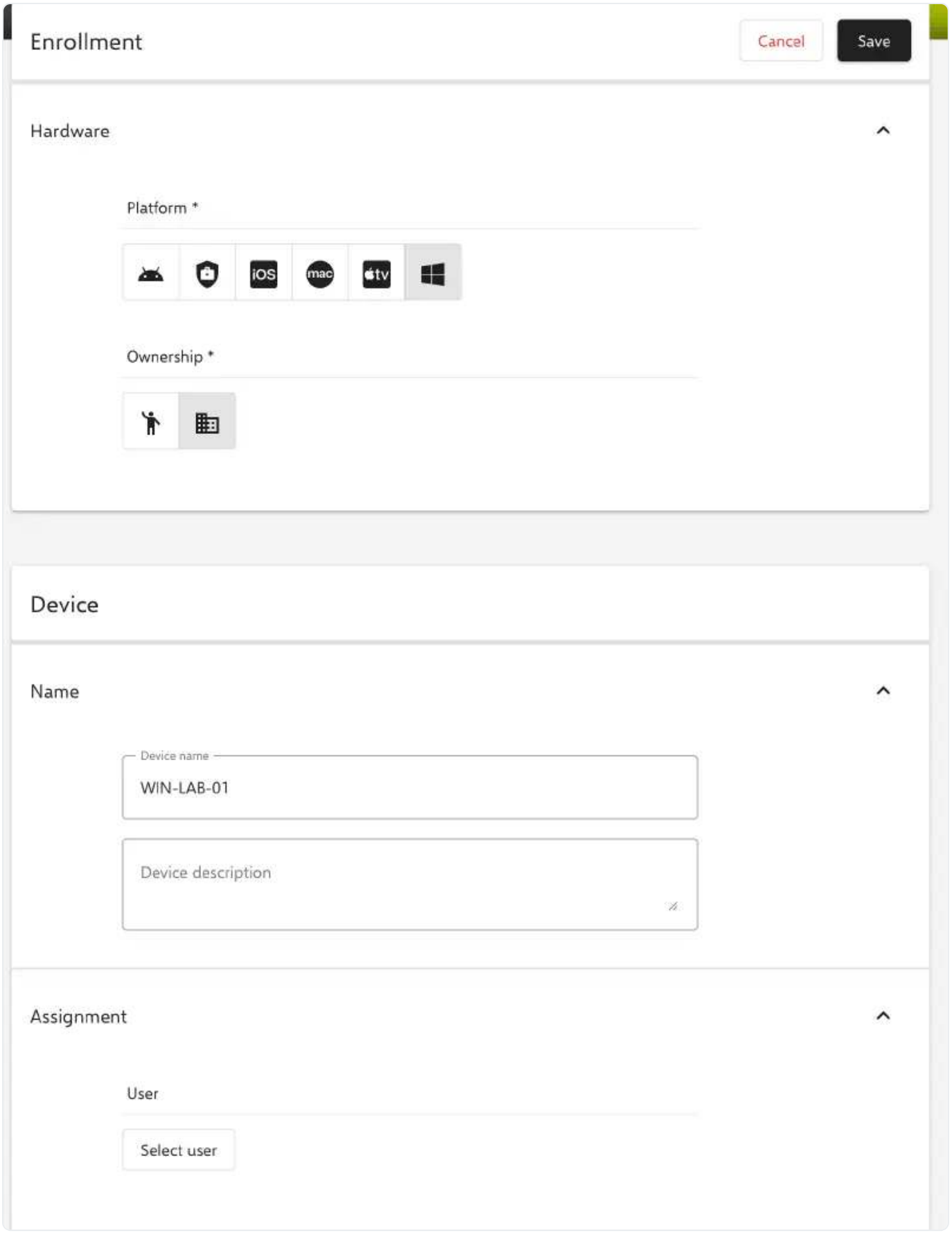
The WCD tool can be used to generate `provisioning packages` that are required to execute mass enrollments. The file format of provisioning packages is a `ppkg` file. This is a container for a collection of configuration settings. `Bulk enrollment` is not done with an `Azure AD` account or `Windows Autopilot`. Registration is done via a `ppkg` file, which can be executed with an administrator account after the device has been put into operation. Alternatively, the `ppkg` can be incorporated into a Windows image; the procedure is described in the following guide (German). Windows Bulk ppkg Image →

> The ppkg must not be used like an auto/unattend.xml on a USB stick when installing the OS. When installing the OS, a temp admin is used, and this and the enrollment would be discarded after some time.

For version 26.4.0

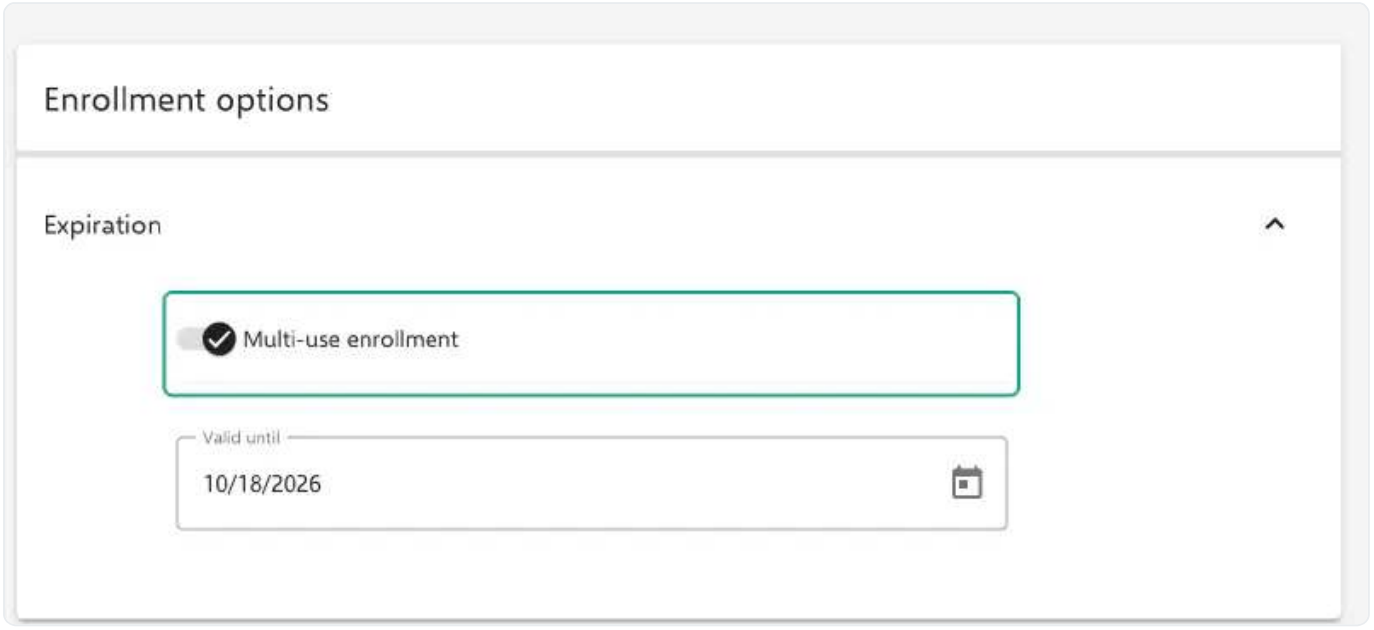
Preparing for enrollment in Relution

For bulk enrollment of Windows 10/11 devices, a manual enrollment must be created in Relution. It is created under `Devices` → `Enrollments` via Add. In the Hardware section, Windows is selected under Platform. Enrollment codes of other platforms are rejected during Windows enrollment.



The settings of the enrollment apply to all devices enrolled with the provisioning package. If a user is selected under Assignment, all devices are assigned to this user; without a user, the devices are not assigned to any user.

In the Enrollment options area, the Multi-use enrollment option is enabled in the Expiration section. Only then can the created enrollment be used for multiple Windows 10/11 devices. The option cannot be changed after the enrollment has been created. An expiration date can optionally be set via Valid until.



After saving, the Enrollment code is displayed in the Enrollment information area of the enrollment together with a copy button; in the enrollment list, it is shown in the Enrollment code column. It is needed in the further process when creating the provisioning package via the WCD tool.



The enrollment code is embedded in the provisioning package. Once the date under Valid until has passed, enrollments with this package fail until the enrollment is extended in the enrollment list via Extend Enrollment(s). If the enrollment is deleted, the provisioning package can no longer be used; it then has to be created again with the enrollment code of a new enrollment.

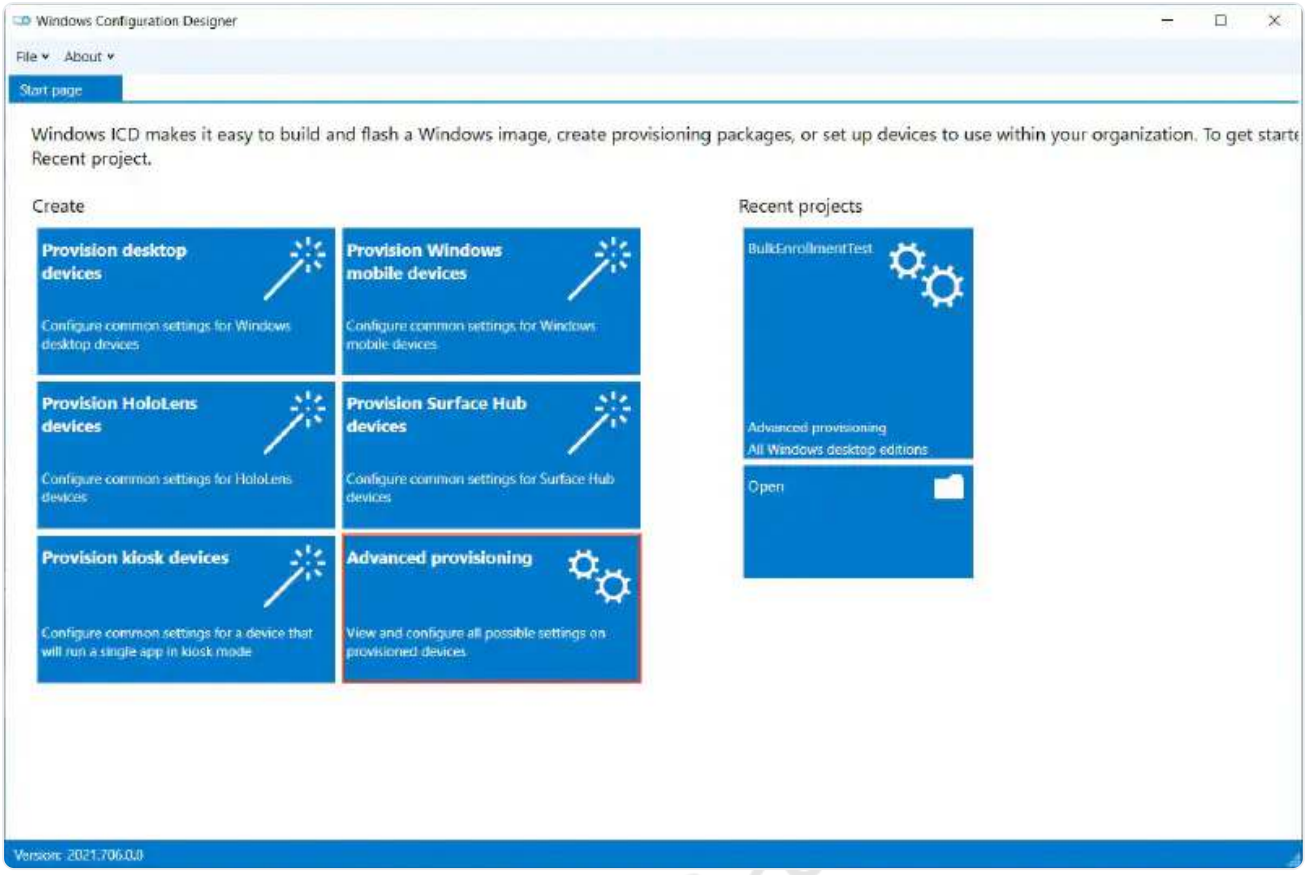
The Bulk Enrollment action in the context menu of the enrollment list, on the other hand, creates several individual enrollments for selected users and is not required for this procedure.

Creating provisioning packages with Windows Configuration Designer (WCD)

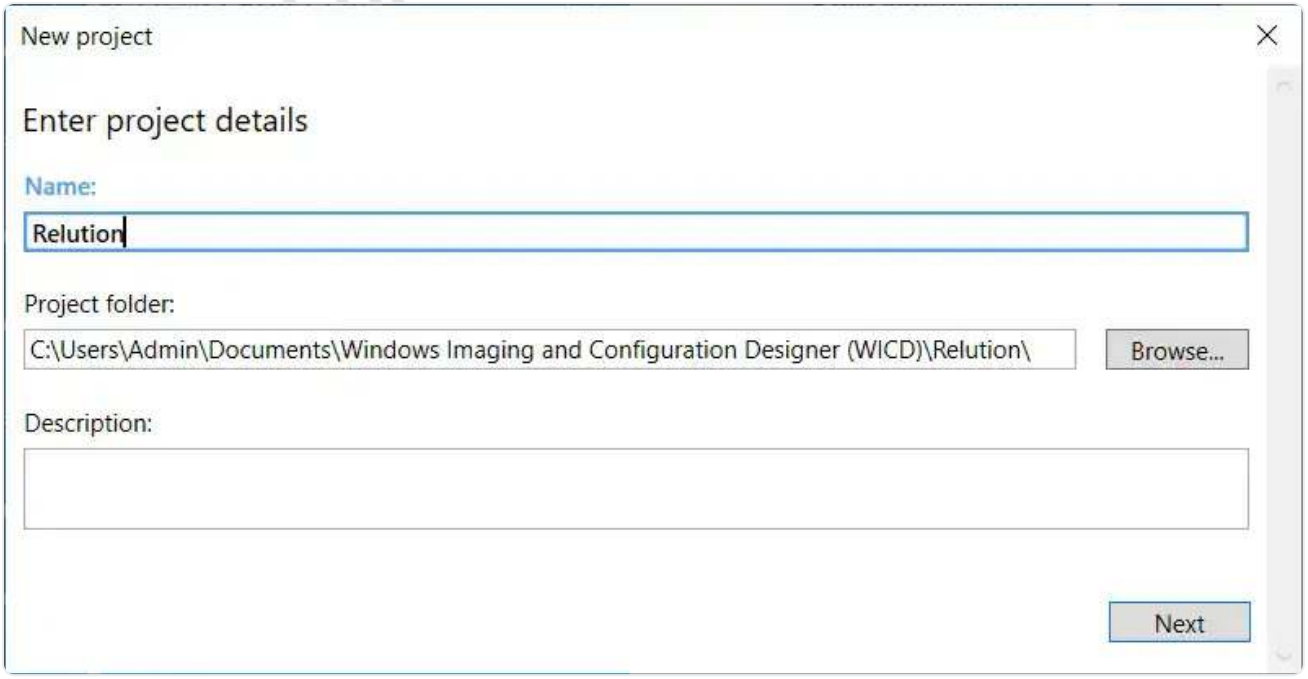
The following steps are performed after downloading and installing the WCD tool to create a provisioning package:

For version 26.4.0

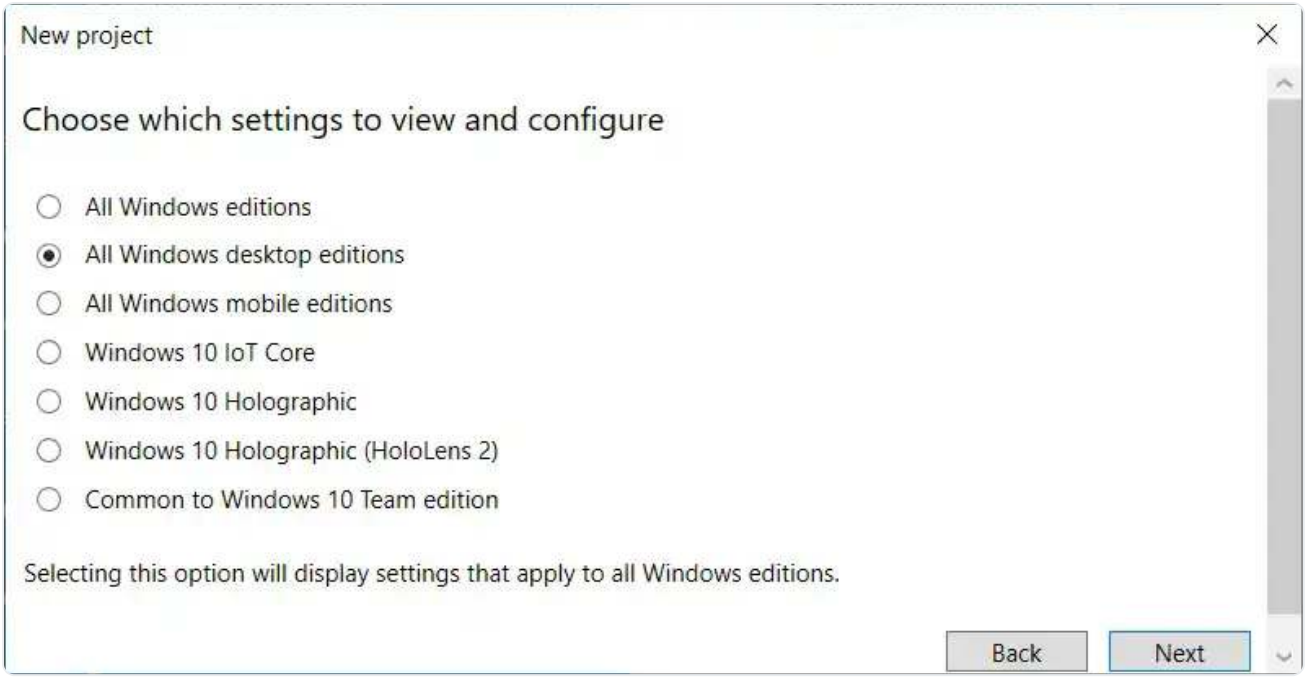
1. In the start screen, the Advanced provisioning tile is selected.



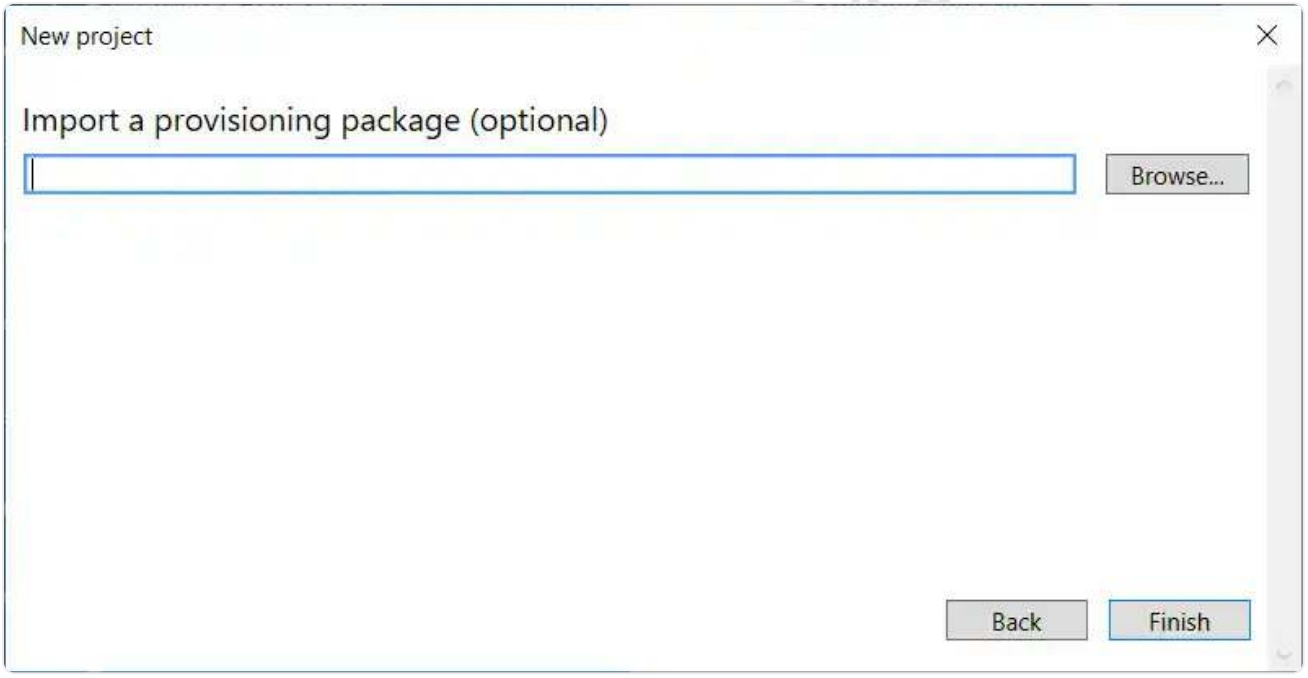
2. A project name is specified, followed by a click on Next.



3. All Windows Desktop Editions is selected, followed by a click on Next.

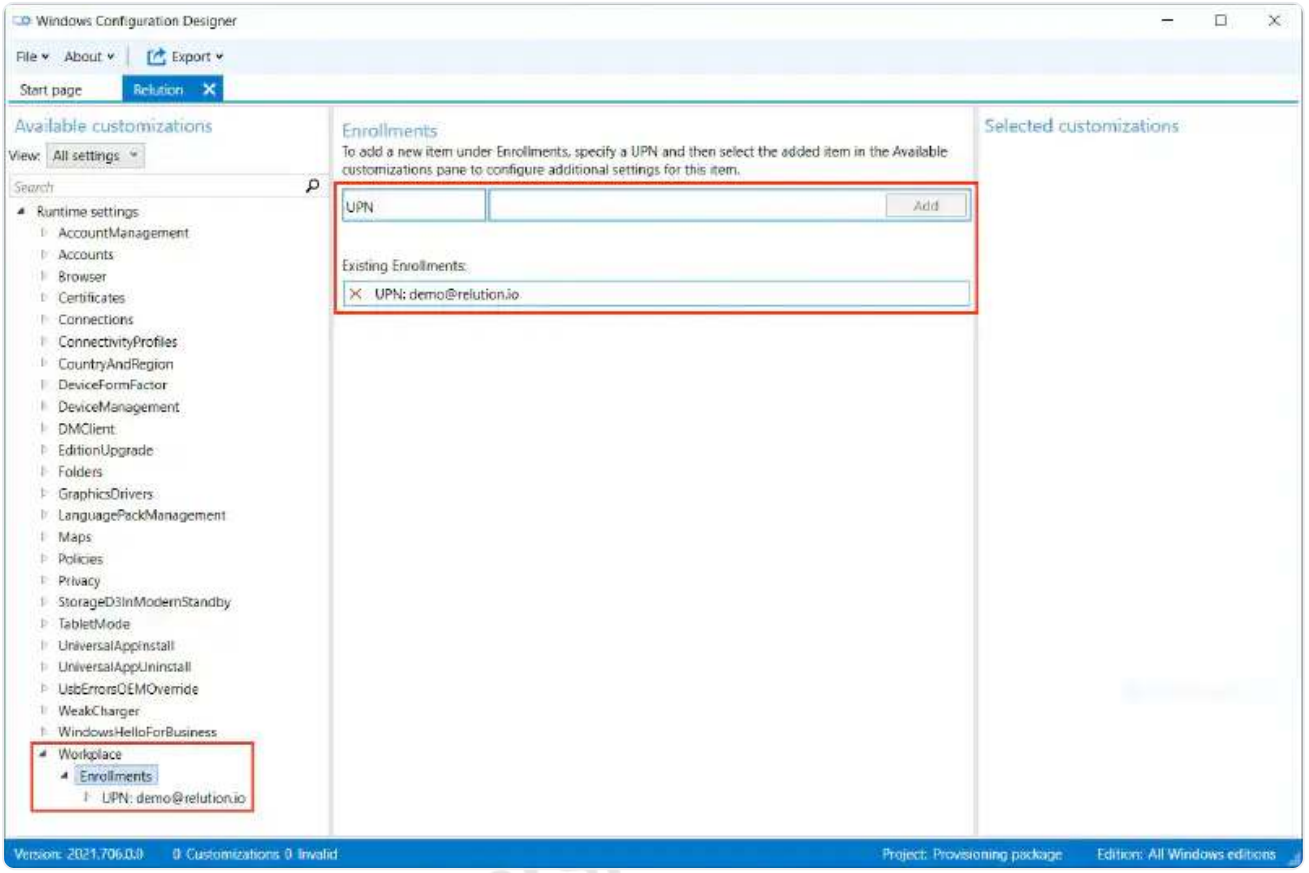


4. Import a provisioning package (optional) is skipped and confirmed with Finish.



5. In the left navigation area, the Runtime Settings menu item and then Workplace are expanded, followed by a click on Enrollments.

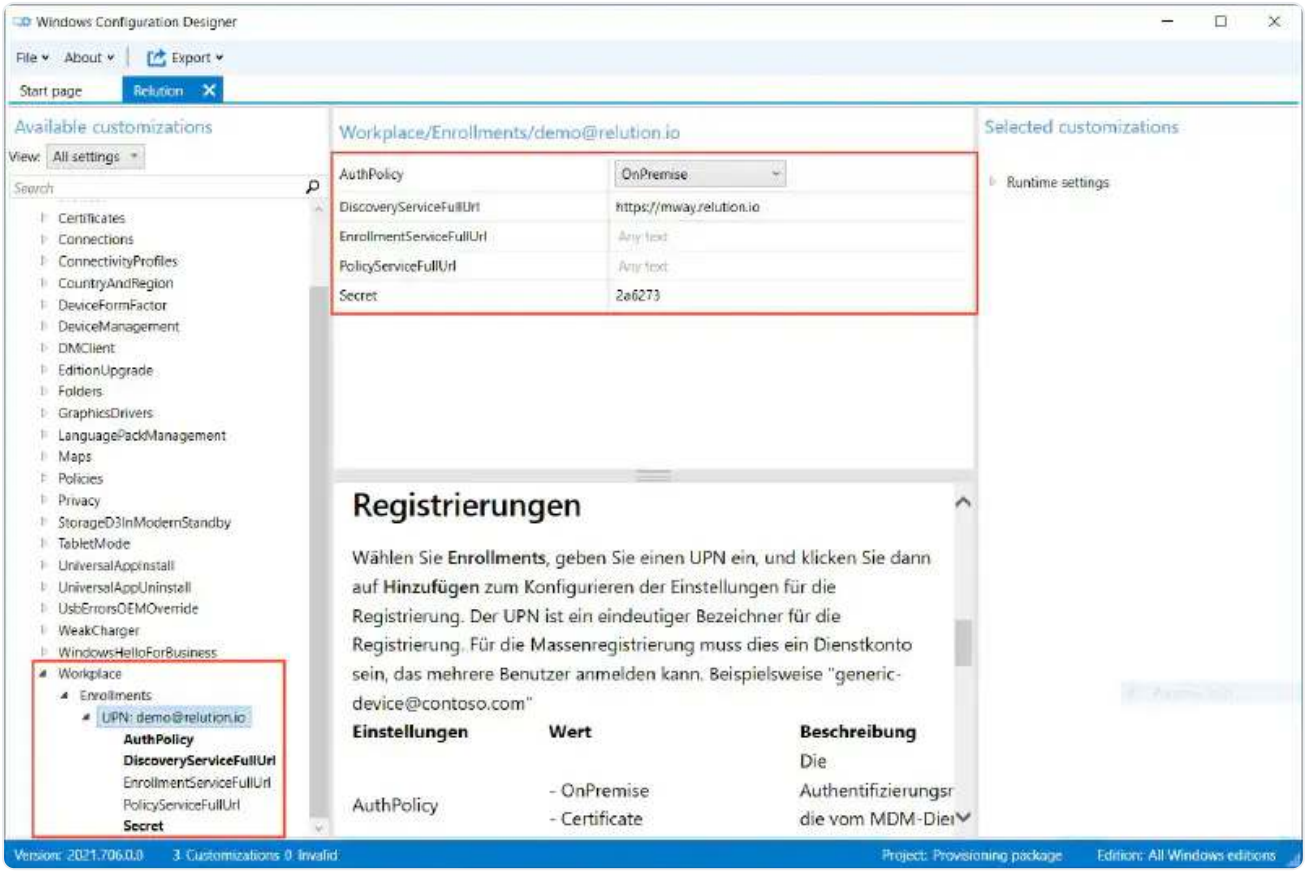
6. Under Enrollments, a UPN in the format of an email address is entered and added. Relution does not evaluate this value during enrollment. The organization and user assignment result from the enrollment in Relution whose enrollment code is entered as `Secret` below.



For ver

7. The newly created entry with the UPN is expanded in the left navigation pane, and the following information is entered for the remaining settings:

   - `AuthPolicy` – select `OnPremise`.
   - `DiscoveryServiceFullUrl` – the corresponding domain of the Relution server used.
   - `EnrollmentServiceFullUrl` – optional.
   - `PolicyServiceFullUrl` – optional.
   - `Secret` – the enrollment code from Relution.

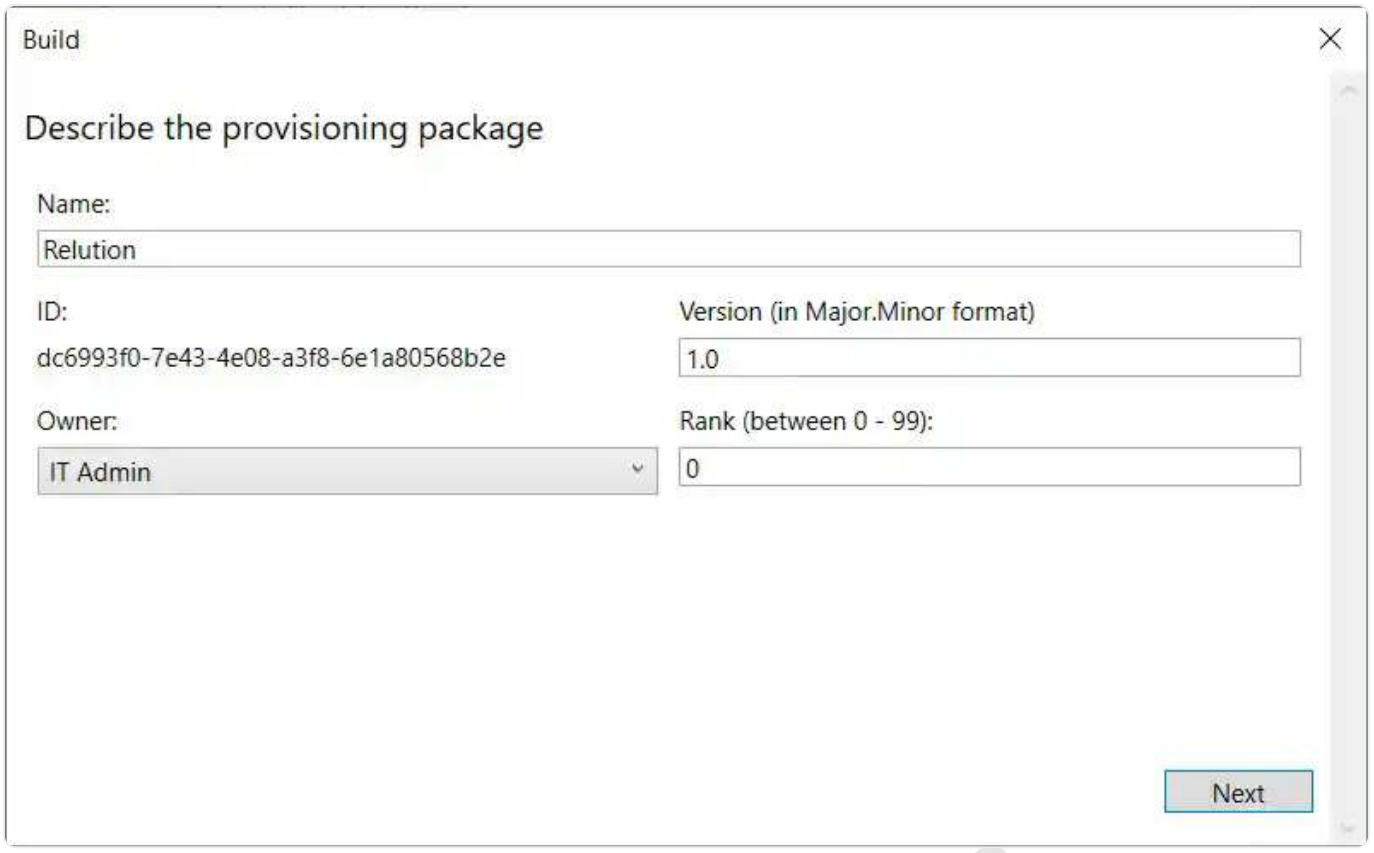


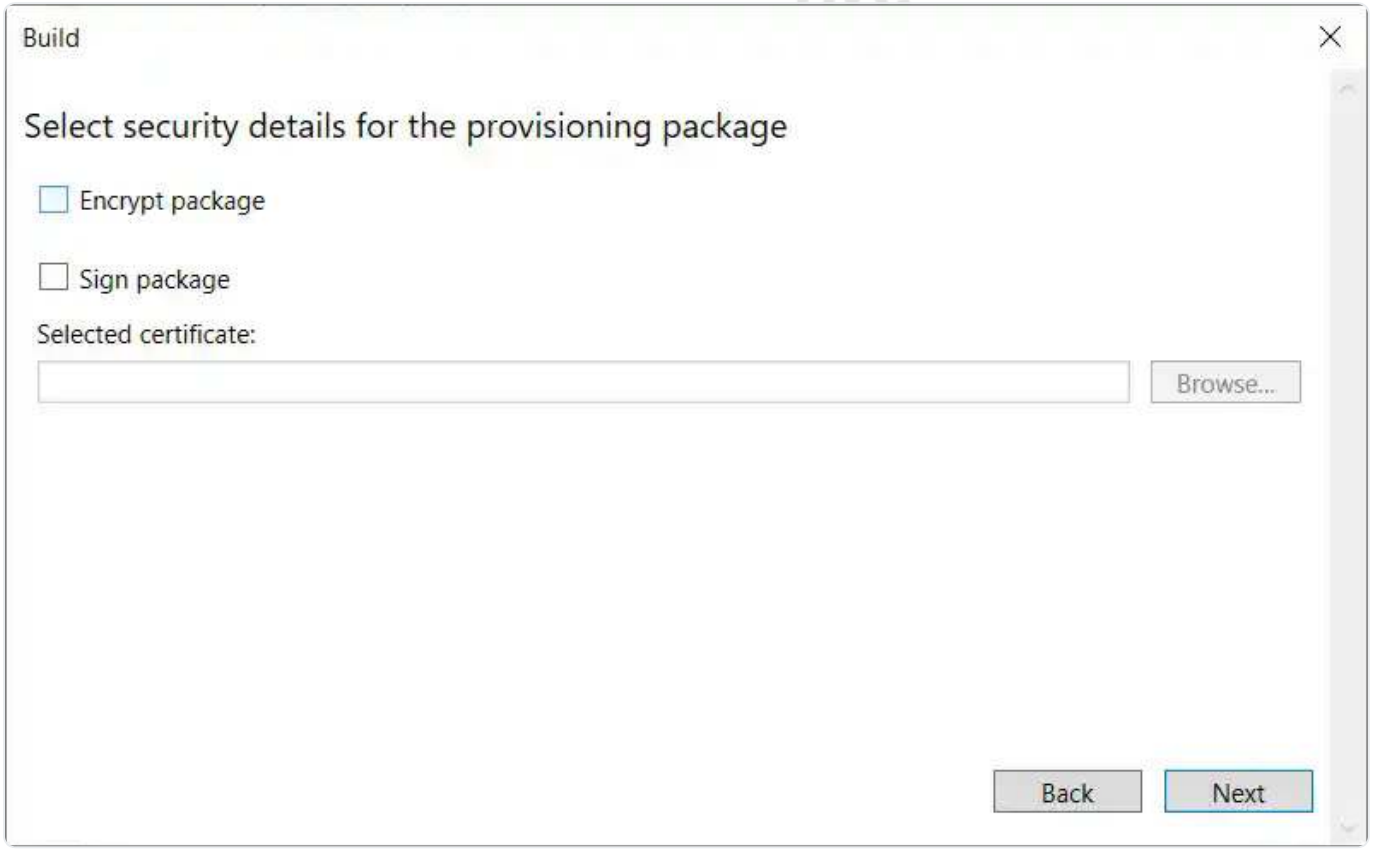
8. After all settings have been entered, `File` → `Save` is selected in the main menu.

9. After that, `Export` → `Provisioning package` is selected in the main menu.

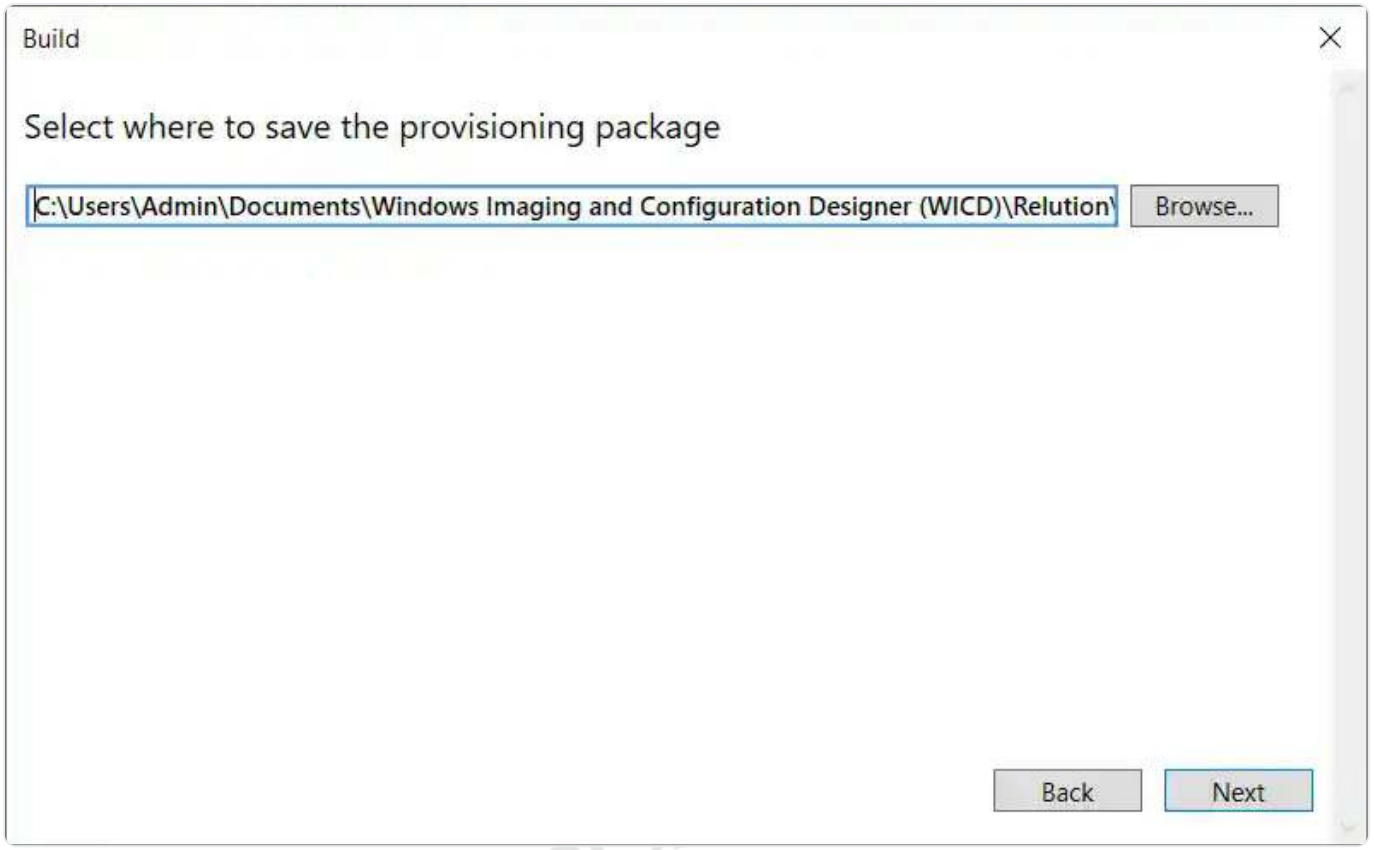


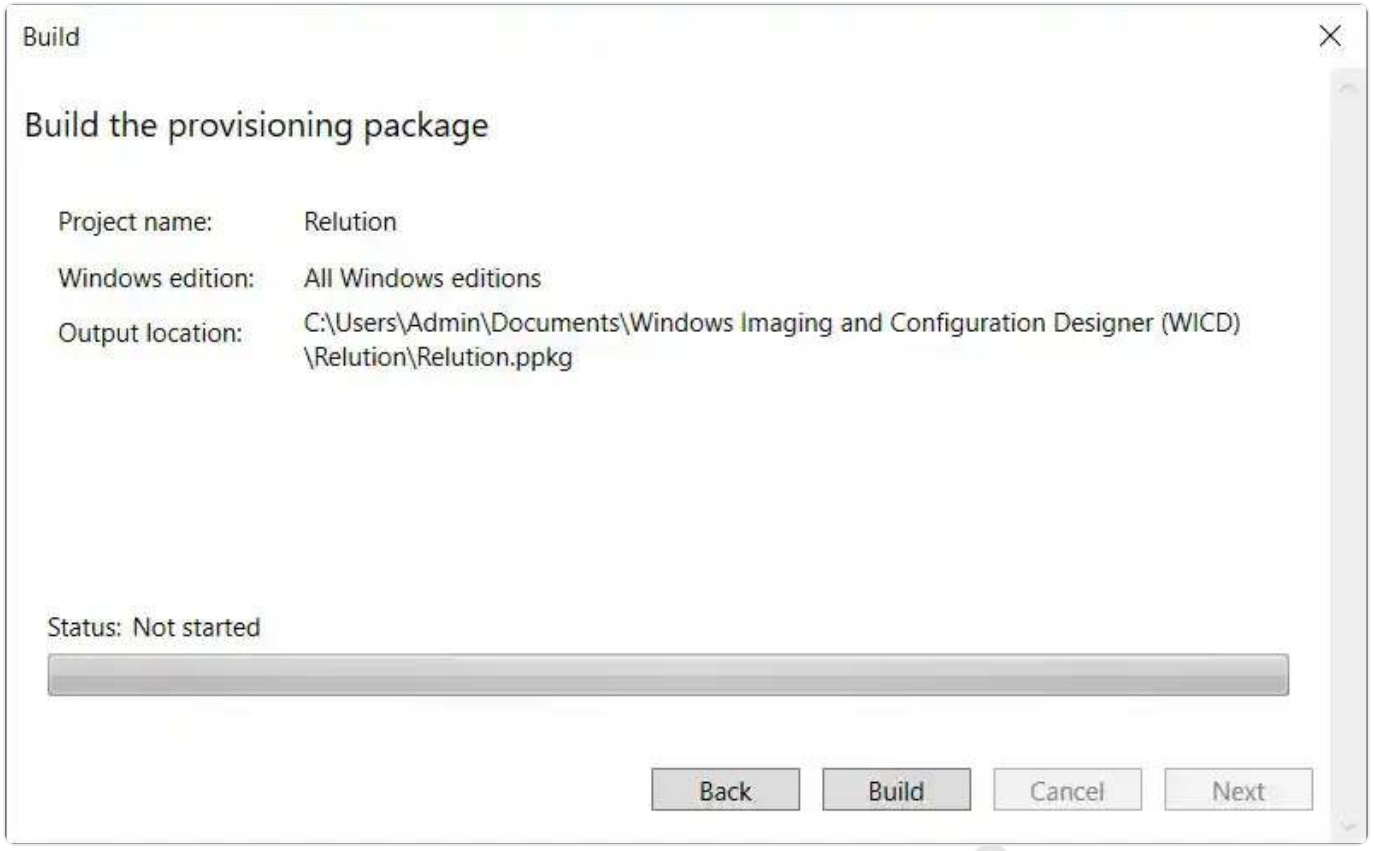
10. In the following dialog, the values for the package must be specified and the location for the package output must be chosen. Then Create must be clicked.

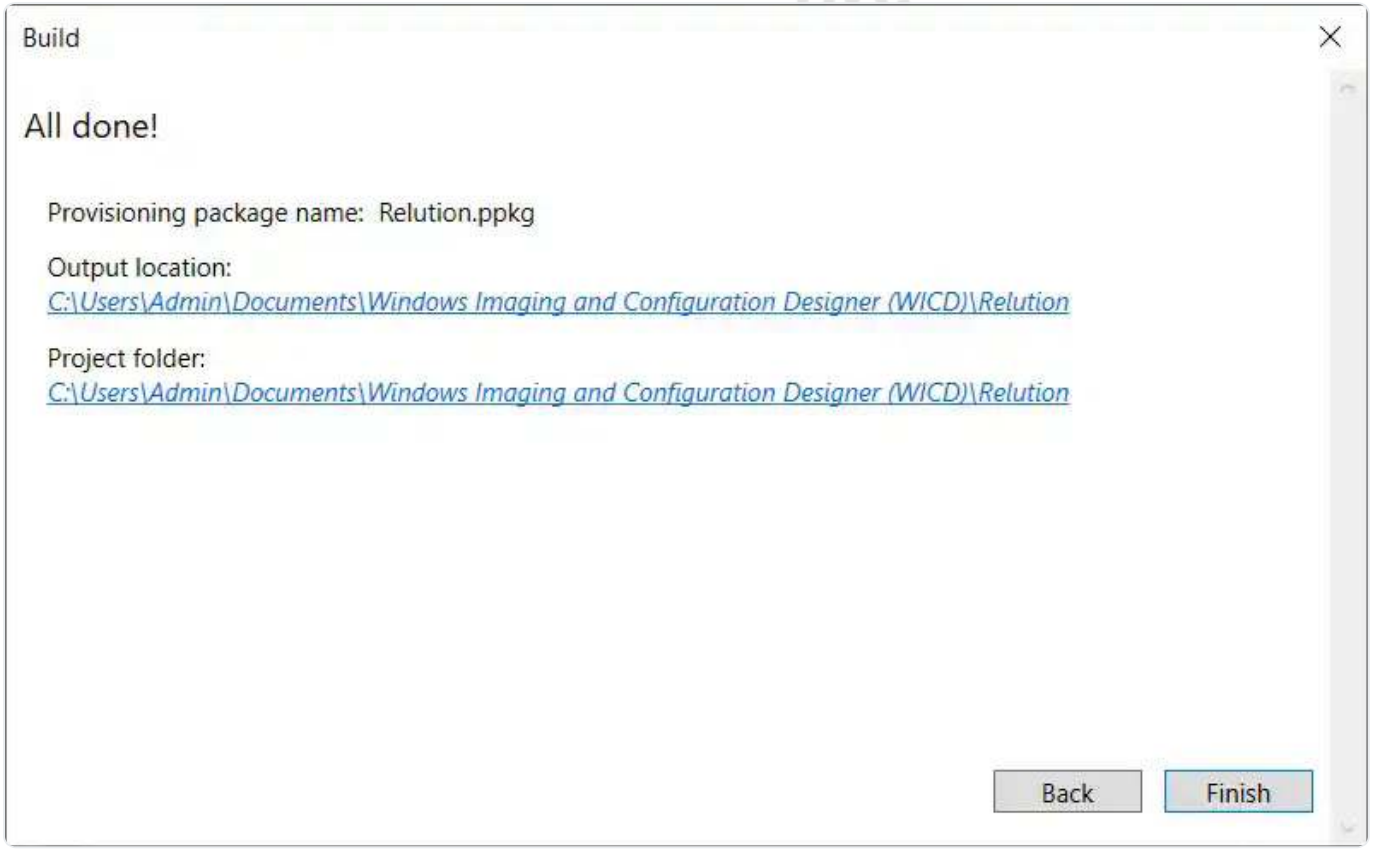

Build
Describe the provisioning package
Name:
Relution
ID:
dc6993f0-7e43-4e08-a3f8-6e1a80568b2e
Version (in Major.Minor format)
1.0
Owner:
IT Admin
Rank (between 0 - 99):
0
Next

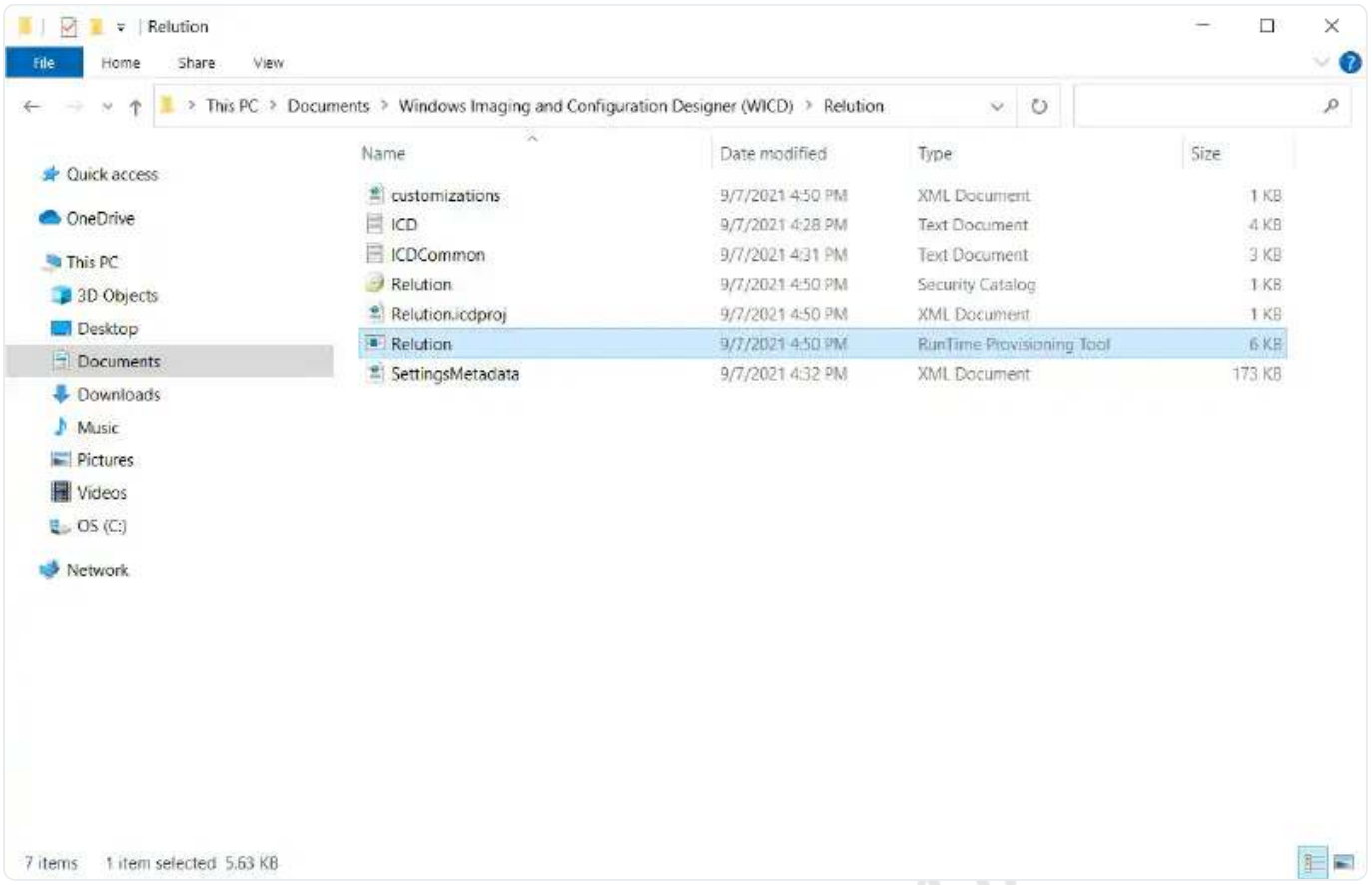

Build
Select security details for the provisioning package
Encrypt package
Sign package
Selected certificate:
Browse...
Back
Next

The provisioning package should be protected (encrypted and/or signed). This provides an extra layer of protection in case a USB stick or SD card is lost. Encryption protects against unauthorized access to the `ppkg` file.




Build
Build the provisioning package
Project name:
Relution
Windows edition:
All Windows editions
Output location:
C:\Users\Admin\Documents\Windows Imaging and Configuration Designer (WICD)
\Relution\Relution.ppkg
Status: Not started
Back
Build
Cancel
Next


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



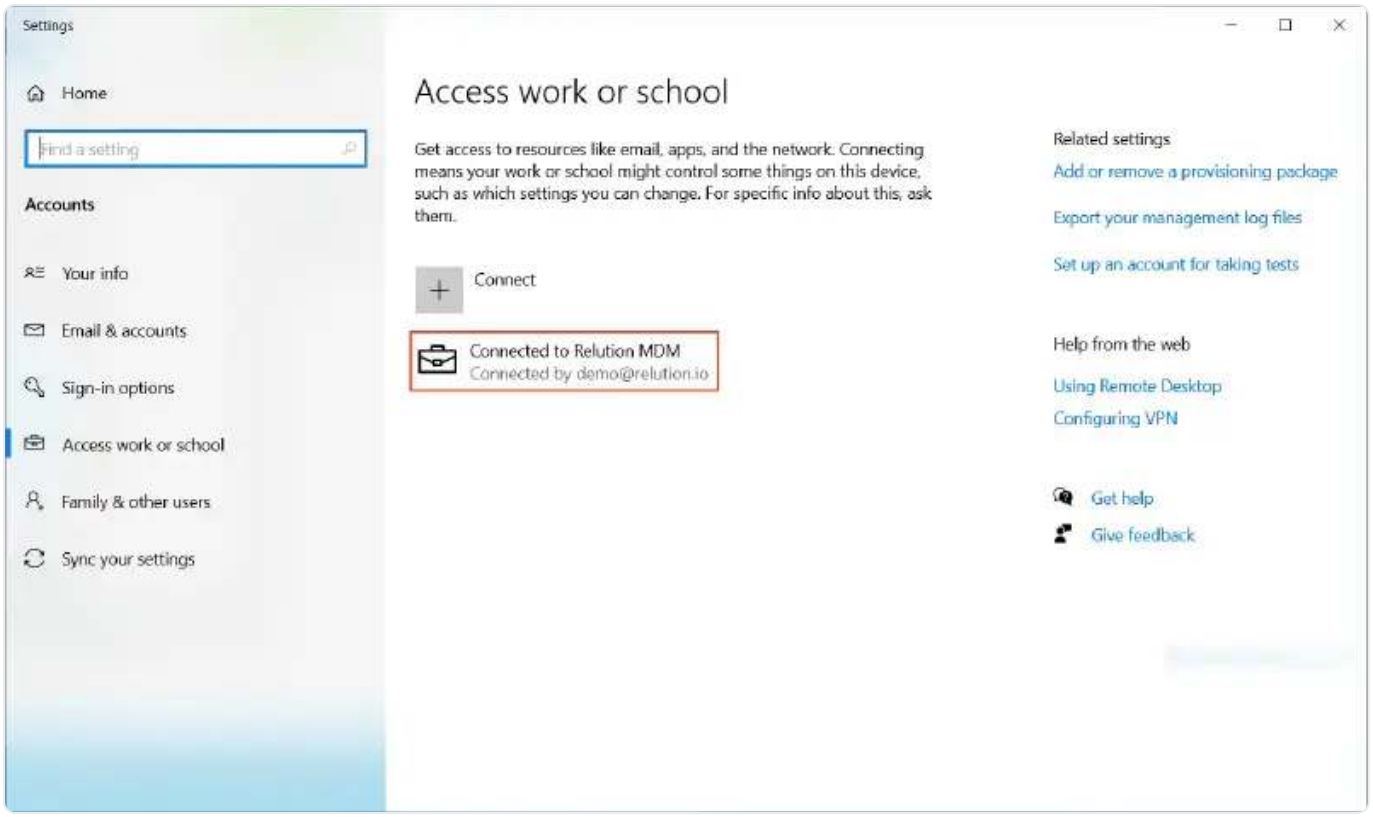
For version 26.4.0

Applying provisioning packages to Windows 10/11 devices

It is sufficient to open the `.ppkg` file on the device by double-clicking it and to confirm the dialogs. The device is then enrolled automatically. Here too, the user needs administrative permissions to perform the enrollment.

Checking the provisioning package on enrolled Windows 10/11 devices

In the Windows settings under `Access work or school`, the connection to the Relution MDM server is displayed.



The account on the device that was used to enroll the device must not be deleted.

For version 26.4.0

Autopilot

`Windows Autopilot` is a cloud-based Microsoft service that enables the automated setup of new Windows 10/11 devices for productive use. The devices do not need to be reinstalled, as `Windows Autopilot` uses the existing `image` already present on the device. Relution supports automatic enrollment through `Windows Autopilot`, allowing Windows 10/11 devices to be quickly and easily added to the Relution inventory.

Requirements for using Windows Autopilot

> Currently only available with an own Relution Server

`Windows Autopilot` can be used with Windows 10/11 Professional, Enterprise, or Education starting with version 1709. To use it, a `Microsoft Entra ID` environment, a `Microsoft Entra ID P1 or P2` license, and a `Microsoft Intune Plan 1` license are required. To configure Microsoft Entra, users must have administrative permissions, for example the `Global Administrator` role. According to Microsoft documentation, the `Microsoft Intune Plan 1` license should not be required. However, in practice it has been shown that Intune cannot be used without it. The license is only required for that purpose.

An internet connection is mandatory during the initial startup of Windows 10/11 devices so that automatic registration and setup can be completed.

Licensing requirements →

For version 26.4.0

How Windows 10/11 device provisioning works

When the `Out Of The Box Experience` (OOBE) starts on a Windows 10/11 device, the system automatically detects, if a network connection is available, that the device should be configured using `Windows Autopilot`. The device sends its ID to Microsoft and checks whether it has been registered in `Autopilot` for a `Microsoft Entra ID` environment. Users must then sign in on the Microsoft sign-in page using their credentials. After sign-in, enrollment in Relution is performed and a user account for the `Microsoft Entra ID` user is created on the device.

Advantages of Windows Autopilot

The goal of `Windows Autopilot` is to avoid the need to manually install an internally created `image` on each new Windows 10/11 device. Instead, devices should transform themselves into preconfigured devices as automatically as possible. This minimizes the effort required to create and maintain images and reduces the time needed for physical registration and provisioning of devices. Microsoft Entra only needs to be configured once, and automatic registration continues to work until the defined expiration date of the `client secret` is reached (see Link Microsoft Entra ID →).

Entra Join

Unlike `Windows Autopilot`, `Entra Join` is not intended for the automatic initial provisioning of a device, but for connecting the device to the company environment. `Windows Autopilot` is used to automatically provision and configure new devices, while `Entra Join` connects the device to the user in `Microsoft Entra ID`.

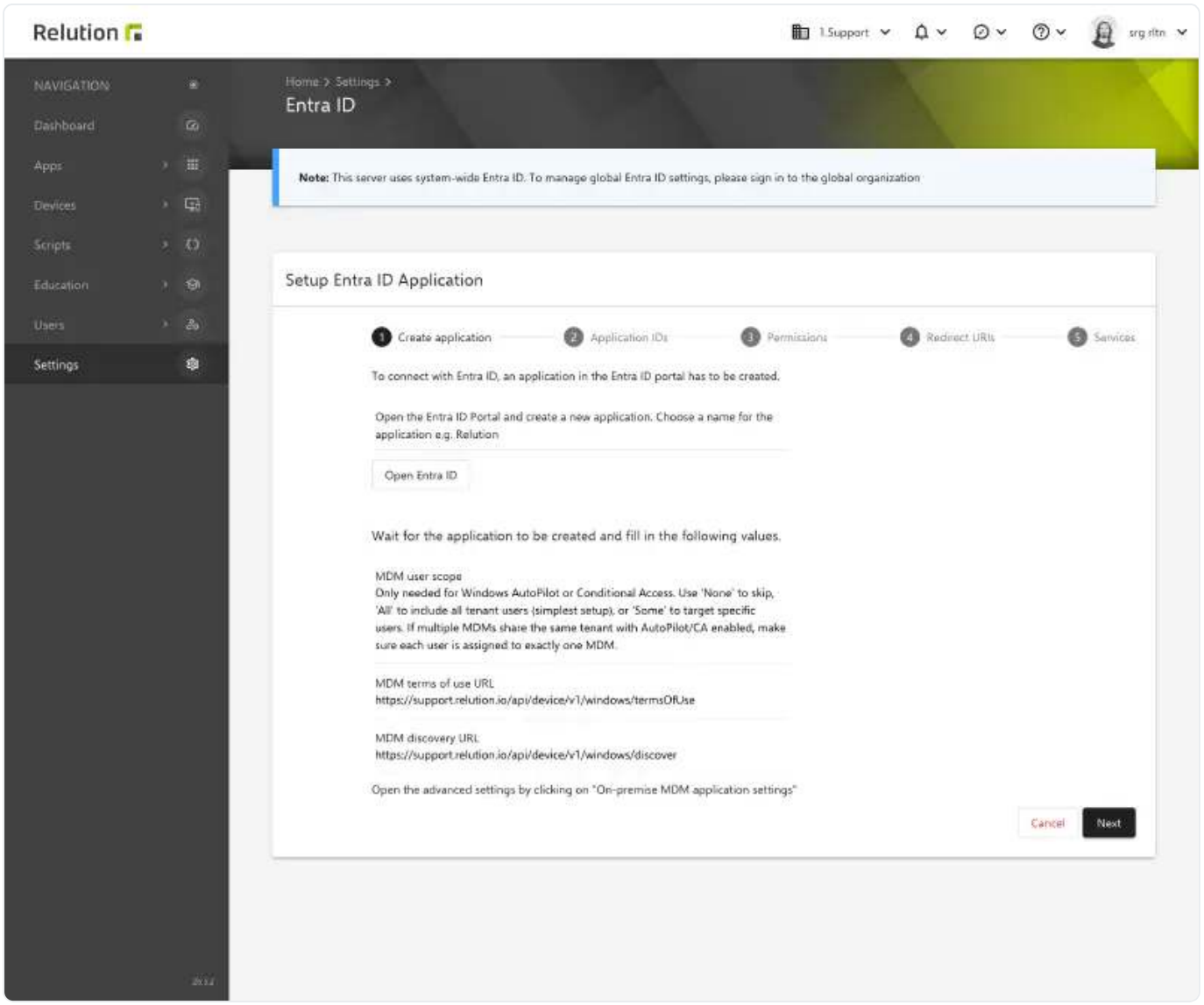
This user-based alternative to Windows Autopilot allows Entra users to enroll any Windows device. The device is joined to Entra ID via `Settings` → `Accounts` → `Access work or school` → `Connect` → `Join this device to Microsoft Entra ID`, followed by sign-in with the Microsoft user credentials. Entering credentials directly in the Connect dialog only registers the device with Entra ID (without joining it). Relution does not support this workflow and cancels it with an error.

Adding the MDM application in Entra

The MDM application is created as part of linking Relution with Entra ID →: under `Settings` → `User Management` → `Entra ID`, the first step Create application of the Relution guide provides the required values. The link is then continued in the Application IDs step with the application ID and directory ID of this application.

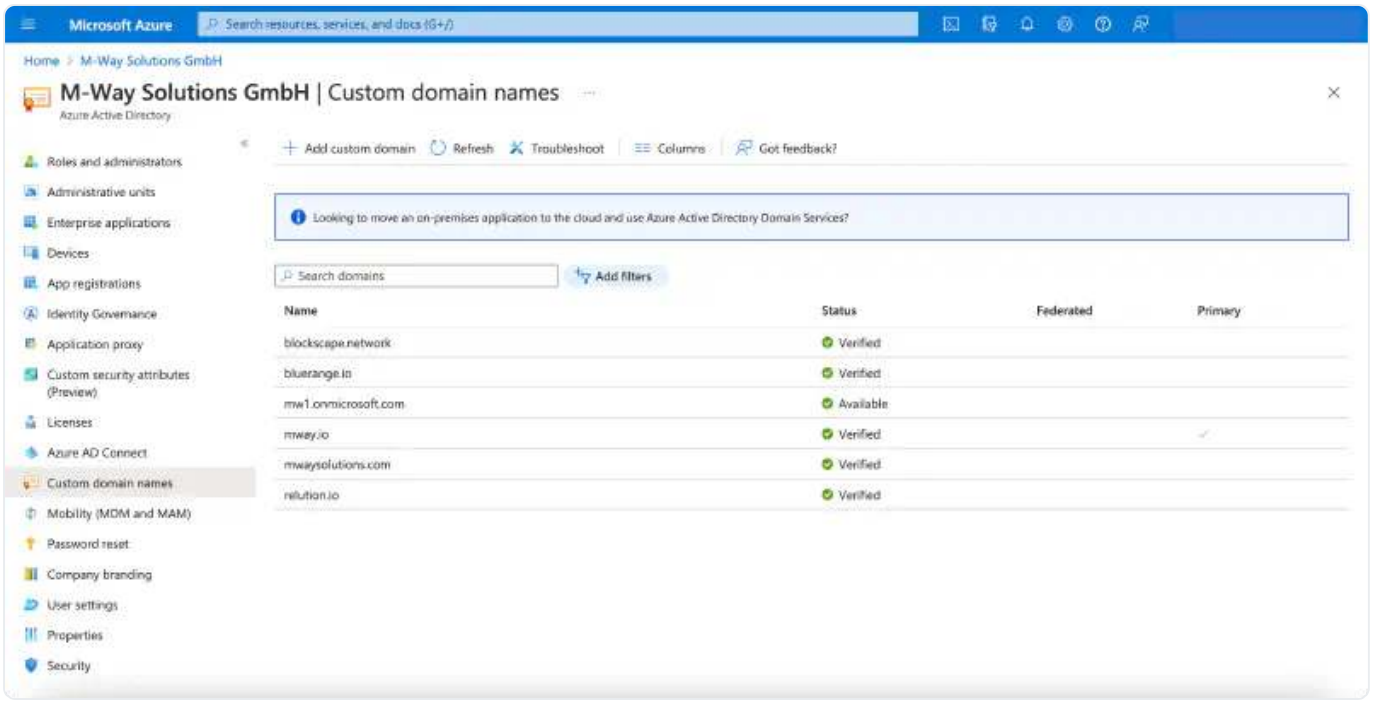
Either the existing MDM application in Microsoft Entra can be used, or a new one can be created and fully configured using the values provided in the Relution guide.

For version 26.4.0

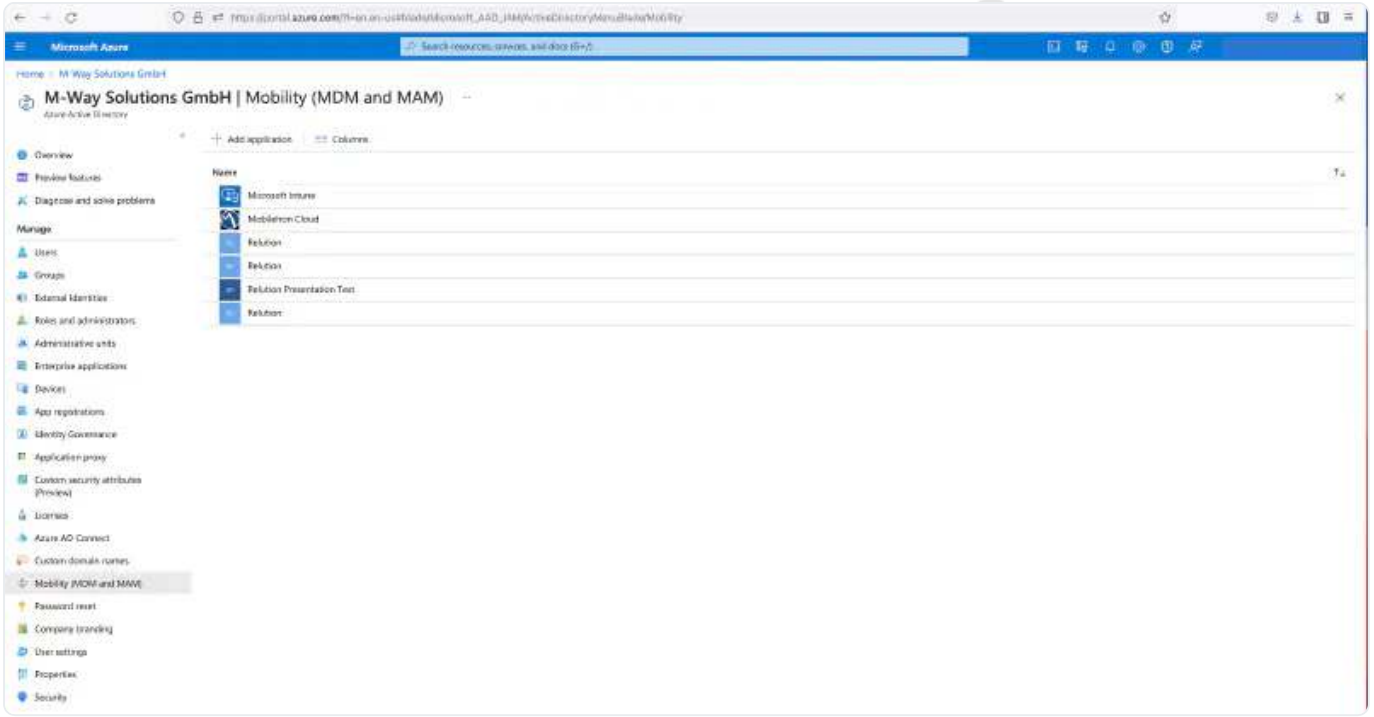


The domain of the corresponding Relution Server is added in `Microsoft Entra ID` under `Custom domain names`. This process may take some time. Further information can be found in the Microsoft documentation.

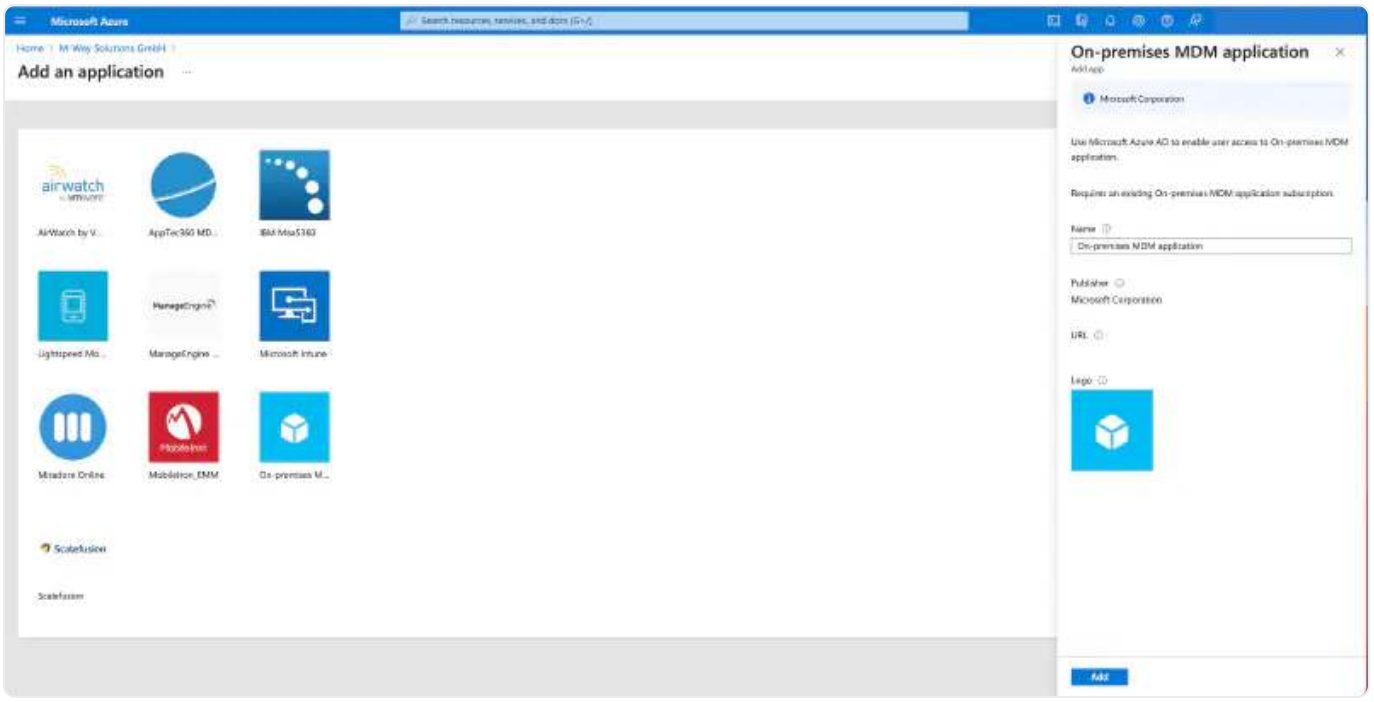
Microsoft documentation →



Under `Mobility (MDM and MAM)`, the desired MDM application is then added and activated:



1. Select the `On-premises MDM application` tile in the lower right corner.
2. Enter a name.
3. Click `Add`.



The new MDM application is then configured using the information provided in the Relution guide:

1. Select the desired setting for `MDM user scope`.
2. Enter the URL for the `MDM terms of use` from Relution:

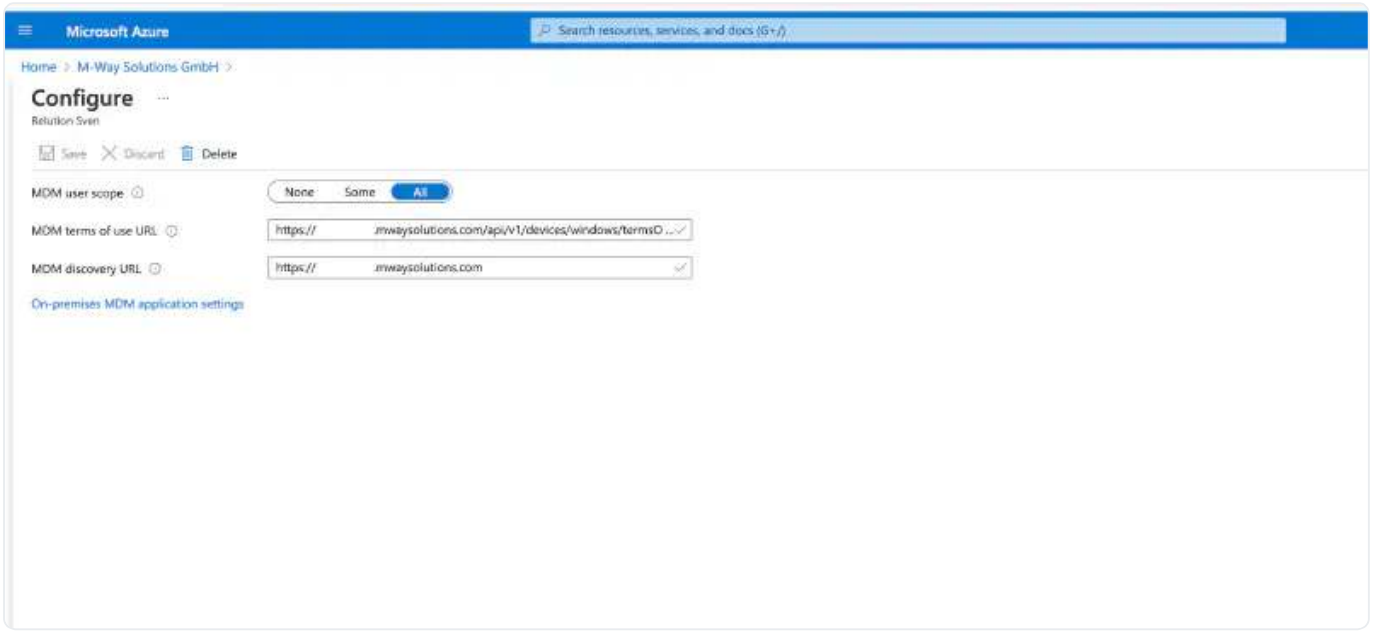
   ```
   https://serverurl/api/device/v1/windows/termsOfUse
   ```

   Microsoft checks this URL before every enrollment. No website is opened.

3. Enter the MDM discovery URL:

   ```
   https://serverurl/api/device/v1/windows/discover
   ```

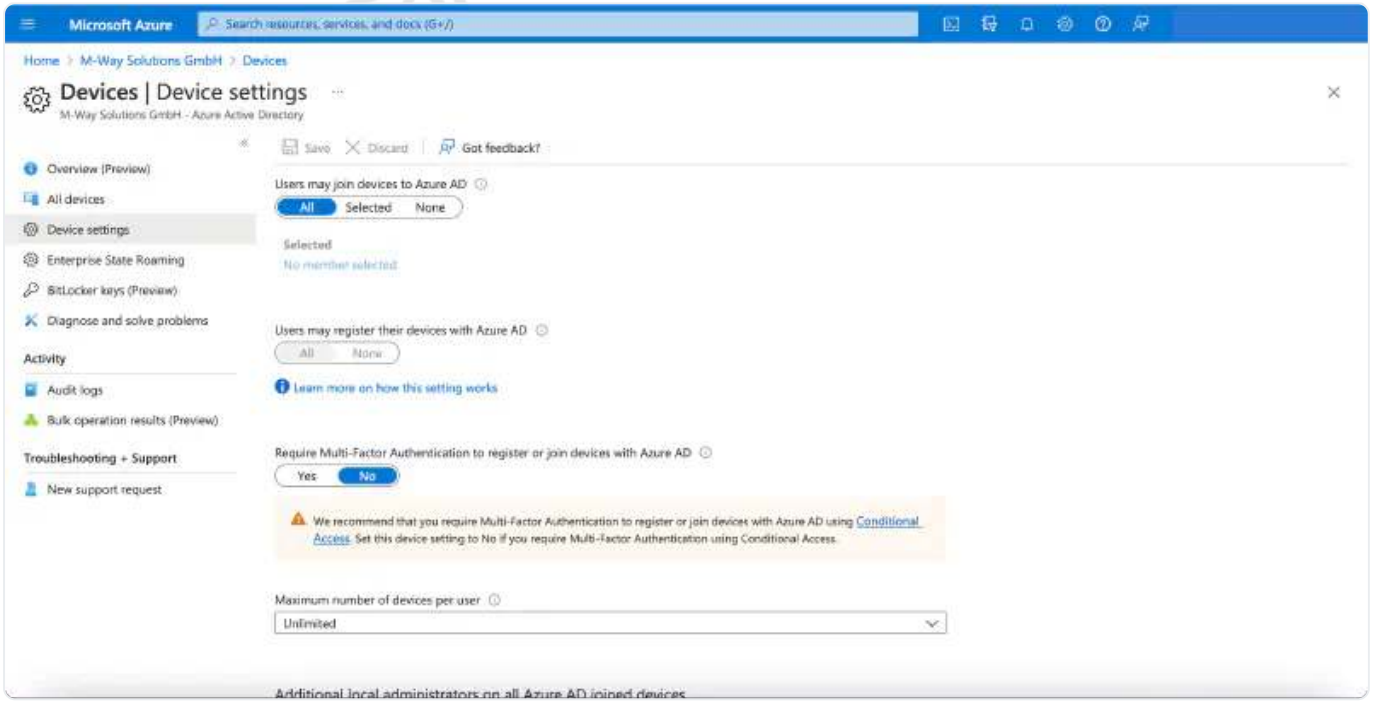
4. Click `Save`.



Check the Entra default settings and complete the setup

After linking Entra ID with Relution → has been completed, the following settings under `Devices` → `Device settings` should be checked to enable Entra Join. This step can be skipped for Windows Autopilot.

- All users may join devices to `Microsoft Entra ID`.
- All users may register their devices with `Microsoft Entra ID`.
- The maximum number of devices per user should be taken into account.



Add Windows 10/11 devices

These steps replace the previously required steps in Microsoft Store for Business.

New devices can be purchased and registered through a partner. In this case, the devices are automatically added to the Intune portal and to `Microsoft Entra ID`, so they do not need to be entered manually.

Devices that have already been used can be added manually. For this, a `CSV` file is required, which is generated on the devices using a PowerShell script. The CSV file is then uploaded to the Intune portal →, and the device can be reset afterward.

The file can be generated with the following script using PowerShell:

```
[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
```

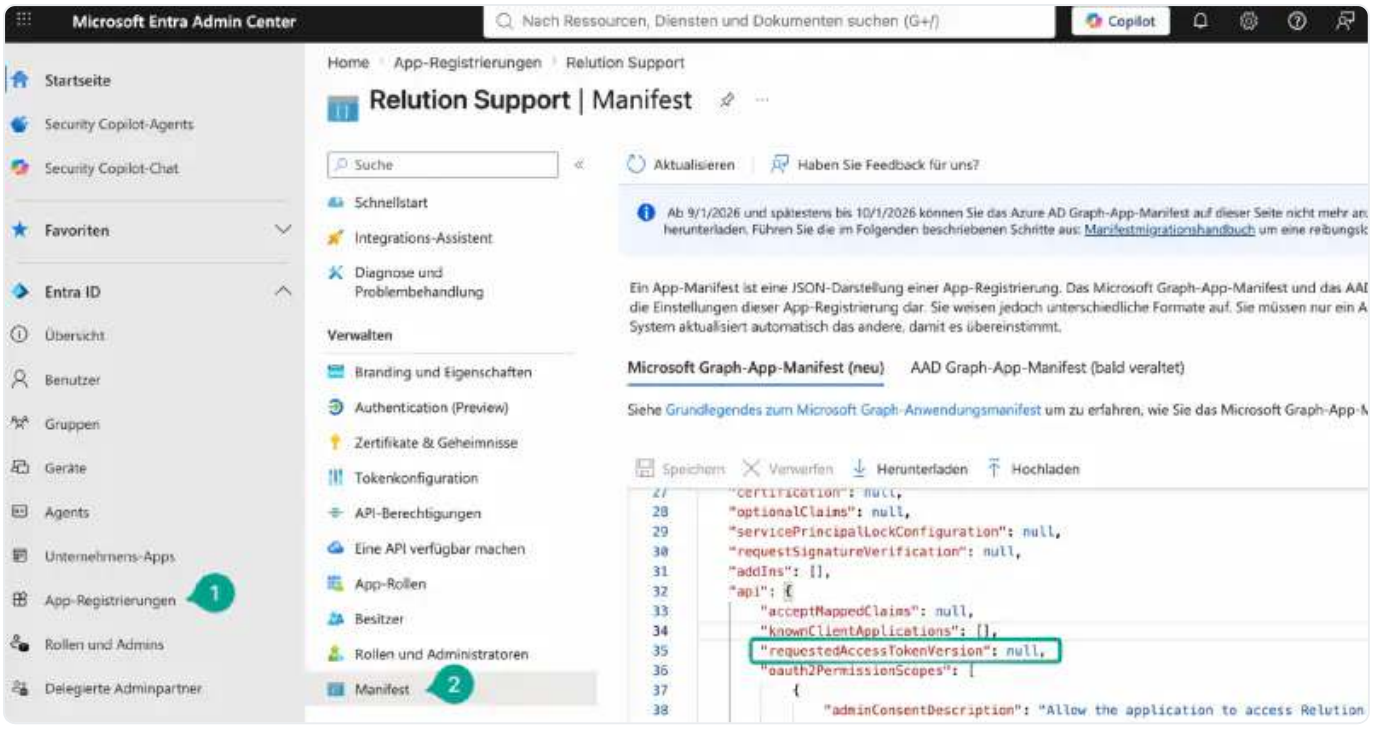
PowerShell must be run as Administrator.

The file must then be uploaded under `Devices` → enter `Enrollment` in the search → click the search result → scroll down on the right-hand side → `Devices` → `Import`.

The devices then appear in the device list and must be assigned to a configured profile.

> If the Entra ID application was created after July 1, 2026, an additional adjustment may be required if devices display an error during OOBE indicating that no connection can be established to the URL of the MDM Terms of Use. In this case, the manifest entry `requestedAccessTokenVersion` of the application must be set to `null` (`"requestedAccessTokenVersion": null,`).

For version 26.4.0



Prepare the Out Of The Box Experience (OOBE) in Microsoft

Next, a profile must be created.

To do this, the feature search is opened again: `Devices` → enter `Enrollment` in the search → scroll down on the right-hand side → `Deployment profiles`.

1. Click `Create profile`.
2. Select `Windows PC`.
3. Enter a name.
4. Click `Next`.
5. Click `Next` again.
6. Select either `Add group` or `Add all devices`.
7. Click `Next`.
8. Click `Create`.

The devices are now linked to the profile.

Synchronize stored Windows 10/11 devices with Relution

Under `Devices` → `Auto Enrollments`, the Windows 10/11 devices can be added to Relution using the Sync devices button. This requires the Sync Autopilot devices option to be enabled in the Entra ID link (Services step of the Relution guide). At this point, the devices must not yet be enrolled.

The same step contains the Enable Autopilot enrollment option, which should remain enabled for Windows Autopilot. Both options are enabled by default for a new link.

In addition, Relution synchronizes the Autopilot devices automatically, every 24 hours by default. Devices that are no longer registered in Windows Autopilot are removed from the auto enrollments in the process.

Automatic enrollment through Windows Autopilot can only be carried out once the Windows 10/11 devices appear in the overview.

Automatic enrollment of Windows 10/11 devices in Relution

After the devices have been reset, or when they are started for the first time, the network connection is established during OOBE. As soon as this is done, the devices communicate with Microsoft Entra and download the `Autopilot` profile.

The Microsoft account sign-in screen then appears. After users enter their credentials, communication with Relution takes place. First, the terms-of-use endpoint is called, and then enrollment in Relution is performed.

Enrollment requires exactly one user in Relution whose email address matches the Entra sign-in name (UPN), and an auto enrollment for the device. If a user is assigned to the auto enrollment, only this user can perform the enrollment. The Windows 10/11 devices then appear in the device inventory of this user's organization and can be further configured using Windows policy configurations and actions.

If a device enrolled through Windows Autopilot is deleted in Relution, it can be enrolled again using the same auto enrollment, even while it is still in the trash.

> The account on the device that was used to register the device must not be deleted.

For version 26.4.0

Available actions

Relution provides a wide range of remote actions to centrally manage and secure Windows devices. These functions support central administration, increase security and simplify deployment and troubleshooting in corporate or educational environments. The actions can be applied to a single device or, via multiple selection in the device list, to several devices at once. They can also be triggered by event or on a schedule through device group membership: Device group actions →

The action dialog is opened under `Devices` → `Inventory` via Apply action, either for the devices selected in the list or in the detail view of a device. The following list summarizes all device actions currently supported for Windows devices in Relution:

For version 26.4.0

Available Device Actions

Action	Description
Remove app	Uninstalls selected apps from the device. MSI, EXE and WinGet apps from the Relution Store can be removed. According to the notice in the action dialog, the apps are removed only for the currently managed user; other users can still see and use them. Use case: Removes unwanted or outdated apps. Requirement: Relution Companion; Windows 10 version 1511 or later, not available for Windows Home.
Add Accounts	Adds new local user accounts to the device. A User name and Password are specified for each account; the Administrator toggle grants the account administrator rights. If the password does not meet the complexity requirements set on the device, the account is not added. Use case: Onboarding new users with separate local profiles. Requirement: Windows 10 version 1803 or later, not available for Windows Home.
Enable Bitlocker	Enables BitLocker on one or more drives and starts encryption. For each drive, the drive letter (e.g. `C:`) and the Protector are specified: Recovery Password or TPM (operating system drive only). With Used space only, only the used space is encrypted instead of the full drive. Use case: Adds protection by encrypting the drives. Additional info: If Recovery Password is selected as protector, the recovery password is generated automatically and saved in the device details in Relution. Requirement: Relution Companion.
Disable Bitlocker	Disables BitLocker on one or more drives. Use case: Removes protection by decrypting the specified drives. Requirement: Relution Companion.
Wipe device	Resets the device to factory settings and deletes all data. Use case: Prepares for re-use or removes compromised systems. Caution: All data is deleted permanently! Requirement: Windows 10 version 1709 or later, also available for Windows Home.
Reboot device	Restarts the device. Use case: Applies changes or resolves system issues.
Locate device	Queries the current location of the device. Use case: Helps track and recover lost or stolen devices. Note: Requires an internet connection and enabled location services.
Scan Device	Starts a Microsoft Defender scan for malware and security threats. The Scan Type is either Quick Scan or Full Scan. Use case: Ensures compliance and detects threats. Note: Microsoft Defender is the antivirus software built into Windows. Requirement: Windows 10 version 1809 or later, also available for Windows Home.
Refresh device info	Updates the device information stored in Relution. Use case: Keeps device info up to date.
Deploy Office 365	Installs Office 365 for Business on the device. Install Office 365 Configuration uploads a Configuration XML created in the Microsoft 365 Apps admin center (`config.office.com`). Clear Office installation data

Action	Description
	removes the installation data on the device so that a failed installation can be attempted again; optionally, the installed Office suite is uninstalled in the process without losing any files. Use case: Easy deployment of Office 365 on company devices. Requirement: Windows 10 version 1703 or later, not available for Windows Home.
Reset password (Windows)	Sets a new password for a local user account on the device. The user name and the new password are specified. Use case: Support for forgotten or locked passwords. Requirement: Relution Companion.
Execute PowerShell script	Runs a PowerShell script managed in Relution on the device. Optionally, Command line arguments, Environment variables and a Timeout (in minutes) are set. Use case: Automates complex configuration tasks. Note: PowerShell knowledge required. Requirement: Relution Companion; Windows 10 version 1511 or later, not available for Windows Home.
Deploy Relution store app	Installs an app from the Relution Store on the device. The available types are Deploy Microsoft Store app, Install MSI app, Install exe and Deploy winget app; each type requires its own permission. The apps are installed system-wide, except for WinGet apps, which are installed for the logged-in user. Use case: Distributes company-approved apps on Windows devices. Requirement: Windows 10 version 1511 or later, not available for Windows Home. MSI, EXE and WinGet apps require the Relution Companion.

For version 26.4.0

Requirements

Several actions are executed exclusively by the Relution Companion for Windows →: Remove app, Enable Bitlocker, Disable Bitlocker, Reset password (Windows), Execute PowerShell script and the deployment of MSI, EXE and WinGet apps via Deploy Relution store app.

Some actions require a minimum version and edition of Windows. The action dialog marks the supported editions with badges. On Windows Home, Remove app, Add Accounts, Deploy Office 365, Execute PowerShell script and Deploy Relution store app are not available: Windows Home limitations →

Available configurations

A policy is a collection of one or more configurations. Each policy can be applied to one or more devices at the same time. In addition, one or more policies can be associated with each device.

For version 26.4.0

Available configurations

Configuration	Description
Antivirus	Manages antivirus settings
App compliance	Manages app-specific restrictions (Windows 10 version 1511 or later, not available for Windows Home)
App Control →	Manages Windows Defender Application Control (WDAC) policies (Windows 10 version 1903 or later, not available for Windows Home)
Bitlocker →	Configures disk encryption (Enterprise and Education from Windows 10 version 1703, Pro from version 1809, not available for Windows Home)
BranchCache	Configures BranchCache content caching (Windows 10 version 2004 or later, not available for Windows Home)
Certificate →	Selects a certificate to be installed on the device by default
Custom CSP →	Combines any CSP settings in a single configuration
Device name →	Configures the device name
E-mail	Adds email configurations for multiple users
Exchange →	Manages Exchange accounts
Global proxies	Configures global proxies (Windows 10 version 1703 or later, not available for Windows Home)
Local device security options	Manages policies for local device security options
Passcode →	Manages password policies
Remote desktop service	Manages the Remote Desktop service
Restrictions →	Manages device restrictions
Script →	Manages automatic script execution based on events or schedules via the Relution Companion
Shared PC →	Manages the Windows Shared PC policy
Start menu	Personalizes the Start menu (Windows 10 version 1703 or later, not available for Windows Home)
VPN →	Manages VPN settings (Windows 10 version 1607 or later, also available for Windows Home)
Wallpaper	Manages the background image (Windows 10 version 1709 or later, not available for Windows Home)

Configuration	Description
Wi-Fi →	Manages Wi-Fi settings
Windows Companion →	Manages the behavior of the Relution Companion for Windows: logging, app handling, server communication and automatic device user change
Windows Firewall →	Manages Windows Firewall settings (Windows 10 version 1709 or later, not available for Windows Home)
Windows Hello →	Manages the Windows Hello configuration
Windows Kiosk Mode →	Manages kiosk mode settings
Windows Licensing	Manages the Windows licensing policy
Windows Office →	Deploys Microsoft Office via an externally created configuration XML (Windows 10 version 1703 or later, not available for Windows Home)
Windows Update →	Manages the Windows Update policy (Windows 10 version 1607 or later, not available for Windows Home)

The configurations App Control, Custom CSP, E-mail, Exchange, Script, VPN, WiFi and Certificate can be added to a policy multiple times, all others only once. If a configuration that is allowed only once is already part of the policy, it is no longer offered in the selection dialog.

In the selection dialog, badges indicate the supported Windows editions and the respective minimum version; the details in brackets reflect these badges. Further limitations of the Home edition are described in Windows Home limitations →

The Script and Windows Companion configurations are applied by the Relution Companion for Windows →.

For version 26.4.0

App Control

With version 5.24.0 the configuration App Control has been introduced. With this feature, Windows Defender Application Control (WDAC) policies can be applied to Windows devices. These policies define which applications are trusted, allowing only those trusted applications to run on the device. The configuration is supported on Windows Pro, Enterprise and Education version 1903 and later.

Microsoft provides all necessary information for WDAC policies in their documentation →.

WDAC policy generation

Microsoft explains the design and creation of WDAC policies in their design guide →.

It is recommended to thoroughly test any WDAC policies before deploying them to production devices via Relution.

It must be ensured that the *Relution Windows Companion* application is not blocked or restricted by the defined rules.

Create the needed WDAC policy file

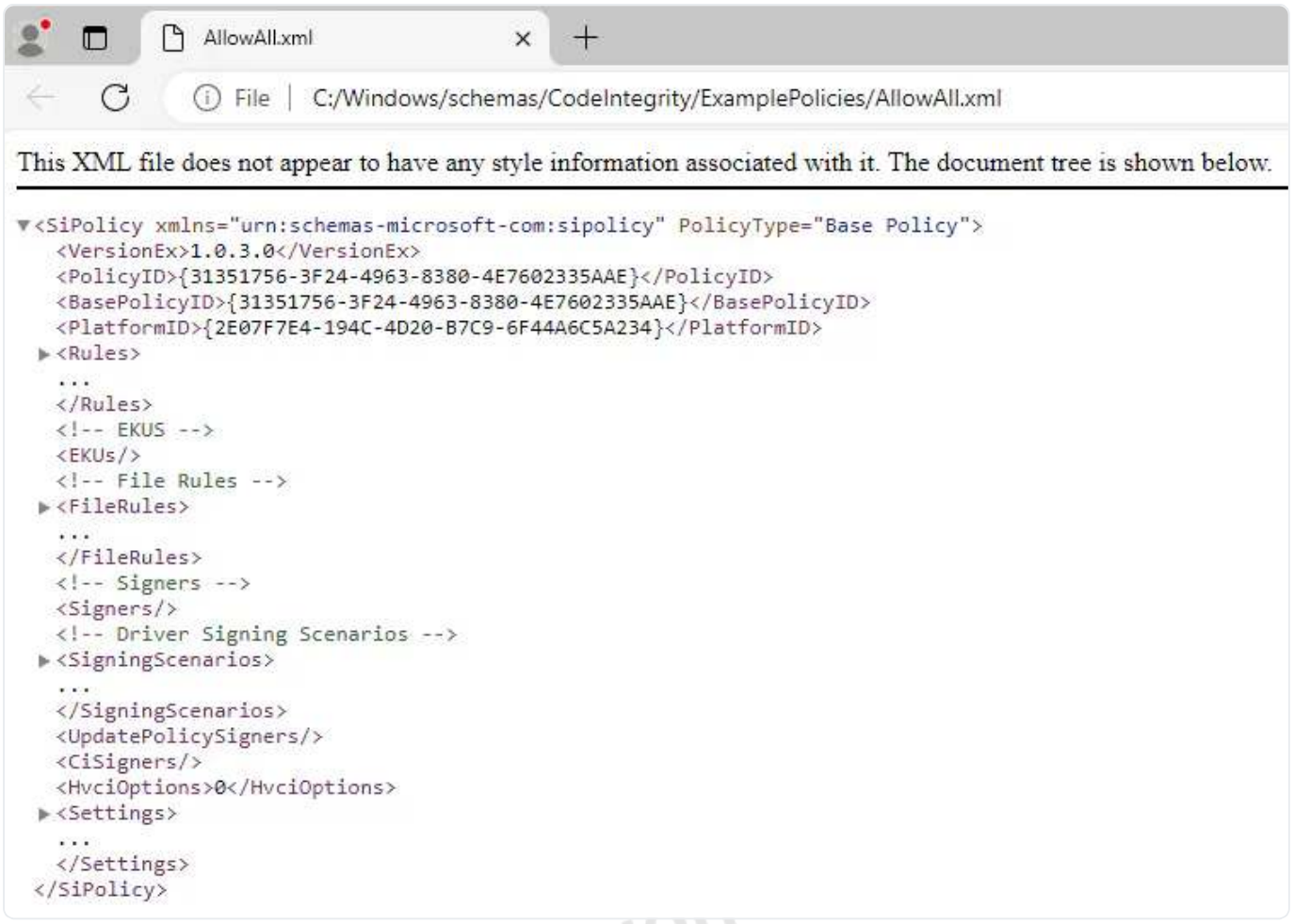
For version 26.4.0

For the generation the WDAC Wizard → and the example base policies → can be used.

The Windows Defender Application Control (WDAC) Policy Wizard generates two files when used for policy generation: an XML file and a CIP file. The MDM interface of Microsoft requires the policy as a binary file. The CIP file is already in this binary format and can be uploaded to Relution directly. The XML file must first be converted into a binary file; this is explained in the following sections.

Xml file

The WDAC policy xml file contains two pieces of information that are critical to successfully applying the configuration to the Windows devices via Relution.



The `<PolicyID>` is a GUID that uniquely identifies this WDAC policy. It is therefore used for applying, updating and deleting the configuration.

The `<VersionEx>` is used as versioning for the WDAC policy. Therefore, `<VersionEx>` must be increased for every update of a WDAC policy. If the version is lower than the most recently applied one, Windows rejects the policy and the update of the configuration via Relution fails.

Convert the xml file

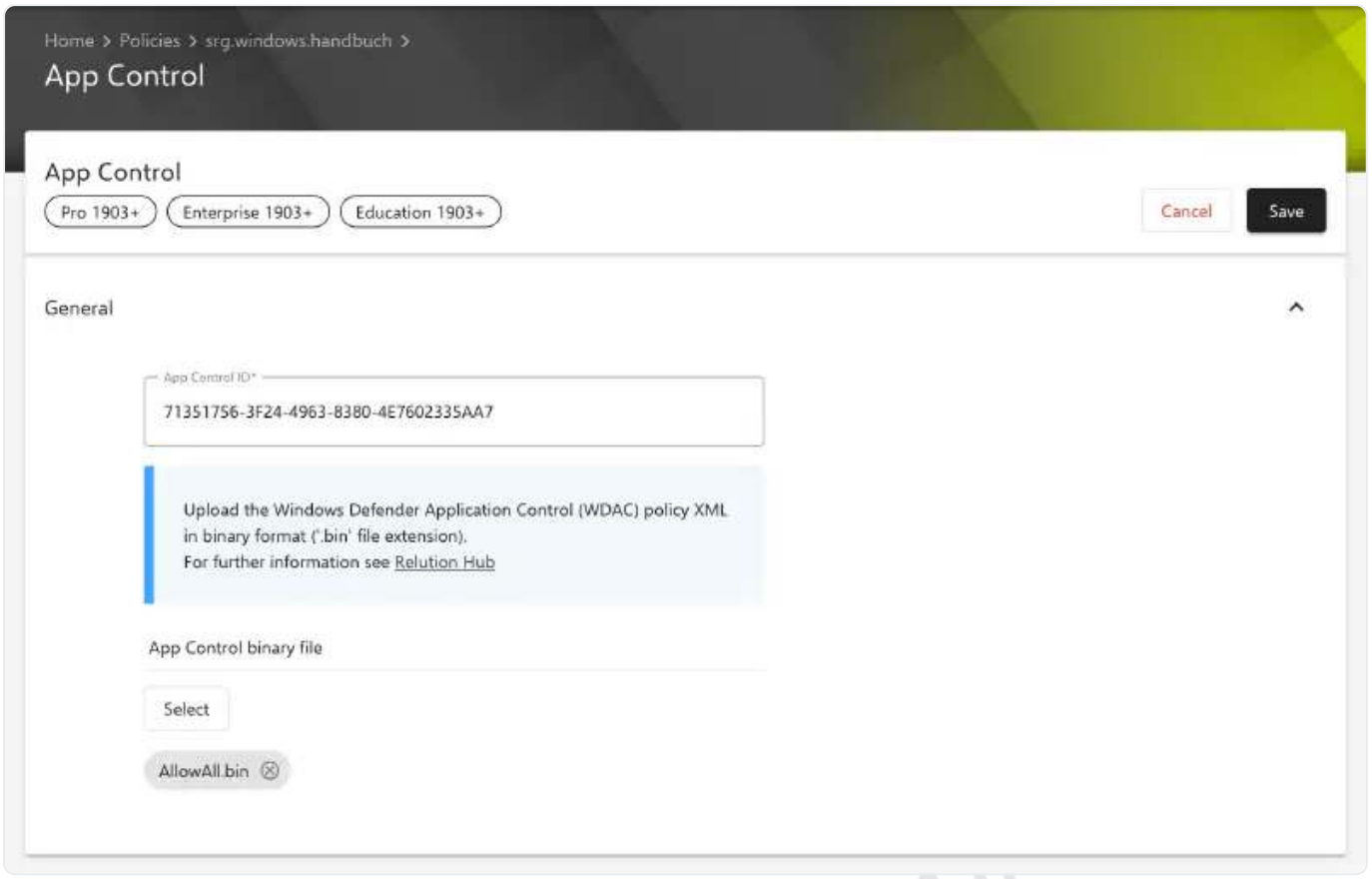
The xml file must be converted into a binary file. This can be done using the ConvertFrom-CIPolicy → PowerShell command.

Example:

```
ConvertFrom-CIPolicy -XmlFilePath .\AllowAll.xml -BinaryFilePath .\AllowAll.bin
```

The resulting binary file can be uploaded to Relution in the App Control configuration.

App Control configuration



The App Control configuration consists of two mandatory fields:

- Field App Control ID: For the configuration to be successfully applied to the device, the App Control ID must contain the same value as the `<PolicyID>` from the WDAC policy, but without the curly brackets. A GUID in the format `XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX` is expected; other input is marked as invalid.
  - Example:
    - PolicyID in WDAC policy: `<PolicyID>{31351756-3F24-4963-8380-4E7602335AAE}</PolicyID>`
    - App Control ID in configuration: `31351756-3F24-4963-8380-4E7602335AAE`
  - It is not possible to change the entered App Control ID after saving for the first time. However, it is possible to create several (complementary) App Control configurations and apply them to one device.
- Field App Control binary file: upload of the WDAC policy in binary format, see WDAC policy generation →. The note in the form mentions the `.bin` file extension. Relution does not check the extension, however, so the CIP file of the WDAC Wizard can also be uploaded without renaming it.

Update

In order for a new version of the App Control configuration to be successfully applied to the device, the `<PolicyID>` in the WDAC policy must have the same value as the App Control ID of the configuration and the `<VersionEx>` must have a value higher than in the previous version.

Delete

In order for deleting a WDAC policy to be applied to the device, a device restart is required.

Microsoft recommends a workaround so that the app restrictions are removed without restarting, see Microsoft documentation →.

Delete an unsigned application control configuration

In Relution, removal without restarting can be implemented as follows:

1. Creation of an *Allow-All* WDAC policy
    - The `<PolicyID>` must match the App Control ID
    - The `<VersionEx>` must be higher than the previous version
2. Conversion of the XML file into the required binary format
3. Creation of a new policy version in Relution
    - Upload of the new binary file of the *Allow-All* WDAC policy to the App Control configuration
4. Publication of the new policy version
    - This removes the existing restrictions from the device
5. Removal of the policy from the device
    - This deletes the App Control configuration from the device. However, this is only active after the restart.

Delete a signed application control configuration

Removing a signed WDAC policy (without requiring a restart) can therefore be implemented in Relution as follows:

1. Creation of a signed WDAC policy that allows unsigned WDAC policies
    - The `<PolicyID>` must match the App Control ID
    - The `<VersionEx>` must be higher than the previous version
2. Conversion of the XML file into the required binary format
3. Creation of a new policy version in Relution
    - Upload of the new binary file of the signed WDAC policy (allowing unsigned WDAC policies) to the App Control configuration
4. Publication of the new policy version
    - This allows unsigned WDAC policies to be applied on the device
5. Delete an unsigned application control configuration →

For version 26.4.0

Custom CSP

The MDM interface uses Configuration Service Provider (CSP) policies for managing Windows devices. These policies are applied, removed, and queried on the device using the SyncML Protocol →, a specialized XML-based format. The complete list of available CSP policies can be found in the official Microsoft MDM documentation →.

With the Custom CSP configuration, any combination of CSP policies can be combined into one or more configurations of this type and applied to Windows devices. This means that the functionality available through the MDM interface is only limited by the CSP policies offered by Microsoft. Microsoft continuously extends these policies. An overview of the latest changes is available in the official Microsoft documentation →.

Important Notes

When working with the Custom CSP configuration, the configurations are not implemented by Relution; Relution therefore accepts no liability for any resulting damage. The CSPs used should be reviewed and tested carefully before being applied to a device. Further guidance can be found under Best practices →.

Some CSPs may also be used internally by Relution. In such cases, conflicts can occur that may impair or overwrite Relution-managed configurations.

For version 26.4.0

Functionality

The following specifics of the SyncML protocol need to be considered when using CSP policies.

General

Not all CSP policies can be applied to every device. They depend on the Windows *edition* and *operating system version*. Relevant details are provided in the documentation of each individual CSP. If a device does not meet the requirements, deployment of the CSP policy will fail.

CSP policies can be applied in the device or user context →. The user context only applies to the user who enrolled the device. Therefore, it is generally recommended to use CSP policies in the device context.

Not all SyncML commands are supported for every CSP. Some CSPs may be read-only and only support querying (e.g., the *Get* command).

Example: To allow or block Cortana on a device (already included in the Relution configuration *Restrictions*), the following CSP can be used: Policy CSP/Experience/AllowCortana →.

- This CSP can be used for *all editions* and from *version 1507* onwards
- Only the device context is supported
- These SyncML commands are allowed: Add (*Add*), Delete (*Delete*), Get (*Get*), Replace (*Replace*).

Add and Replace

SyncML contains several specifics that need to be considered for the deployment of the configuration.

Some CSP policies must initially be applied using the *Add* command. For subsequent deployments of the configuration (updates), the *Add* command may fail if the setting already exists. In such cases, the *Replace* command must be sent instead, see also Best Practices →.

Delete

A CSP policy can be removed by issuing a *Delete* command on the specific node. In some cases, it is also possible to delete a parent or *root* node. In these cases, all CSP policies under the deleted node will be removed.

If the deletion fails, the affected CSP policies remain active on the device. In that case, the Delete SyncML field must be adjusted accordingly. After that, the policy should be reapplied and then removed again.

Atomic and Sequence

The *Sequence* command allows multiple CSP policies to be grouped and executed sequentially within it. However, if one policy fails, the remaining ones will still be applied. This can lead to inconsistent or unintended behavior. Additionally, the failed CSP policy may need to be explicitly removed.

When the SyncML is executed within an *Atomic* command, the entire command will be rolled back if any single CSP policy fails. This ensures that either all changes are applied or none at all. Therefore, the *Atomic* command is preferred and, for the time being, is the only one supported.

For version 26.4.0

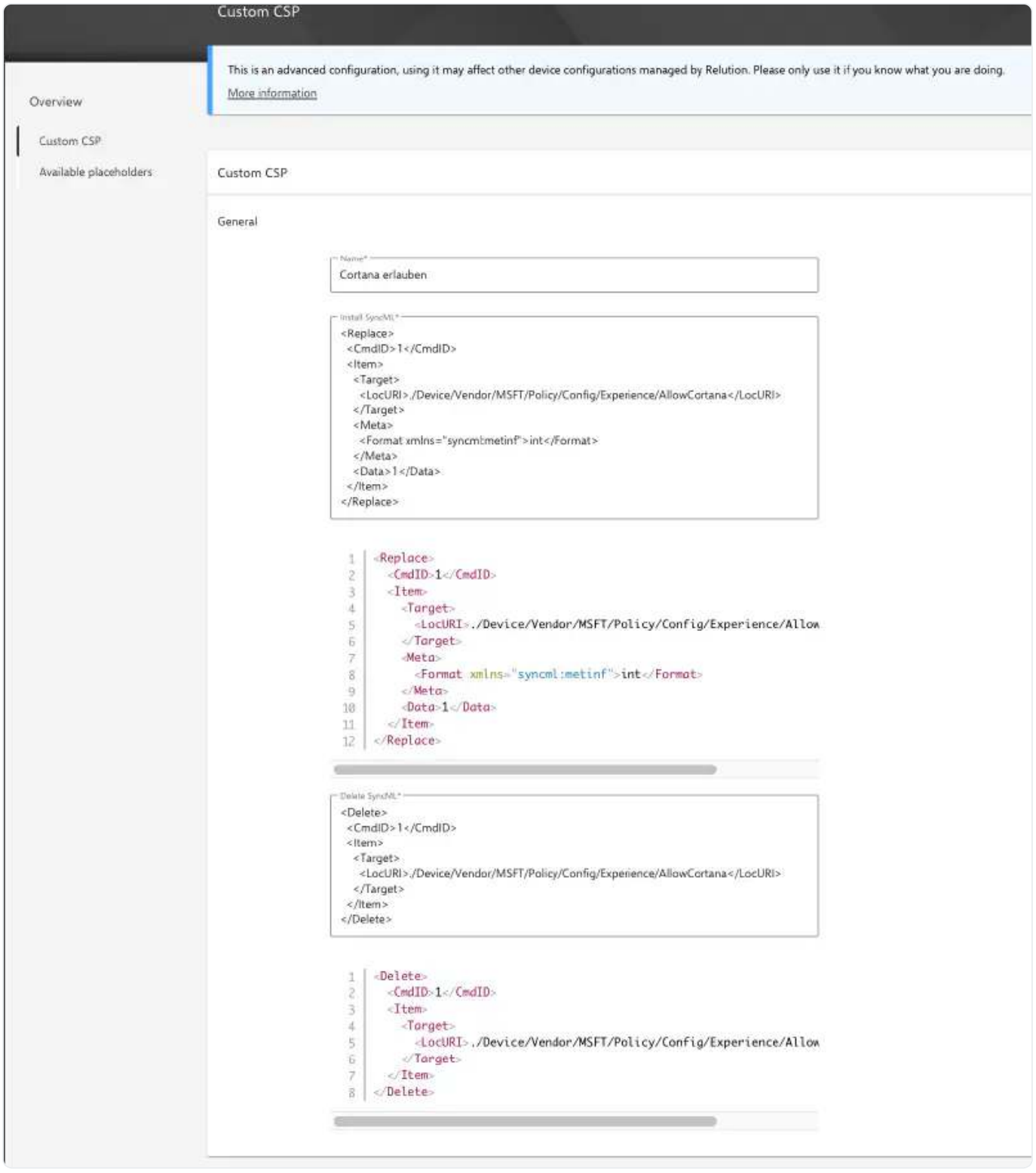
In Relution

To apply a custom configuration to Windows devices, the Custom CSP configuration is added to a Windows policy under `Devices` → `Policies`. Once the policy is published, the configuration is applied to the devices of the device groups the policy is assigned to (see Policies →).

Each configuration requires two SyncML commands: one in the Install SyncML field for installing or updating the configuration, and one in the Delete SyncML field for removing it. When the configuration is published multiple times, the command in Install SyncML must be adjusted accordingly.

The Custom CSP configuration includes the following properties (all of them mandatory):

Property	Information
Name	Sets a name for the configuration (maximum 255 characters)
Install SyncML	The SyncML to be executed when the configuration is applied to the device
Delete SyncML	The SyncML to be executed when the configuration is removed from the device



Relution automatically extends the specified SyncML to ensure the configuration can be properly applied, evaluated, and its status displayed in Relution:

- If the specified SyncML contains a `<Format>` or `<Type>` element, the required *namespace* will be added automatically after saving the configuration.
- An *Atomic* will be wrapped around the specified SyncML. This is necessary to associate the device response with the correct configuration. This occurs when the configuration is delivered.
- The SyncML will be automatically wrapped with the required `SyncBody`, `SyncHdr`, and `SyncML` elements to ensure the message is compliant and can be processed by the device. This also occurs at the time of delivery.

> The Install SyncML and Delete SyncML fields may only contain the commands themselves (e.g. `<Replace>`, `<Add>`, `<Delete>`), without the `SyncML`, `SyncHdr` or `SyncBody` elements. If the SyncML contains one of these elements or is not valid SyncML, the configuration is rejected when saving. Complete SyncML messages from the Microsoft documentation therefore have to be reduced to the commands first.

Placeholders can be used in both SyncML fields, including certificate placeholders. The available placeholders are shown in the Available placeholders section below the configuration and are replaced with the values of the respective device or user on delivery (see Advanced placeholders →).

Whenever the policies of a device change, for example after a new policy version has been published, Relution sends the Install SyncML of all assigned Custom CSP configurations again, even if the configuration itself is unchanged. Unlike other Windows configurations, the state on the device is not queried beforehand. An `Add` command can therefore fail on subsequent deliveries (see Best Practices →).

If the configuration fails on the device, Relution reports a compliance violation of the type Custom CSP configuration on the device.

Examples

Policy CSP/Experience/AllowCortana →

- Allow Cortana

Install SyncML:

```
<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>
```

- Block Cortana

Install SyncML:

```
<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>
```

- Remove the CSP policy *AllowCortana* from the device

Delete SyncML:

```
<Delete>
  <CmdID>1</CmdID>
  <Item>
    <Target>
      <LocURI>./Device/Vendor/MSFT/Policy/Config/Experience/AllowCortana</LocURI>
    </Target>
  </Item>
</Delete>
```

Best Practices

- An *update of the configuration* can be applied by creating a new policy version (possibly with an adjusted Install SyncML).
- If deletion fails, the included CSP policies will remain active on the device. In this case, the Delete SyncML must be revised, and the policy should be reapplied and then removed again.
- It is recommended to use *Replace instead of Add* unless the corresponding CSP policy does not support it.
- If a *Replace* command is not permitted for the initial deployment of a CSP policy, it is recommended to first apply the configuration using an *Add* command. Afterwards, the configuration's Install SyncML should be switched from *Add* to *Replace* and deployed again using a new policy version.
- It is recommended to *extensively test the desired behavior on suitable test devices*. At a minimum, the following scenarios should be tested:
  - Initial deployment of the configuration
  - Updating the configuration
  - Deleting the configuration

Sample Policies

A comprehensive example of custom policies has been published on the Relution Community Board: Relution Community Board - Custom CSP →.

Many thanks to the community for this valuable contribution.

Device Name

As of Relution Server version 5.33, the device name for Windows devices can be set via the Device name policy. The name is entered in the required Name field in the General section. User and device placeholders can be used; the portal lists them below the configuration under Available placeholders. One device name configuration is possible per policy.

Notes

> After adjusting the device name, the device must be restarted for the new name to take effect. Until the restart, the old name will still be displayed during every Refresh device info action. The device name may only contain letters, numbers, and hyphens. This also applies to placeholders.

For version 26.4.0

Relution first inserts the placeholder values and then removes all characters except letters (a–z, A–Z, no umlauts), digits and hyphens, including from the inserted values. Leading and trailing hyphens are removed as well. The entered name and the name set on the device may therefore differ, e.g. `Müller PC_01` becomes `MllerPC01`. After the placeholders have been inserted, the device name should be no longer than 63 characters.

Further functions such as substrings, default values for unset fields, or replacing umlauts are described in Advanced placeholders →.

If the configuration or the policy is removed from the device, the most recently set device name is retained.

Apply restrictions

To ensure that Windows 10/11 devices are only used in accordance with specified restrictions, restrictions can be defined in the Restrictions policy configuration and applied to enrolled Windows devices.

Available categories

The configuration is divided into the following groups:

- Accounts
- App Management
- Camera
- Connectivity
- Experience
- System
- Settings
- WiFi
- Power (sections On battery and Plugged in)
- Privacy

Next to each option, the portal shows which Windows editions and which minimum Windows version it applies to. Settings that a device's edition or version does not support are not transferred to that device by Relution. Most restrictions only apply to Windows Pro, Enterprise and Education (see Windows Home Limitations →).

The download icon at the top of the form (Export restrictions as CSV file) downloads the configured values, including unsaved changes, as a CSV file.

For version 26.4.0

Prevent MDM connection removal

To ensure that Windows 10/11 devices (Pro, Enterprise, Education) remain enrolled in the system and the connection to Relution is maintained, a restriction can be used to prevent the user from removing the MDM profile. The delete option is still displayed, but no longer has any function.

- Allow unenrollment from Relution MDM (group Experience) - If disabled, this ensures that users cannot manually disconnect connected devices from the MDM server. Unenrollment by the MDM server remains possible.
- Allow user to reset the device (group System) - If disabled, this prevents a factory reset from being performed on the devices. This would delete the enrollment on the devices and the connection to the MDM server.

Both options are enabled by default. The protection therefore only takes effect once they are explicitly disabled in the configuration.

Both options are only applied to Windows 10/11 Pro, Enterprise and Education. Relution does not transfer them to devices running Windows Home, so these devices can still be disconnected from the MDM server or reset to factory settings despite the restriction (see Windows Home Limitations →).

Combining both options secures the MDM control of enrolled Windows 10/11 devices (Pro, Enterprise, Education) and any configurations and functional restrictions.

Windows Hello

Relution allows Windows Hello for Business to be configured in a policy for Windows devices. Windows Hello allows users to sign in with a PIN, facial recognition, or a fingerprint instead of a password.

Configuration

- Tenant ID – ID of the Entra ID tenant in GUID format, required field.
- Use a Trusted Platform Module (TPM) – restricts provisioning to devices with a usable TPM. Enabled by default.

PIN Policy

- Minimum PIN length and Maximum PIN length (4–127 characters each, default: 4) – the maximum length must not be smaller than the minimum length. Without changes, this results in a fixed PIN length of 4 characters.
- Lowercase letters in PIN, Uppercase letters in PIN, Special characters in PIN – each Allowed (default), Required or Not allowed
- PIN expiration and PIN expiration (days) – enforces a PIN change after 1–730 days (starting with Windows 1511). The toggle is disabled by default, in which case the PIN does not expire; when enabled, 5 days are preset.
- Remember PIN history and Size of PIN history – prevents reuse of the last 1–50 PINs (starting with Windows 1511). Enabled by default with 5 PINs; if the toggle is disabled, no PIN history is kept.

Biometrics and Recovery

For version 26.4.0

- Allow biometric authentication – enables sign-in via face or fingerprint (starting with Windows 1511). Enabled by default.
- Use enhanced anti-spoofing, when available – additional protection for facial recognition (starting with Windows 1511). Enabled by default.
- Enable PIN recovery – allows resetting a forgotten PIN (starting with Windows 1703). Enabled by default.
- Certificate for on-premise resources – Windows Hello for Business uses a certificate to sign in to on-premises resources. When enabled, Windows Hello provisions the PIN only after the device has received a certificate from the management server, e.g. via the Certificates → configuration with the Certificate Key Location Windows Hello for Business. Enabled by default. Without such a certificate deployment, no PIN is provisioned; in this case, the option has to be disabled.

Options with a version note are only transferred to devices running the respective Windows version or later.

> Windows Hello for Business requires an Entra ID connection. The exact minimum requirements for hardware (TPM version) and Windows version should be verified in the Microsoft documentation →.

Wi-Fi

Relution allows Wi-Fi networks to be centrally set up on Windows devices without requiring users to enter credentials themselves.

Configuration

- The network's SSID – required, maximum 32 characters, no leading or trailing spaces, must be unique within the policy version.
- This network is hidden – for networks that do not broadcast their SSID (disabled by default).
- Join Network automatically – enabled by default.
- Authentication type: Open (default), Personal WPA, Personal WPA2, Personal WPA3, Enterprise WPA, Enterprise WPA2, Enterprise WPA3, Enterprise WPA3 192-bit
- Encryption type – for WPA and WPA2 (personal or enterprise) either AES (default) or TKIP; fixed to AES for Personal WPA3 and Enterprise WPA3, fixed to GCMP-256 for Enterprise WPA3 192-bit; not shown for Open.
- Password – network key for the personal authentication types, maximum 64 characters. The portal also shows the field for Open, but it is not transferred there. If left empty, no key is transferred.
- Transition mode – only for Personal WPA3

If several policies assign Wi-Fi configurations with the same The network's SSID to a device, only the configuration from the policy with the highest priority is applied.

For Version 26.4.0

Enterprise Authentication (EAP)

For the enterprise authentication types, the Encryption settings section is displayed. At least one EAP type must be selected. As soon as an EAP type is selected, the Trust section with trusted server names and certificates is displayed as well.

- Accept EAP Types – TLS, TTLS, and/or PEAP
- Identity Certificate – only for TLS/TTLS; required there. Two options are available:
  - Select certificate – a manually uploaded certificate (see Certificate Management →) or a certificate template, e.g. of the Built-In CA →.
  - Use user certificate – the user certificate from the profile of the user assigned to the device (see User certificates →). The optional Certificate name field selects a specific certificate by name if the user has several and may contain placeholders. If left blank, the longest-lived certificate is used.
- Inner authentication type – for TTLS: PAP, CHAP, MSCHAP or MSCHAPv2 (required); as soon as PEAP is selected, only MSCHAPv2 (optional)
- Inner authentication – text field, only for TTLS without PEAP; required for PAP, CHAP or MSCHAP
- Anonymous username – for TTLS/PEAP, optional
- Prompt user for server certificate – PEAP only. If enabled, the server certificate is not validated automatically, and Windows may prompt the user if the certification authority is not found.
- Trusted Server Names
- Trusted Certificates – multiple selection of certificates (PKCS#1 or PKCS#12) from Certificate Management →

Windows Update

Relution allows the update behavior of Windows devices to be centrally controlled. The policy is available starting with Windows 10 version 1607 for the Pro, Enterprise, and Education editions.

Automatic Update

- Auto update behavior: auto install and restart (default), auto install and restart at a specified time, auto install and restart without end-user control, auto install and then prompt the user to schedule a restart, notify before downloading, or turn off automatic updates entirely.
- For “at a specified time”: Frequency of update installation (starting with version 1709) with Every week (default) or one or more specific weeks of the month (first to fourth week); Every week excludes the selection of individual weeks. In addition, the time (0–23, default 3 AM) and day (default: every day) the update is installed.
- Scan for app updates from Microsoft Update (off by default)

General

For version 26.4.0

- Accept updates signed by entities other than Microsoft (only from an intranet update service, signed with a certificate from the “Trusted Publishers” store; off by default)
- Allow downloads over metered networks (starting with 1709, off by default)
- Enable auto-restart notifications (off by default) and the period for reminders (15, 30, 60, 120 or 240 minutes, default 15; starting with 1703)
- Period for restart warnings (2, 4, 8, 12 or 24 hours, default 4) and for imminent warnings (15, 30 or 60 minutes, default 15; each starting with 1703)
- Automatic maintenance/wake-up (starting with 1903, on by default)
- Allow dual scan (starting with 1709, on by default)
- Deadline grace period (0–7 days, default 2; starting with 1903), no auto-restart outside of active hours until the deadline and grace period have expired (starting with 1903, off by default)
- WSUS server URL plus an alternate URL; both must be valid `http` or `https` URLs
- Target release version (starting with 1803) and product version (starting with 2004, only effective together with the target release version); for the product version, the portal suggests `Windows 10`, `10`, `Windows 11` and `11`

User Interface

Starting with version 1809: allow end users access to Windows Update or the ability to pause updates (both on by default).

Active Hours

- Start and end of active hours (0–23, default 8 AM to 5 PM), maximum range of 18 hours. Active hours may span midnight; if the end is before the start, it applies to the following day.

Quality Updates

- Auto-restart deadline (2–30 days, default 7; starting with 1703)
- Pause start date (starting with 1703): quality updates are paused for 35 days from the selected date.
- Deadline in days (0–30, default 7; starting with 1903)
- Deferral period in days (0–365 days)

Feature Updates

- Auto-restart deadline (2–30 days, default 7; starting with 1809)
- Uninstall period (2–60 days, default 10; starting with 1803)
- Deferral period in days (0–365 days)
- Deadline in days (0–30, default 7; starting with 1903)
- Pause start date (starting with 1703): feature updates are paused for 35 days from the selected date.

For version 26.4.0

Exchange

Relution allows an Exchange ActiveSync account to be centrally set up on Windows devices.

Configuration

The configuration is divided into the sections General, Account settings, Synchronization settings and Logging settings. Account name, Email address, User name and Exchange Host are required; Exchange Domain and Password are optional.

General

- Use Secure Mail Gateway: If this feature is enabled, the URL and domain of the Secure Mail Gateway → will be distributed to the devices instead of the Exchange URL and Exchange domain. This allows the devices to communicate with the Exchange server via the Secure Mail Gateway. Exchange Host and Exchange Domain are then set automatically and cannot be edited; the unique name of the organization is used as the domain. If the user name contains an `@`, Relution transfers it in the format `<domain>\<user name>`. The option is only available if the Secure Mail Gateway is configured and enabled in the settings. If Windows or a Windows version is restricted in the Secure Mail Gateway settings, the form displays a warning.
- Exchange Host – required, without protocol (without `https://`).
- Exchange Domain – optional.
- Exchange Server is using SSL for authentication – enabled by default.

For version 26.4.0

Account settings

- Account name – required.
- Email address – required, supports placeholders such as `${user.email}`; with Use the user's email address, the email address of the assigned user is used.
- User name – required. Either entered Manually, or the username (`${user.name}`) or email address (`${user.email}`) of the assigned user is used. The user name cannot be changed after the configuration has been created.
- Password – optional, stored encrypted and no longer displayed in plain text after saving.

If a placeholder is used, a user must be assigned to the device.

Synchronization settings

- Synchronize emails, contacts, calendar, and tasks – each individually toggleable, all enabled by default.
- Synchronization period for emails: all, 3 days, 1 week (default), 2 weeks, or 1 month.
- Synchronization interval: push (default), manual, every 15 or 30 minutes, or every hour.

Logging settings

- Logging: Disabled (default), Enabled, or Advanced.

Windows Office

Relution allows a Microsoft Office installation to be centrally deployed to Windows devices using a previously created configuration XML. The policy is available starting with Windows 10 version 1703 for the Pro, Enterprise, and Education editions.

Configuration

The configuration consists of a single file:

- Configuration XML – required, XML file upload. After the upload, the form shows the content of the file for review.

This XML file is not created in Relution but generated using the official Microsoft tool config.office.com →. There, licensing, the update channel, and which Office apps and languages to install are defined.

Installation and uninstallation

The installation runs asynchronously on the device. As long as it is in progress, the Change policy action remains in the Not now status.

- Office suite already installed: Relution compares the product ID (`<Product ID="…">`) of the installation reported by the device with the product ID of the new XML. If they differ, the existing Office suite is first uninstalled completely, and the new configuration is only installed in a subsequent step. If the product ID is the same, the installation is repeated directly without prior uninstallation.
- Removing the configuration: If the configuration or the policy is removed from the device and the device reports an Office installation, Relution uninstalls Office from the device.
- Errors: If the device reports an error during the installation, the compliance violation Windows Office configuration is invalid is created.

The Deploy Office 365 device action should not be used in addition to this policy. Information on stuck installations is available under Office installation is stuck →.

For version 26.4.0

Passcode

The Passcode policy configuration defines the requirements a device password has to meet on managed Windows devices, and how the device behaves on inactivity or failed sign-in attempts.

As soon as the configuration is assigned, Relution enables the password-based device lock on the device. This setting is always active and cannot be switched off in the configuration.

> These settings are not applied to all types of Windows accounts. The official Microsoft documentation for the respective CSP is authoritative: DeviceLock CSP →

Configuration options

- Allow simple passwords — Specifies whether PINs or passwords such as “1111” or “1234” are allowed. Enabled by default.
- Minimum passcode length — Minimum number of characters of the password (4–16). Default value is 4.
- Passcode Quality — Specifies whether a passcode should be numeric (e.g. “1042”), alphanumeric (e.g. “A42B”) or free to choose. Default value is Alphanumeric.
- Minimum passcode age (in days) — Period of time (in days) that a password must be used before the user can change it (0–41). Default value is 0 – changes are allowed immediately. If a maximum age is set, the value must be smaller than the maximum age.
- Maximum passcode age (in days) — Number of days until the password expires (0–730). Default value is 0 – passwords do not expire.
- Passcode history — Number of most recent passwords that cannot be reused (0–24). Default value is 0 – the current password can be changed to any password, even the same one. With a setting of 1 the user cannot reuse the current password; a setting of 5 means that neither the current password nor any of the previous four passwords can be reused.
- Idle time before display is locked — Time in minutes (0–999) that the device can remain idle before it is locked and the PIN or password has to be entered. Default value is 0 – the device does not lock.
- Number of failed passcode attempts before all data is erased — Number of failed sign-in attempts after which the device is put into BitLocker recovery mode (0–16). The data is then inaccessible but recoverable; the device is not reset to factory settings. BitLocker has to be enabled. Default value is 0 – disabled.

The minimum passcode age is transferred from Windows 10 version 1709, the maximum passcode age and the passcode history from version 1511. On older versions these values are not set.

Passcode Quality

Three values are available for Passcode Quality:

- Numeric
- Alphanumeric (default)
- User choice

For version 26.4.0

Related topics

- BitLocker → — drive encryption and recovery keys.
- Windows Hello → — biometric sign-in and PIN policies.

For version 26.4.0

Windows kiosk mode

The Windows Kiosk Mode policy configuration restricts a device to a single application. The policy is available starting with Windows 10 version 1803 for the Pro, Enterprise, and Education editions. Typical use cases are information terminals, self-service stations and examination devices.

> The selected app and the kiosk browser are not installed automatically. Both have to be deployed separately via app distribution before the configuration takes effect.

User sign-in

User login type determines which account runs in kiosk mode:

- Auto login (default): the device signs in automatically with a kiosk account that Windows provides for this purpose.
- Local user: kiosk mode applies to the account entered in the User login name field. The field only appears with this option and is then required. No automatic sign-in takes place; kiosk mode takes effect as soon as the account signs in.

For version 26.4.0

Application type

Application type determines what is shown in kiosk mode: Microsoft Edge browser (default), Kiosk browser or Store App. The further fields depend on this selection and are described in the following sections. When the type is changed, Relution removes the browser settings of the previously selected type from the device.

Microsoft Edge

These fields appear with Microsoft Edge browser:

- Edge Kiosk URL – address of the start page, required field. A valid URL must be entered.
- Microsoft Edge Kiosk mode type – Multi-Tab (default) or Tabless.
- Refresh browser after idle time – time in minutes (0–1440). If the field is empty, Relution uses 5 minutes for Multi-Tab and 0 for Tabless.

Kiosk browser

These fields appear with Kiosk browser:

- Default homepage URL – start page of the kiosk browser.
- Show home buttons, Show navigation buttons and End session button – show the respective buttons in the kiosk browser.
- Refresh browser after idle time – time in minutes (1–1440). If the field is empty, Relution does not set a value.
- Allow URLs (max 500) – without an entry, all websites can be reached in the kiosk browser. As soon as at least one URL is entered, only the entered URLs can be reached and all other websites are blocked. Wildcards (`*`) are not allowed, each entry must be a valid URL.

Store App

With Store App, the Select app button is used to choose the Windows app from the Relution App Store that is shown in kiosk mode (required field).

The app must already be installed on the device (see the note above). If it is not installed, the configuration is not applied on the device.

Related topics

- Shared PC → — configure Windows devices for shared use.
- Restrictions → — further restrictions for Windows devices.

For version 26.4.0

VPN

The VPN policy configuration distributes VPN profiles to managed Windows devices centrally. Besides the connection itself, the configuration covers authentication, name resolution, split tunneling and proxy settings. Windows Home, Pro, Enterprise and Education version 1607 or later are supported.

The form is divided into the sections General, Apps, DNS settings, Split tunneling and Proxy configuration.

> The profile name is the unique identifier of a VPN profile on the device. It has to differ from every other VPN configuration within the same policy version; upper and lower case are not distinguished. If several policies with VPN configurations of the same profile name apply to a device, only the configuration from the policy with the higher priority is applied.

General

Field	Description
Profile name	Required. Name of the VPN profile on the device; without leading or trailing spaces
VPN type	Automatic (default), L2TP, PPTP or IKEv2. The type determines which authentication types are offered
Server names	Required. At least one VPN server; several entries are possible
Connect automatically	The VPN connection is established automatically
Remember credentials	The credentials for the VPN connection are stored on the device

Authentication

Depending on the VPN type, the Authentication type field offers the following options. When the VPN type changes, the authentication type is reset.

Option	Available with	Description
None	all types	Default. The profile does not specify an authentication method
EAP	all types	Authentication via EAP; the EAP configuration is entered in the EAP XML field
Pre Shared Key	L2TP	The Pre Shared Key field appears and is then required; the Identity Certificate block is not shown
Machine certificate	IKEv2	The device authenticates with a machine certificate; the EAP XML field is not shown

With the VPN type L2TP, either a pre-shared key or an identity certificate is required (certificate, certificate template or user certificate). If both are missing, the configuration is not saved.

EAP XML

EAP is not set up through individual fields but as an XML configuration in the EAP XML text field. Above the field, the portal links to the Microsoft documentation on how to build this configuration: EAP configuration →.

The field is available for all combinations except IKEv2 with Machine certificate. The XML is only transferred to the device with the authentication type EAP; with None and Pre Shared Key it is ignored.

For version 26.4.0

Identity certificate

Except with the authentication type Pre Shared Key, Identity Certificate defines which certificate is used for the connection:

- Use user certificate: Uses the user certificate. The optional Certificate name field selects a specific certificate by name if the user has several certificates of this type; the name may contain placeholders. If the field is left empty, the certificate with the longest validity is used. This requires a user to be assigned to the device for whom a user certificate exists.
- Select certificate: Selection of a certificate or a certificate template from certificate management.

The certificate is only installed on the device together with the VPN profile with the authentication type EAP.

IKEv2 parameters

With the VPN type IKEv2, the cryptography parameters can also be defined. The default value of all fields is Not configured.

- IKE SA Params: Encryption Algorithm, Integrity Algorithm and Diffie-Hellman group
- Child SA Params: Encryption Algorithm, Integrity Algorithm and Diffie-Hellman group (PFS group, additionally with the option Use parent Diffie-Hellman group)

Either all six values or none are set; a partial specification is not saved.

Apps

Field	Description
Apps	Apps whose launch establishes the VPN connection automatically. For desktop apps, the file path to the app is entered; for universal (UWP) apps, the package family name
Restrict VPN connection to these apps	If enabled, only the traffic of the apps entered under Apps is sent through the VPN

DNS settings

The DNS suffix field takes DNS suffixes that are added to the DNS search list so that short names are resolved correctly. The first suffix in the list is also used as the primary connection-specific DNS suffix of the VPN interface.

The Name Resolution Policy table (NRPT) rules define how DNS names are resolved while a VPN connection is established. Each rule specifies a domain and the DNS servers or web proxy server used to resolve that domain. Add creates a rule with the following fields:

For version 26.4.0

Field	Description
Domain	Required. Domain the rule applies to
DNS Servers	One or more DNS servers for this domain
Proxy	Web proxy server for this domain
Automatically Connect	The device connects to the VPN automatically when it connects to this domain
Persistent	The rule remains active even when the VPN is not connected

Split tunneling

Split tunneling is enabled with the Split tunneling switch. Only then are the entries under Split tunneling routes for this VPN connection transferred to the device, and only traffic to these destinations is sent through the VPN.

> If the Split tunneling switch is disabled, the profile is set up as a force tunnel: all traffic is sent through the VPN and any routes entered are ignored.

Each route is added with Add as a Destination prefix in CIDR notation, as an IPv4 or IPv6 address with prefix length (e.g. `10.22.0.0/16`). The prefix length (subnet mask) must be greater than 0.

Proxy configuration

The Proxy type field determines which further fields appear:

Option	Description
None	Default. No proxy is configured for the VPN connection
Automatic	Required field Proxy configuration URL: valid URL of the proxy configuration script
Manual	Required fields Proxy server and Proxy server port (value 1–65535, prefilled with 1)

For version 26.4.0

Related topics

- Certificates → — provide identity and trust certificates.
- Wi-Fi → — network profiles for Windows devices.

Windows Firewall

The Windows Firewall policy configuration manages the Windows firewall on managed devices. It consists of three parts: global properties, settings per network profile and individual firewall rules.

> At least one of the three parts has to be configured before saving — global properties, a profile or a firewall rule.

> A firewall configuration can break the communication between the device and the MDM server. Communication with the MDM server and with the Windows Notification Service (WNS) must not be blocked, otherwise the device can no longer be managed.

Global properties

The global properties apply across profiles to the entire device and are located in the General section. They are unlocked with the Configure global settings toggle; without it, the following fields cannot be edited and are not transferred. If the toggle is disabled, the previously transferred global properties are removed from the device again.

For version 26.4.0

- Block stateful File Transfer Protocol (FTP)
- Security association idle time before deletion: number of seconds without network traffic after which a security association is deleted (300–3600).
- Pre-shared key encoding
- IPsec exemptions (selection):
  - None
  - Neighbor discover IPv6 ICMP type-codes
  - ICMP
  - Router discover IPv6 ICMP type-codes
  - Both IPv4 and IPv6 DHCP traffic
- Certificate revocation list (CRL) verification (required, default: Disabled):
  - Disabled
  - Fail CRL verification on revoked certificate only
  - Fail CRL verification on any error encountered
- Opportunistically match authentication set per keying module
- Enable packet queuing (default: Disabled):
  - Disabled
  - Queue inbound encrypted packets only
  - Queue packets after decryption is performed for forwarding only

Profile properties

Each network profile – Domain (workplace) network, Public (non-discoverable) network and Private (discoverable) network – has its own section with the Configure profile properties toggle. Only when it is enabled can the following settings be edited, and only then are they transferred to the device. If it is disabled, the previously transferred settings of the profile are removed from the device again.

- Enable firewall
  - Shielded: only selectable if Enable firewall is set; together with the firewall, it blocks all incoming traffic.
- Allow default action for inbound connections (default: enabled)
- Allow default action for outbound connections (default: enabled)
- Disable inbound notifications
- Disable stealth mode
  - IPsec secured packet exemption with Stealth Mode: only selectable if Disable stealth mode is set.
- Disable unicast responses to multicast broadcasts
- Authorized application firewall rules from the local store (default: enabled)
- Global port firewall rules from the local store (default: enabled)
- Allow firewall rules from the local store (default: enabled)
- IPsec rules from the local store (default: enabled)

If the default actions for inbound or outbound connections are not allowed, a firewall rule is required that permits the connections with Relution. Otherwise, Relution can no longer manage the device.

Firewall rules

The firewall rules are shown in a list with the columns Rule name, Rule description, Traffic direction and Rule enabled. Rules are created, changed or removed via Add, Edit and Delete. A maximum of 100 firewall rules is possible per configuration.

Application, ports and network types can be defined per rule:

For version 26.4.0

- Rule name (required)
- Rule description
- Rule enabled (default: enabled)
- Allow connection for this rule (default: enabled): specifies whether the rule allows or blocks the network traffic.
- Edge Traversal setting enabled (default: disabled)
- Traffic direction: Incoming or Outgoing (default)
- Network types (required, multiple selection):
  - All existing network sets and any future network sets (default; excludes the other options)
  - Domain
  - Private
  - Public
- Package family name, Full file path and Windows service (Application section)
- Local address range and Remote address range (IP Address section): IPv4 or IPv6 addresses, as a single address or as a range with Lower range limit and Upper range limit
- IP Protocol: number from 0 to 255, with a list of suggestions (e.g. 6 - TCP, 17 - UDP)
- Local port range and Remote port range: ports from 1 to 65535, as a single port or as a range
- Interface types (multiple selection, default: all): Local Area Network, Wireless, Remote Access
- Local user authorization list: authorized local users in SDDL format; if not specified, the rule applies to all users. No list is possible for rules that target a Windows service.

A maximum of 20 entries is possible per range list (Local port range, Remote port range, Local address range, Remote address range); ranges within a list must not overlap. Port ranges are only available if 6 - TCP or 17 - UDP is selected as IP Protocol.

Related topics

- VPN → — VPN profiles for Windows devices.
- Custom CSP → — settings that have no dedicated configuration.

For version 26.4.0

Install certificates

The policy configuration Certificate for Windows can be used to install certificates on Windows 10/11 devices via Relution. Depending on the certificate type, either the certificate store or the location of the certificate and its key can be specified.

Upload certificates to Relution

To be able to distribute certificates via Relution, they must first be uploaded to the certificate store of Relution (see also Certificate Management →).

- To do this, one has to go to `Settings` → `Certificates`.
- Then the button Add has to be clicked.
- A name has to be assigned, the password has to be entered for password-protected certificate files (e.g. PKCS#12) and finally, the certificate file has to be selected.
- The entry is then confirmed with Save.

Applying certificates on Windows 10/11 devices

For version 26.4.0

1. One has to navigate to `Devices` → `Policies` in the Relution Portal and click on Add.
2. A Windows policy has to be created and a name has to be assigned. Then, Save has to be chosen.
3. After clicking Add, the Certificate option is selected and the process is continued with Add details.
4. Under Certificate, the Select certificate option is chosen and the certificate uploaded in the previous section is selected. The further options depend on the certificate type:
   - Certificate without private key (PEM/DER): a Certificate store is selected (default: Automatically).
   - PKCS#12 certificate (.p12/.pfx), certificate template or user certificate: under Certificate Location, either Device (default) or User is selected, the Certificate Key Location is set (TPM, TPM if available, Software or Windows Hello for Business; default: Software) and Key is exportable is enabled if required. The toggle is only available with Software.
5. The configuration has to be saved and the current version of the policy has to be published (Publish).
6. To apply the policy to Windows 10/11 devices, one must add the desired devices via the Devices with this policy tab. The selected certificates will then automatically be installed on the devices.

> For the installation of MSIX files, the Trusted Root Certificate Authority option must be selected as the certificate store and a single certificate exported from the PKCS#12 container (PEM format) must be used.

With Automatically, Relution chooses the store based on the certificate: self-signed CA certificates are installed under Trusted Root Certificate Authority, other CA certificates under Intermediate Certificate Authority and all other certificates under Personal. If the certificate store of an existing configuration is changed, Relution removes the certificate from the previous store.

The certificate of an existing configuration cannot be changed afterwards. A different certificate requires a new configuration. Configurations created with a version prior to Relution 5.25 can no longer be edited and must also be created again.

Distribute certificates from certificate templates

Since Relution 26.0, it is also possible to distribute certificates from certificate templates directly to Windows devices. The template (e.g. a template of the Built-In CA →) is selected in step 4 via Select certificate instead of an uploaded certificate. The options for PKCS#12 certificates (location of the certificate and of the key) then apply.

Distribute user certificates

As an alternative to Select certificate, the Use user certificate option can be chosen under Certificate. The user certificate from the profile of the user assigned to the device is then installed (see User certificates →). The optional Certificate name field selects a specific certificate by name if the user has several and may contain placeholders. If left blank, the longest-lived certificate is used. The options for PKCS#12 certificates apply here as well.

For version 26.4.0

Windows Shared PC

With the Windows Shared PC policy configuration, Relution makes it possible to use Windows 10/11 devices across users. To ensure privacy-compliant use at all times and to ensure the deletion of user-specific data on the devices, Shared PC allows various data-related settings and restrictions.

This feature is particularly useful in school, education and research contexts, as well as for public institutions and companies that want to use shared PCs in a privacy-compliant manner at all times without each user needing their own computer.

The configuration is applied to Windows 10/11 Pro, Enterprise and Education. Windows Home is not supported.

How to configure the Windows Shared PC policy configuration?

To successfully run Shared PC on a Windows device, a new policy is first added under the `Devices` → `Policies` menu item.

Once the policy is created, the Shared PC configuration can be selected and added to the policy. Alternatively, existing policies can be supplemented with the Shared PC configuration.

For version 26.4.0

The following settings can be made in the configuration:

- Allow only a single user to be signed in at a time: This switch enables the Shared PC mode of the device and is enabled by default. If it is disabled, Shared PC mode is turned off on the device.
- Accounts that can sign in: Determines whether only domain accounts (Domain) or additionally password-less guest accounts (Guest and Domain, default) can sign in to the devices. After signing out of guest mode, all temporary data is always deleted automatically.
- Automatically delete Accounts after maintenance or sign off: If enabled, Windows deletes cached accounts to free up disk space (disabled by default). Specify when Accounts are deleted offers the following options:
    - Delete immediately: Accounts are deleted when the user signs out.
    - Delete at disk space threshold: Accounts are deleted as soon as free disk space drops below the value in Start deletion of accounts when free diskspace is below. Deletion stops once the value in Stop deletion of accounts when free diskspace is above is reached. Both values are specified as percentages (0–100, default 25). Accounts that have been inactive the longest are deleted first.
    - Delete at disk space or inactivity threshold (default): As above; in addition, accounts are deleted after the number of inactive days specified in Inactive days after the Account is deleted (default 30).
- Restrict access to local storage: When this setting is enabled, the user only has access to their own data (disabled by default).
- Enable Education environment: Online searches can be severely restricted and completely blocked for certain websites (disabled by default).
- Require sign in when waking up from sleep mode: If the device is put into sleep mode while a user is signed in, signing in again is required. The setting is enabled by default.
- Go into sleep mode after specified amount of time: To save the battery, the field Seconds after which the device goes into sleep mode defines after which time the device switches to sleep mode (enabled by default, 300 seconds).
- Time of day at which Maintenance starts: Time of day at which the daily Windows maintenance window starts (default: 00:00). During this window, Windows performs maintenance tasks, e.g. deleting accounts according to the configured deletion option.

On Windows Pro devices, a wallpaper configuration requires the Education environment to be enabled. If a Shared PC configuration with Enable Education environment disabled (default) is applied to the device, no wallpaper can be configured. Without a Shared PC configuration, the wallpaper configuration enables the Education environment itself.

For version 26.4.0

Windows Script Configuration

A policy configuration for PowerShell scripts is available in Relution for managed Windows devices. In the selection, the configuration is called Script and can be added to Windows policies as usual. It is executed by the Windows Companion →, which must be installed on the device for this purpose.

However, in preparation, the PowerShell script to be distributed must be stored in the menu under Scripts.

> The script is not implemented by Relution, so no guarantee is given for any damage. The script should be inspected carefully before it is applied to a device. In addition, Relution cannot provide support for any errors that may occur or for the creation of the scripts.

Policy configuration

The policy offers, besides the selection of the desired script, various other configuration options. At least one of the two execution types (event based or time based) must be enabled.

Script to execute

The previously stored script must be selected here. Only one script per configuration can be selected at a time; PowerShell scripts for Windows are available for selection. Placeholders in the script content are replaced for each device before delivery (see Advanced placeholders →).

For version 26.4.0

Event based execution

The Execute script for the following events on the device switch makes the execution of the script dependent on certain events on the device. At least one of the following events must then be selected under Device events:

- Device started
- User logged in – the optional field Limit login trigger to a specific user restricts execution to one user. The user's SID as well as the formats `Domain\Username` and `Username` are supported. If the field is left empty, the script is executed when any user logs in.
- User logged out – on shutdown, only a few seconds remain for execution; after that, the device cancels it.

Time based execution

The Execute script in the following period of time switch executes scripts regularly at specific times on the target device. Required settings are the days of the week under Repeats on, the Start time (default: 08:00) and the Time zone (default: Europe/Paris).

Restrict execution

The execution of the script can also be prevented or the behavior adjusted under certain circumstances. All options are disabled by default. Possible configurations are:

- Disallow execution when running on batteries
- Stop execution when switching to battery power
- Wake device for script execution
- Hide script execution task on device
- Allow to start the script execution on demand

For version 26.4.0

Windows Bitlocker

With Relution, BitLocker encryption can be configured in a policy for Windows devices. Details about BitLocker and its functionalities can be found in the Microsoft documentation →.

Configuration

Four sections are available within the configuration: Base Settings, OS Volumes, Fixed Drives and Removable Drives.

For OS volumes, fixed drives and removable drives, the Encryption type (Full, Used space only, User choice or Not configured) and the Encryption method (AES 128bit CBC, AES 256bit CBC, XTS 128bit AES or XTS 256bit AES) are set individually. The encryption method must be set in all three sections or set to Not configured in all three; otherwise the policy cannot be saved.

Changes to the configuration have no effect on drives that are already encrypted or currently being encrypted.

Base Settings

- Require device encryption: Enables full disk encryption for OS drives and fixed data drives (default: enabled).
- Allow standard users to enable BitLocker encryption silently: Allows silent encryption for users without administrator rights as well. BitLocker must be configured for silent encryption for this to work.
- Show warning about third-party disk encryption: Only takes effect on devices joined to Microsoft Entra ID. The option is automatically disabled and locked as soon as silent encryption for standard users is enabled.

For version 26.1.0

OS Volumes

- Pre Boot Recovery option (text or URL shown on the pre-boot recovery screen when the OS drive is locked):
  - Default pre boot recovery message and URL
  - Custom pre boot recovery URL
  - Custom pre boot recovery message
- Startup authentication required: Once enabled, the following additional settings are available:
  - Minimum pin length: 4 to 20 digits, default 6.
  - Trusted Platform Module (TPM) on incompatible devices: Allows BitLocker without a TPM. A password or a startup key on a USB flash drive is then required.
  - TPM startup, TPM startup PIN, TPM startup key and TPM startup PIN and key: each Not configured, Optional, Required or Blocked. If one of these options is set to Required, the other three must be set to Blocked. If Trusted Platform Module (TPM) on incompatible devices is not enabled, not all four may be blocked.
  - Configure Recovery with:
    - Allow data recovery agent
    - Create recovery password
    - Create recovery key
    - Hide recovery page during BitLocker setup
    - Save recovery information to Active Directory Domain Services (either recovery passwords only, or recovery passwords and key packages)
    - Do not enable BitLocker until recovery information is stored in Active Directory Domain Services

Fixed Drives

- Require encryption: Fixed drives that are not protected by BitLocker are mounted as read-only.
- Recovery Options: Once enabled, the following settings are available:
  - Allow data recovery agent
  - Create recovery password
  - Create recovery key
  - Hide Recovery Page during BitLocker setup
  - Save BitLocker recovery information to Active Directory Domain Services (either recovery passwords only, or recovery passwords and key packages)
  - Do not enable BitLocker until recovery information is stored in Active Directory Domain Services

Create recovery password and Create recovery key can each be set to Allowed, Required (default) or Blocked. The same rules apply to OS volumes and fixed drives:

- Password and key cannot both be blocked.
- The recovery password cannot be blocked if recovery information is saved to Active Directory Domain Services.
- The recovery password cannot be set to Required if the recovery page is hidden and saving to Active Directory Domain Services is not enabled.
- The recovery key cannot be set to Required if Require encryption is enabled for removable drives.

Removable Drives

- Require encryption: Removable drives that are not protected by BitLocker are mounted as read-only.
- Deny write access to devices configured in another organization: Only drives whose identification fields match those of the computer are given write access.

No recovery options are available for removable drives.

For version 26.4.0

BitLocker Information in the Device Details

As of Server 5.21, Relution shows Volume, Volume status, Protection status and Extra information for each drive in the device details under Bitlocker information. If a recovery password exists for a drive, it is stored there with a timestamp under Recovery password. The information is only loaded after clicking Show.

Devices Encryption Without User Interaction

BitLocker can be enabled on devices under certain conditions without requiring user interaction. This applies even to users without administrative privileges.

Requirements

Devices must meet the following conditions:

- Version 1803 or higher for users with administrator privileges.
- Version 1809 or higher for users with standard privileges.
- Devices must be enrolled in Microsoft Entra or Microsoft Entra hybrid (e.g., via Autopilot) or activated through the Enable Bitlocker action in Relution (requires the Relution Companion for Windows →).
- Minimum of TPM 1.2.
- BIOS Setting: Native UEFI.

Microsoft Entra or Microsoft Entra Hybrid Enrolled Devices

For devices enrolled in Relution and also connected to Microsoft Entra (e.g., via Autopilot), the BitLocker configuration can be set up as follows so that the devices are encrypted automatically once the configuration is applied.

Base Settings:

- Require device encryption: Enabled.
- Allow standard users to enable BitLocker encryption silently: Enabled.

OS Volumes:

- Encryption type: Full.
- Startup authentication required: Enabled.
- TPM startup: Optional or required.
- TPM startup PIN: Blocked.
- TPM startup key: Blocked.
- TPM startup PIN and key: Blocked.
- Configure Recovery: Disabled (or enabled with the options below).
    - If recovery is enabled, additional requirements include:
        - Create recovery password: Allowed (Required only if Save recovery information to Active Directory Domain Services is also enabled).
        - Create recovery key: Allowed or required. Required is not permitted if Require encryption is enabled for removable drives.
        - Hide recovery page during BitLocker setup: Enabled.

For version 26.4.0

Other configuration options may be adjusted as needed, but unsupported settings could lead to activation issues.

Activate BitLocker via Action

For devices not enrolled in Microsoft Entra or Microsoft Entra hybrid, the BitLocker encryption can be started using the Enable Bitlocker action in Relution. This applies to standard users as well.

The Enable Bitlocker action is executed exclusively by the Relution Companion for Windows →, which must be installed on the device.

The action defines the Protector and the Used space only option for each Drive (drive letter followed by a colon, e.g. `C:`). Available protectors are TPM (operating system drive only) and Recovery Password. The recovery password is generated by Windows and appears in the device details under Bitlocker information. The Disable Bitlocker action removes the encryption from selected drives.

It is advised to apply a BitLocker configuration beforehand to define the encryption method or other parameters. This step is not mandatory for automatic activation but ensures consistent compliance and settings.

Compliance Messages

If the state of the device deviates from the BitLocker policy, Relution reports a compliance violation on the device with the description `BitLocker Configuration violated. Messages:` followed by a list of the causes reported by Windows. The messages are only available in English. Solutions for common messages are described below.

The BitLocker policy requires a TPM protector to protect the OS volume, but a TPM is not used

- Apply the following configuration in the OS Volumes section:
  - Startup authentication required → Enabled
  - Trusted Platform Module (TPM) on incompatible devices → Enabled
  - TPM startup → Required
  - TPM startup PIN → Blocked
  - TPM startup key → Blocked
  - TPM startup PIN and key → Blocked

The encryption method of the OS volume doesn't match the BitLocker policy

- Use the following command to determine the encryption method on the device:

```
manage-bde -status
```

- Result: AES or XTS with 128 or 256 Bit
- Set Encryption method accordingly in the OS Volumes section of the policy (e.g. XTS 256bit AES). The value must be set for all three sections (OS volumes, fixed drives, removable drives), or all of them must be set to Not configured; otherwise the policy cannot be saved.

The BitLocker policy requires a TPM-only protector for the OS volume, but TPM protection is not used

- The Encryption type in the OS Volumes section must be changed from Full to Used space only.

Related Topics

- Manual Windows Enrollment → — Manual enrollment of Windows devices.

Configure Companion

The Windows Companion policy configuration controls the behavior of the Relution Companion for Windows → on managed Windows devices. The configuration is divided into four sections: General, App handling, Server communication and User change on login.

Log level

Defines how detailed the log entries written by the Windows Companion are. Available options are None, Critical, Error, Warning, Information, Debug and Trace — verbosity increases with each level. The default is Information.

Action Timeout

Defines the maximum time in minutes for an action to be processed until it is aborted by the Windows Companion. The default is 45 minutes; values from 15 to 180 minutes are allowed.

For version 26.4.0

App installation timeout

Defines the maximum time in minutes for an app installation to be processed until it is aborted by the Windows Companion. The default is 45 minutes; values from 1 to 150 minutes are allowed.

App removal timeout

Defines the maximum time in minutes for an app uninstallation to be processed until it is aborted by the Windows Companion. The default is 45 minutes; values from 1 to 150 minutes are allowed.

Manage WinGet and its dependencies

Defines whether WinGet and its dependencies, like Microsoft VC Redistributable, are managed and updated automatically by the Windows Companion. The option is enabled by default. If it is disabled, the Companion no longer updates WinGet, but still installs a missing Microsoft VC Redistributable so that WinGet commands keep working.

Server communication

Communication between the Relution Companion and the Relution Server is necessary for Relution to work properly. Communication is initiated either by:

- the Server, telling the Companion to start communicating
- the Companion, if no interaction between Server and Companion occurred for some time

The settings below allow administrators to optimize the behavior of this mechanic, although this should not usually be necessary. After the time defined by Check interval, the Companion will start communication if the last communication with the server is older than the time specified by Time since last communication.

Check interval

Defines the interval in minutes at which the Windows Companion checks whether a request to the Relution Server is necessary. The default is 180 minutes; values from 15 to 1,440 minutes are allowed.

Time since last communication

Defines the minimum duration in minutes the Windows Companion waits before sending the next request to the Relution Server. The default is 120 minutes; values from 15 to 600 minutes are allowed.

For version 26.4.0

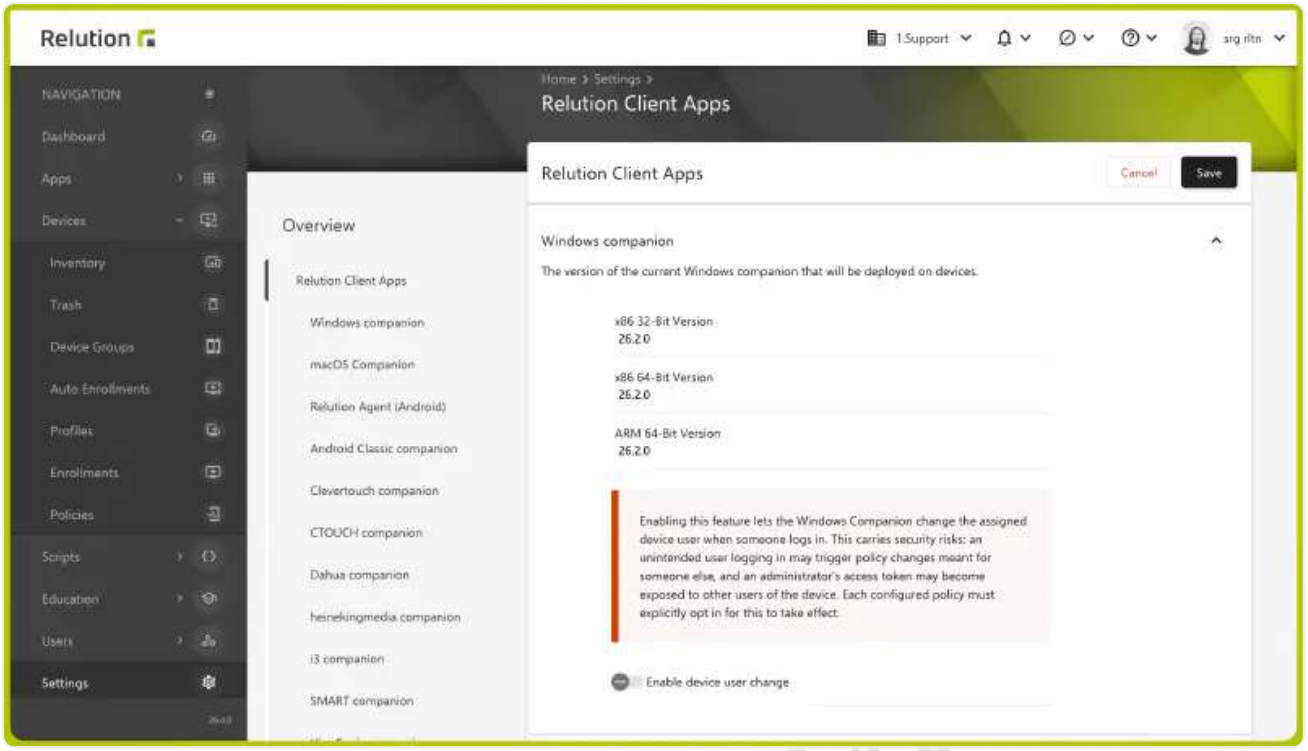
User change on login

As of version 26.4, the Relution Companion for Windows can automatically update the device user assigned in Relution as soon as a different person logs into the Windows device. This is especially useful for devices shared by several people, e.g. in a classroom or open-plan office: the device user stored in Relution always matches the person actually logged in on the device.

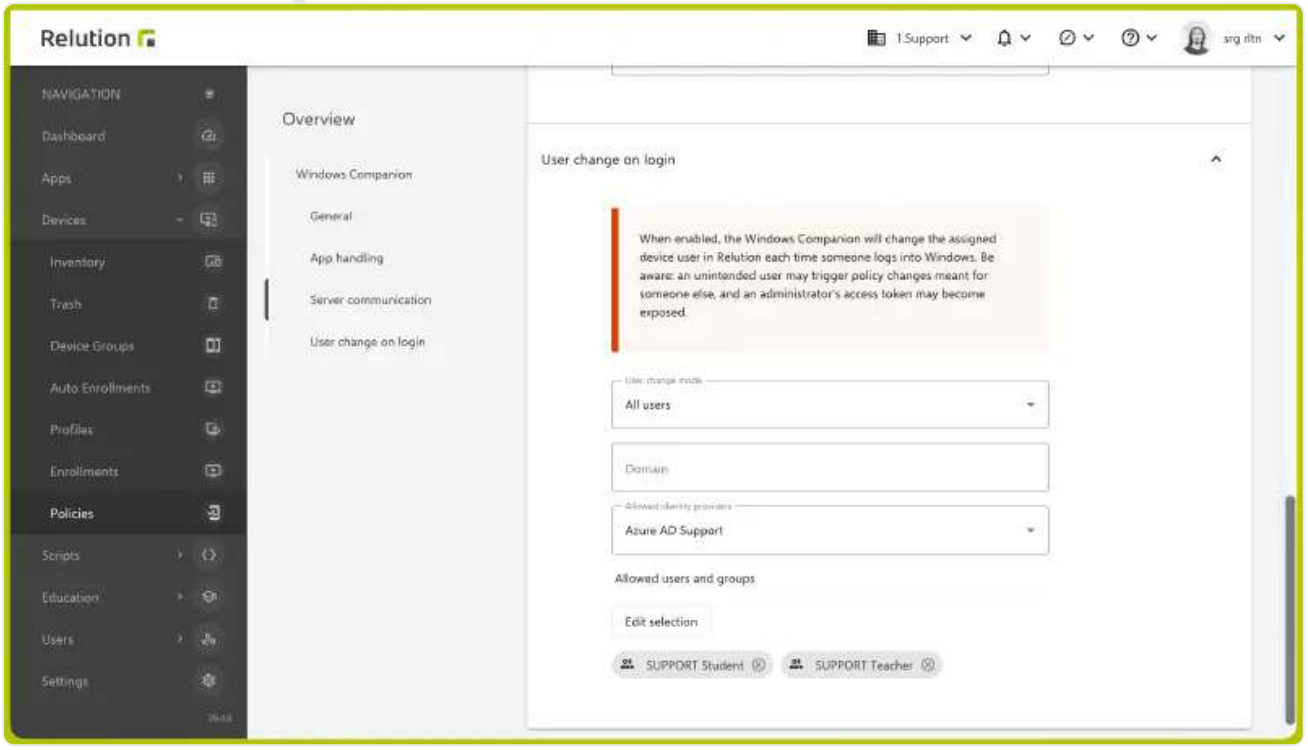
Enabling the feature

The feature must be enabled in two places before it takes effect:

1. Organization-wide under `Settings` → `Relution Client Apps` → `Windows companion` using the Enable device user change toggle. The setting is only available in organizations below the global organization and requires the permission for Relution Client Apps.



2. Additionally, in every policy that should use it, in the `Windows Companion` → `User change on login` section via the User change mode. If the toggle is disabled at the organization level, the policy can only be saved with the mode Disabled; if the toggle is switched off later, existing policies show a corresponding error when opened.



When enabled, the Windows Companion will change the assigned device user in Relution each time someone logs into Windows. This carries security risks: an unintended user who logs in may trigger policy changes meant for someone else, and an administrator's access token may become exposed to other users of the device. Each configured policy must explicitly opt in for this to take effect.

User change mode

- Disabled: No automatic user change.
- Only domain users: The change only happens if the logging-in person's UPN matches the domain entered in the Domain field (case-insensitive) and the person belongs in Relution to one of the providers selected under Allowed identity providers. A domain and at least one allowed identity provider are required for this. At least one active identity provider must exist in the organization; without one, the Allowed identity providers field cannot be selected and the policy cannot be saved in this mode.
- All users: Domain and Allowed identity providers are optional. If a domain is specified, the change only happens if the UPN matches it (case-insensitive); if identity providers are selected, the person must belong to one of them. If both fields are left empty, no filtering is applied.

In both active modes, the change can additionally be restricted via Allowed users and groups (Edit selection button). Only the selected users and members of the selected groups are then allowed. If the field is left empty, no additional restriction applies.

The match is made using the Windows login name, which is compared against the username in Relution within the same organization. If the logging-in person is not known in Relution or does not meet the configured conditions, the assigned device user is removed, but no error is shown on the device. With each change, the Last connected Entra ID user field in the device details is updated; for persons unknown in Relution, it shows the Windows login name in the format `Domain\User`.

For version 26.4.0

Windows App Installation

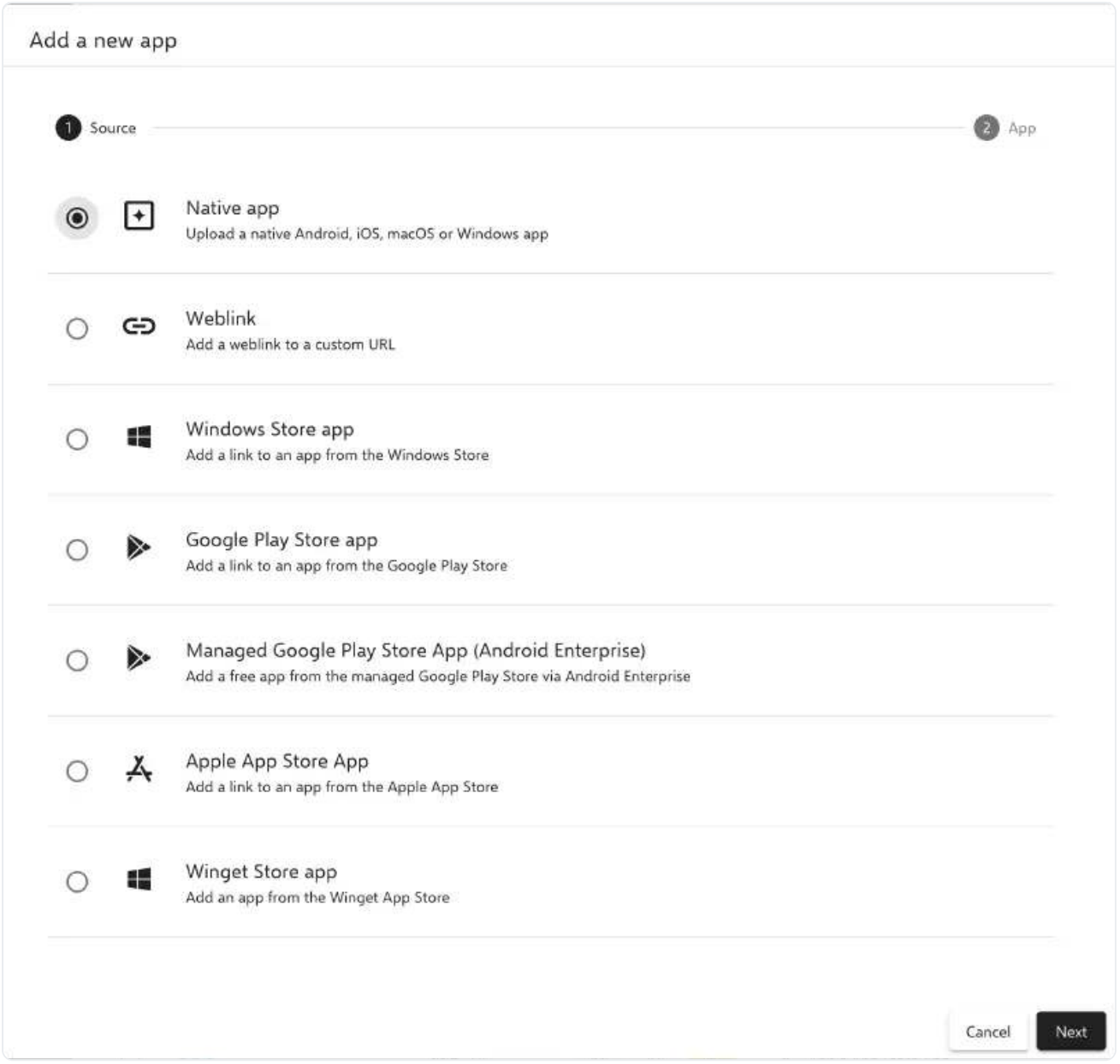
Classic apps (`.msi` and `.exe` applications) can be uploaded to the Relution App Store via the portal and installed and uninstalled on all Windows devices managed by Relution. Installation, detection and uninstallation are handled by the Relution Companion on the device, so it must be installed on the target devices: Windows Companion →

Packages in `.msix`, `.msixbundle`, `.appx` or `.appxbundle` format are also uploaded as a Native app, but require neither detection rules nor install parameters: Create MSIX files →

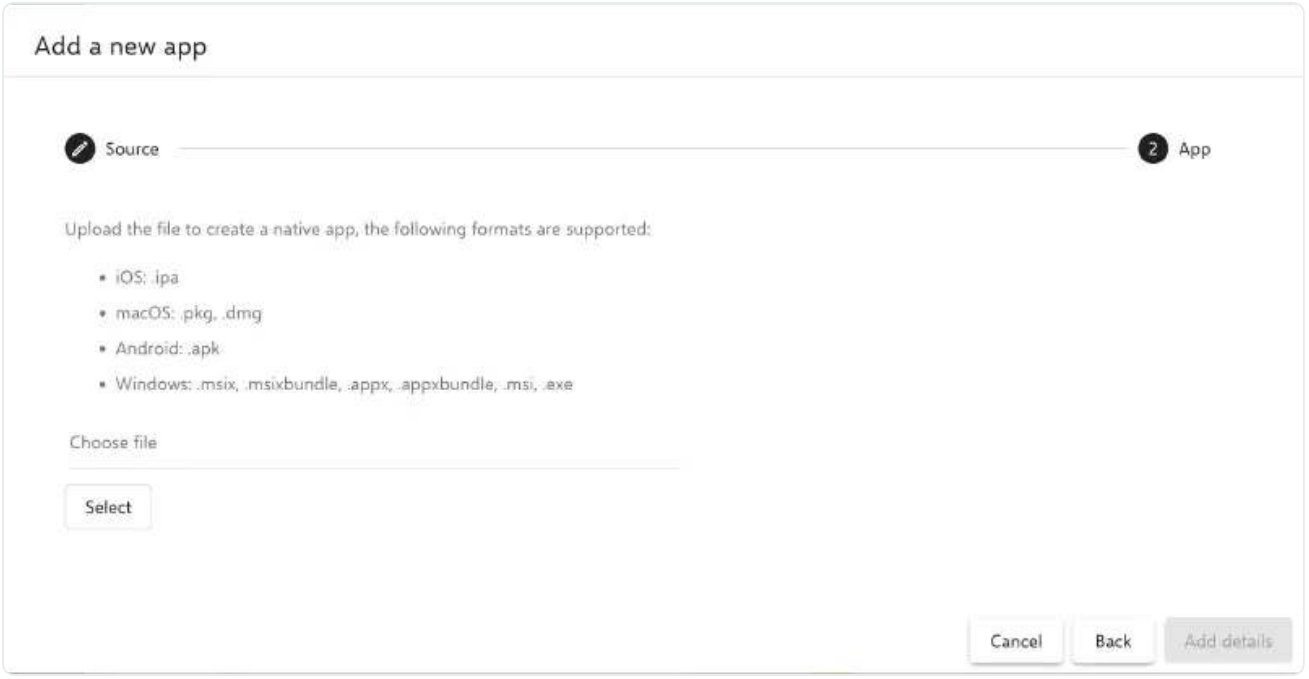
The following steps must be followed for a successful installation:

For version 26.4.0

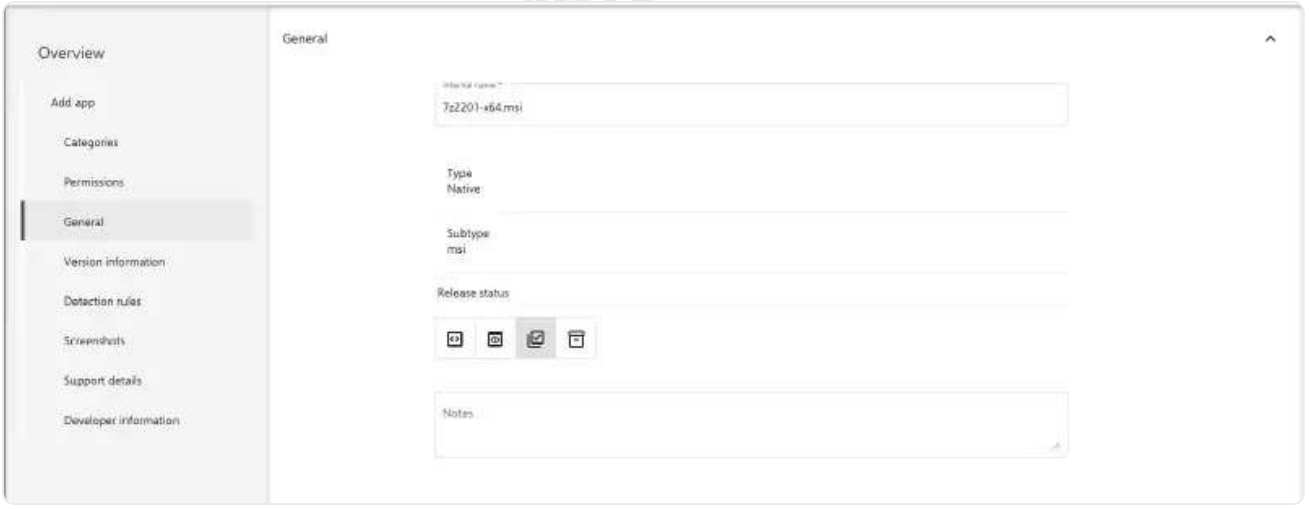
1. Under `Apps` → `App Store`, the Native app option is selected via Add.



2. In the next step, the appropriate file in the correct format (`.msi` or `.exe`) is uploaded under Choose file via the Select button and the native file manager.



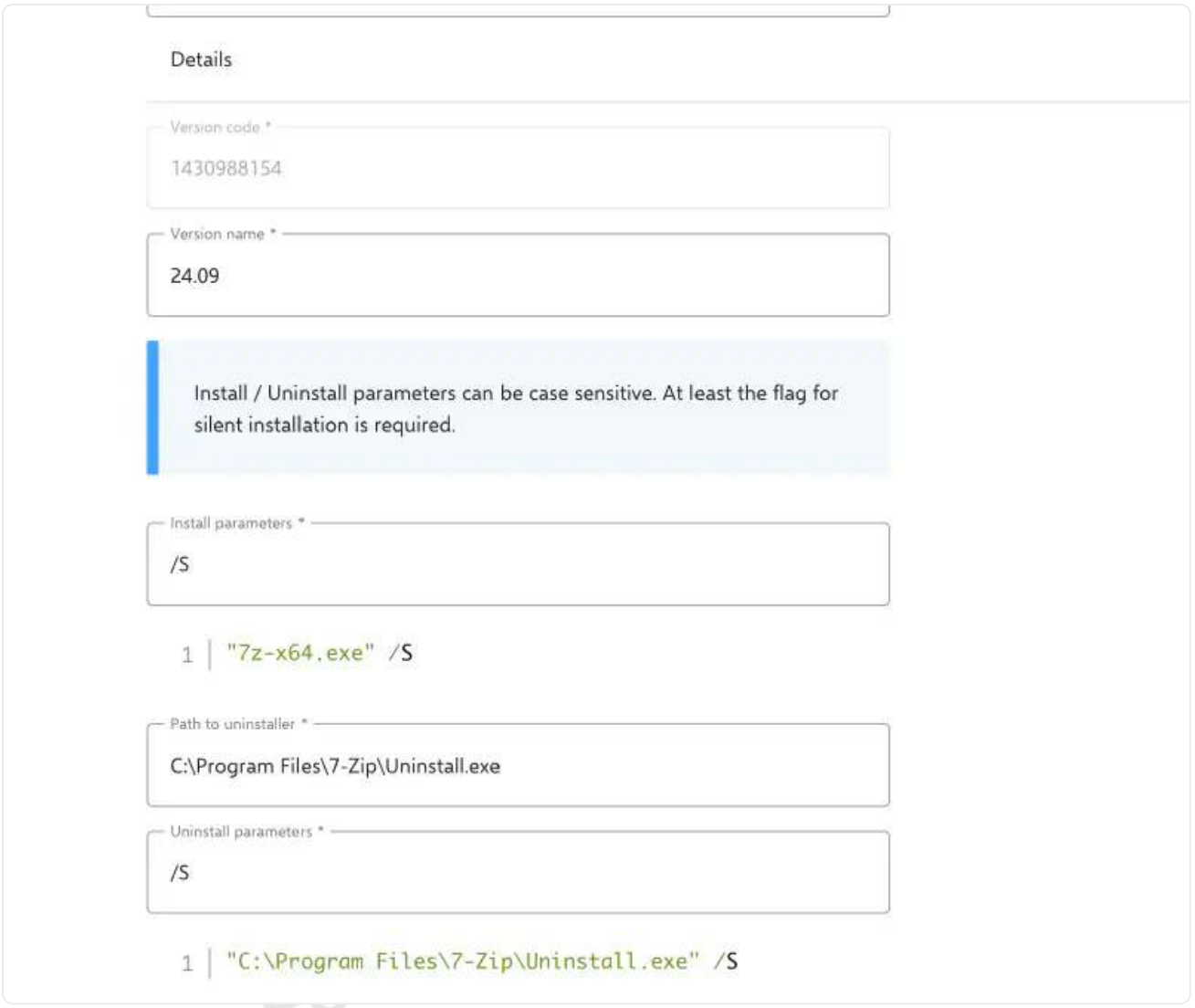
3. After the upload, the app details page opens. The required parameters must be found out by the administrator and entered manually. The minimum information is the Version name and at least one detection rule; for `.exe` apps, the required fields from step 4 are needed as well. As long as required information is missing, the app cannot be saved.



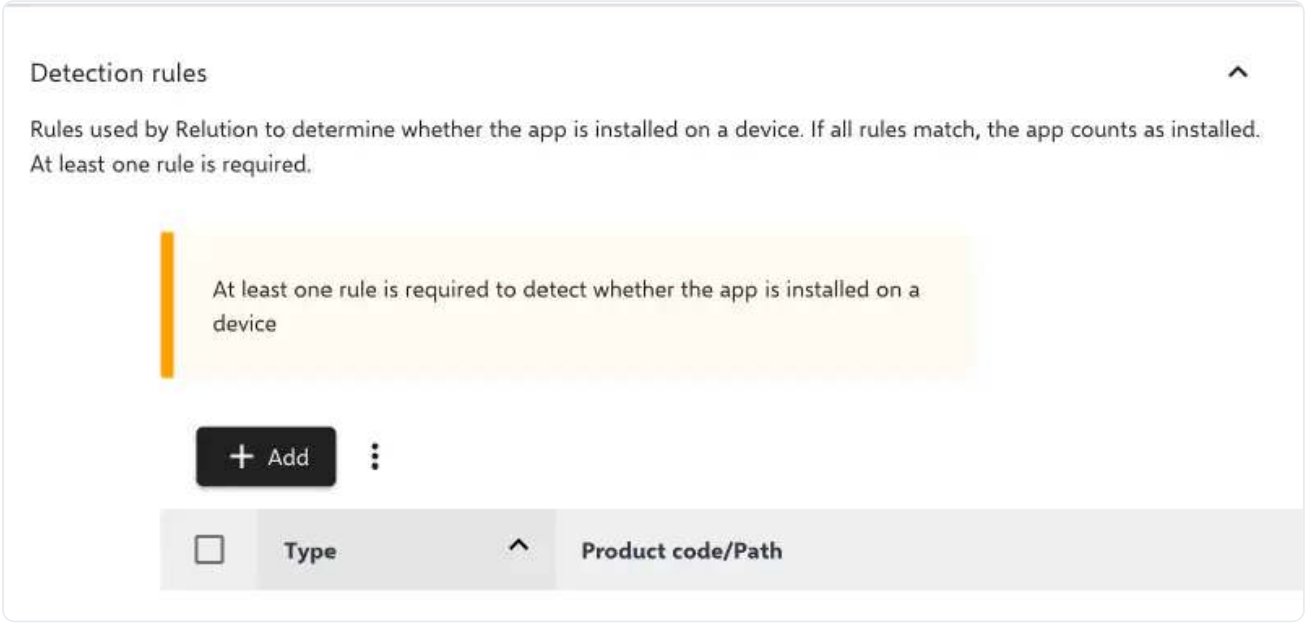
4. Under Version information, the parameters for installation and uninstallation are set:
    - For `.msi` apps, Install parameters and Uninstall parameters are optional. Uninstall parameters can only be edited once an MSI detection rule has been added (see step 7).
    - For `.exe` apps, Install parameters, Path to uninstaller (a valid Windows path to the uninstall program) and Uninstall parameters are required. At least the parameter for a silent installation is needed; parameters can be case sensitive.

    To make installation and uninstallation run in the background without manual intervention, the silent parameter matching the installer is set, e.g. `/s` or `/quiet`. Below the fields, the portal shows a preview of the resulting command, for `.msi` apps for example `msiexec /i <file name> <parameters>` for installation and `msiexec /x {<product code>} <parameters>` for uninstallation.

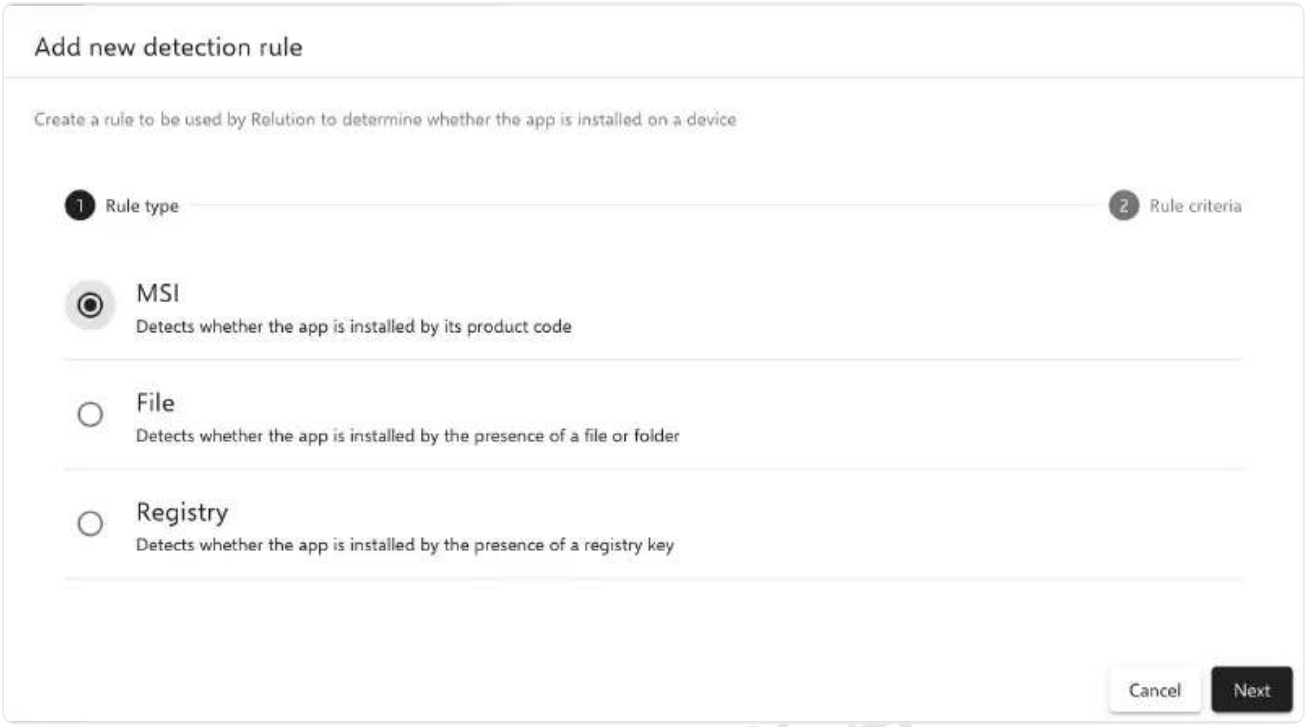




5. Subsequently, detection rules are added that allow the Relution Companion for Windows to uniquely identify the application on the Windows machine.

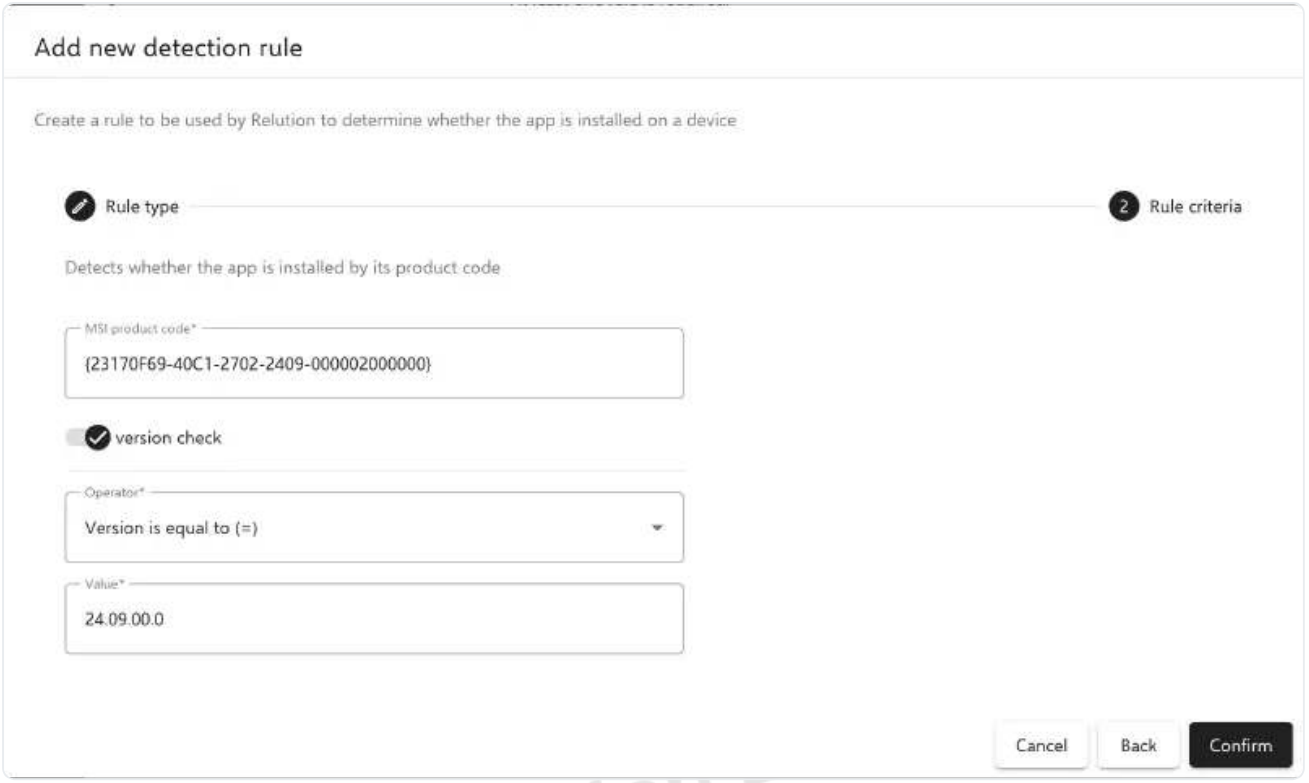


6. Three types of detection rules are available: MSI, File and Registry. At least one rule is required to detect the program on the Windows device. For `.msi` files, the MSI detection rule is required in order to be able to uninstall the app. For `.exe` files, the two detection rules File and Registry are suitable. Several detection rules can be combined; the app only counts as installed if all rules match. One MSI detection rule is possible per app.



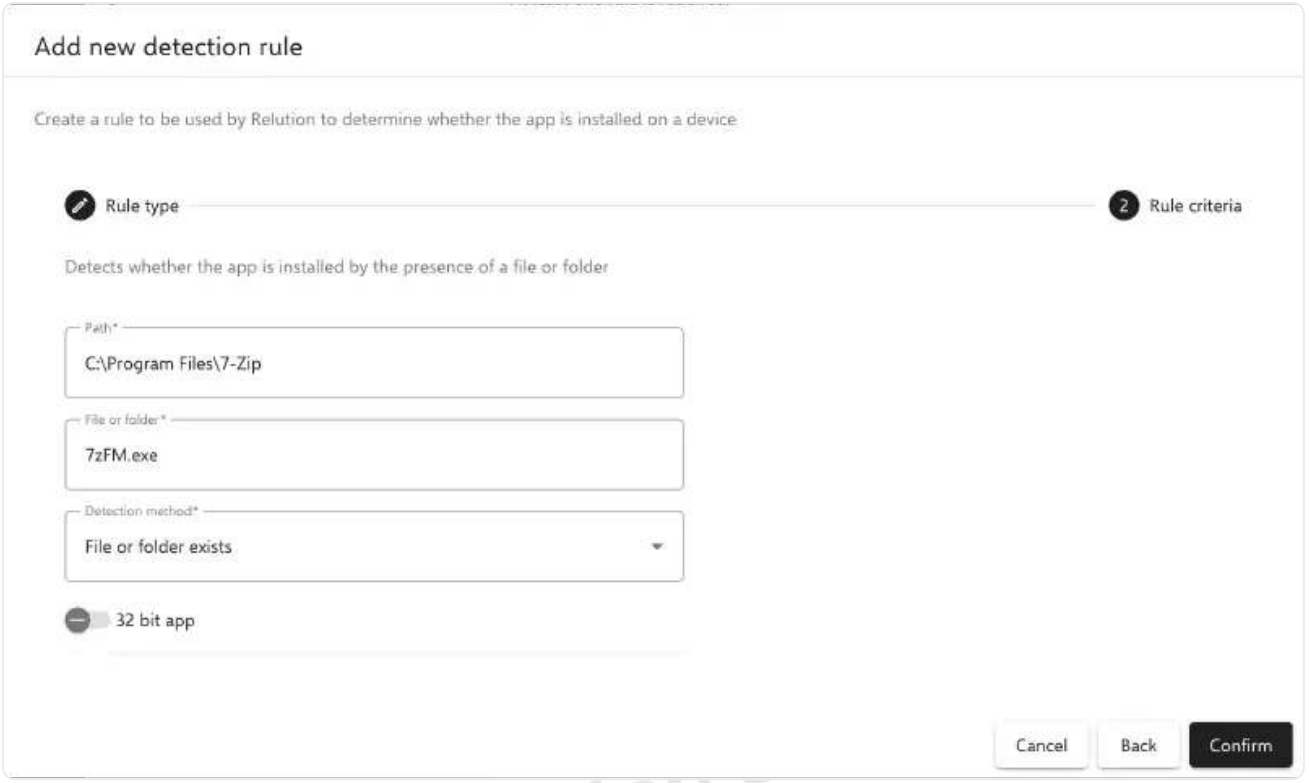
For version 26.4.

7. For the MSI detection rule, the MSI product code of the application is entered in the format `{AAAAAAAA-BBBB-CCCC-DDDD-EEEEEEEEEEEE}`. Since there can be multiple versions of an application, the version check toggle additionally checks the version number. For this, Version is equal to (=) is selected in the Operator field and the version number is entered in Value. With Version does not equal (≠), the rule matches if a version other than the specified one is installed.



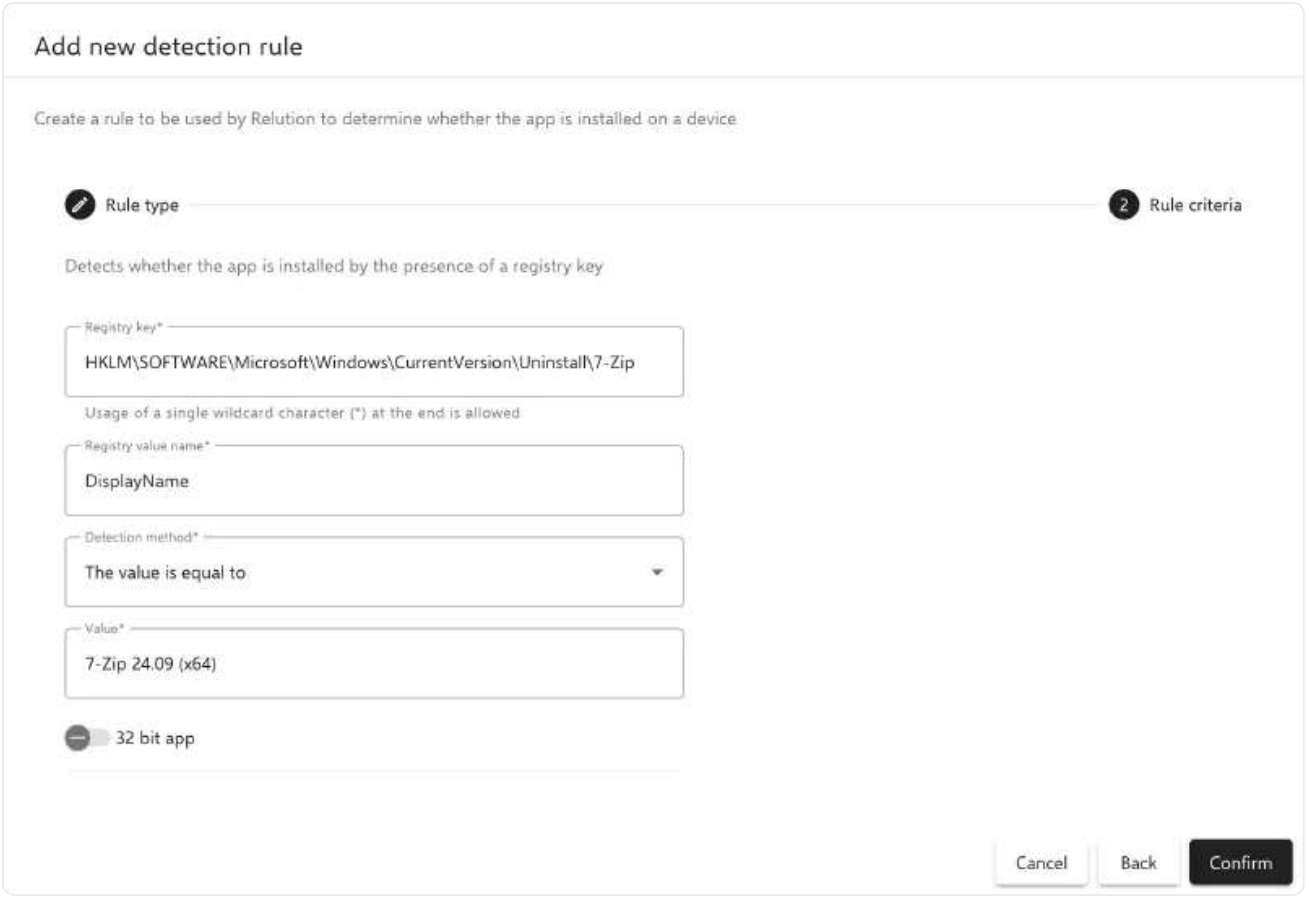
For version

8. The File detection rule detects whether the application is installed on the Windows device by the presence of a file or folder. For this, Path (e.g. `C:\Program Files\myApp`), File or folder (e.g. `myApp.exe`) and the Detection method (File or folder exists or File or folder does not exist) are specified. For 32-bit applications, the 32 bit app toggle is enabled; on 64-bit clients the path is then adjusted automatically, e.g. from `C:\Program Files` to `C:\Program Files (x86)`.

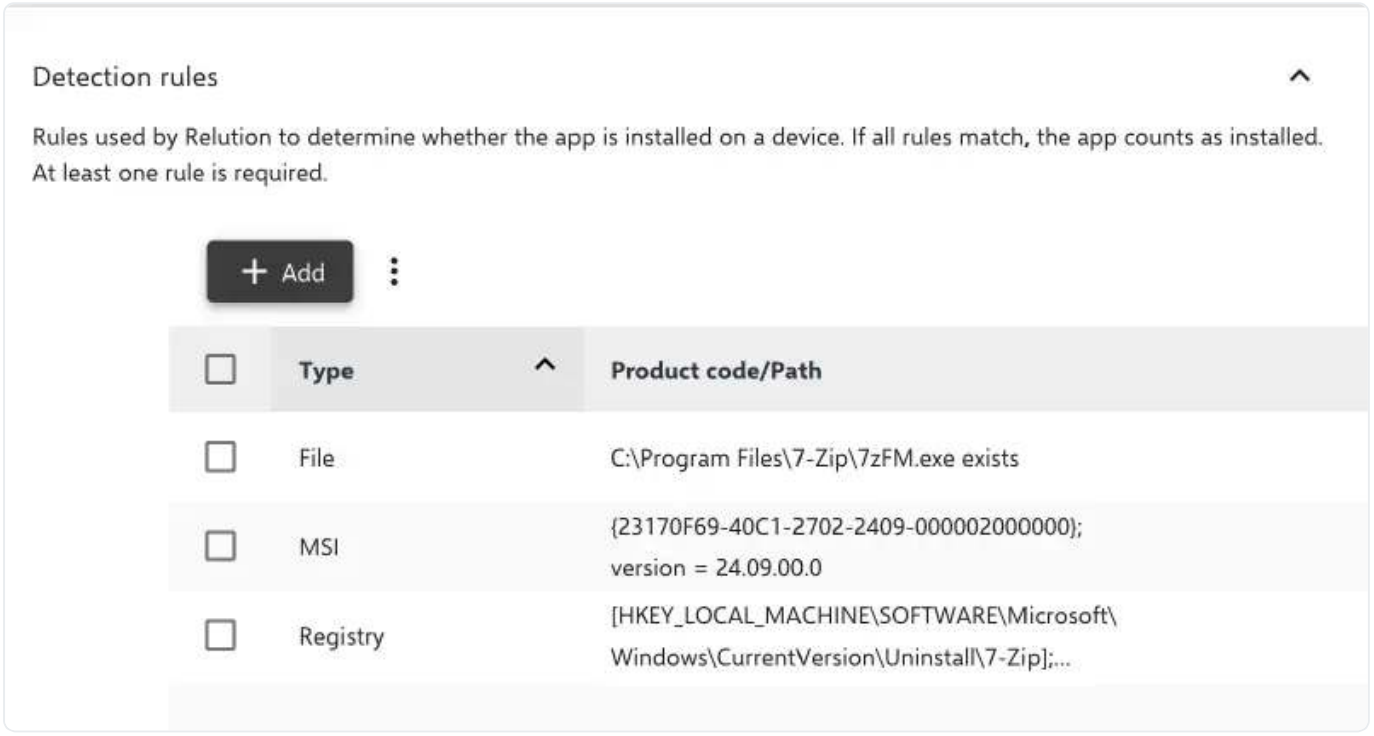


For version

9. The Registry detection rule checks the existence of the application on the Windows device against a registry key. The Registry key, Registry value name and Detection method fields are specified manually; a single wildcard character (`*`) is allowed at the end of the registry key. The registry value name can be chosen freely; a common choice is `DisplayName` in the application's uninstall key. The Detection method options are A value with the specified name exists (default), A value with the specified name does not exist and The value is equal to. The Value field is only active with The value is equal to. To uniquely detect the application on the Windows device, The value is equal to is recommended; the required Value is taken from the installed application. The 32 bit app toggle automatically adjusts the registry key for 32-bit applications on 64-bit clients, e.g. from `HKLM\SOFTWARE\Microsoft` to `HKLM\SOFTWARE\WOW6432Node\Microsoft`.



After adding the required detection rules, the application can be saved.



Afterwards, the native app can be installed and uninstalled on all managed Windows devices via the Relution App Store.

Uninstalling Windows Store Apps

Windows Store apps cannot be uninstalled via the graphical interface. Therefore, it is necessary to remove them locally or via Relution using a PowerShell script. Below are the general steps:

For version 26.4.0

Find the app on the device

```
Get-AppxPackage -Name *<AppName>* -AllUsers
```

Uninstall the app via script

```
Get-AppxPackage -Name *<AppName>* -AllUsers | Remove-AppxPackage -AllUsers
```

> The app's provisioning package may remain on the device. To completely remove the app, first query the provisioning package and determine the PackageFullName.

```
Get-AppxProvisionedPackage -Online | Select PackageName
```

Then remove it completely:

```
Remove-AppxProvisionedPackage -Online -PackageName <PackageFullName>
```

Recommendation: Use WinGet

Whenever possible, WinGet should be used. It provides access to significantly more apps and makes uninstallation easier: WinGet →

For version 26.4.0

WinGet

With Relution 5.26, it is possible to use the WinGet package manager → for app deployments on Windows devices.

> The Limitations and Known issues sections describe important restrictions.

Requirements

1. The WinGet client must be installed on the device. It is available by default on all Windows 11 versions and on Windows 10 from version 2004 (May 2020 Update).
2. The Microsoft Visual C++ Redistributable must be installed on the device, see Limitations →.
3. Relution Server version 5.26 or higher
4. Windows Companion version 1.11 or higher
5. WinGet version 1.6 or higher

Supported Features

For version 26.4.0

Before a broad rollout, each WinGet app should be tested on a test device.

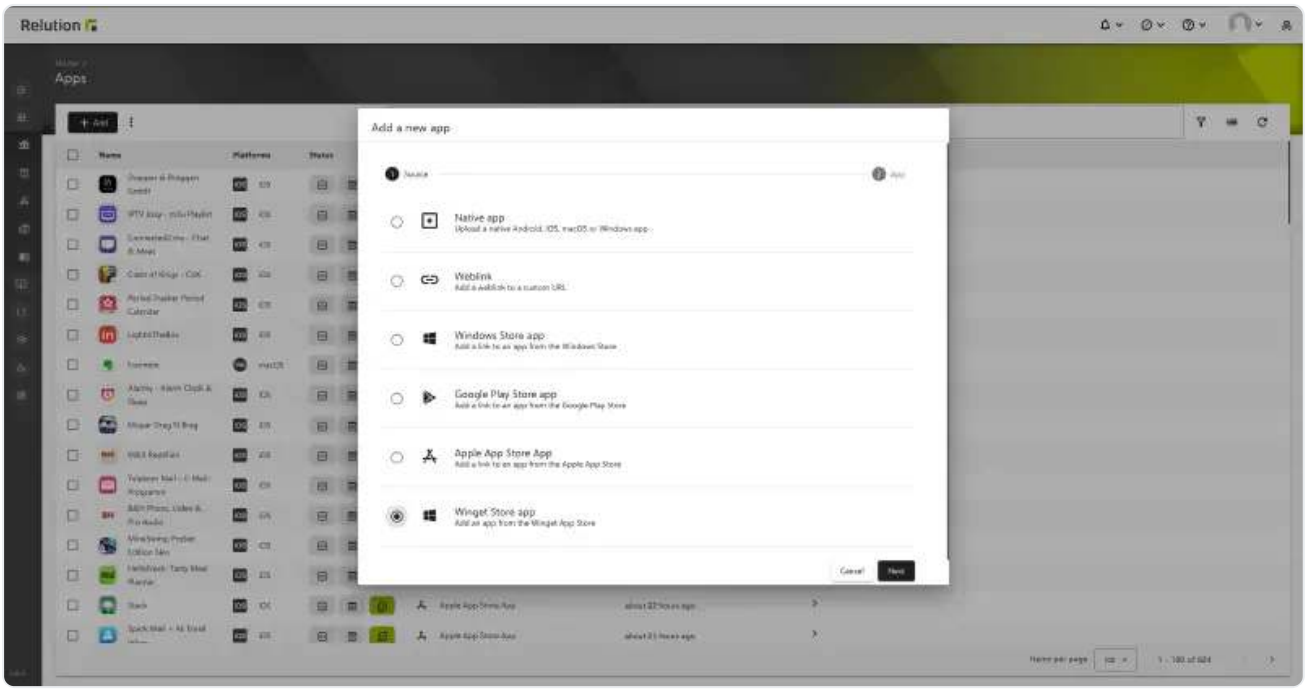
The limitations → and known issues → sections contain more details.

- Searching for and adding WinGet apps to the Relution AppStore
- Deployment of WinGet apps via action, app compliance and auto deployments
- Display of installed WinGet apps in the installed apps list of a device
- Removal of WinGet apps via action
- Automatic update of WinGet apps on the devices

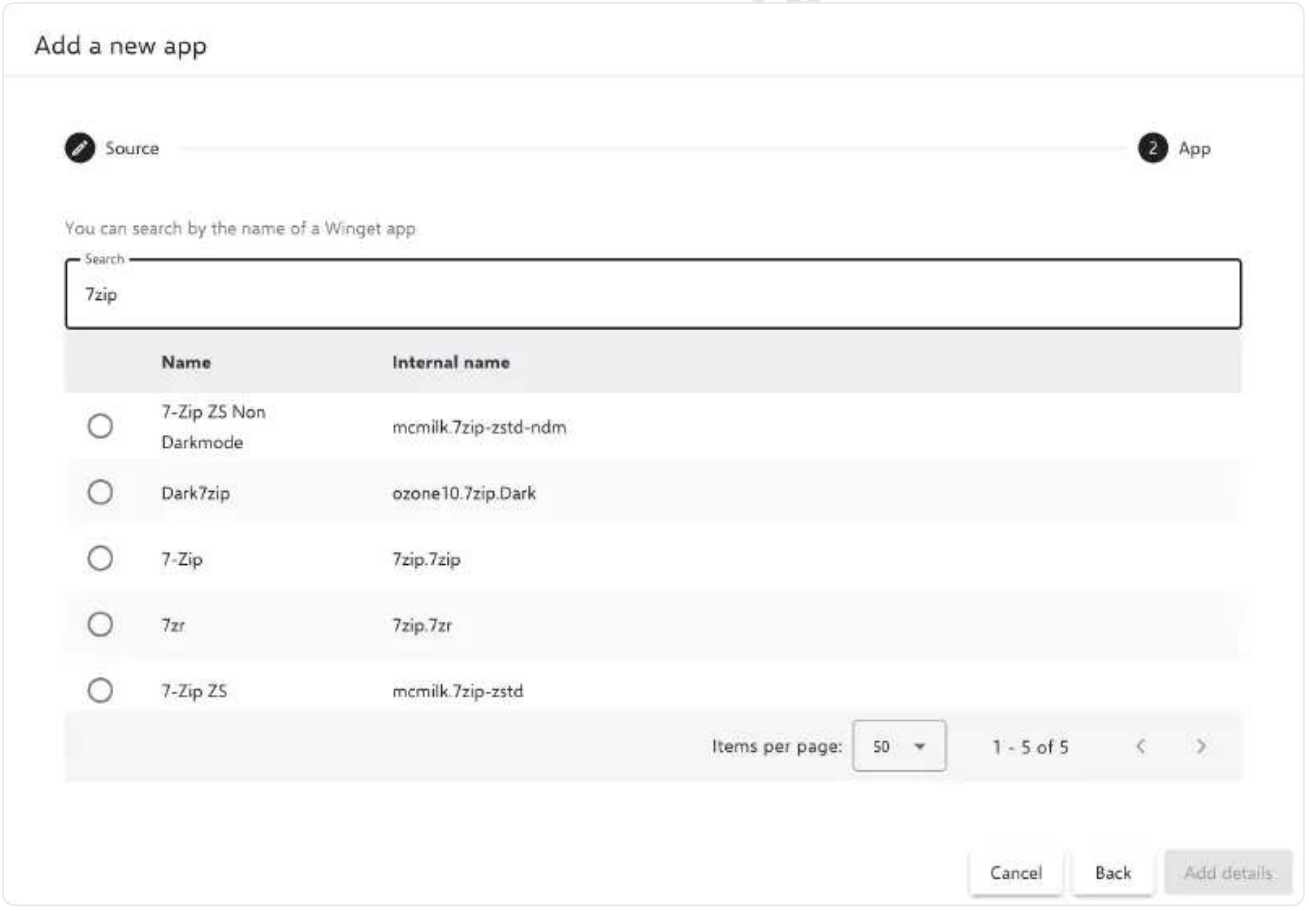
Add WinGet apps to Relution AppStore

WinGet apps must be added to the Relution AppStore before they can be deployed on devices.

1. Under `Apps` → `App Store`, the Add button opens the Add a new app dialog. Winget Store app is selected as the Source.

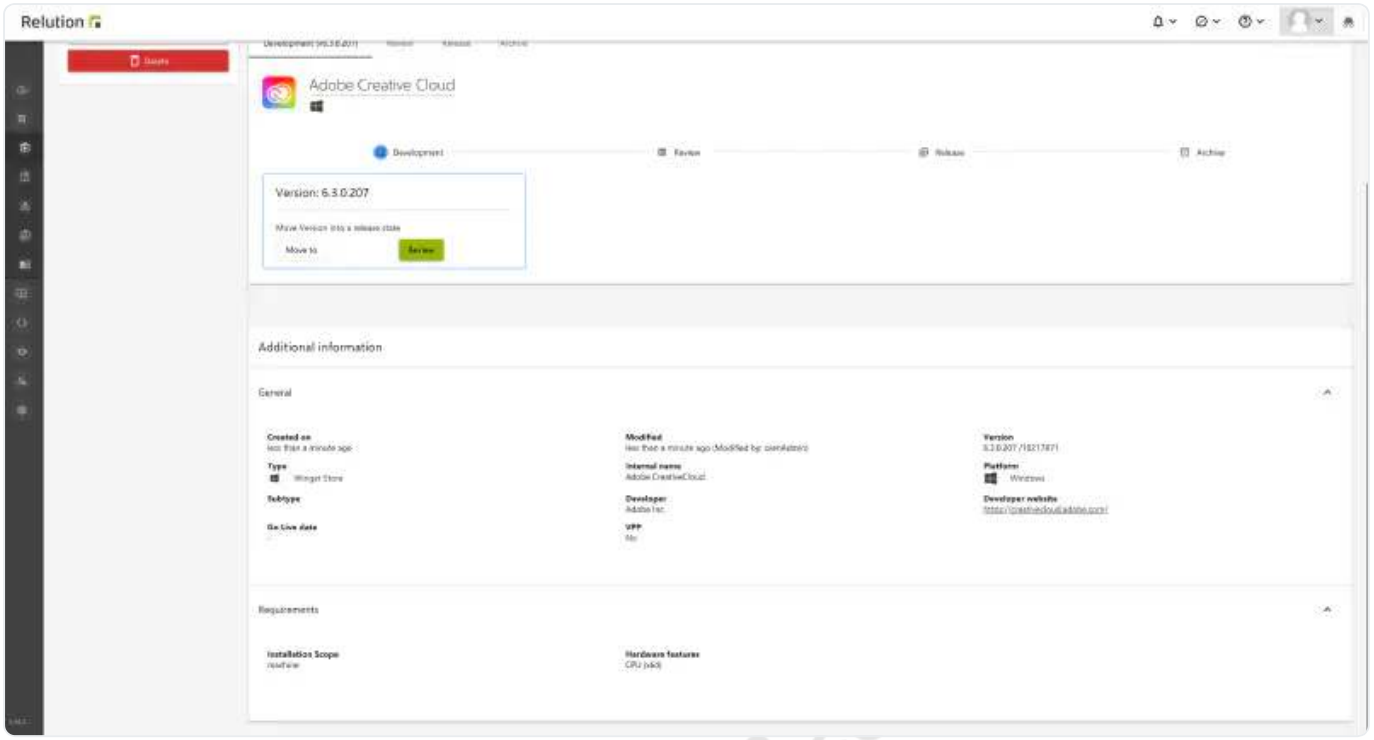


2. The WinGet app is searched for by name, selected and added to the Relution AppStore with Add details.



3. Since WinGet manifests do not contain an icon, Relution uses the favicon of the publisher's website as the app icon where possible. An existing icon, e.g. one uploaded manually, is not replaced. In the app details of a WinGet app, only the icon can be edited; all other fields are read automatically from the store.

The WinGet app details can contain additional information like installation scope, if it is provided for the WinGet app.



For version 26.4.0

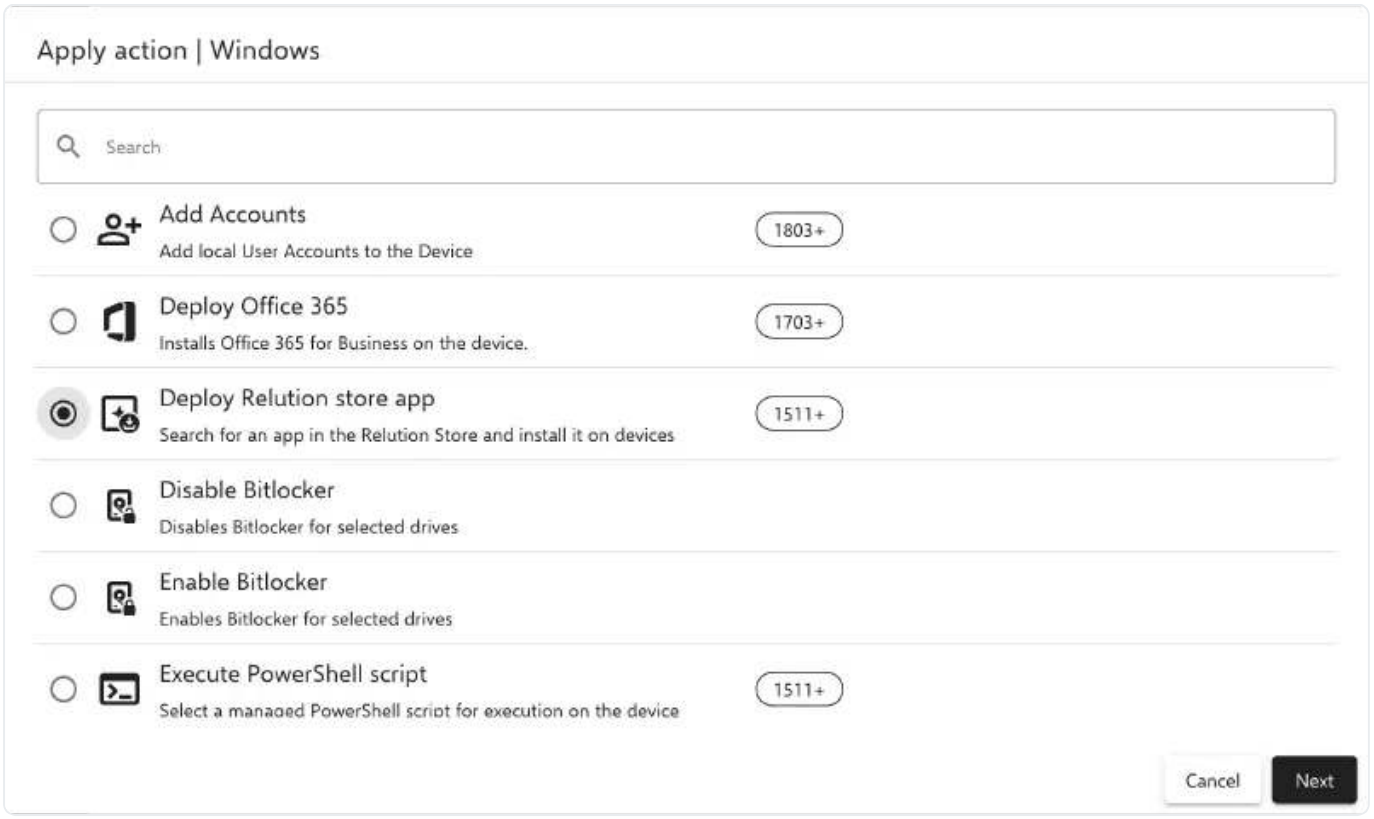
Deploy WinGet apps

After the WinGet app has been added to the Relution AppStore and has a version in the status Release, it can be deployed to Windows devices.

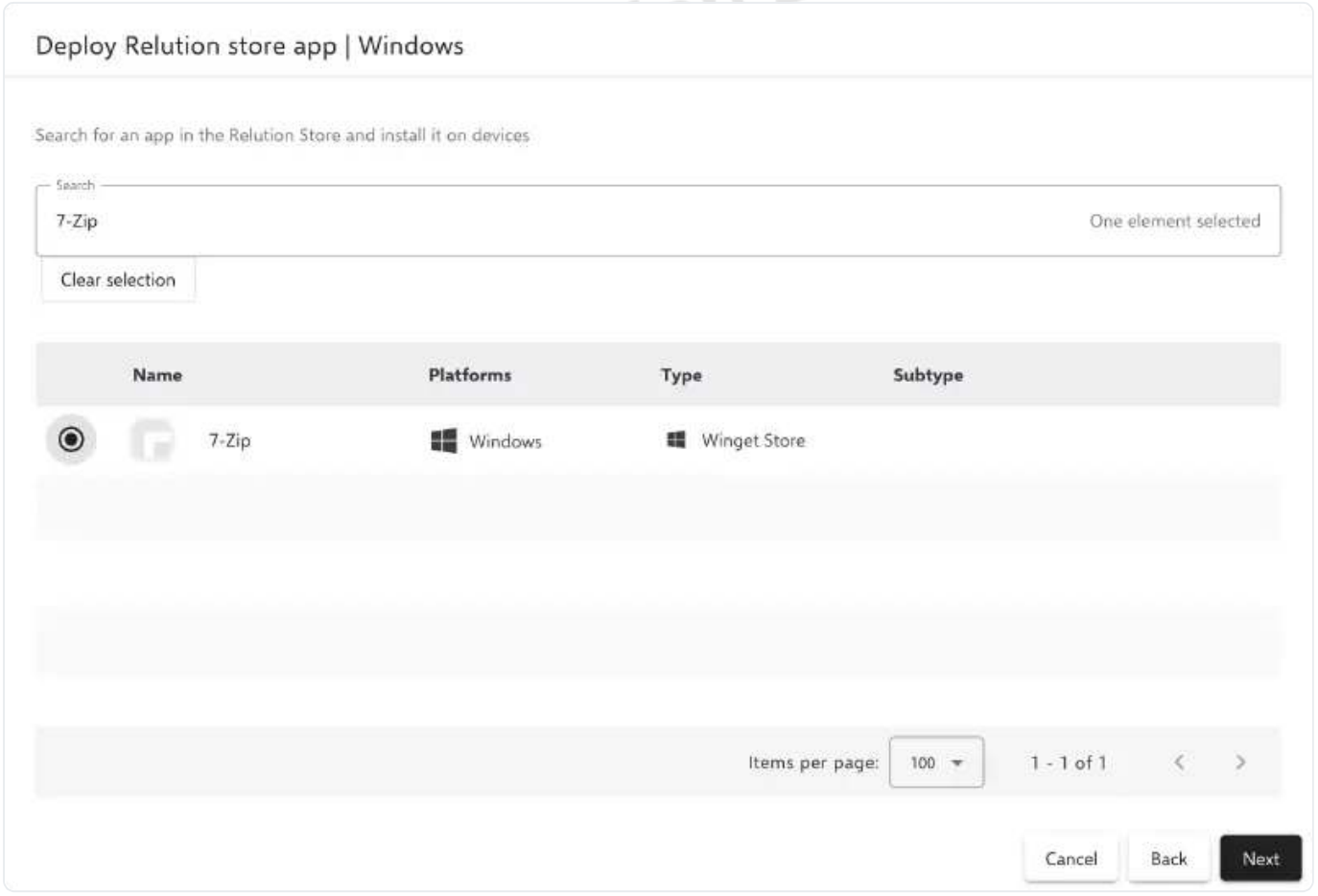
Relution must install the WinGet app completely silently, see Limitations →. Due to this limitation all source and package agreements are automatically accepted when installing a WinGet app via Relution!

Deploy via action

In the action modal of a Windows device, Deploy Relution store app must be selected.



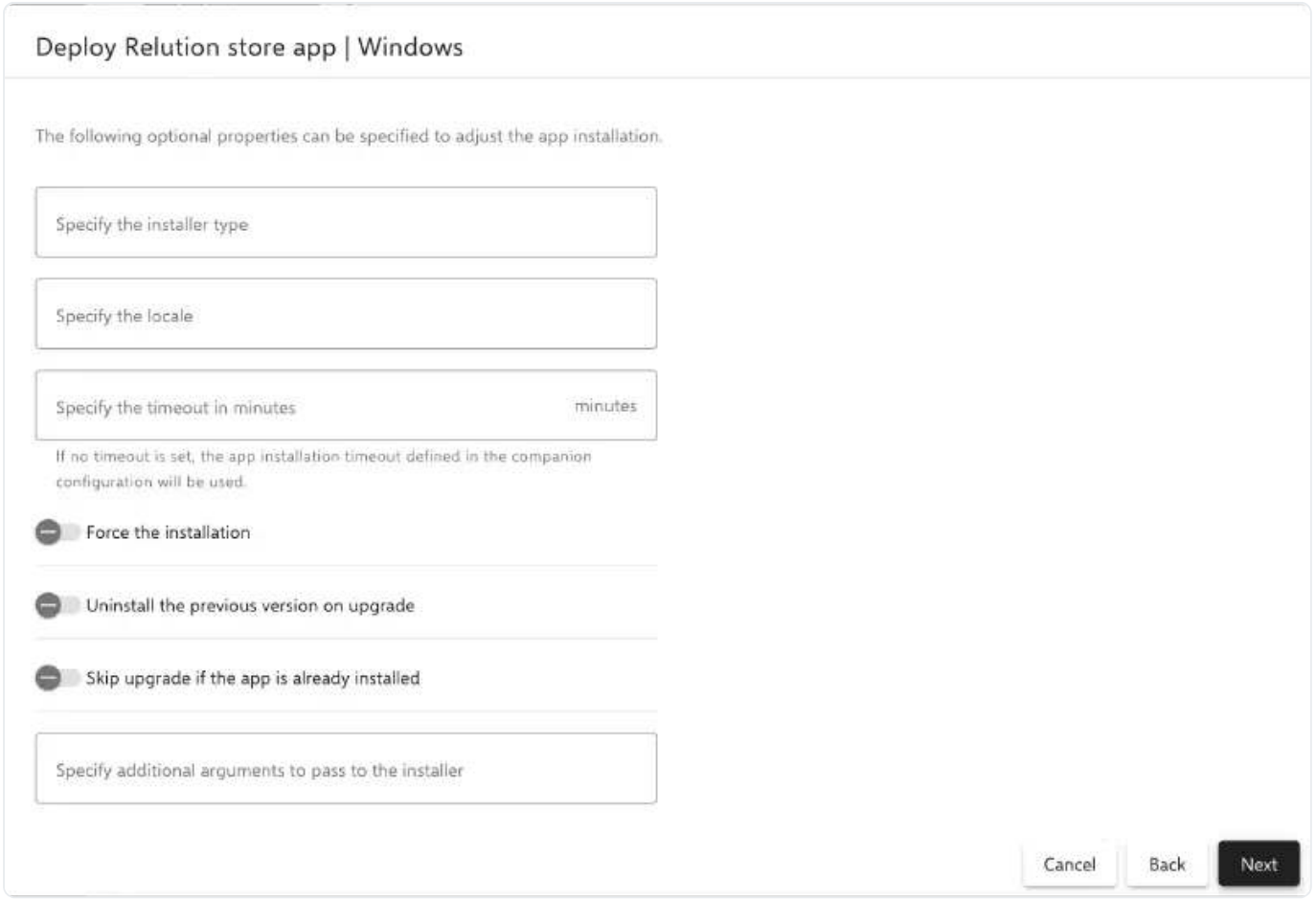
The WinGet app to be deployed is then searched for and selected.



In the next step the deployment can optionally be adjusted. This is currently only possible for the deploy action and not for the app compliance or the auto deployments.

- Installer type: Specifies the installer type to be used, see supported installer types →. The app must support the specified installer type or the install will fail.
- Locale: Specifies the locale to be used (BCP47 format, at most 5 characters, e.g. `en-US`).
- Timeout: Time in minutes (1 to 150) after which the Windows Companion aborts the installation. If the field is left empty, the App installation timeout from the Windows Companion → policy configuration applies.
- Force the installation: Runs the command and continues with non security related issues.
- Uninstall the previous version on upgrade: The previous version of the app is uninstalled on upgrade.
- Skip upgrade: Skips the upgrade if the app is already installed.
- Additional arguments: Passes the specified arguments on to the installer in addition to the defaults.

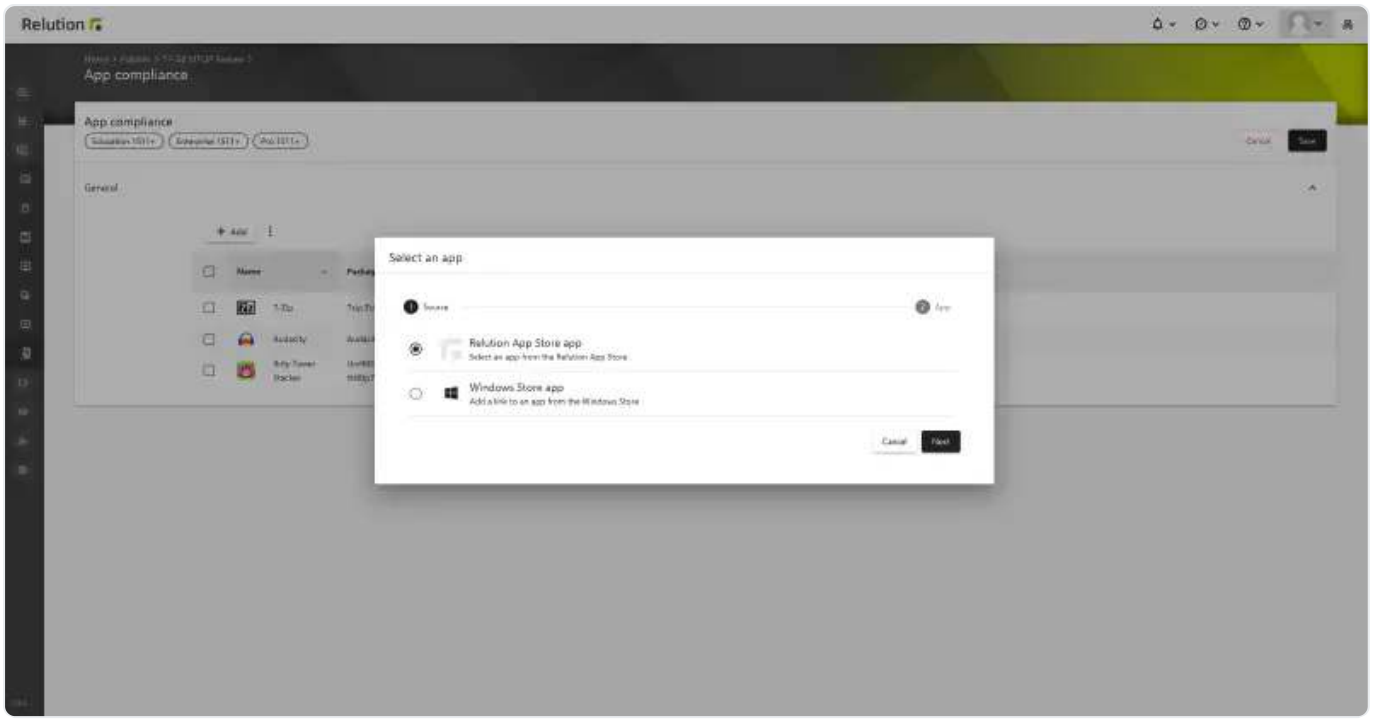
Uninstall the previous version on upgrade and Skip upgrade are mutually exclusive: enabling one of the two options disables the other.



After the confirmation in the last step a deploy app action is created.

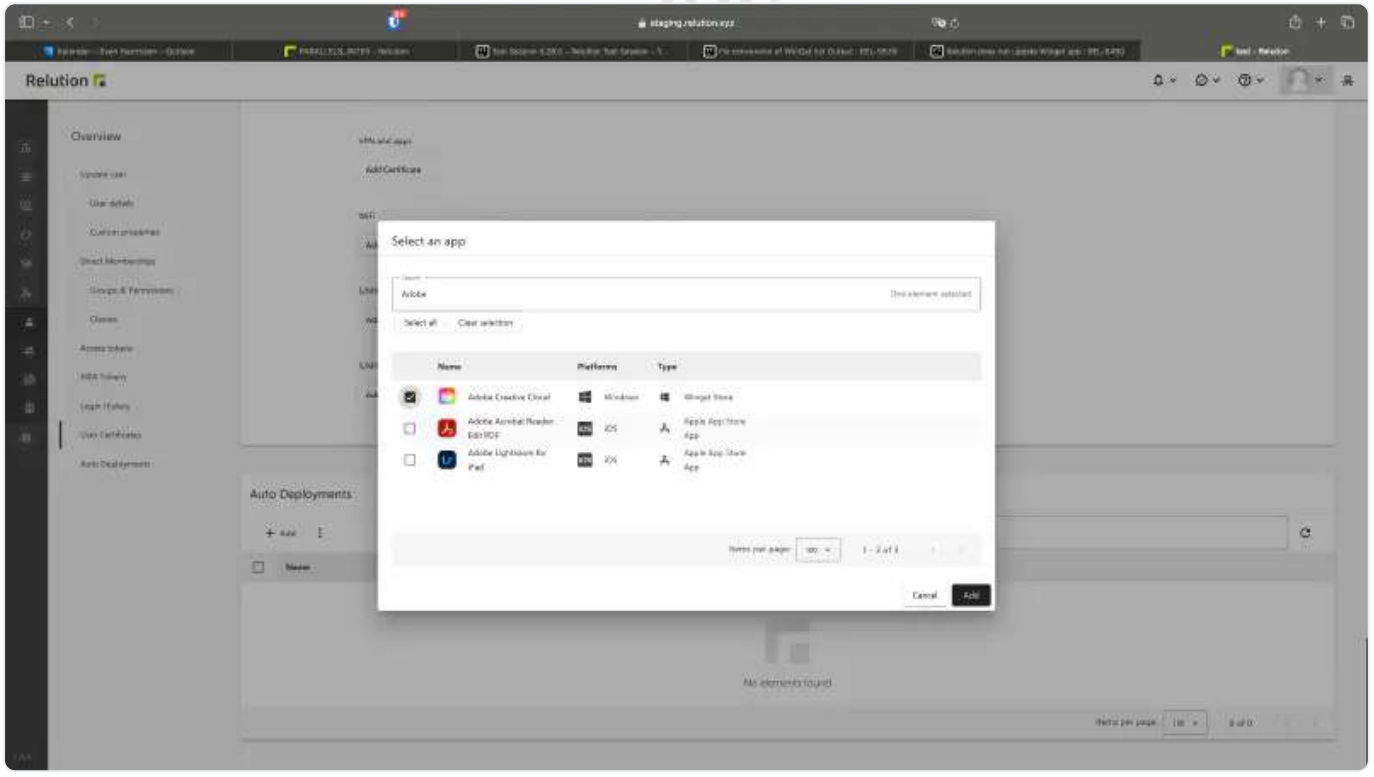
Deploy via app compliance

WinGet apps can be added to the App Compliance of a Windows policy.



Deploy via auto deployments

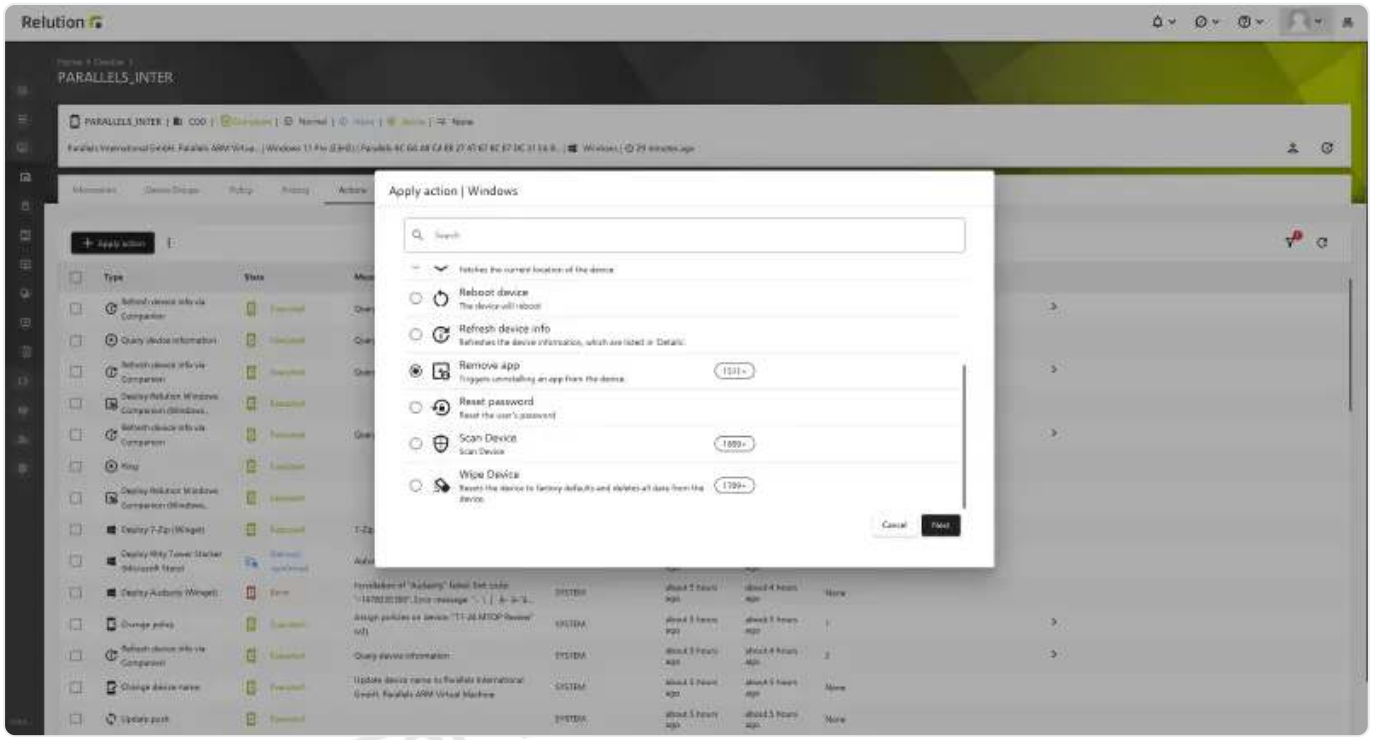
Winget apps can be added to the auto deployments of a user.



Remove WinGet apps via action

WinGet apps can be uninstalled from a device with the Remove app action. The WinGet apps contained in the Relution AppStore are available for selection.

The Windows Companion will execute the winget uninstall command silently, see Limitations →. Due to this limitation the source agreements are automatically accepted when removing a WinGet app from the device.



Automatic update of WinGet apps on the devices

Relution will automatically update installed WinGet apps on the devices.

Requirements:

- The WinGet app must be added to the Relution app store
- The WinGet app must be contained in the installed apps list of the device

The Relution app store checks every day for each contained WinGet app, whether an update is available and refreshes the information of the app. When the Windows Companion refreshes the device details in Relution, Relution compares the version of the installed WinGet app with the version in the status Release in the Relution app store. Only entries of the installed apps list with WinGet as their source are taken into account. If it detects a newer version in the Relution app store, it triggers a deploy app action for this device and the app gets updated. As long as a deploy action for the app is still open on the device, no further action is created.

If the version comparison fails, the automatic update is not triggered (see Known issues →)

Limitations

The following restrictions generally apply to the use of WinGet apps in Relution.

Microsoft Visual C++ Redistributable must be installed

The Windows Companion executes WinGet commands in system context. This requires that the Microsoft Visual C++ Redistributable is installed on the device.

When the Windows Companion starts, it checks if this dependency is installed. If it is missing the Companion tries to download and install it. If it could not be installed, the Windows Companion writes a log entry into the event viewer on the device.

If this issue occurs, WinGet actions will fail. The error code -1073741515 of the failed action can be an indicator for this. In that case it is possible to install the latest Microsoft Visual C++ Redistributable → manually as a native app with a detection rule, see Known issues →

WinGet client must be installed on the device

Relution does not install the WinGet client. If the option Manage WinGet and its dependencies is enabled in the Windows Companion → policy configuration (default), the Windows Companion updates WinGet and its dependencies, such as the Microsoft Visual C++ Redistributable, when it starts. If the option is disabled, the Windows Companion does not update WinGet; it still installs a missing Microsoft Visual C++ Redistributable. The WinGet client is available by default on all Windows 11 versions and on Windows 10 from version 2004 (May 2020 Update). It is packaged in the AppInstaller, which can be installed from the Microsoft Store.

For version 26.4.0

Only silent install and uninstall is supported

The WinGet app installation or uninstallation is executed by the Windows Companion. The Windows Companion is a background process, which cannot show any UI on the device. Therefore it will fail to install or remove the app, if it cannot be executed completely silent.

The Windows Companion will automatically add all possible commands to execute the install or uninstall silently:

```
winget install --silent --disable-interactivity --accept-package-agreements --accept-source-agreements
```

```
winget uninstall --silent --disable-interactivity --accept-source-agreements
```

But for some apps even those commands do not prevent the app from showing a dialog. One example is Mozilla Firefox during uninstallation.

Known issues

It is recommended to test the install and uninstall of each WinGet app on a test device before using it in production.

If the WinGet app should be used in an app compliance or in auto deployments, it must be contained in the installed apps list on the device after it has been installed and the device details have been refreshed.

If the automatic update of an installed WinGet app is important, the installed apps list must contain the app and have a correct value in the version column.

Some apps cannot be prevented from showing a dialog

If an app cannot be prevented from showing a dialog the install or uninstall will fail.

It may be possible to use a different installer in the deploy app action to work around this issue.

How to find out

- PowerShell is opened as administrator on a test device
- For the installation, the command `winget install --id <id> --silent --disable-interactivity --accept-source-agreements --accept-package-agreements` is executed, with `<id>` replaced by the WinGet ID of the app
  - If no dialog or prompt is shown, the app can be installed silently
  - Otherwise, another installer can be used by adding `--installer-type <installer-type>` to the command, if the app supports more than one.
- For the uninstallation, `winget uninstall --id <id> --silent --disable-interactivity --accept-source-agreements` is executed
- If no dialog or prompt is shown, the app can be removed silently

Alternative

If the app cannot be installed or uninstalled, using a native app with detection rules is recommended instead.

Some apps cannot be installed in system context

The WinGet client is currently not supported to be used in system context. But the Windows Companion runs in this context and therefore for some apps the installation might fail.

How to find out

- On a test device, it is tested whether the app can be installed silently, see Known Issues →.
- The app is removed from the test device again.
- The same app is installed on the same test device via Relution.
- If the installation fails, it might not be installable via system-context

Alternative

If the app cannot be installed or uninstalled, using a native app with detection rules is recommended instead.

For version 26.4.0

Some apps are not shown in the installed apps list

Some apps are not shown in the installed apps list, although WinGet recognizes them as installed. These apps should not be used in an app compliance configuration or in auto deployments, because they can currently not be detected correctly and that would cause a lot of failing deploy actions.

How to find out

- A WinGet app is installed on a test device
- The device details are refreshed in Relution
- The app should now be shown in the installed apps list

Alternative

If this issue occurs, using a native app with detection rules is recommended instead.

Some apps have wrong values in the installed apps list

Some detected WinGet apps have wrong values in the installed apps list, e.g. for the version. These apps can still be used in the app compliance configuration, but if the version is incorrect the automatic update might not work.

How to find out

- A WinGet app is installed on a test device
- The device details are refreshed in Relution
- The app is shown in the installed apps list, but has wrong values in the columns

For version 26.4.0

Alternative

If the automatic update of this app is not important, it can be used. Otherwise, using a native app with detection rules is recommended.

Duplicate detection of installed apps

If native apps with detection rules have been deployed on a device, the app might be shown twice in the installed apps list.

This does not mean that the app is installed twice.

It just means that the app is detected by the detection rule and by WinGet.

How to find out

- An app with detection rule is installed on a test device
- The device details are refreshed in Relution
- The app is shown twice in the installed apps list. The name and other displayed information might differ slightly

Alternative

Currently there is no alternative for this behaviour. The duplicate entries can only be prevented, if the corresponding native app with detection rule is removed from Relution app store and the WinGet app is used instead.

Due to the limitations → and known issues → of WinGet apps it is not recommended to switch from native apps with detection rules to WinGet apps!

Missing dependency Microsoft Visual C++ Redistributable

As mentioned in limitations section → the dependency *Microsoft Visual C++ Redistributable* is required to be able to work with WinGet apps in Relution.

Therefore, the Windows Companion tries to install it on the device, if it is missing. This check is executed when the Windows Companion is started, e.g. after it is fresh installed or the device is rebooted.

It may happen that the automatic installation of the Microsoft Visual C++ Redistributable fails, which causes all WinGet commands to fail.

How to find out

- A WinGet app is installed via Relution
- The app is not installed on the device
- The action is marked as failed and possibly contains the error code -1073741515

Alternative

The latest Microsoft Visual C++ Redistributable → can be manually installed as a native app with a detection rule.

For version 26.4.0

1. Downloading the .exe file for the architecture (x64, arm64, x86) of the device
2. Adding a new native app
    - It is suggested to add the architecture in the app name to avoid confusion, e.g. *VC Redist x64*
    - Suggested install parameters: `/install /quiet /norestart`
    - Suggested uninstall parameters: `/uninstall /quiet`
    - Path to uninstaller: must be determined for each version and architecture, see below
    - Suggested detection rule:
        - Registry
        - Registry key: HKLM\SOFTWARE\Microsoft\VisualStudio\14.0\VC\Runtimes\{x64|x86|arm64}, see Microsoft documentation →
        - Registry value name: Version
        - Detection method: A value with the specified name exists
3. Deploying the app on the devices with the same architecture
4. The action should succeed
5. Refreshing the device details
6. The app should be contained in the installed apps list

How to detect the path to the uninstaller:

- Opening the registry key: HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\
- Searching for the key of the vc_redist.{x64|x86|arm64}.exe. The key is a product code, e.g. *{2d48c97b-0c1e-4160-b3c4-c6dabebde745}*
- The path to the uninstaller can be found in the value: QuietUninstallString, e.g. *C:\ProgramData\Package Cache\{2d48c97b-0c1e-4160-b3c4-c6dabebde745}\VC_redist.arm64.exe*

WinGet upgrade fails with broken manifest

Some apps fail to upgrade with `winget upgrade`, even when a newer version is listed in the Relution app store. If the cause is a broken upstream manifest on the WinGet side, the upgrade command exits with one of the following error codes -1978335189 (*no applicable upgrade*), -1978335215 (*package not found*), -1978335192 (*no applicable installer found*), or -1978335216 (manifest / installer failure) and the app may still be installable via a script.

How to find out

- The automatic update or a deploy action for the app fails
- The failed action reports one of the error codes above

Alternative

The upgrade can be retried as a forced install via a Relution script, see WinGet Upgrade Workaround →.

For version 26.4.0

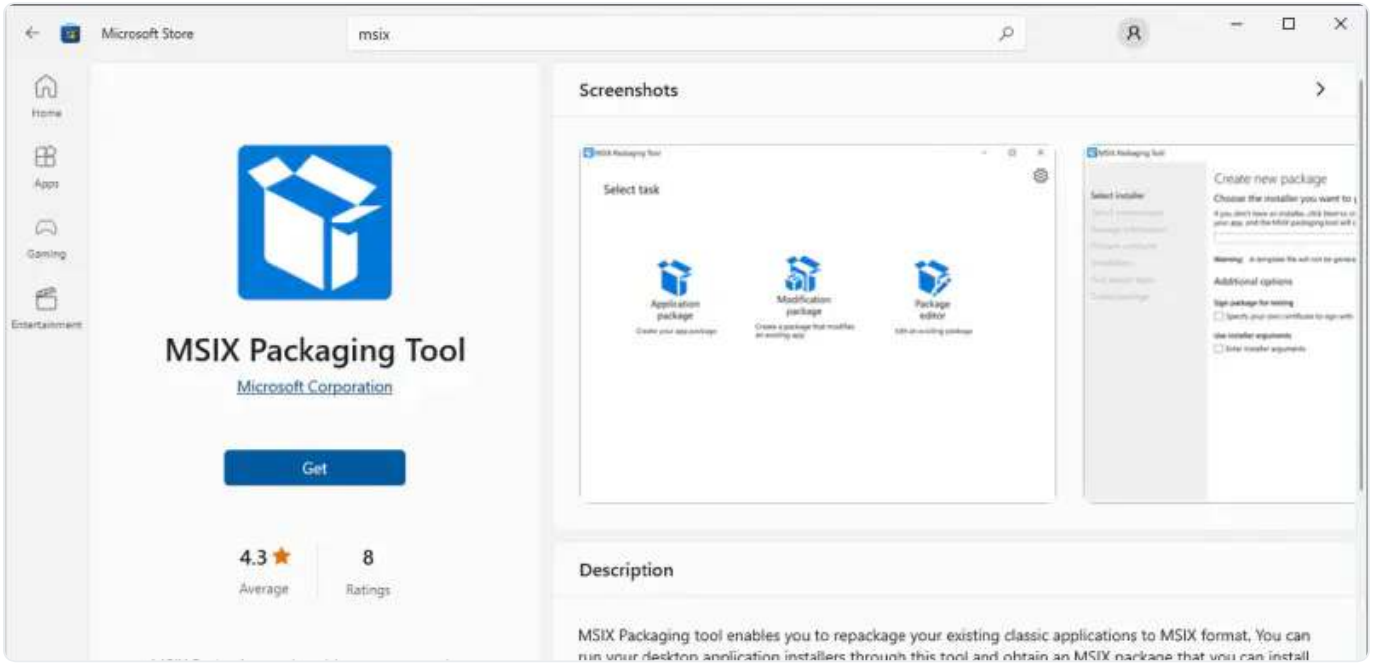
Create MSIX files

The MSIX format is a Windows app package format used to create and distribute applications in Windows 10/11. These MSIX files are usually not available via a simple download, as they need to be certified and “repackaged” before being installed on Windows devices.

> MSIX files, APPX and Microsoft Store apps cannot be uninstalled from devices via Relution directly; only MSI and EXE files and WinGet apps can be uninstalled.

MSIX Packaging Tool

The creation of MSIX files requires the MSIX Packaging Tool, which can be downloaded from the Microsoft Store → and installed on a Windows device.



Certificate creation

The next step is to create a certificate. This can be done comfortably via PowerShell. If necessary, the name of the certificate and/or the password are adjusted in the script.

```
# Generate a new self signed certificate with the subject 'CN=Relution', the key
algorithm RSA,
# the key length 2048, the key usage DigitalSignature and the type CodeSigningCert and
save it
# in the personal certificate store of the current user
$Newcert = New-SelfSignedCertificate -Subject 'CN=Relution' -KeyAlgorithm RSA -
KeyLength 2048 -KeyUsage DigitalSignature -Type CodeSigningCert -CertStoreLocation
Cert:\CurrentUser\My

# Get the thumbprint of the newly generated certificate
$thumbprint = $Newcert.Thumbprint

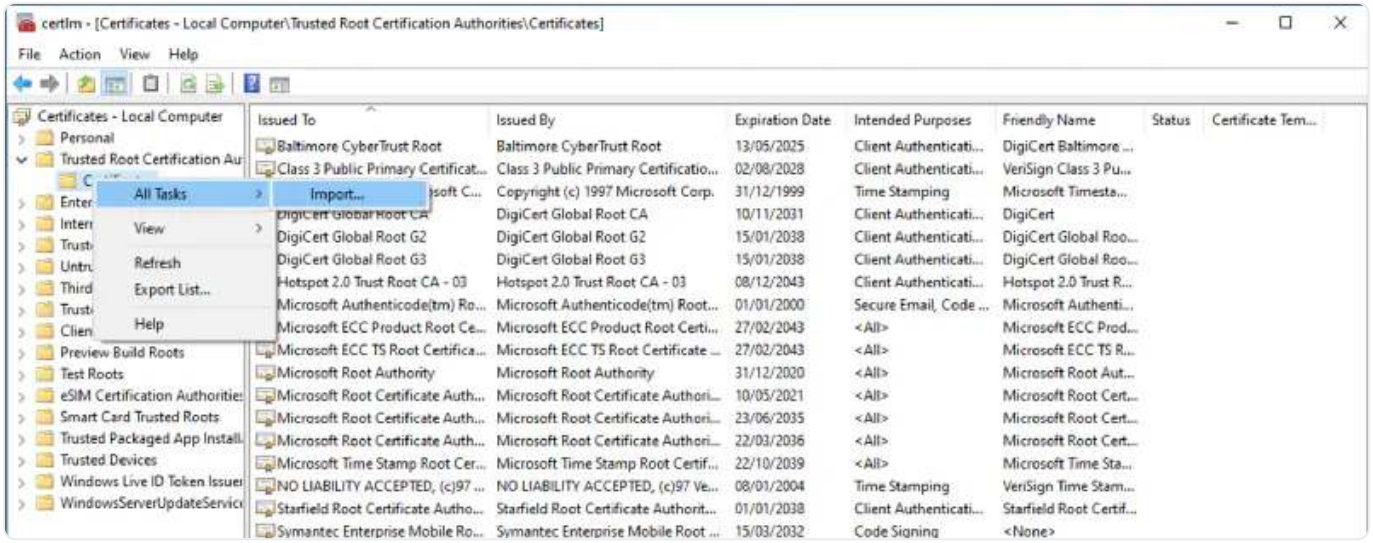
# Get the certificate object from memory by its thumbprint
$cert = (Get-ChildItem -Path cert:\CurrentUser\My\$thumbprint)

# check if the certificate was retrieved successfully
if ($cert -ne $null) {
    # convert the plaintext password string to a secure string
    $Secure_String_Pwd = ConvertTo-SecureString "Passw0rd" -AsPlainText -Force

    # Export the certificate to a PKCS#12 file on the user's desktop
    Export-PfxCertificate -Cert $cert -FilePath
$env:USERPROFILE\desktop\MSIXZertifikat.pfx -Password $Secure_String_Pwd

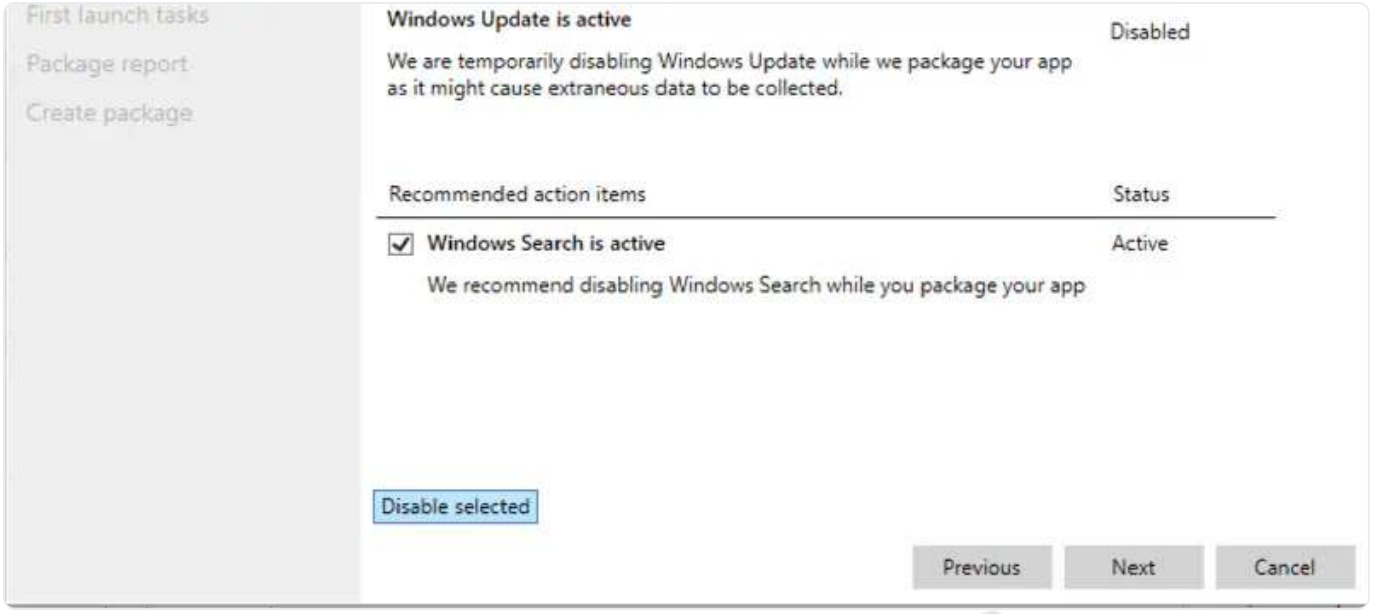
    # Remove the certificate from memory
    Remove-Item cert:\CurrentUser\My\$thumbprint
}
```

The created certificate must be stored in the Trusted Root Certification Authorities category on all Windows 10/11 devices where MSIX files are to be installed. This can be done either with Relution via the policy configuration Certificate or manually, directly on the devices. The password string in the example is Passw0rd. To add the certificate manually, the certificate management Manage Computer Certificates is started as an administrator.



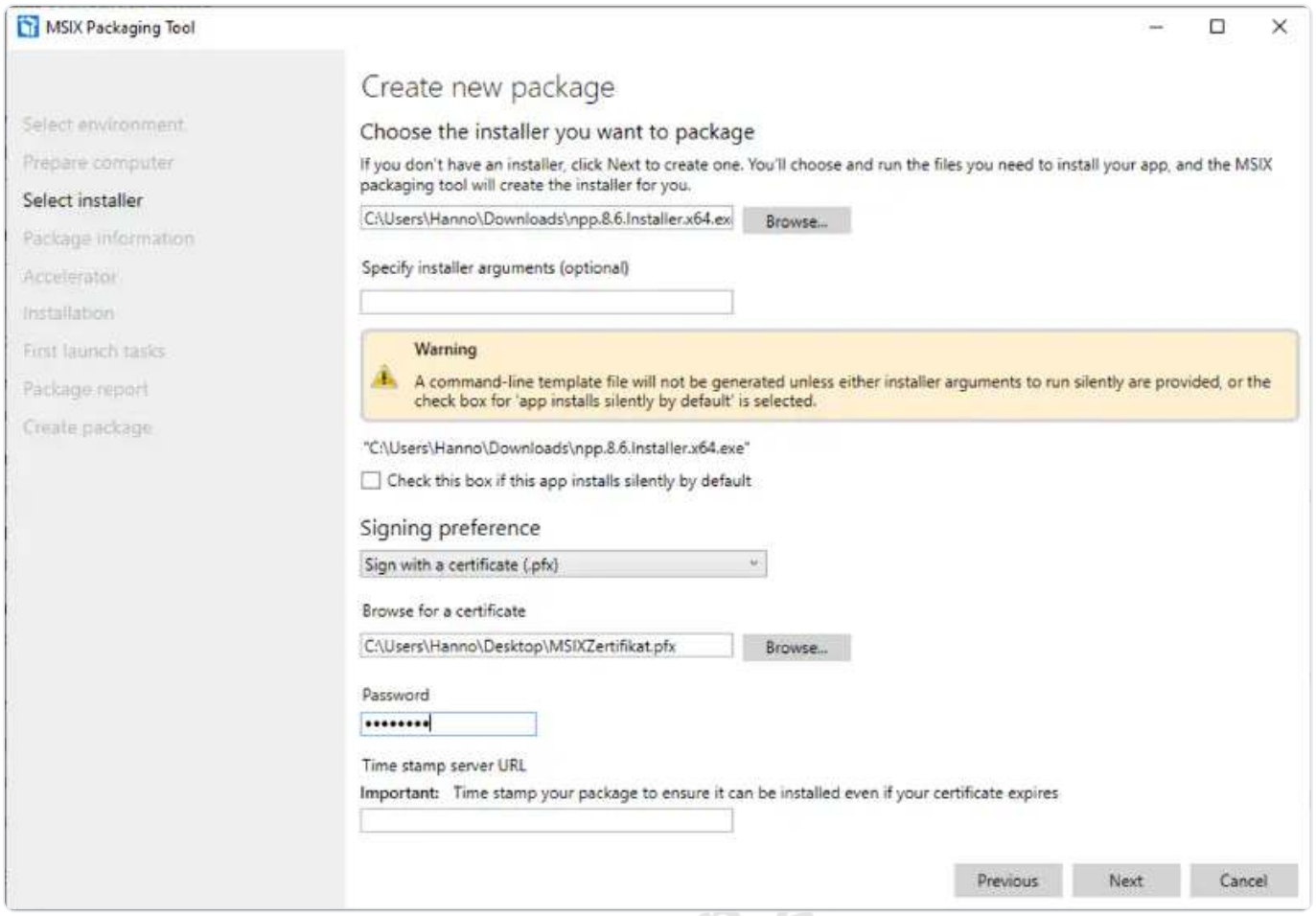
Creation of MSIX files

In the MSIX Packaging Tool, the option to create a new app package is selected. In the following dialog, Windows Search is active is unchecked.



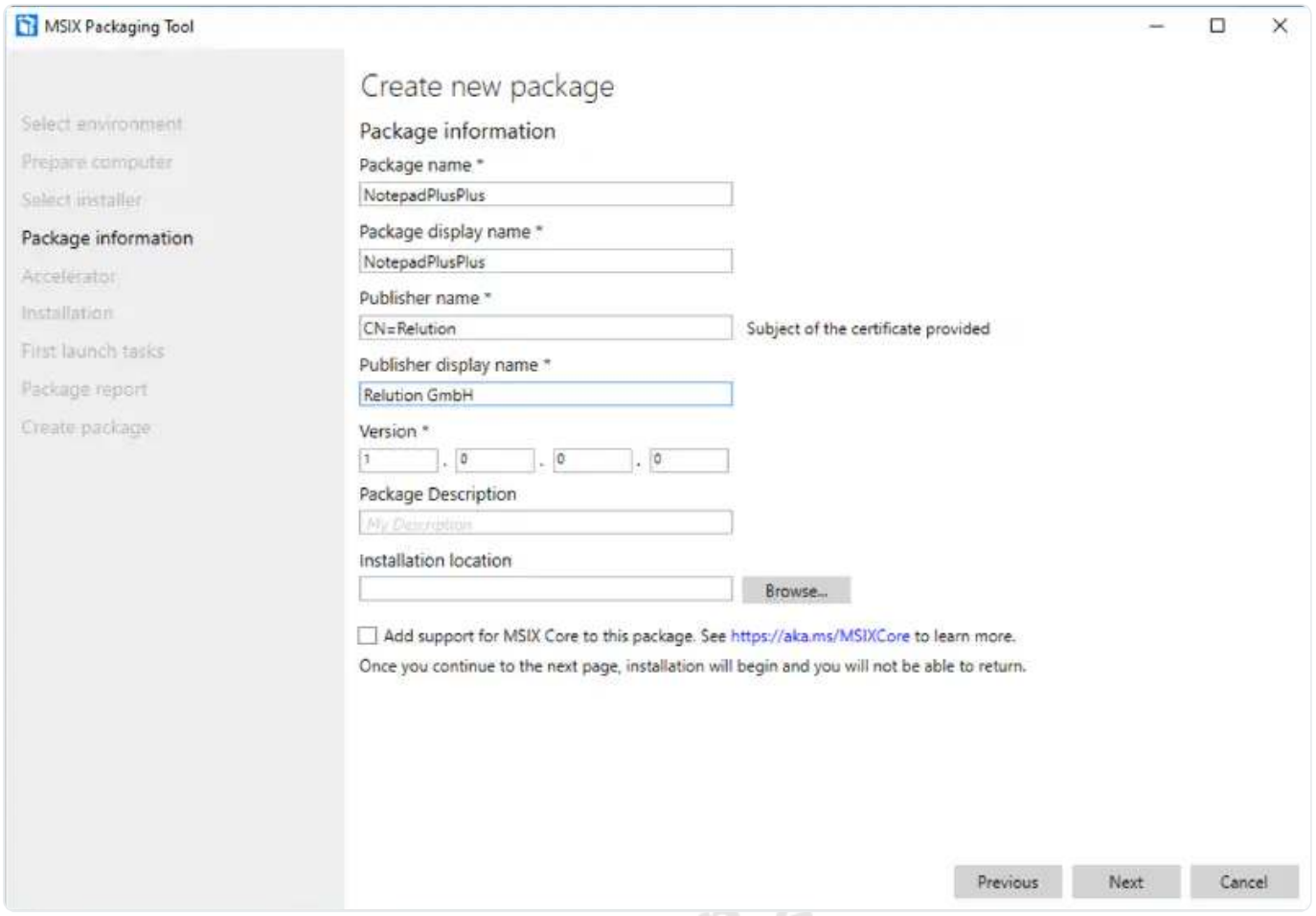
In the example, an MSIX file is created for Notepad++. First, the setup file has to be downloaded. Then the file and the certificate have to be selected in the MSIX Packaging Tool. The Signing preference must be set to Sign with a certificate (.pfx).

For version 26.4.0



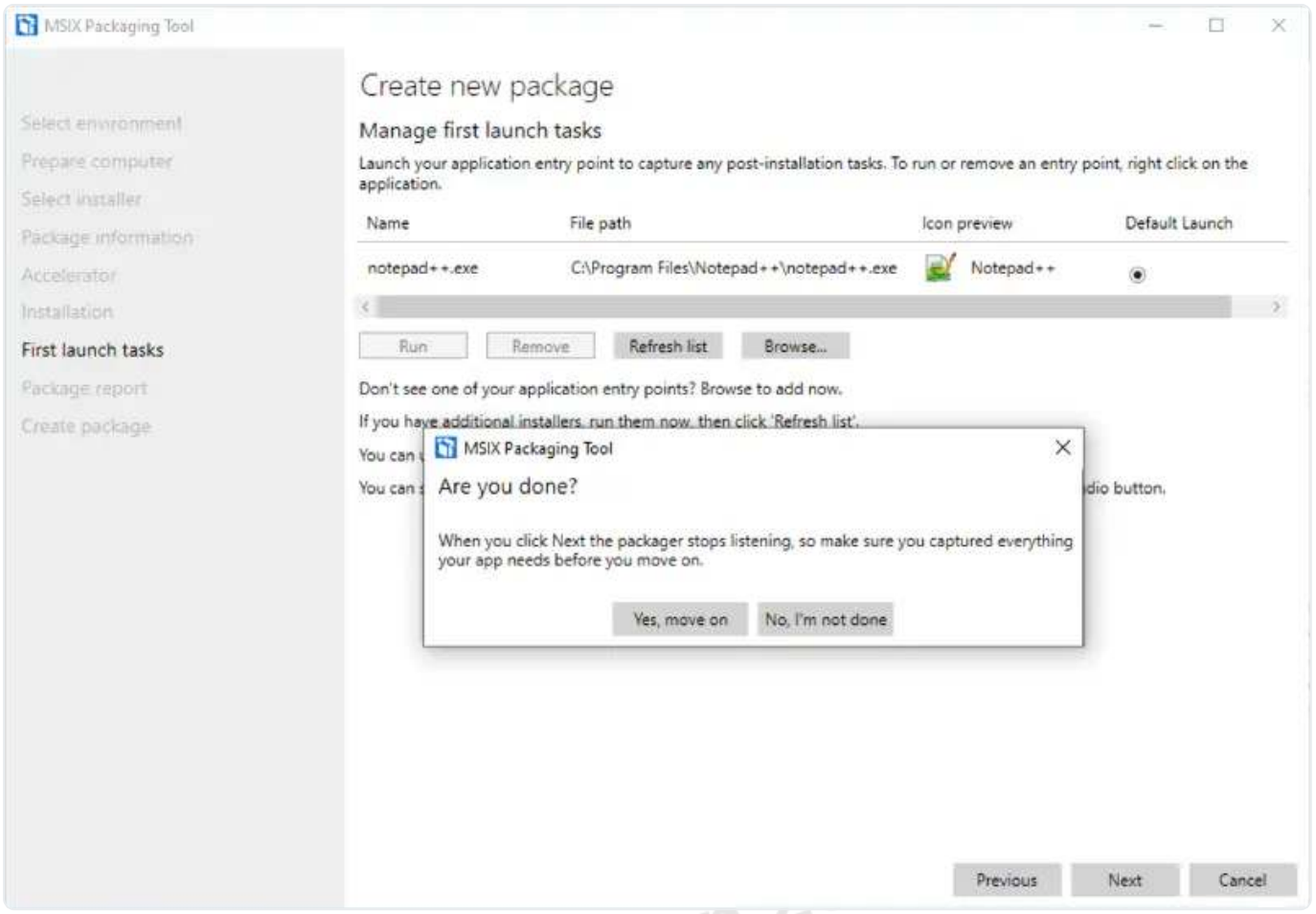
The appropriate fields have to be filled in.

For version 2

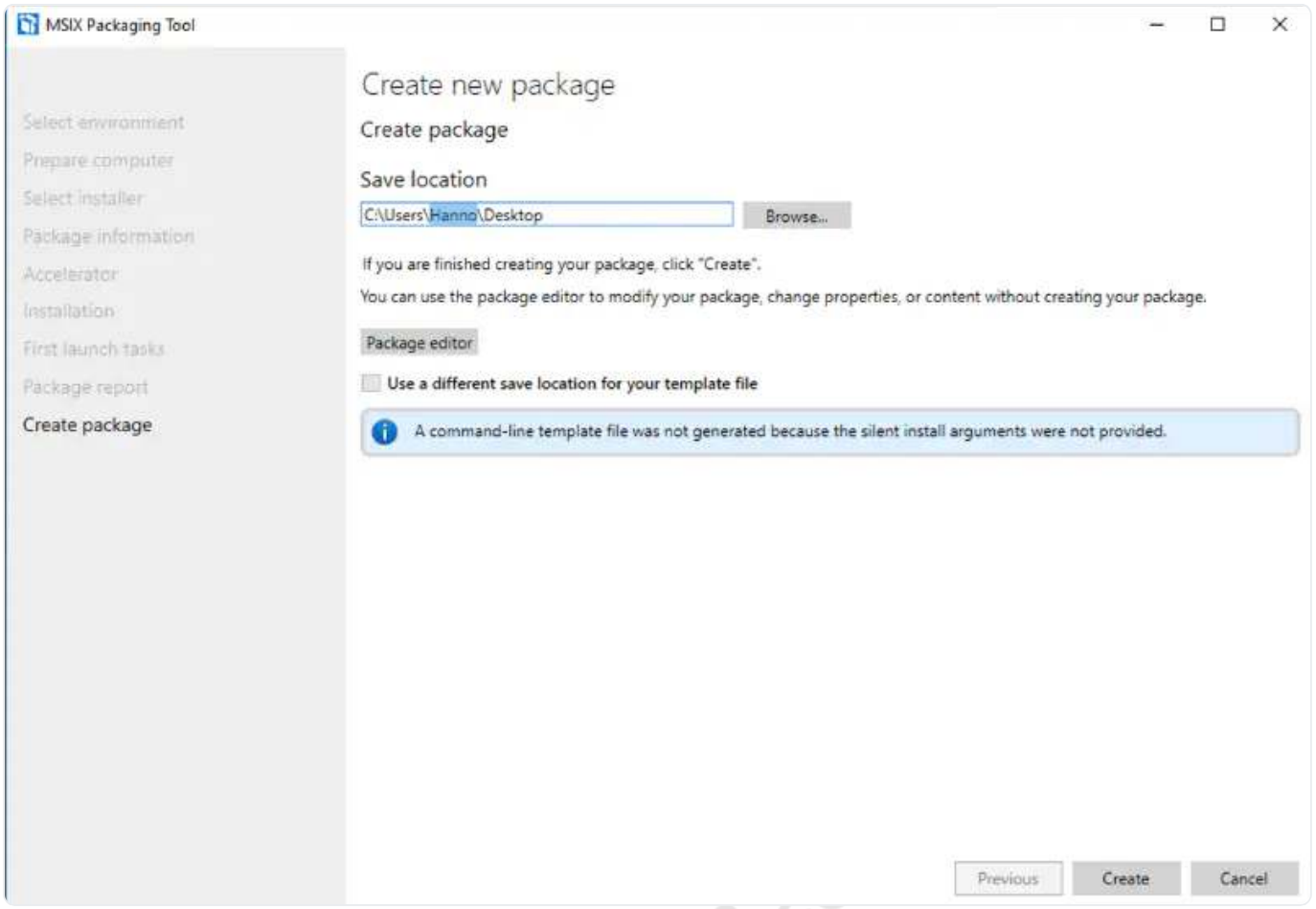


Now, the installer of Notepad++ starts. It should be run normally and the configurations have to be set according to the needs.

When the installation of Notepad++ is finished, Next and Yes, move on are clicked in the MSIX Packaging Tool.



The tool will indicate that no services have been installed and detected. In the last dialog box, the location of the package can be specified. Clicking Create completes the creation.



Deploy certificate on other Windows PCs

In order to be able to install the MSIX package on other Windows PCs, the certificate must be provided on these. To do this, the certificate must be exported from the PKCS#12 container (`.pfx`) as a single certificate (PEM format) using OpenSSL. OpenSSL must be installed on the system for this. This works with this command:

```
openssl pkcs12 -in MSIXZertifikat.pfx -clcerts -nokeys -out MSIXZertifikat.der
```

OpenSSL 3.x and higher:

```
openssl pkcs12 -in MSIXZertifikat.pfx -clcerts -nokeys -out MSIXZertifikat.der -passin
pass:Passw0rd #Put your passphrase there
```

The PKCS1 certificate that has just been converted can then be uploaded to Relution under `Settings` → `Certificates`. The conversion is necessary because Relution installs an uploaded `.pfx` file as a client certificate and only offers the choice of certificate store for single certificates (PKCS1).

Finally, the certificate must be delivered to the devices in a policy for Windows devices. To do this, the Certificate configuration must be used and the certificate selected, see Install certificates →.

It is mandatory to select Trusted Root Certificate Authority as the Certificate store. The default setting Automatically would place the certificate created in the example in Personal, as it is not a certificate authority certificate; Windows would then not trust the MSIX package.

Upload the MSIX file to Relution

The finished package is uploaded under `Apps` → `App Store` via Add with the source Native app. Relution accepts the formats `.msix`, `.msixbundle`, `.appx` and `.appxbundle`. The app can then be distributed to the Windows devices on which the certificate is installed.

For version 26.4.0

Set up opsi server

This manual provides a detailed description of the process for setting up an opsi server to efficiently deploy Windows installations and automate device enrollment into Relution. The goal is to configure a functioning opsi server that can install Windows operating systems on client devices via netboot while seamlessly integrating them into Relution for centralized management.

The guide covers all essential steps, including installation and configuration of the opsi server, preparation of Windows and Windows Preinstallation Environment (WinPE) installation files. Additionally, it explains the process of automating Relution enrollment using local opsi products.

Glossary

Term	Explanation
admin console	Refers to the UI which is included in the opsi server and runs on *https://localhost:4447*
configed	Refers to the additional Java application which may run on any device to connect to the opsi server
client debug console	Refers to the opsi agent UI which runs on *https://<opsi-client-IP>:4441*

For vers

Setup opsi server

This section describes the process of setting up the opsi server, providing a detailed walkthrough of the necessary configurations, installation steps, and preparation of critical packages.

Server installation

It is recommended to use the Docker-based installation for setting up the opsi server on Linux environments. However, it is important to note that the Docker setup cannot be used on macOS devices due to compatibility issues with the integrated TFTP server. For macOS systems, the preconfigured VirtualBox → option should be used instead.

The opsi config server is set up according to the opsi documentation below. After the installation, the admin console is available at *https://localhost:4447*. The Java application → for `configed` is also required.

Documentation

- Quick Start →
- Docker installation →
- opsi-webgui →
- Network configuration →

Install required opsi-packages

The required opsi packages are installed in the Terminal tab of the admin console with the following command:

```
opsi-package-updater -v install <package-name>
```

An overview of all available local and netboot products can be found in the opsi repository →.

The following packages need to be installed:

Package	Description
opsi-client-agent	Client installed on the device to execute commands
opsi-script	Used by the client agent to execute opsi scripts
opsi-uefi-netboot	Required for UEFI netboot to change boot order
opsi-winpe	Creates a WinPE on the device
hwaudit (optional)	Inventory tool which gathers information about the device

Client registration

This section covers the process of registering devices that already have a Windows operating system installed with the opsi server. The opsi client agent is installed on the device to establish communication with the server, enabling centralized control and execution of actions.

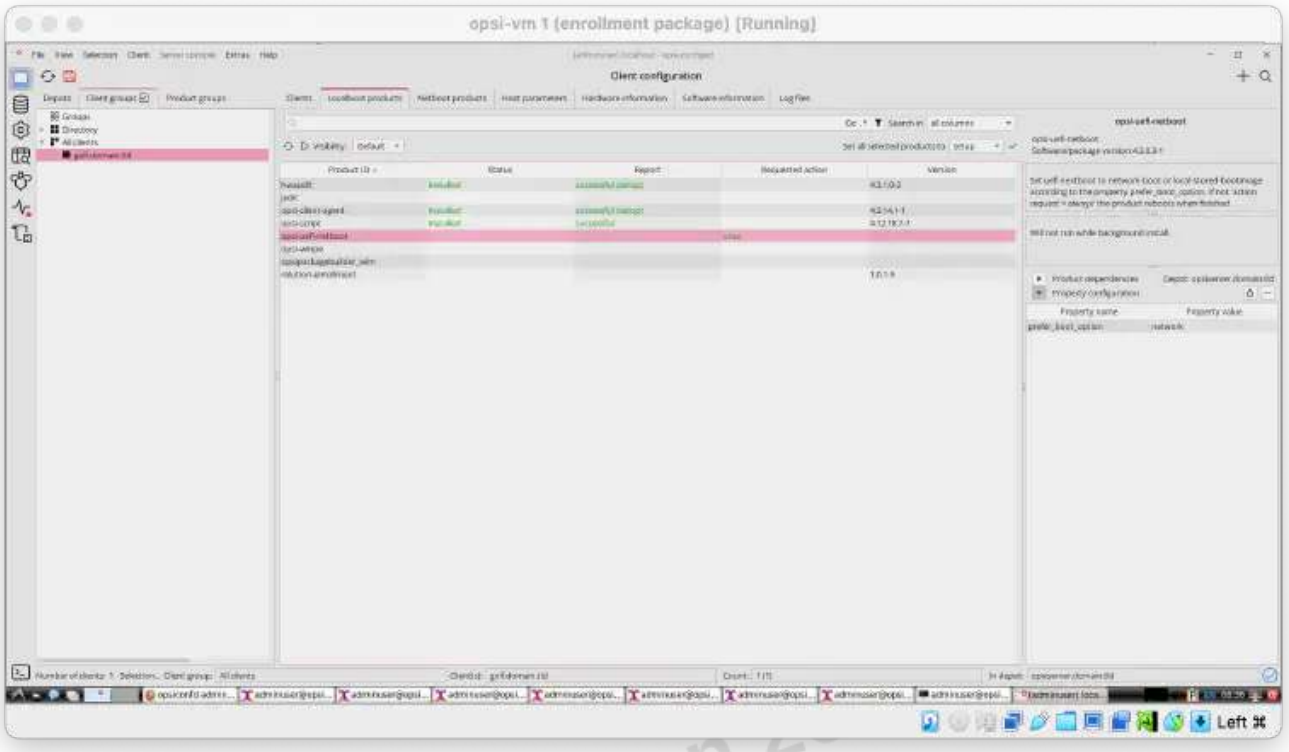
For clients that do not yet have Windows installed, additional steps are required to initialize and install the operating system using netboot. In such cases, users should refer to the official opsi documentation below for detailed instructions on initial client setup.

The opsi client agent can be downloaded from `https://<opsi-server-ip>:4447/public/opsi-client-agent/`. After the client was installed on the device, the opsi server address and admin account credentials have to be entered.

Once the registration is complete, the client will appear in the device inventory of the `configed`. To check the connection between opsi server and client a pop-up message can be sent (`Top menu` → `Client` → `Send pop-up message`).

The UEFI netboot product is installed on the device by setting the Requested action to `once`.

The Log files tab provides detailed information for troubleshooting installed opsi-client agent and linux-boot-image. This is helpful for debugging the installation of local and netboot products.



For version 26.4.0

Documentation

- Client installation →

Prepare Windows installation files

This section provides instructions for acquiring the necessary Windows ISO file, creating a compatible WinPE environment, and organizing these files into the required directory structure for netboot products. In this setup, Windows 11 was installed on the device.

Windows ISO and WinPE

To prepare the opsi server for deploying Windows installations, several key components are required. First, the Windows ISO file is required for the specific version to be installed, such as Windows 11. The ISO file can be downloaded from the official Microsoft website.

Next, a WinPE must be created. The WinPE must match the Windows image version being deployed. This can be achieved by using the opsi-winpe package, which requires the installation of Windows ADK and the PE plugin. Alternatively, the WinPE can be created directly with Windows ADK, as described in the opsi documentation.

The documentation on netboot products → describes two options to prepare a WinPE:

1. Using `opsi-winpe` package (Windows ADK and the PE plugin → need to be installed!)
2. Using Windows ADK

Setup directory structure for netboot product

The matching wrapper package for the Windows image is installed from the opsi Netboot Repository → via the package manager, e.g. `opsi-local-image-win11-x64_4.3.0.2-13` for Windows 11.

A new directory will be added on the opsi server (e.g. */var/lib/opsi/depot/win11-x64*). The Windows Image and the WinPE have to be placed in the correct directories (see Directory Tree overview → for reference).

Install files

The contents of the Windows ISO have to be placed at the `installfiles` directory.

WinPE

The WinPE needs to be placed in the `winpe` directory.

> All files from the subdirectories (*fwfiles*, *media*, *mount*) are extracted and placed on root level. As there may be issues with the detection of the `setup.exe`, the directories are placed here as well.

In the end, all files and all directories of the WinPE are at the root level in this directory:

> Show full configuration example

Documentation

- Windows OS installation →
- Netboot products →

For version 26.4.0

Configure DHCP server

To configure a DHCP server for PXE boot, specific options need to be provided that supply PXE boot clients with the information they need to locate the TFTP server and download the bootloader file. These are commonly defined as DHCP options 66 (TFTP server) and 67 (bootloader file).

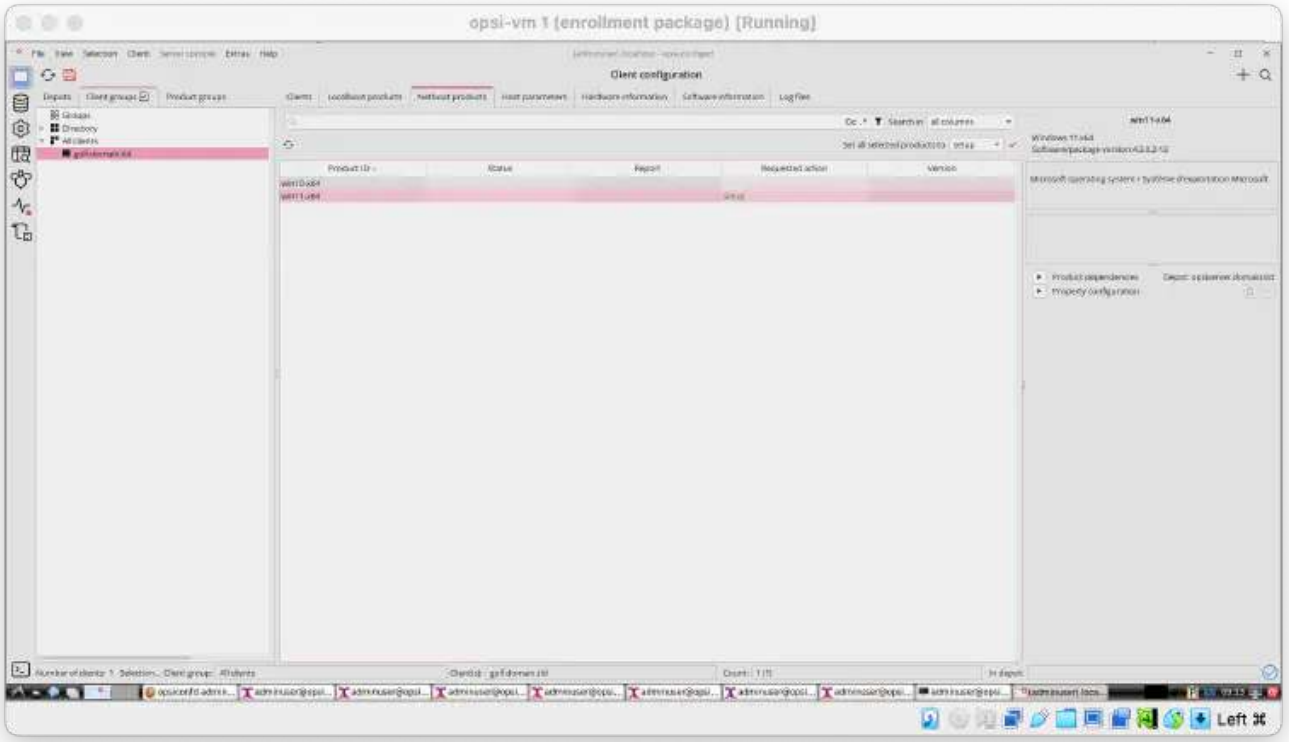
If the router does not provide a UI to set these options, e.g. when using a Linux or Windows DHCP server, the following options have to be added to the `dhcpd.conf` file:

```
next-server <opsi-server-IP>;
filename "opsi/opsi-linux-bootimage/loader/opsi-netboot.efi";
```

Start netboot

To initiate the installation of a netboot product, the Netboot products tab in the configed interface is opened. The Requested action for the selected product is set to `setup` and saved by clicking the save icon located in the top-left corner.

Once the action is sent, the process can be monitored by checking the logs in the `configed` client details and the `client debug console`. These logs will indicate whether the opsi client has successfully received and processed the action. After completing these steps, the Windows client will check for netboot sources on the next reboot, initiating the installation process.



For troubleshooting, the following commands can be run to view the TFTP traffic on the opsi server:

```
sudo tcpdump -i lo0 port 69
```

```
journalctl -f
```

Documentation

- opsi with UEFI/GPT →

For Windows 11 installations, the device must support TPM 2.0. The BIOS menu should be checked to confirm that the option is enabled. Sometimes it is required to turn it off and on or to reset it on the next reboot.

Relution enrollment

This section outlines the process of enrolling devices into the Relution platform using the `relution-enrollment` local boot product. This product automates the installation of a provisioning package via PowerShell, ensuring seamless integration of devices into Relution.

Prepare provisioning package

A provisioning package must be prepared according to the instructions for Windows bulk enrollment →.

The package must be named relution so the opsi-script can detect the correct file.

Install Relution-enrollment opsi package

The `relution-enrollment` package is available as an *experimental* version in the public opsi-repository →.

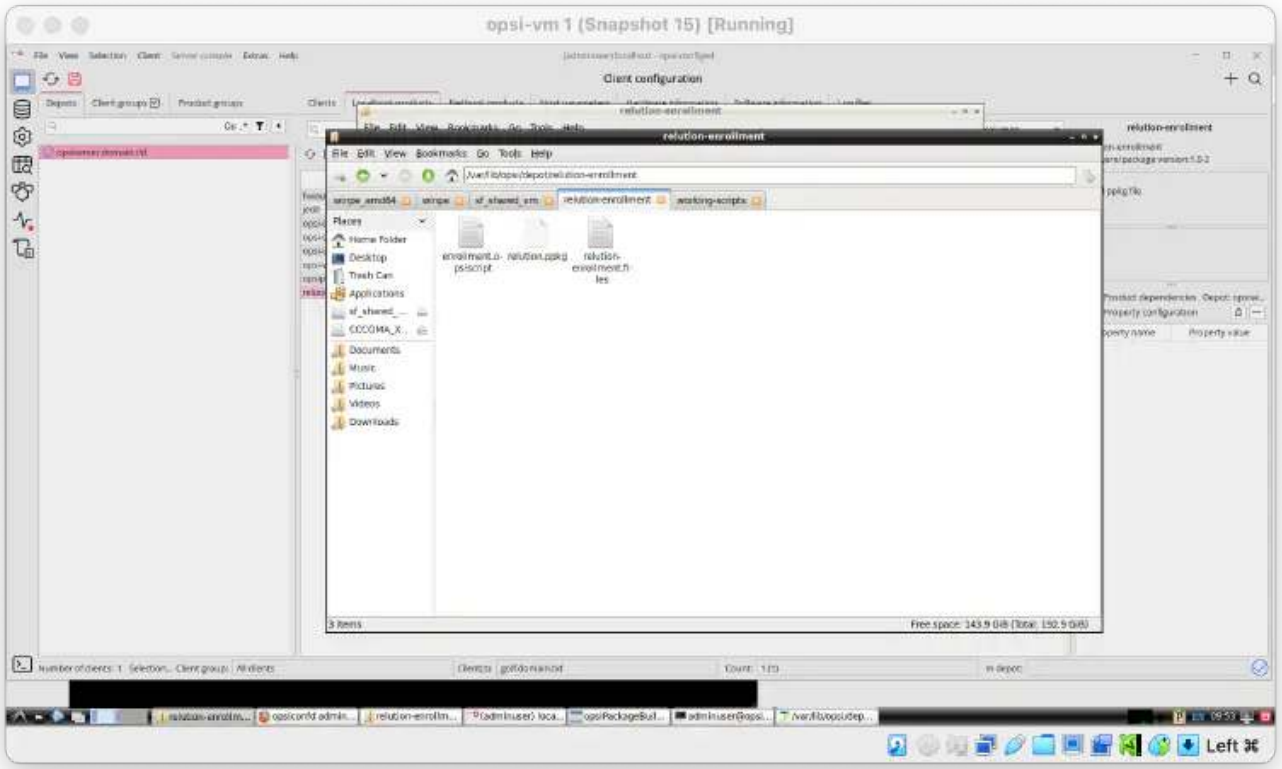
The `relution-enrollment_<package-version>.opsi` file is downloaded using the `wget` command. The following command installs the opsi package so that it becomes available in `configed` as a localboot product:

```
opsi-cli package install relution-enrollment_<package-version>.opsi
```

After the installation, the package is available in the depot folder (`/var/lib/opsi/depot/relution-enrollment`). The generated provisioning package is placed in this folder, and `opsi-set-rights` is run in this directory.

```
/var/lib/opsi/depot/relution-enrollment/
├── enrollment.opsiscript
├── relution.ppkg
├── relution-enrollment.files
```

For version 26.4.0

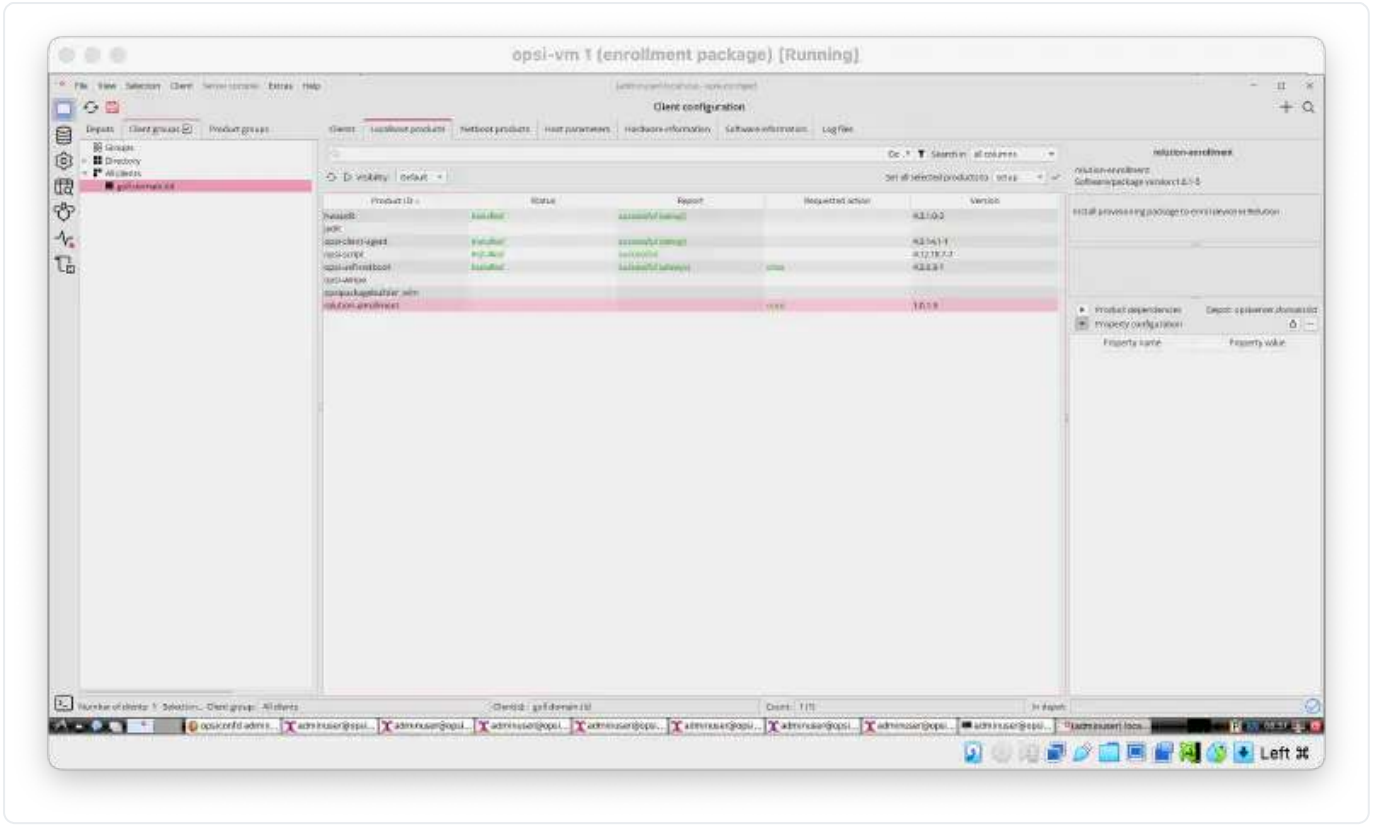


Old version 26.4.0

Install product

To install the package, the client is selected and the Localboot products tab is opened. For the `relution-enrollment` product, the Requested action is set to `once`. The state is then saved and an `on_demand` action is triggered (`Menu` → `Client` → `Trigger opsiclientd event` → `on_demand`). As the PowerShell command that installs the provisioning package always marks the action as successful, the logs should be checked for errors. Error `Package installation failed, error code -2147024713 (800700B7)` indicates that a package with the same id is already installed.

If the provisioning package was installed already, it needs to be removed first.



For version 26.4.0

Common issues

This section highlights common issues encountered during the opsi server setup and netboot installation and provides solutions or references to relevant documentation for troubleshooting.

- Unable to get geometry for disk '/dev/nvme0n1' →
  - The password for the root user is set via the host parameter `netboot.linux-bootimage.cmdline.pwh`.
  - When the error occurs, `Ctrl + Alt + F3/F4/F5` switches to the active terminal.
  - There, the root user logs in with the password.
  - The command `sgdisk --zap-all /dev/nvme0` deletes the partition.
  - After switching back to the other terminal, the netboot is retried.
  - More information is available in the documentation on netboot products →
- opsi winPE is empty →: all files from the WinPE subdirectories (e.g. media) are moved to the root level
- WinPe init does not work →

Identity Certificate

Apple and Windows devices enrolled in Relution receive an Identity Certificate. This is valid for one year and is automatically renewed as long as active communication with the device exists.

However, it can happen that devices are stored or inactive, preventing the identity certificate from being renewed in time. For security reasons, Relution blocks all communication with the device if the identity certificate has expired.

Checking and Renewing the Identity Certificate

Affected devices can be checked under `Navigation` → `Devices` → `Inventory` → `[Device]` in the Information tab within the Security block.

Three relevant fields are available here:

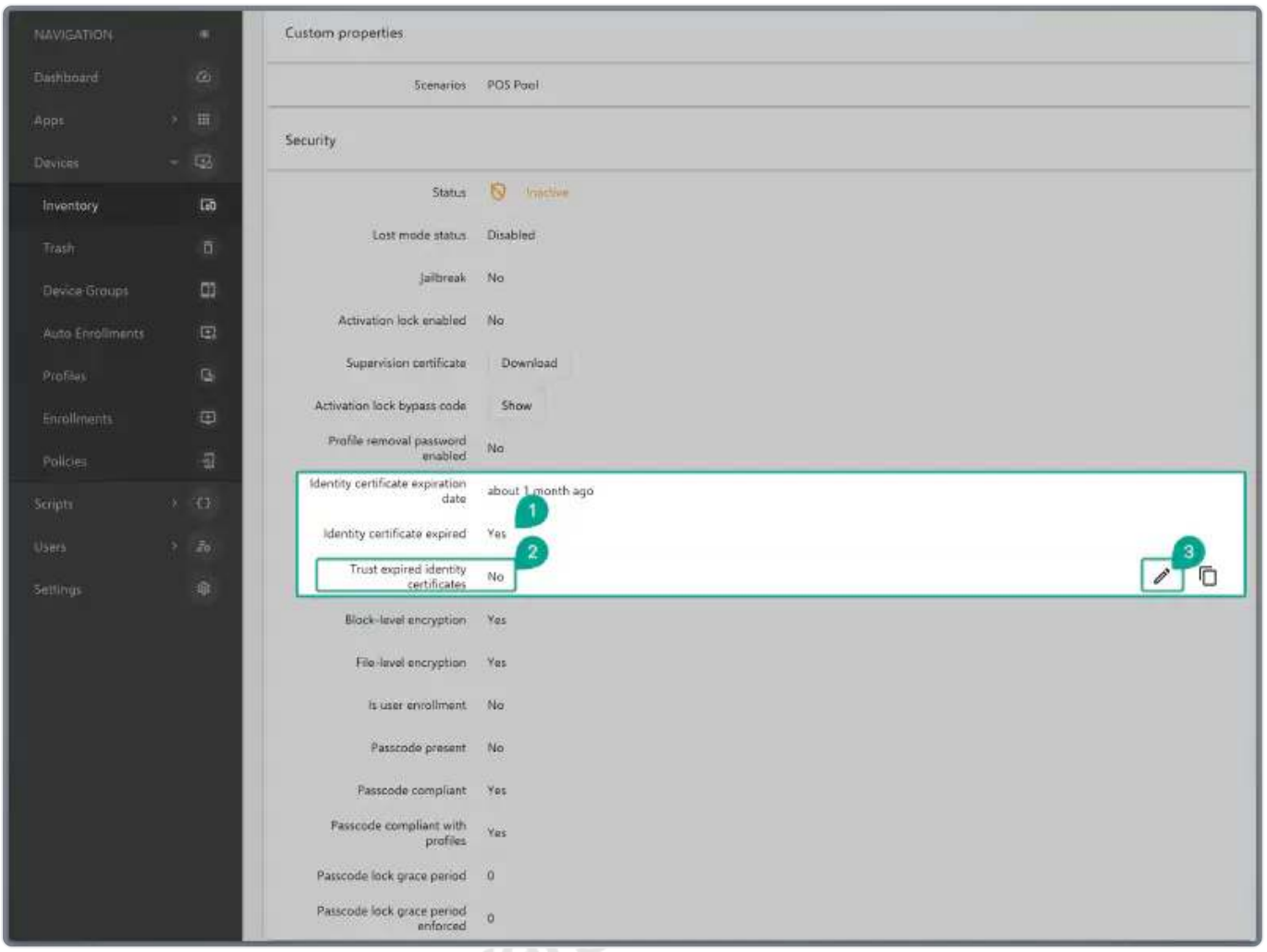
- Identity certificate expiration date
- Identity certificate expired
- Trust expired identity certificates

If the identity certificate has expired and Trust expired identity certificates is not yet active, hovering the mouse over this row displays the Edit button (pencil icon). Clicking it opens a confirmation dialog. With Confirm, Relution temporarily accepts MDM messages signed with the expired certificate and initiates the renewal: for Windows devices, an action to renew the client certificate is queued; for Apple devices, the MDM profile is updated. This restores the communication with the device as trustworthy, allowing MDM commands to be processed. Once the device has received a new identity certificate, Relution resets Trust expired identity certificates automatically.

For version 26.4.0

The action requires the permission to edit devices.

> Trusting expired certificates poses a security risk, for example if the identity certificate has been exposed to a third party.



Important Note: The action is available as soon as the identity certificate has expired and can also be performed while the device is offline. As soon as the device is online again, it receives a new, valid identity certificate.

Multiple affected devices can be found under `Navigation` → `Devices` → `Inventory` using the filters Identity certificate expired and Trust expired identity certificates.

Publish scripts globally

With Relution `Server Version 5.22` it is possible to publish Windows scripts centrally and thus make them available to all organizations. This is done in the Global organization (up to version 5.22: store organization).

> A script created in the Global organization is initially only visible there. Only after Set visibility to global is it available to all organizations, including those created later. This step cannot be undone. Afterwards, the script can only be edited or deleted in the Global organization.

Add script

Once logged in to the Global organization, the Scripts section can be reached via the navigation on the left-hand side, where new scripts can be created using the Add button. The creation is divided into 3 points.

General

- Name - The global display name for the script (required, maximum 255 characters)
- Description - A supplementary description of the script (maximum 4000 characters)
- Platform - For Windows scripts, Windows is selected (required, preselected). `*.ps1` files and the Environment variables field are only offered for Windows. The platform cannot be changed after saving and is also locked while a script file is loaded.

For version 26.4.0

> Subsequent changes to a globally available script apply in all organizations. On devices whose policy uses the script, the script is updated automatically.

Content

- Script file - A local `*.ps1` file can be loaded using Select (or by drag and drop). Its content is transferred to the Content field.
- Content - Alternatively, the script can be entered directly in the text field. As soon as the field contains text, Script file is hidden.

Execution

- Timeout (in minutes) - After the specified time period has expired, the script execution is forcibly aborted. Default: 5 minutes, permitted range: 1 to 30 minutes.
- Environment variables - The environment variables and their assigned values are inserted at the beginning of the script when it is executed on the device (maximum 512 characters). Each variable assignment except the last one must end with a semicolon. The variables can be used in the script by their names.

Example:

```
# Variables (field "Environment variables")
$arg1=10; $arg2='text'

# Use in the script
Write-Host $arg1

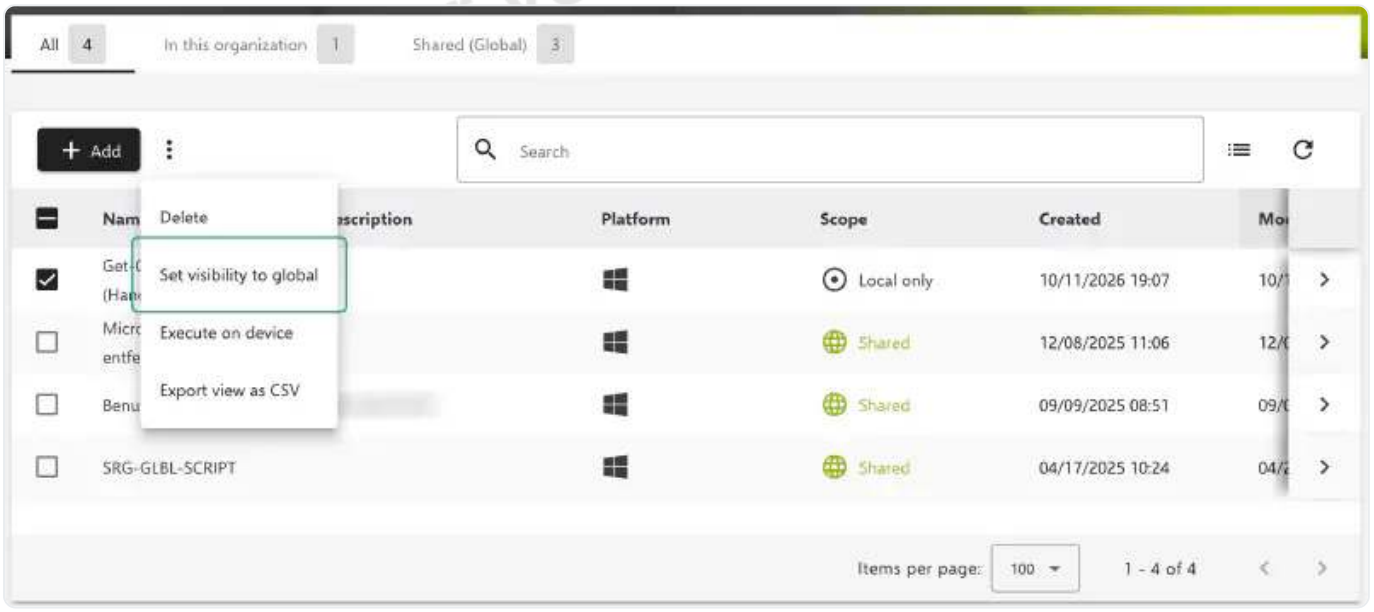
# Execution on the device: ./test.ps1
# Result output: 10
```

Available placeholders

The available placeholders can be used both directly in the script content (Content point) and in the Environment variables field under Execution. The placeholders available in the form are displayed below the input fields. Example of a variable: `$serial='${device.serialnumber}'`. Further functions such as substrings or default values are described in the article Advanced placeholders →.

Set script visibility to global

After saving, the script is only visible in the Global organization. To provide it to all organizations, the script is selected in the list under Scripts, and Set visibility to global is chosen in the context menu (three-dot menu of the row or of the action bar). The following dialog lists the affected scripts; Publish applies the change. The function requires the permission to edit scripts.





> This action cannot be undone.

In the other organizations, the script then appears read-only in the From Global tab of the script list. It can be used there in a policy with the Windows Script Configuration → or via the Execute PowerShell script action. As long as the script is used in a published policy of any organization, it cannot be deleted, not even in the Global organization.

In a meta organization, the same function is available as Set visibility to meta; the script is then visible in the organizations of this meta organization.

For version 26.4.0

Office installation is stuck

With Relution Server version 5.21, it is possible to install Microsoft Office on managed Windows devices using a configuration file (XML). With version 5.22, a corresponding configuration and an extension of the action has been added. The installation is possible via the policy configuration Windows Office → or via the Deploy Office 365 action and is supported on Windows Pro, Enterprise and Education from version 1703, not on Windows Home.

This installation can fail for many different reasons.

In principle, the Deploy Office 365 action should not be used if this has already been configured in the policy. A restart should be avoided during the installation.

Problem cases

1. The Change policy action has the status Not now.
2. Office does not install, although no errors may be visible in the list of actions.

In both cases, it is always worth taking a look at the task manager of the device. Often background activities are running that indicate an ongoing installation or the network card shows download traffic.

For version 26.4.0

Case 1 - Not now

The Change policy action for a policy with the Windows Office configuration remains in the Not now status. This status only occurs when Office is installed via a policy while an installation is still running on the device or another Office suite has to be uninstalled first. The Deploy Office 365 action never receives this status.

1. A Refresh device info action is sent to the device.
2. The installation may contain large amounts of data that need to be downloaded and processed. Depending on the connection and hardware used, this can take a very long time. At least one hour should be allowed to pass if this status occurs.
3. After the hour has passed, another Refresh device info action is sent to the device. If the Change policy action was delivered at least 60 minutes ago, Relution continues applying the policy, even if the device still reports an installation in progress. Without this refresh, this only happens with the next automatic refresh of the device information or when the device reports that the Office installation has completed.
4. If there is still no change in the status, the installation can be reset using the Deploy Office 365 action with the Clear Office installation data option. Optionally, the Uninstall the current Office 365 Suite switch additionally removes the installed Office suite. If there is no installation data on the device and the switch is not enabled, the action fails.
5. At least five minutes should pass before the installation is run again.

Case 2 - Office does not seem to install for no reason

This case can occur when using the policy configuration. In this case, Re-apply policies should always be run first and the further behavior observed.

If this is not successful either, the Office installation, which may be stuck, can be reset as described in case 1, step 4 (Deploy Office 365 action with the Clear Office installation data option).

Re-apply policies should then be run again.

If the device reports an error during installation via the policy, the Change policy action changes to the Error status and the compliance violation Windows Office configuration is invalid is raised. The Deploy Office 365 action, on the other hand, already reports success as soon as the device has accepted the command; a later failure of the installation is not visible there.

For version 26.4.0

Windows Companion

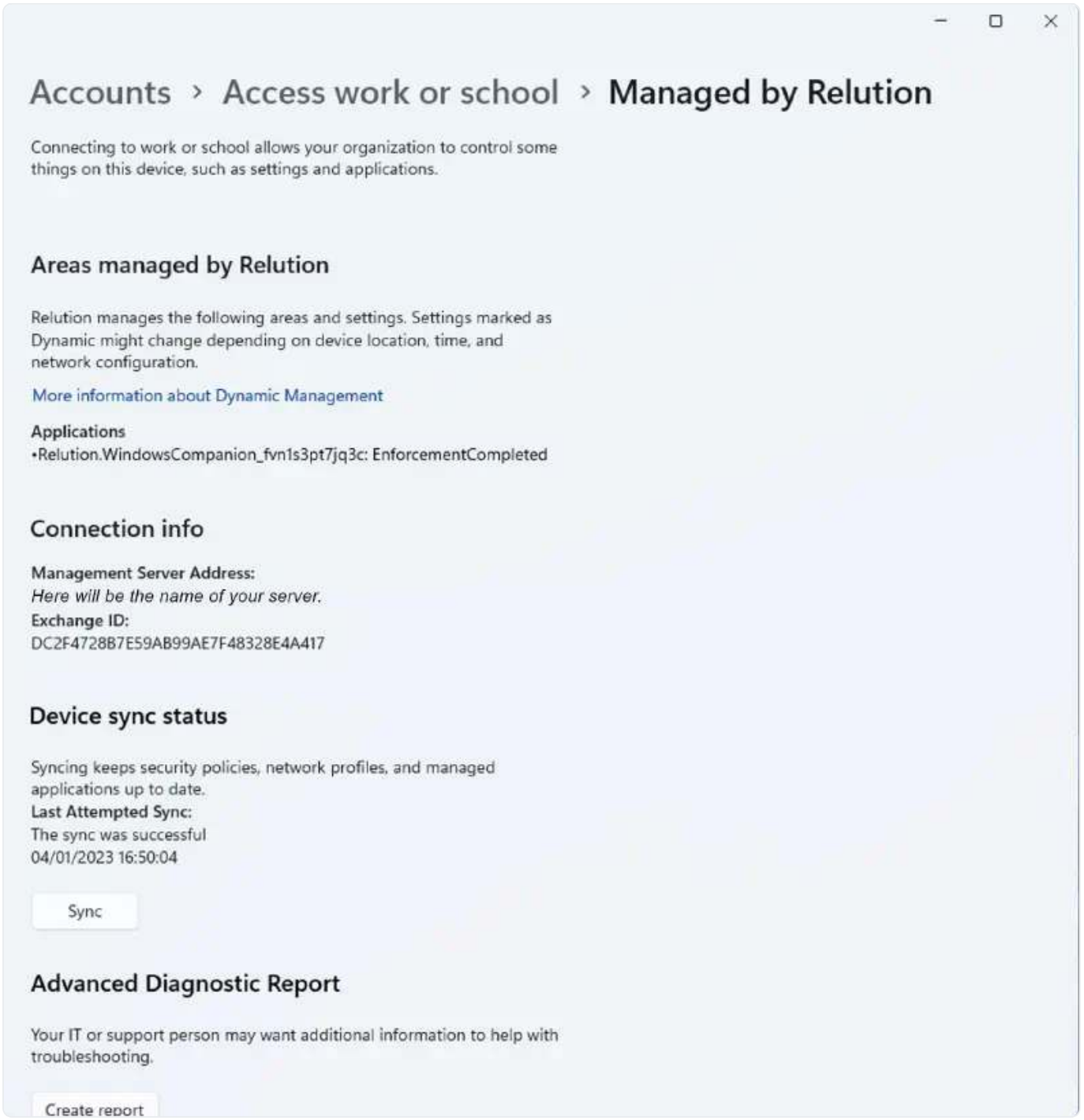
The Relution Companion for Windows is a Windows service that is installed on all Windows devices managed by Relution, except devices running Windows Home Edition and devices whose edition is not recognized. It is not a regular app available in the Windows App Store or the Relution App Store. Relution Companion for Windows has administrative rights, is intended for administrators only, and runs entirely in the background. It does not interact with end users.

Installation

With Relution Server version 5.15, the Relution Companion for Windows is automatically installed on all newly enrolled Windows devices, unless they run Windows Home Edition. If the Windows device is already managed by Relution, the Relution Companion for Windows will be installed automatically as well. On Windows Home, the Companion is not available, and neither are PowerShell scripts or the installation of MSI and EXE packages: Windows Home Limitations →

On the Windows device under Settings, the Relution enrollment Connected to Relution is displayed. In the submenu Info, it is visible that the Relution Companion for Windows has been installed successfully.

For version 26.4.0



Until the Companion reports to the server for the first time after installation, the device shows the compliance notice “The Windows Companion is not installed!”. If an installed Companion stops responding, this becomes a compliance violation and the Companion is reinstalled. When a newer Companion version is available on the server, the Companion on the device is updated automatically.

If a Windows device is no longer managed by Relution, the Relution Companion for Windows is automatically removed from the device.

Purpose of the Relution Companion for Windows

By default, the configuration of enrolled Windows devices in Relution uses the so-called Configuration Service Providers (CSP), which allow access to certain settings in the Windows system. The configuration possibilities are however limited here. By means of the Relution Companion for Windows, configuration options are significantly extended.

Additional options

With the Relution Companion for Windows, additional one-time Windows-based PowerShell scripts can be executed on enrolled Windows devices via Relution actions.

Another advantage of Relution Companion for Windows is the installation and uninstallation of classic applications in the device context. This allows `.msi` and `.exe` files to be installed and uninstalled on enrolled Windows devices via the Relution App Store.

In addition, the following functions run exclusively via the Companion: the installation of WinGet apps, recurring script execution via Windows Script Configuration → and the actions Reset password (Windows), Enable Bitlocker and Disable Bitlocker. The behavior of the Companion itself is controlled by the Configure Companion → policy.

Applying Powershell scripts to Windows devices

PowerShell scripts are text files that contain at least one PowerShell command that is executed by Windows when the file is opened. Processes, both on the computer and at Relution, can be greatly facilitated by this. The script files are written by the administrator and saved with the extension `.ps1`. Only PowerShell scripts that do not require any user interaction can be executed, since the Relution Companion for Windows runs completely in the background. For resetting forgotten user passwords, the dedicated action Reset password (Windows) is now available.

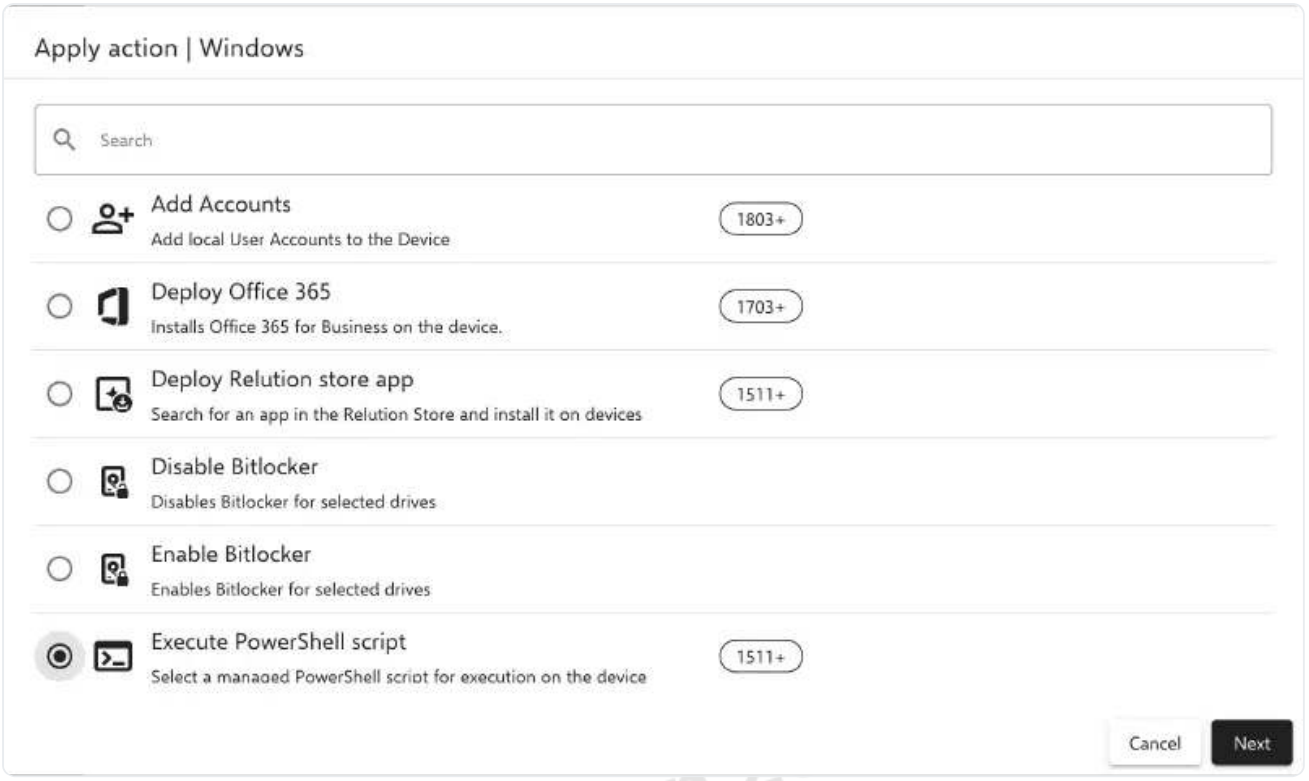
Since Relution 5.16, PowerShell scripts are managed centrally in Relution. A script is therefore no longer uploaded in the action, but created beforehand under `Scripts` → `Scripts` via Add. The default values for Timeout (in minutes) and Environment variables are stored there as well. Selecting a script in the action requires the permission to read scripts; without it, no script list is shown.

To successfully run a PowerShell script on a Windows device, the following steps must be performed:

For version 26.4.0

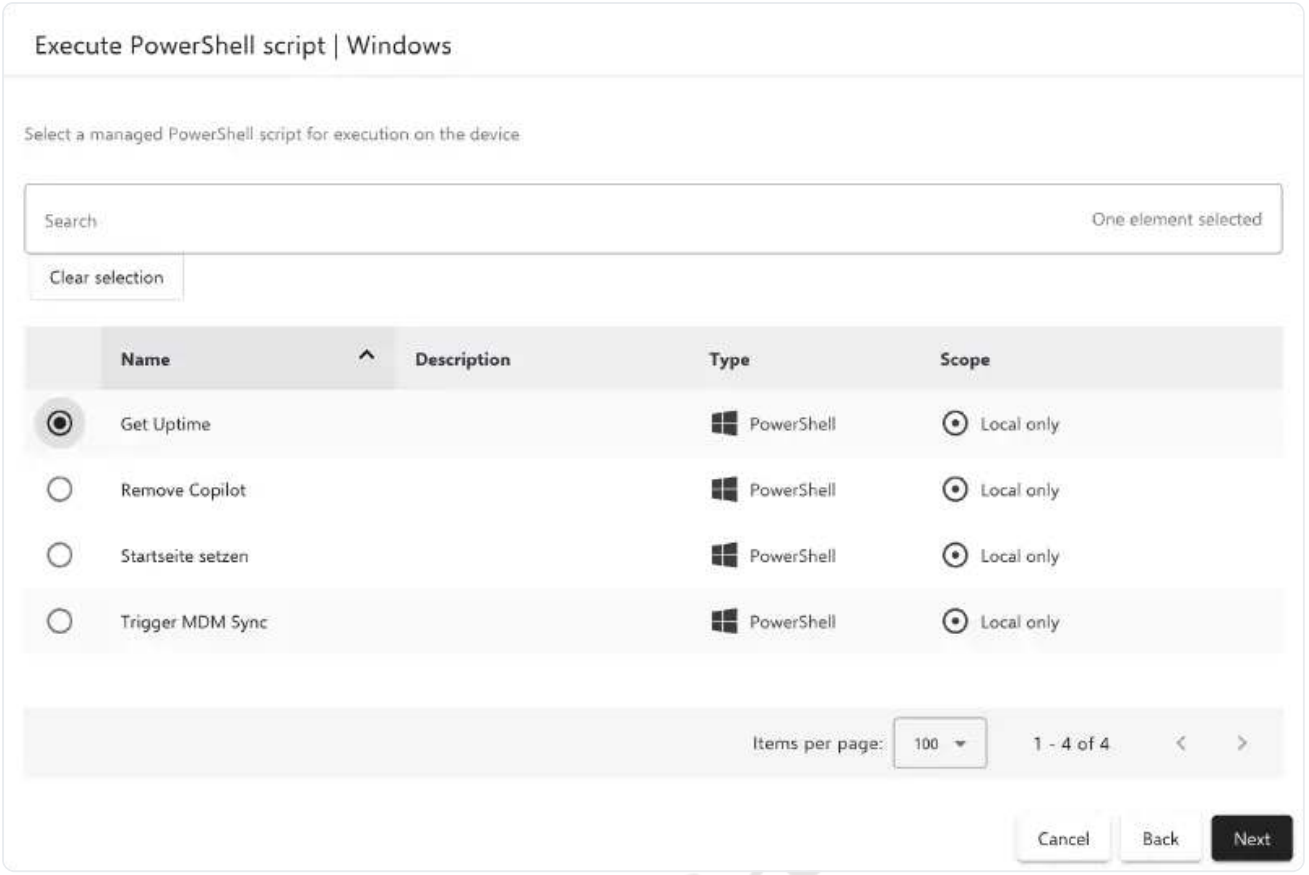
1. In the device inventory, the desired Windows device is opened; on the device details page, the Apply action button is clicked in the Actions tab.

2. Then the action Execute PowerShell script is selected.



For version 2

3. The desired PowerShell script is selected from the list of managed scripts.



4. In the second step, Set script execution parameter, the values of the selected script are pre-filled and can be adjusted for this execution:

   - The mandatory Timeout (in minutes) field (1 to 30) defines after how many minutes script execution is forcibly aborted.
   - The Environment variables field takes variable assignments in the format `$arg1=10; $arg2='text'` (up to 512 characters; each assignment except the last one ends with a semicolon). They are inserted at the beginning of the script before execution, and the script can use the variables by name, e.g. `Write-Host $arg1`.



5. The executed PowerShell script is listed on the device details page in the Actions tab.

Alternatively, a script can be started directly under `Scripts` → `Scripts` via Execute on device. The execution state as well as the result and error output of each execution can be viewed in the history of the respective script under `Scripts` → `Scripts` (Show result output, Show error output).

For version 26.4.0

Windows Home Limitations

The Windows Home edition is limited in terms of administration possibilities compared to other editions. Functions that are not available can often be recognized in the web interface by the fact that they have badges indicating which editions are supported. Accordingly, the Home Edition is not included here. However, not all affected functions carry such a badge.

Devices running Windows Home can be found in the device list via the OS Edition column or filter (value Home).

The restrictions affect the following functions, among others:

Installation of applications

The Microsoft MDM API (CSP) for installing MSIX and Microsoft Store Apps is not available on Windows Home. Relution is therefore unable to install such applications. As a result, policies that depend on it (app compliance) are also not available.

This restriction also affects the automatic installation of Relution Companion for Windows. As a result, the installation of MSI and EXE packages is also not available on Windows 10/11 Home, since this function requires an installed/configured Companion.

Thus, the following actions are not available on Windows 10/11 Home:

- Deploy Relution store app (including the installation of MSI, EXE and WinGet apps)
- Remove app
- Deploy Office 365
- Clear Office 365 Installation data

For version 26.4.0

Furthermore, the following policy is not available:

- App compliance

Running PowerShell scripts

Running PowerShell scripts requires an installed Relution Companion for Windows. Due to the restriction regarding App installation, it is not possible to install the Companion. Therefore, it is also not possible to run PowerShell scripts via the Companion on devices running Windows Home Edition.

Thus, the following action is not available on Windows 10/11 Home:

- Execute PowerShell script

Other Companion functions

The Relution Companion for Windows → is never deployed on Windows Home; the same applies to devices whose edition Relution does not recognize (OS Edition Other). Besides PowerShell scripts and app installation, all other functions that run via the Companion are therefore also missing, e.g. the actions Reset password (Windows), Enable Bitlocker and Disable Bitlocker as well as recurring script execution via policy.

Other actions and policies

The following actions are not supported on Windows Home either:

- Reboot device
- Add Accounts

The following policies are not applied on Windows Home:

- Bitlocker
- Windows update
- Windows Firewall
- Windows Kiosk Mode
- Shared PC
- Windows Office
- Local device security options
- Global proxies
- BranchCache
- Wallpaper
- App Control

For version 26.4.0

In the Restrictions, numerous individual settings are not supported on Windows Home either.

Still available on Windows Home are, among others, the actions Wipe device (from version 1709) and Scan Device (from version 1809) as well as the VPN and Antivirus (partially) policies.

Display installed applications

The Microsoft MDM API (CSP) for querying installed Modern Apps (Microsoft Store/MSIX) is not available on Windows 10/11 Home. Thus, Relution cannot discover installed apps for enrolled devices and accordingly cannot display them in a device's details under Installed Apps.

Discovering apps installed via EXE / MSI requires an installed Relution Companion for Windows. Due to the limitation regarding app installation, it is not possible to install the Companion. Therefore, it is also not possible to detect apps installed via the Companion on devices running Windows Home Edition.

Thus, the following information is not available on Windows 10/11 Home:

- Display of installed apps.

Upgrade to a higher edition

The Windows Licensing policy can upgrade a device running Windows Home to a higher edition using a product key, see Available configurations →. An upgrade performed this way cannot be undone by removing the policy.

Microsoft Store URLs

Managed Windows devices that use the Microsoft Store to acquire, install, or update apps need access to these endpoints over TCP ports 80 and 443 through the firewall.

Microsoft Store API (AppInstallManager):

- `displaycatalog.mp.microsoft.com`
- `purchase.md.mp.microsoft.com`
- `licensing.mp.microsoft.com`
- `storeedgefd.dsx.mp.microsoft.com`

At the time of creating this document, these are the currently required endpoints.
The full documentation is provided by Microsoft here:
Microsoft documentation →

For version 26.4.0

WinGet Upgrade Workaround

Some WinGet apps cannot be upgraded by `winget upgrade`, even though the newer version is listed in the Relution app store. The cause is almost always a broken upstream manifest on the WinGet side — the upgrade command then fails with *no applicable upgrade*, *package not found*, *no applicable installer found*, or a related error.

Microsoft's own workaround is to install the app again with the `--force` flag. The script below automates that recovery for a single WinGet app and can be run on devices with the Execute PowerShell script device action.

> This is a workaround. It should only be used for apps where a regular upgrade is known to fail. Forcing an install replaces the existing package files and can mask other installation problems.

Script

The script is created as a PowerShell script under `Scripts` → `Scripts` via Add and then run on devices with the Execute PowerShell script device action or via Execute on device in the script list. It is executed by the Windows Companion in device context (SYSTEM). At the top of the script, the `$AppIdentifier` variable must be set to the exact WinGet identifier of the app to repair (for example `Nextcloud.NextcloudDesktop`).

Alternatively, the identifier can be passed in the Environment variables field (for example `$AppIdentifier='Nextcloud.NextcloudDesktop'`), so that one script can be used for several apps. In this case, the first line of the script must be removed, since it would otherwise overwrite the passed value.

By default, scripts have a Timeout (in minutes) of 5 minutes. Since the upgrade and forced installation of large apps can take longer, the value should be increased accordingly when creating the script or in the action (30 minutes at most).

For version 26.4.0

Show full script

How it works

1. The script resolves `winget.exe` inside `C:\Program Files\WindowsApps\Microsoft.DesktopAppInstaller_*` — the installation used by the Windows Companion in System context.
2. It calls `winget list --id <AppIdentifier> --exact` to check whether the app is already installed. If not, the script exits without doing anything.
3. It calls `winget upgrade --id <AppIdentifier> --exact` with Relution's mandatory silent flags →. The flags are splatted with `@SilentFlags` so PowerShell passes each element as a separate argument — required for WinGet to parse them. If the upgrade succeeds, the script exits.
4. If the upgrade exits with one of the recoverable WinGet error codes, the script retries as `winget install --id <AppIdentifier> --exact --force` with the same silent flags. The recoverable codes are:
   - `-1978335189` — *no applicable upgrade*
   - `-1978335215` — *package not found*
   - `-1978335192` — *no applicable installer found*
   - `-1978335216` — manifest / installer failure observed in practice
5. Every other WinGet exit code is surfaced unchanged.

Detection relies solely on WinGet exit codes. The text output would depend on the device language and would differ between English and German Windows installations.

The execution state as well as the result and error output of the script (for example the `Write-Host` messages) can be viewed in the history of the script under `Scripts` → `Scripts` (Show result output, Show error output).

If the repair should run regularly, the script can also be executed on a schedule or on events via the Windows Script Configuration → policy configuration.

For version 26.4.0

WinGet Error Code

WinGet Error -1073741515

The installation of WinGet apps via Relution fails with the following error code: `-1073741515` (`0xC0000135`)

Cause

During the installation of apps via WinGet, an error may occur if the Microsoft Visual C++ Redistributable is not installed on the target machine.

Solution

The Windows Companion installs a missing Microsoft Visual C++ Redistributable itself, even if the Manage WinGet and its dependencies option is disabled in the Configure Companion → policy. If the error still occurs, a manual installation helps.

The full description of the cause, together with the solution using a manual installation as a native app with a detection rule, the required registry paths, and how to determine the uninstaller path, is described in the WinGet → article, in the Known issues section.

For version 26.4.0

WinGet Error -1978335230

The installation of WinGet apps via Relution fails with the following error code: `-1978335230` (`0x8A150002`)

One of the following error messages is displayed:

```
Argumentname wurde für den aktuellen Befehl nicht erkannt: --disable-interactivity
```

```
Argument name was not recognized for the current command : --disable-interactivity
```

Cause

The installed WinGet version is too old and does not yet support the required argument `--disable-interactivity`.

Solution

WinGet must be installed at least in version 1.6.

If the Manage WinGet and its dependencies option is enabled in the Configure Companion → policy (default), the Windows Companion updates WinGet and its dependencies when it starts.

If the option is disabled or not available, WinGet must be updated manually. An update is available in the Microsoft Store (App Installer package).

WinGet versions older than 1.6 cannot update themselves yet.

On request

To inquire about managing Linux devices, send us a message at sales@relution.io →.

For version 26.4.0

Built-In CA

Relution supports the use of integrated certificates. These certificates are used in many areas, for example SSL/TLS encryption, email security, VPN and Wi-Fi connections and signing.

The following instructions describe creating a built-in certification authority (CA) and a certificate template with variables for assignment. A policy containing the certificate configuration is then created and assigned to the appropriate devices. This enables the generation of the certificate for the end devices.

Create built-in CA

In Relution, a built-in CA is created for this under `Settings` → `Certificate Authorities` → `Add`. In the General section, a Name is entered (optionally a Description) and Built-in is selected in the Authority type field. The authority type cannot be changed after saving.

In the Certificate settings section, Generate next to the Certificate field creates a new root certificate. Alternatively, Select allows an existing PKCS#12 certificate to be used that was previously uploaded under `Settings` → `Certificates` (see Certificate Management →). The certificate authority is then created with Save.

The Built-in option is only available with the permission to read certificates, and the Generate button only with the permission to create certificates.

For version 26.4.0

Generate built-in root certificate

Generate opens the dialog Generate built-in root certificate. Confirm creates the root certificate and inserts it into the Certificate field.

Mandatory fields

- Name: Name of the certificate.
- Password: Password for the root certificate.
- Common name: Usually the domain name.
- Expires on: A validity of 10 years is preset. The earliest selectable date is the following day.

Optional fields

- Organization, Organization unit, Federal state, Locality: Further details about the owner, which are included in the distinguished name of the root certificate.
- Country: Germany is preset.

Certificate template

The certificate template `Settings` → `Certificate Templates` → `Add` is used to define parameters for the certificate.

Mandatory fields

- Name: Name of the template.
- Certificate Authority: The previously created built-in CA is selected via Select.
- Subject name: as an example, `CN=MyUseCase-${user.email}`. Variables such as `${user.name}`, `${device.serialnumber}` or `${user.email}` can be used, see Advanced placeholders →. Special characters are escaped with a preceding backslash (e.g. `CN=John\, Doe`).

The free text in `CN=MyUseCase` should be chosen to match the use case, e.g. VPN or WLAN.

Further options

- Certificate template type: Cannot be changed after saving.
  - Certificate (default): Relution generates the key and the certificate and provides both via the policy.
  - SCEP on device: For iOS, macOS and tvOS, the template is turned into a SCEP configuration. The device generates the key itself and requests the certificate from Relution via SCEP. The related settings (e.g. Retries, Retry Delay, access to the private key) are located in the SCEP configuration section.
- Subject alternative names: Additional names in the certificate, each with one of the following types (for SCEP on device only Email, DNS, User Principal Name and URI):
  - Directory Name
  - DNS
  - Email
  - IP Address
  - User Principal Name (UPN)
  - URI
- Key algorithm: RSA (default) or EC. EC is only available for a built-in CA with the template type Certificate.
- Key length: 4096 bits are preset. For the template type Certificate, 3072 and 4096 bits are available for RSA and 256, 384 and 521 bits for EC; for SCEP on device, 2048 and 4096 bits. Templates that have already been saved keep a previously selected key length until it is changed.
- Certificate key usages: Multiple selection, e.g. Signature, Key Encipherment, Data Encipherment or Non Repudiation.
- Certificate extended key usages: Multiple selection, e.g. Client Authentication or Server Authentication.
- Enable automatic renewal: Issued certificates are renewed automatically. The switch is off by default. Only when it is enabled can the following two fields be edited:
  - Automatic renewal period (in days): A certificate is automatically renewed if its expiration date falls within this period. The default is 1 day. The value must be shorter than the Period after which the certificate expires (in days).
  - Certificate renewal behaviour: Old certificates remain valid (default) or Directly invalidate old certificates.
- Period after which the certificate expires (in days): A certificate is no longer valid after this period. Preselected are 365 days.

For version 26.4.0

Policy with certificate configuration

For the steps to take effect and a certificate to be created, a policy with a certificate configuration must be created in Relution. Here is an example for iOS:

Under `Devices` → `Policies` → `Add`, the platform (here iOS) is selected in the General section, a name is entered for the policy and the policy is saved.

In the created policy, the configuration Certificate is added. After a name has been entered, Select next to the Certificate field opens the dialog Select a certificate or a certificate template. In this dialog, the previously created certificate template is selected on the Certificate templates tab and applied with Confirm.

Likewise, the certificate template can be used for VPN and WLAN configurations.

Validation

The following entry should be created in the Relution device history after distribution:

`A certificate for the certificate template $Template was issued by device user $User.`

In addition, the new certificate can be found on the Installed Certificates card in the device information of Apple and Linux devices (provided the device information is up to date).

An overview of all certificates issued via certificate templates, including the option to revoke them, is available under `Settings` → `Issued Certificates` (see Certificate Management →).

For version 26.4.0

Certificate Management

In addition to the Built-In CA → for automatically issued certificates, Relution offers two further views for certificate management: Certificates for uploaded certificates and certificates stored by Relution, and Issued Certificates for an overview of the certificates issued or assigned to devices by a certificate policy.

Certificates

Under `Settings` → `Certificates`, existing certificate files can be uploaded and managed (e.g. `crt`, `cer`, `der`, `pem`, `p12` / `pfx`).

Required fields when uploading

- Name: Name of the certificate.
- Certificate file: The certificate file to upload.

Optional

- Password: Password for the certificate file, if encrypted.

An uploaded certificate can then be selected in many policy configurations as a generic certificate — similar to a Built-In CA certificate template, but without automatic per-device issuance. Typical use cases include VPN, Wi-Fi (EAP-TLS), and Exchange/email configurations, as well as Windows and Android Enterprise certificate configurations.

In addition to uploaded certificates (usage Generic), the list shows certificates stored by Relution by default, such as the Built-in PKI root certificate, Built-in pool certificates from a certificate pool →, and push and signing certificates. The view can be narrowed down using the Usage, Type (`PKCS1` / `PKCS12`) and State filters. The certificate file of an entry can be downloaded using the download button in the list.

A deleted certificate is not removed permanently but receives the state Deleted. Since the State filter only shows Created by default, deleted certificates only become visible after adjusting the filter; they can be brought back via Restore certificate.

Issued Certificates (Device Certificates)

Under `Settings` → `Issued Certificates`, an overview is available of all certificates automatically issued or assigned to a device by a certificate policy (Built-In CA, SCEP/Microsoft ADCS or certificate pool →) — including the certificate, device, certificate template used, certificate authority, and issuance, expiry, and (if applicable) revocation dates. Revoked certificates are hidden by default and are shown via the Revoked certificates filter; the list can also be filtered by Certificate template. For revoked certificates, the Revoked by and Reason of revocation columns show who revoked the certificate and why.

Manual issuance is not possible from this view — certificates are only created as the result of an enrollment or policy process. Two actions are available:

For version 26.4.0

- Delete: Removes the entry from Relution. If a device requests the certificate again, a new certificate is issued. Certificates that have not yet expired and are assigned to a revocation list (CRL) managed by Relution cannot be deleted, only revoked. This also applies after revocation, until the certificate has expired.
- Revoke: Revokes the certificate via the certificate revocation list (CRL) of the associated certificate authority. A reason must be selected in the mandatory field Reason of revocation: unspecified, key compromise, CA compromise, affiliation changed, superseded, cessation of operation, privilege withdrawn or AA compromise.

Revocation is only possible for certificates issued by a Built-In CA, as Relution only maintains a revocation list for these. Certificates from a SCEP or Microsoft ADCS certificate authority and certificates from a certificate pool cannot be revoked in Relution, only deleted; they are revoked at the issuing certificate authority. Certificates that have already been revoked or have expired cannot be revoked either.

Important: Revocation is a genuine PKI operation: Relution then generates an updated, signed revocation list (CRL). Systems that check the certificate (e.g. a RADIUS server or VPN gateway) retrieve it via the CRL distribution point stored in the certificate or query the status via OCSP. This action cannot be undone.

For version 26.4.0

Certificate Pool

In addition to the Built-In CA →, which issues certificates itself, Relution supports certificate authorities of the type Certificate pool. In this case an existing, external PKI serves as the source: the certificates issued there are imported into Relution as an archive and kept as a pool. Whenever a certificate is required for a configuration, it is assigned from this pool instead of being generated.

Create a certificate authority of the type Certificate pool

The authority is created under `Settings` → `Certificate Authorities` → `Add`. In the Authority type drop-down menu, the entry Certificate pool is selected. This type is only available in regular organizations, not in the global organization or a meta organization.

Mandatory fields

- Name: Name of the certificate authority in Relution.

Details related to certificate issuance — such as a password for the root certificate, a common name or an expiration date — are not required, because a certificate pool does not sign certificates itself.

For Version 26.4.0

Import certificates into the pool

The import is performed by editing the previously saved certificate authority; the Import certificate pool field only appears after the authority has been saved for the first time. There, a ZIP archive containing the externally issued certificate files is uploaded. Below it, Relution lists the certificates already contained in the pool.

Optionally, a subtype can be set in the Default certificate subtype field. It determines the function for which the certificates are available later on. The available options are the same functions as for user certificates: General certificate, WiFi, Exchange, VPN and apps, S/MIME Encryption and S/MIME Signing (see User certificates →). If a subtype is selected, it applies to all certificates in the archive; the `#Zertifikatstyp` column of the CSV file is then ignored and may be omitted. With the default setting None, the subtype is taken from the `#Zertifikatstyp` column row by row; rows without a valid subtype are reported as errors.

Structure of the archive

The ZIP archive contains the externally issued certificate files as well as exactly one CSV file (UTF-8) that specifies an identifier and the import password for each certificate. Accepted certificate files are PKCS#12 containers (`.p12` or `.pfx`) and PEM files (`.pem` with private key, certificate and certificate chain). The separator is a semicolon, the header row is:

```
#E-Mail-Adresse;#P12-Passwort;#Zertifikatstyp
```

Column	Content
`#E-Mail-Adresse`	Identifier of the certificate, used as the certificate name — must match the file name of the corresponding certificate file in the archive
`#P12-Passwort`	Import password of the corresponding certificate file
`#Zertifikatstyp`	Function of the certificate: `GENERAL_CERTIFICATE`, `WIFI`, `EXCHANGE`, `VPN`, `SMIME_ENCRYPTION` or `SMIME_SIGNING`; only evaluated if no Default certificate subtype is selected for the import

The columns are mapped via the header row, so their order does not matter. One row per certificate, for example:

```
#E-Mail-Adresse;#P12-Passwort;#Zertifikatstyp
max.mustermann@example.com;secretPassword;WIFI
```

The CSV row and the certificate file are matched by file name: the certificate file in the archive is named after the identifier in the `#E-Mail-Adresse` column, in this example `max.mustermann@example.com.p12`. If the file name differs from the identifier, the certificate cannot be matched. Certificate files without a corresponding CSV row are ignored.

> No assignment to user accounts
>
> The `#E-Mail-Adresse` column only serves as an identifier; certificates are not assigned to user accounts. During distribution, each device receives a not yet assigned, valid certificate of the required subtype from the pool, preferring the one with the earliest expiration date. A certificate pool is therefore not suitable for scenarios in which the certificate must contain a specific user identity.

After the upload, the form shows the result: the number of imported certificates, skipped duplicates and errors. The affected identifiers are listed under Failed imports. Faulty rows do not abort the import; the remaining certificates are imported nonetheless. A certificate counts as a duplicate if its serial number already exists in the pool of the organization.

Imported certificates in the certificate management

The imported certificates then appear under `Settings` → `Certificates` with the usage Built-in pool certificate, each with the subtype selected during the import or specified in the CSV file — WiFi in the case described here. This view allows the certificates to be inspected and managed like all other stored certificates, see Certificate Management →.

Certificate template for a certificate pool

So that the certificates from the pool can be used in policy configurations, a template is created under `Settings` → `Certificate Templates` → `Add`.

If a certificate pool is selected as the certificate authority, the fields for certificate generation are omitted (Subject name, Subject alternative names, Key algorithm, Key length, Certificate key usages, Certificate extended key usages). The following are displayed:

- Name: Name of the template.
- Certificate template type and Description (optional).
- Certificate Authority: The previously created certificate authority of the type Certificate pool.
- Enable automatic renewal with Automatic renewal period (in days): If the expiration date of an assigned certificate falls within this period, it is replaced by a free certificate of the same subtype from the pool. The previous certificate is marked as deleted and is not assigned again.
- Certificate renewal behaviour and Period after which the certificate expires (in days) (mandatory, default value 365).

The required subtype results from the configuration in which the template is used, e.g. WiFi for a Wi-Fi configuration. If the pool no longer contains a free certificate of this subtype, no certificate can be assigned and Relution reports a compliance violation; the pool then has to be replenished with further certificates. If only a renewal is due, the previous certificate remains assigned until it expires, and Relution creates a compliance notice.

Validation

For version 26.4.0

The setup is complete once

- the certificate authority of the type Certificate pool has been created,
- the import of the ZIP archive (in the example with the subtype WiFi) has completed without duplicates and without errors,
- the imported certificates are listed under `Settings` → `Certificates` with the subtype WiFi, and
- the certificate template for the certificate pool authority is displayed without any fields for certificate generation, but with the renewal and expiration options.

Using the template in a policy follows the same procedure as with the Built-In CA, see Built-In CA →.

IP block after failed logins

As of Relution version 5.19, a global server setting can be used to define whether an IP address is blocked in the event of incorrect login attempts. The settings are located in the Global organization under `Settings` → `System Security`. The configuration allows specifying after how many failed login attempts an IP address is blocked and whether the block is lifted automatically after a defined time. In addition, the system administrator has the option of permanently allowing or blocking logins from an IP address or an entire IP range (IP access rules).

Configuring IP blocking

The General section provides the following options:

- Enabled: Turns IP blocking on (default: off).
- Maximum failed logins (default 10): If the failed logins from an IP address exceed this value, the IP address is blocked. A successful login from this IP address resets the counter.
- Clear blocked IP addresses after specified time with Clear blocked after (in minutes) (default 60): Lifts the block automatically after the defined time. If this option is not enabled (default), the IP address remains blocked until the entry in the IP access rules is removed manually or the IP address is allowed there.

IP access rules

The IP access rules table lists the automatically recorded and blocked IP addresses (with Blocked since). Add IP address can be used to add individual IPv4 addresses or entire ranges (IP address or CIDR) with a status: Allowed, Blocked, Permanently allowed or Permanently blocked. Selected entries can be changed collectively via Block selection, Permanently allow selection or Permanently block selection.

For version 26.4.0

> The IP access rules, including entries with the status Permanently blocked or Permanently allowed, only take effect if the Enabled toggle is switched on in the General section.

The meaning of the status values, CIDR examples and recommendations to avoid accidental lockout are described under Security optimization →.

User lock after failed logins

Independently of IP blocking, each organization can define under `Settings` → `Login Management`, section Failed login attempts, with User deactivation on failed consecutive login attempts and Maximum failed login attempts (default 10), whether and after how many failed login attempts a user is blocked.

The user is deactivated once the maximum number of failed attempts has been reached. The user can be reactivated by the administrator. Only login attempts of users who log in with a password stored in Relution are counted; users who authenticate exclusively externally (e.g. via LDAP) are not blocked. A successful login resets the counter of failed attempts.

Details: Login Management →

Global Organization

With version `5.23`, the Global organization has been introduced in Relution. This combines the Store organization and the System organization. Until version 5.22, the store organization had to be activated manually. With version 5.23, this activation is automatic.

Identification of the global organization

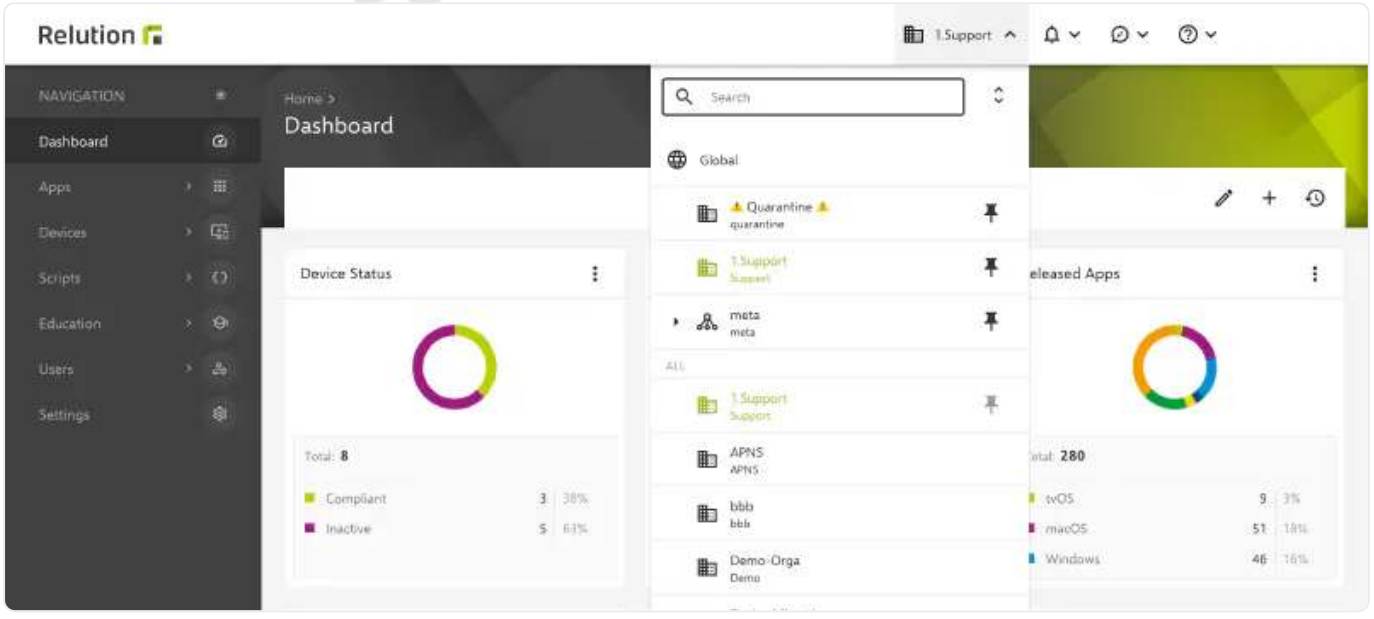
The new organization has the name Global. Accounts with the authorization of the system administrators and accounts with the authorization of the former Store organization have access to it.

In the organization switcher in the upper right corner, the global organization can be recognized by the globe icon. Meta organizations have a structure icon, sub-organizations have their own icon and standalone organizations have a building icon.

Organization switcher

New in 26.4

Clicking the organization name in the top right of the header opens the organization switcher. As of version 26.4, the Global organization is always shown fixed at the top of the list. In addition, individual organizations can be pinned as favorites using the pin icon, so they appear above the full list of organizations for quicker access.



For Version 26.4.0

Functionality

The full range of functions is available to users with system administrator authorizations. New organizations can also be created in this organization. This is possible via the newly added menu item Organizations.

Users without authorization for organization administration, i.e. users who have been migrated from an existing store organization, have access to the typical range of functions of the store organization.

Devices cannot be enrolled in the global organization itself. Devices are enrolled and managed in the subordinate organizations.

Apps, policies and scripts can also be provided at the level of a meta organization for its sub-organizations (Meta Organizations →).

Global Users

Users can be created centrally at the global organization level and subsequently assigned to various tenants with specific roles or permissions.

This structure enables flexible identity management: For example, a global user can act as an administrator in Tenant A, while only holding the role of a teacher in Tenant B.

Further information on permissions →

For version 26.4.0

System-wide Automated Device Enrollment

Via Apple School Manager or Apple Business Manager, devices for Automated Device Enrollment (ADE, DEP in the portal) can be assigned to the Global Organization. A DEP profile in the Global Organization with the option Username + Password selected under User authentication assigns the Apple devices to the organization of the signed-in user.

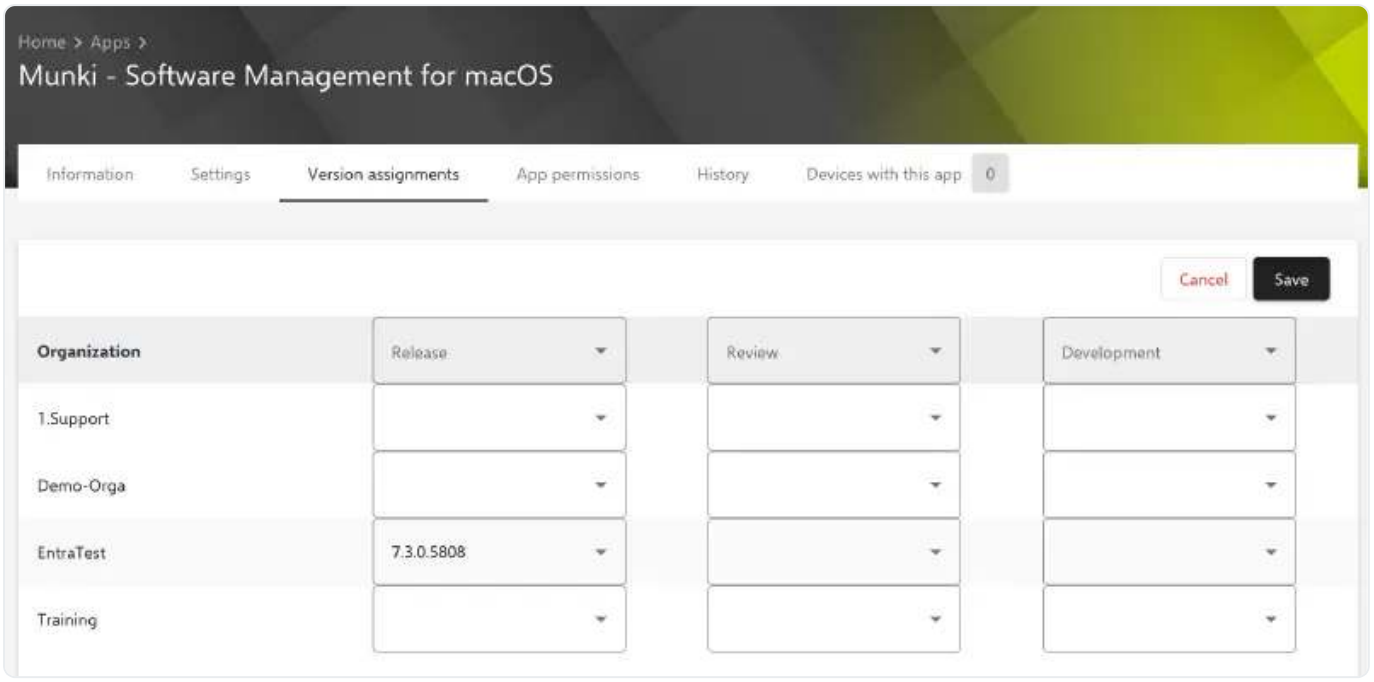
Alternatively, a target organization can be set for an automatic enrollment in the global organization in the Enroll to organization section. The device is then enrolled in this organization, even without user authentication. If Username + Password is also selected, the signed-in user must belong to the target organization. The same approach is possible via meta organizations.

DEP →

It is still possible to add DEP tokens to other organizations.

Native app distribution and versioning

Native apps can be distributed via a policy with the App compliance configuration. The version assignment can be defined in the Global Organization within the app on the Version assignments tab.



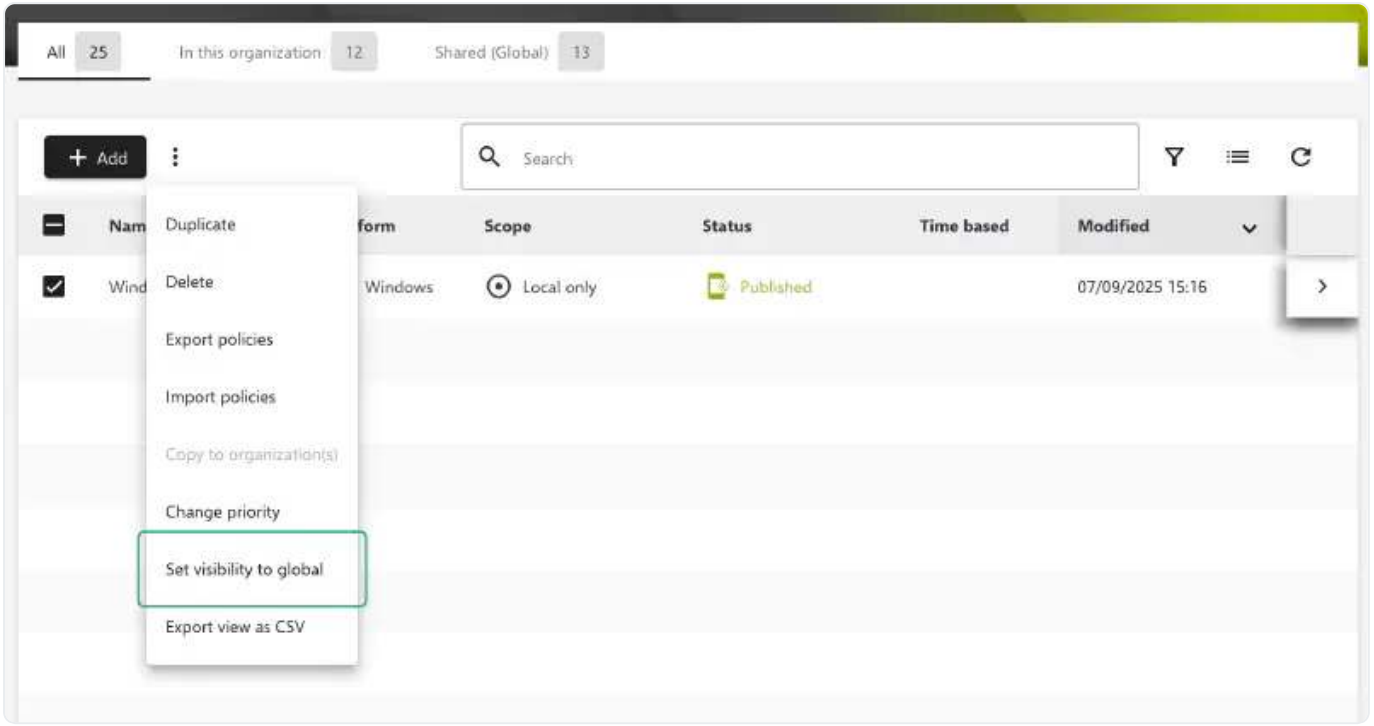
Publish policies or copy them to organizations

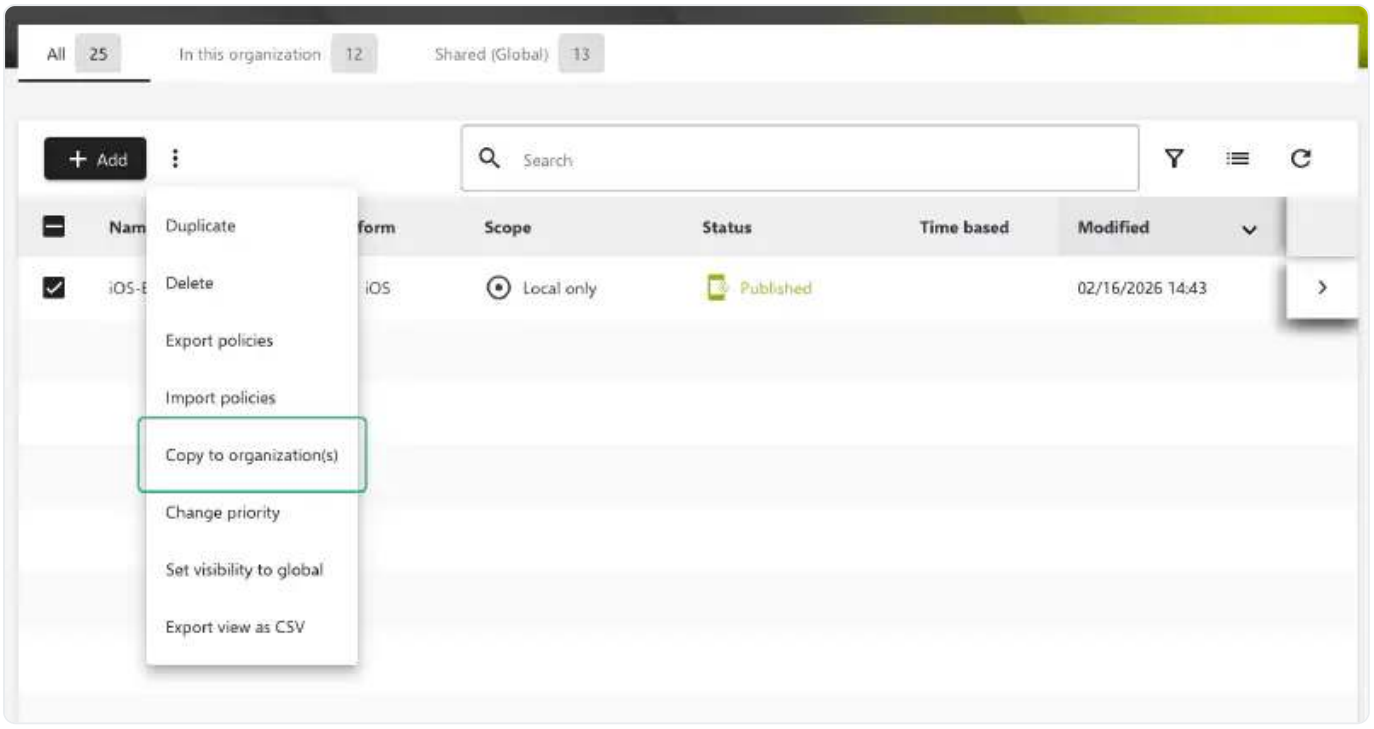
For version 26.4.0

Policies created in the Global Organization can be distributed in two ways:

- Copy to organization(s): copies the policy to one or more organizations. Only available for iOS and tvOS policies.
- Set visibility to global: makes the policy available to all organizations. Available for published policies of all platforms.

Policies made globally available are read-only in the subordinate organizations; changes can only be made in the Global Organization. Global policies take precedence in the prioritization.





General policies →

Global provision of scripts

Scripts created in the Global Organization (PowerShell scripts for Windows and shell scripts for macOS) can be made available read-only in all subordinate organizations. This works in a similar way to the publication of policies or apps. This is done via the three-dot menu of the script entry in the table using the Set visibility to global function.

Publish scripts globally →

System-wide LDAP configuration

The LDAP → configuration can be made here in the Settings and an organization-specific mapping can be made. The advantage is that the LDAP provider only needs to be configured centrally once.

This configuration can be set for user accounts, groups, classes, teacher and student accounts as well as teacher and student groups in the Map objects to organizations area. The mapping filters only distribute objects that are already covered by the import filters of the LDAP configuration.

The Sync unmapped objects to this organization option determines what happens to objects that match no mapping: If it is enabled (default), they are synchronized to the organization containing the LDAP configuration. If it is disabled, they are not imported and are reported as synchronization errors.

For version 26.4.0

Moving devices to other organizations

Via the Move to button in the device list of the Global Organization, iOS/iPadOS, tvOS, macOS, Windows and Android Legacy devices can be moved to other organizations. This is not possible for other platforms (including Android Enterprise, ChromeOS, Linux, visionOS, watchOS).

Moving removes user- and organization-specific data from the device, including the assigned user, device groups and certificates. Only policies that have been made globally available via the global organization will be retained on the devices.

Move device to organization →

Global Applications

From Relution `5.29` onwards, it is possible to distribute native apps to other organizations via the global organization. In simple terms, this involves creating a link to the app in the child organizations. This saves database/memory resources and considerably simplifies the deployment of the app.

Apps created via an Apps and Books account (VPP in the portal) of the global organization automatically replace existing apps in other organizations.

Requirements

For version 26.4.0

1. To distribute the desired app, access to the global organization must be possible. It can be recognized by the globe icon in the organization switcher in the upper right corner, usually also by the name Global.
2. An uploaded native app or a Google, Apple or Windows store app that has not yet been distributed globally:
   - iOS: .ipa
   - macOS: .pkg, .dmg
   - Android: .apk
   - Windows: .msix, .msixbundle, .appx, .appxbundle, .msi, .exe
3. The app has at least one version in the Release status. Otherwise, the Set visibility to global function is disabled (hint Selection contains unreleased apps).
4. The app must not already be available globally.

Execution

1. In the Page Navigation on the left under `Apps` → `App Store`, the mouse pointer is moved over the desired native app.
2. The 3-point menu next to the app name is clicked.
3. The Set visibility to global option is selected.
4. For apps that are already (partially) assigned, a dialog window with conflicts and notes may appear.

   This action cannot be undone. The following apps already exist in other organizations. If they are made global, the apps in the other organizations will be replaced and deleted. The apps to be made globally available are then selected in the dialog.

   This process may take some time.

5. The app is then shown as Shared in the Scope column. In child organizations it appears as From Global.

For version 26.4.0

Login Management

To further secure the login in Relution, a variety of settings can be configured for the respective organization under `Settings` → `Login Management`. Here, the settings for password complexity, multi-factor authentication (MFA) and failed login attempts are described.

Password Policy

- Allow simple password (default: off): A simple password may match the username, e.g., username test and password test. If the option is disabled, the password must match neither the username nor the organization name.
- Minimum password length: 3 to 72 characters, default 8.
- Maximum password age in days: When the password is older than the maximum age, a new password has to be set at the next login. The default value `0` means that passwords do not expire.
- Minimum numbers of digits
- Minimum numbers of lower case letter
- Minimum numbers of upper case letter
- Minimum numbers of symbols: Any character that is neither a letter nor a digit counts as a symbol.
- Disable forgot password reset

The minimum numbers of digits, lowercase and uppercase letters and symbols default to `0`.

For version 26.4.0

Disabling Password Reset

The Forgot your password? function can be turned off under `Settings` → `Login Management` with the Disable forgot password reset option. If disabled, password reset without administrator intervention is no longer possible. Local accounts that lose their password require an administrator to reset it directly.

The effect depends on the organization level:

- In the Global organization, disabling applies to all organizations.
- In a meta organization, it overrides the setting for the organizations of this meta organization.
- In an organization, it only takes effect on the login screen of this organization.

If the option is set in a parent organization, the toggle is read-only; the portal then indicates that the link has been disabled by the parent organization.

At least one administrator account with a known, recoverable password should exist before this option is disabled.

Multi-Factor Authentication

- E-Mail Authentication (default: on)
- One-time code expiration time: 30 seconds to 1 hour, default 10 minutes.
- Authenticator Apps (TOTP) (default: on)

If both factors are disabled, the portal indicates that all users can log in without MFA.

MFA →

Failed Login Attempts

- User deactivation on failed consecutive login attempts (default: off)
- Maximum failed login attempts (default 10, at least 1)

When a user reaches the maximum number, the user is deactivated and has to be reactivated by an administrator. A successful login resets the counter. Deactivation only applies to local Relution users; users who authenticate exclusively externally (e.g. via LDAP) are not counted.

Blocking IP addresses after failed login attempts is described under IP block after failed logins →.

For version 26.4.0

Multi-factor authentication

Multi-factor authentication, or MFA for short, is a security mechanism that requires users to provide at least two independent verification factors to uniquely identify themselves when accessing an application.

Unauthorized access is made significantly more difficult by the additional authentication method; the security level is thus significantly increased.

MFA and Relution

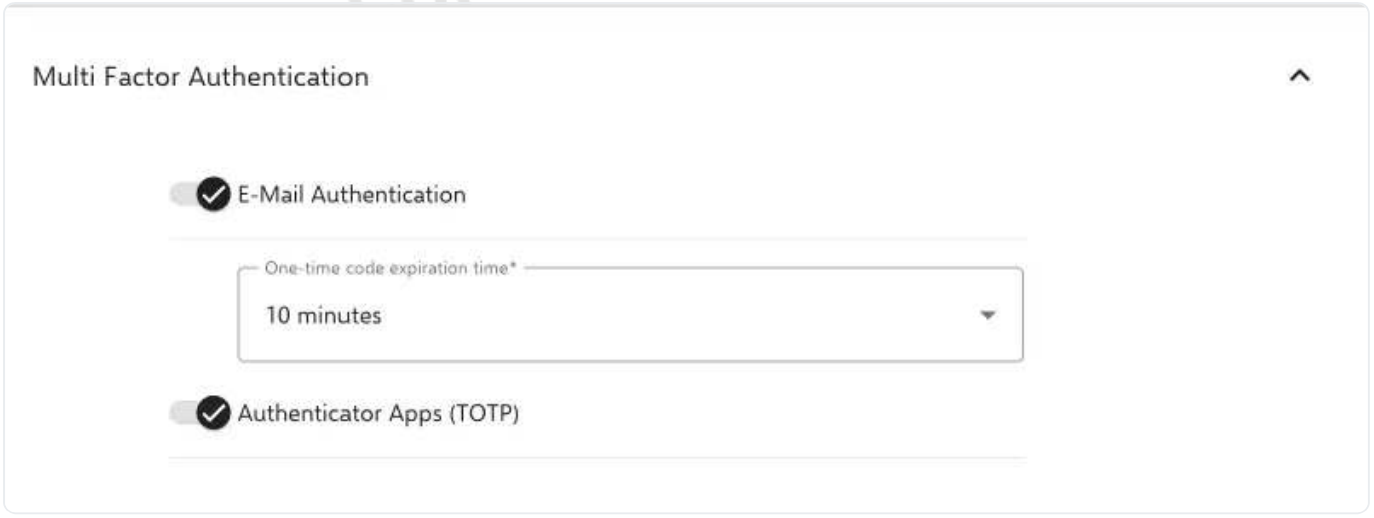
Relution enables LDAP and local users to activate the additional authentication methods E-Mail (one-time code by e-mail) and Authenticator App in the Relution Portal in addition to specifying user name and password.

With the release 5.16, the requirement of the German Federal Office for Information Security (BSI) for MDM providers to implement the provision of an additional security level is taken into account.

How is the MFA configured in Relution?

For version 26.4.0

Under `Settings` → `Login Management`, an organization or system administrator defines in the Multi Factor Authentication section which MFA methods are available in the organization. By default, E-Mail Authentication and Authenticator Apps (TOTP) are enabled. The setting of the organization a user belongs to applies.



For E-Mail Authentication, the One-time code expiration time is defined: 30 seconds, 1, 2, 5, 10, 15 or 30 minutes, or 1 hour (default: 10 minutes). Authenticator Apps (TOTP) allows signing in with a time-based code from an authenticator app. Each of the two methods can be disabled individually; both can also be active in parallel.

If both methods are disabled, Relution no longer requests a second factor at login – neither for roles with enforced MFA nor for users who have already set up MFA tokens.

Force MFA log in

The Relution Permission system has been extended with the possibility of multi-factor authentication. It is possible to define for a role whether MFA log in is required or not.

If the permission/role with activated MFA login is assigned to a user or a group, an MFA login is mandatory when logging in.

If no MFA method has been set up yet, then the user must do this at the first log in.

Enforce MFA for a group

If MFA login is to apply to all members of a group, a role with MFA enabled is created and assigned to the group. Roles from parent groups are also taken into account.

1. Under `Users` → `Permissions`, a new role is created via Add, or an existing custom role is opened.
2. In the Multi-factor authentication section, the option Enforce multi-factor authentication for the role is enabled and applied with Save.
3. Under `Users` → `Groups`, the desired group is opened.
4. Via Manage Permissions, the role is selected and applied with Save.

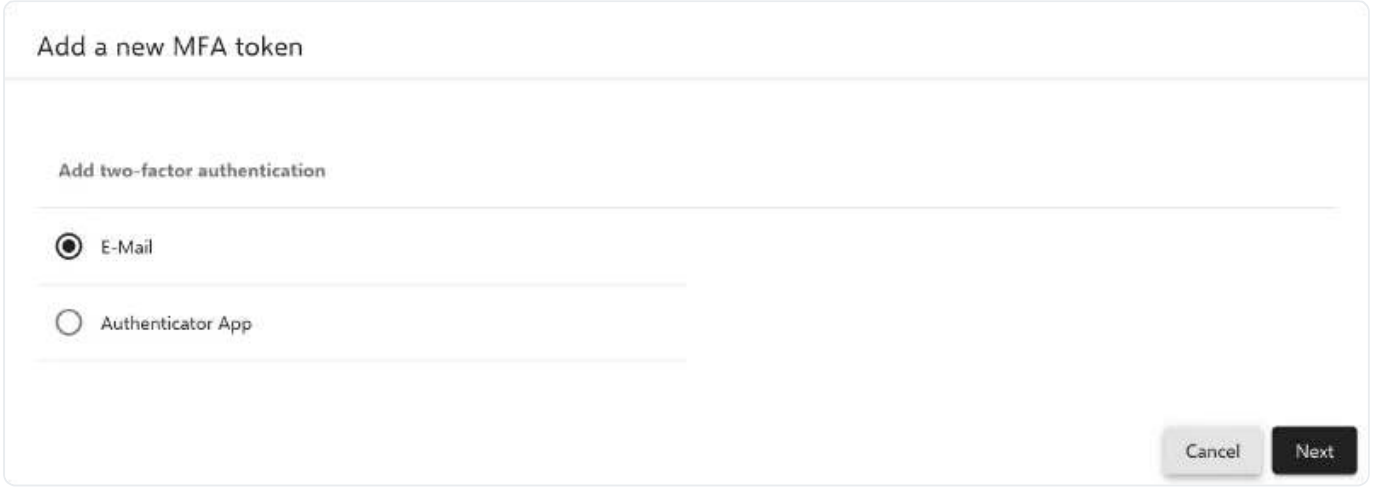
The Multi-factor authentication section only appears in the role once at least one MFA method is enabled under `Settings` → `Login Management`. The default Relution roles cannot be edited; a custom role is therefore required for MFA. The assignment is also possible for groups synchronized via LDAP. Further information on roles can be found in the article Permissions →.

For version 26.4.0

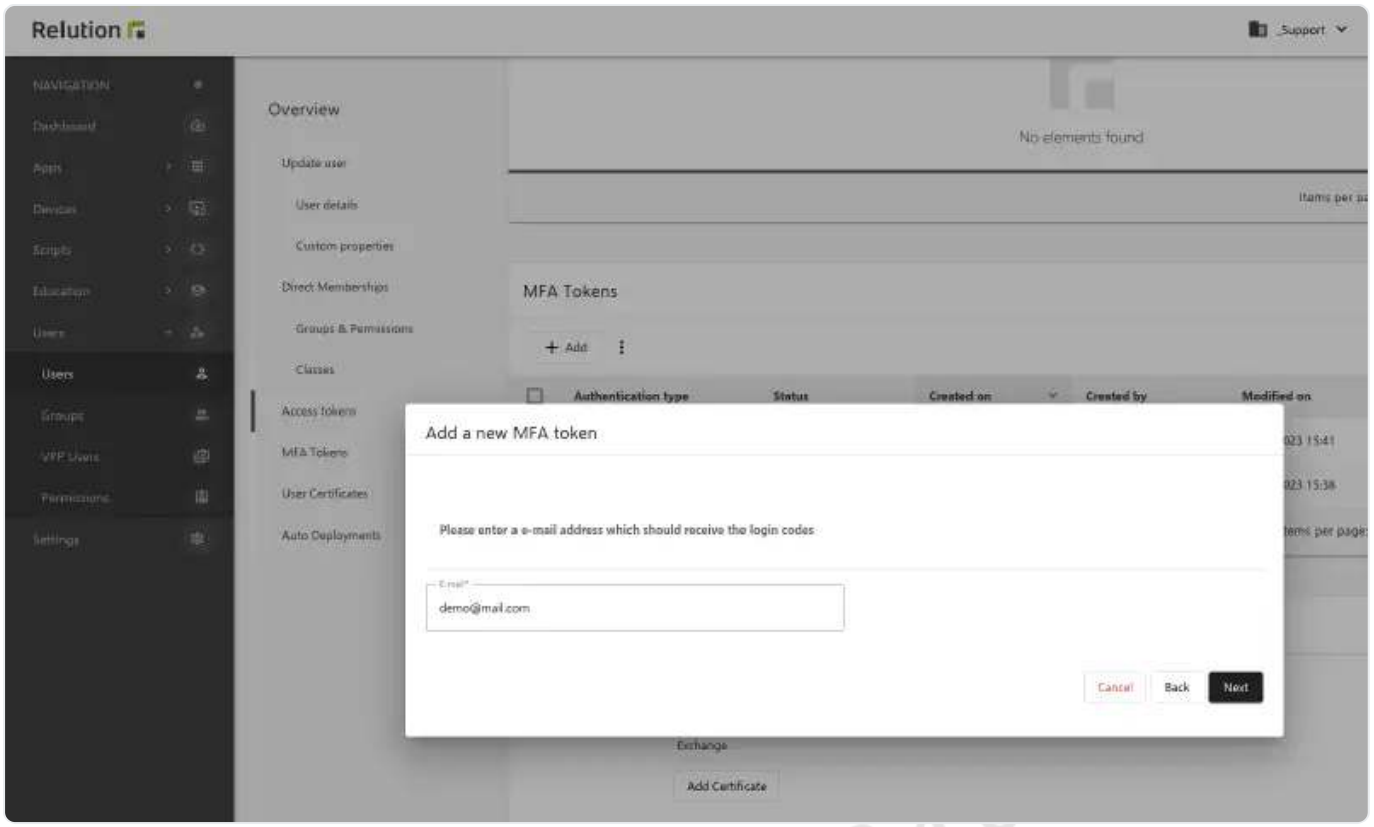
E-mail token

Each user can activate MFA for themselves in the Relution Portal, independently of an administrator. Once an MFA token is set up, the second factor is requested at every login, even without a role enforcing MFA.

In the Relution Portal, the user menu at the top right opens the Profile entry. There, on the MFA Tokens tab, the Add button opens the Add a new MFA token dialog. The tab only exists if at least one MFA method is enabled under `Settings` → `Login Management`. After selecting E-Mail, the e-mail address is entered in the next step.

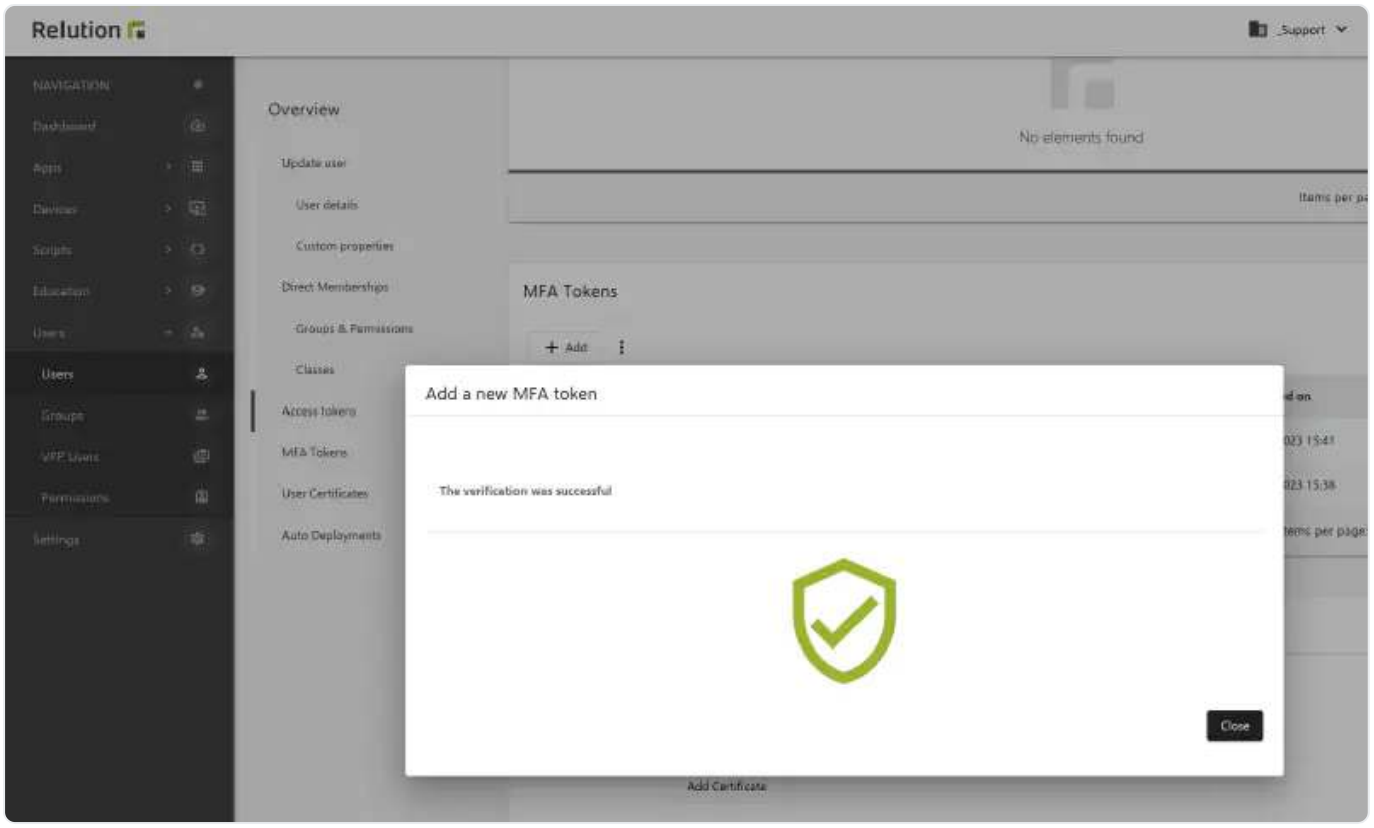


Private as well as user different e-mail addresses can be stored in the system - useful in the school context.



After entering the address, a one-time verification code is sent to the stored e-mail address. It remains valid for the time period defined by the administrator. As soon as the six-digit Verification code from the e-mail is entered, multi-factor authentication is set up. If the setup is cancelled beforehand, the token appears with the status Uncompleted and does not count as an MFA factor.

For version 26.4.0

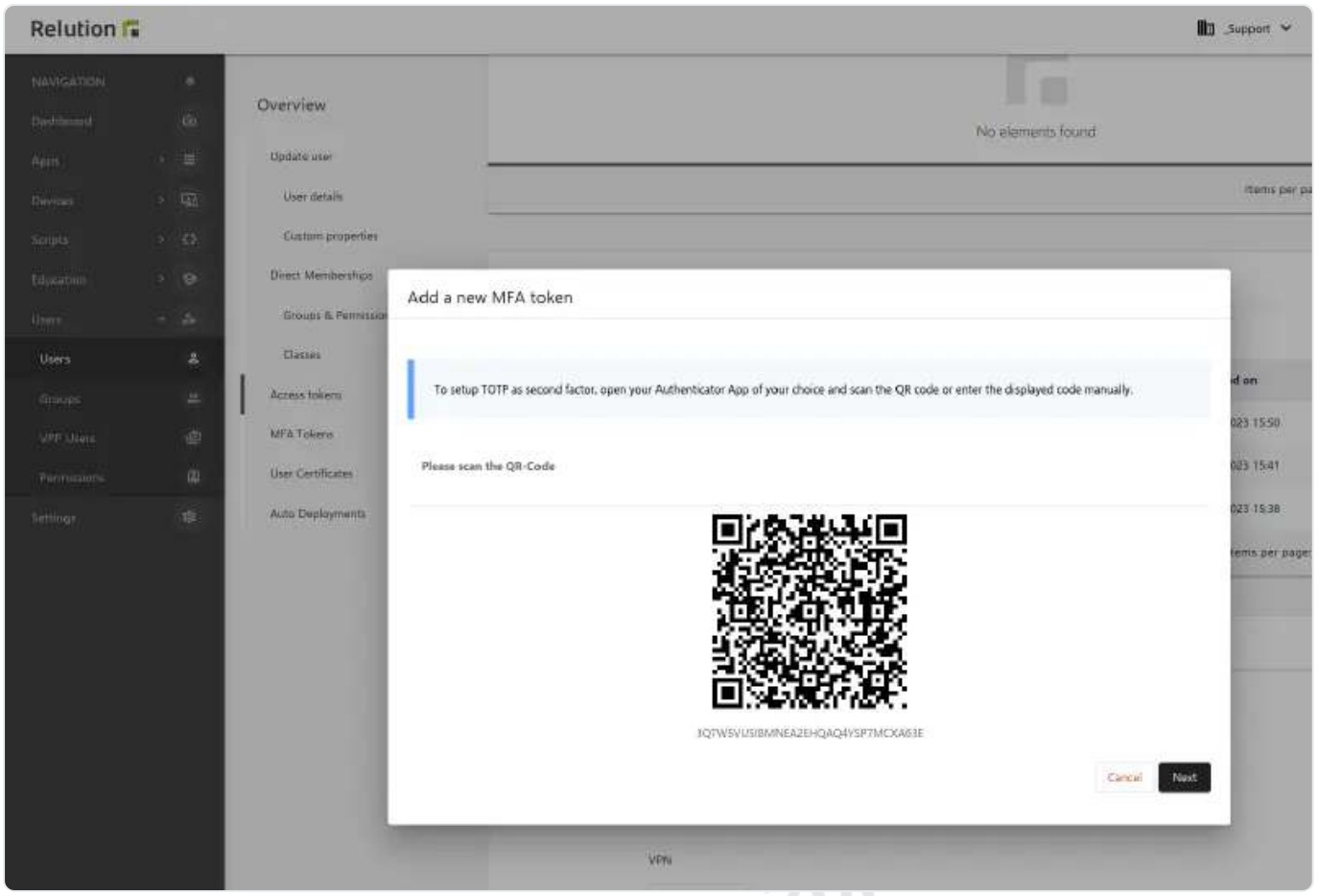


Any number of MFA factors can be stored in the Relution Portal. If several e-mail tokens are set up, the code is sent to all stored addresses at login. In addition to the e-mail variant, the use of various Authenticator Apps is supported.

If the second variant Authenticator App is selected in the Add a new MFA token dialog, a QR code is displayed, which is scanned with an authenticator app previously installed on the end device.

It is also possible to use a setup key for verification.

For version 26.4.0



If various Authenticator apps are in use on multiple devices at the same time, the validity of at least one app is checked for a correct login. When using both multi-factor authentication methods, the Authenticator app is primarily queried; the stored e-mail variant serves as a backup. At login, the Use e-mail button (below No access to the Authenticator App?) switches to the e-mail variant; Re-send e-mail requests a new code.



If only the Authenticator app is in use, there is no email fallback.

Delete MFA tokens manually

MFA tokens can be deleted manually by the user in the Profile on the MFA Tokens tab.

If all MFA variants have been removed manually, but MFA is enforced via a role, multi-factor authentication must be stored again the next time the user logs in to the Relution Portal.

What happens if the MFA is lost?

If the user does not have access to email and/or Authenticator app while the MFA is activated, logging into the Relution Portal is no longer possible - going to the Administrator is mandatory.

Under `Users` → `Users`, the affected user can be opened and the token deleted in the MFA Tokens section. This requires the permission to delete users. With the permission to create users, MFA tokens can also be added for the user there.

The MFA column of the user list shows whether a user has set up MFA; the filter of the same name distinguishes Configured and Not configured.

For version 26.4.0

TLS Trust Configuration

The TLS Trust configuration bundles the server-side settings for establishing trusted TLS connections. It is found under `Settings` → `TLS Trust configuration` and is divided into two areas: the trusted certificates for outbound connections and certificate pinning for Apple enrollment. The TLS Trust configuration is only available in the global organization and applies server-wide to all organizations. Changes in both areas are applied together via Save in the upper area of the page.

Trusted certificates

Relution accepts these CA certificates in addition to the system's default trust store when establishing outbound TLS connections. Add selects CA certificates that were previously uploaded under `Settings` → `Certificates` (see Certificate Management →). The selection dialog only shows certificates marked as a certificate authority (CA); certificate containers such as `pfx` / `p12` are not available for selection. The overview lists Name, Type and the expiry date (Expires) for each entry; selected entries are removed again via Delete.

Certificates used here as a trusted certificate or as an anchor certificate cannot be deleted in the certificate management as long as they are referenced.

Certificate pinning (Apple enrollment)

For version 26.4.0

New in 26.5

When the Enable certificate pinning toggle in the General area is switched on, the MDM server's TLS connection is validated against selected anchor certificates instead of the system trust store. This makes man-in-the-middle attacks and the use of unauthorized certification authorities more difficult. During the enrollment of Apple devices, pinning is written into the MDM profile and then applies to the device's entire communication with the MDM server, including check-in. If pinning is disabled, the device validates the connection against the system trust store.

The certificates to be checked are selected in the Anchor certificates area using Add from the CA certificates stored in the certificate management; the overview lists Name, Type and the expiry date (Expires) for each entry. At least one anchor certificate is required to enable pinning. The Require certificate revocation check toggle additionally enforces a check of the certificate revocation status. If Enable certificate pinning is switched off, Relution clears the list of anchor certificates and resets the revocation check; after switching it on again, the anchor certificates must be selected again.

> Pinning is stored in the MDM profile
>
> Pinning is embedded into the MDM profile at enrollment time. Changes made here affect new enrollments. Relution only transfers the changed configuration to already enrolled devices when their MDM profile is updated (Update MDM profile action or automatic renewal before the identity certificate expires). A misconfiguration can lock devices out of MDM communication; a device that can no longer connect to the MDM server because of a wrong pin also no longer receives a profile update and must be re-enrolled. Only long-lived CA certificates should be pinned; when rotating a CA, both the old and the new anchor remain selected.

Only enable the revocation check with revocation information

The Require certificate revocation check toggle may only be switched on if the server's TLS certificate provides revocation information (OCSP responder URL). If this information is missing, devices may refuse to connect.

Behavior during enrollment

When pinning is enabled, the device's connection to the MDM server is checked against the selected anchor certificates during enrollment. If the server's TLS certificate chain can be traced back to one of the anchor certificates, enrollment succeeds. This check also applies to the subsequent MDM communication of the enrolled device. If it differs, the connection is rejected and enrollment fails.

If pinning is switched on but no anchor certificate is configured or can be loaded, Relution generates the MDM profiles without pinning.

Devices with an operating system version below the minimum required for pinning continue to be enrolled without pinning; enrollment remains functional there.

Anchor certificate notifications

For version 26.4.0

Relution checks the pinned anchor certificates every hour and after each save and reports problems in the notification center so that devices being locked out can be prevented early. The notifications are received by users of the global organization who are allowed to view the TLS Trust configuration. Reported issues include:

- an anchor certificate that expires in less than 90 days or has already expired,
- an anchor certificate that cannot be loaded or is not a CA certificate,
- ineffective pinning, for example when no anchor certificate is configured or none matches the server's TLS certificate chain.

LDAP Configuration

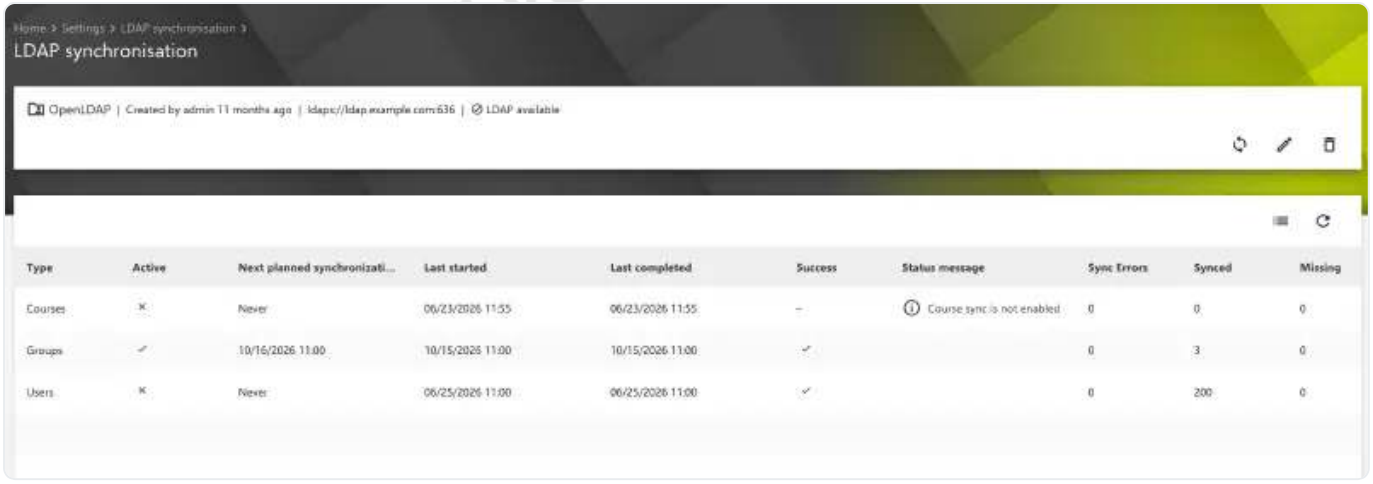
Starting with Relution version `5.18.0`, LDAP providers for user, group and class import can be configured directly via the Relution Portal. The form contains the usual configuration parameters, which can be verified with several functional tests. A restart of the Relution service is not necessary when configuring via the portal, so changes and reconfigurations do not interrupt operations. Configuring LDAP synchronization requires some knowledge of the subject; an LDAP browser that displays attributes correctly is recommended. For Windows, the Softerra LDAP Browser and for Linux or macOS the Apache Directory Studio have proven themselves. Both tools are free of charge.

> Configuring LDAP providers via the Relution Portal requires a paid license with the LDAP UI Connections feature. Without this license, the configuration cannot be saved, and users, groups and classes are not synchronized.

Basics

LDAP is configured under `Settings` → `LDAP synchronisation`. Multiple LDAP providers can be set up per organization. The mail addresses of the users in Relution must be unique. Otherwise, errors may occur and some user accounts cannot be created. A new LDAP provider is created via Add.

A manual synchronization can be started at any time: in this list via Start synchronization for the selected provider, and in the lists of users, groups and classes via One-time LDAP synchronization. The detail page of a provider shows the result of the last synchronization for each type (users, groups, classes).



Basic configuration

The configuration form is divided into several levels. Not all parameters are always required for a given case. Some fields already contain examples that suggest the syntax.

LDAP synchronization

First, a name is assigned to the LDAP provider. A short and meaningful name is recommended.

> This name cannot be changed afterwards.

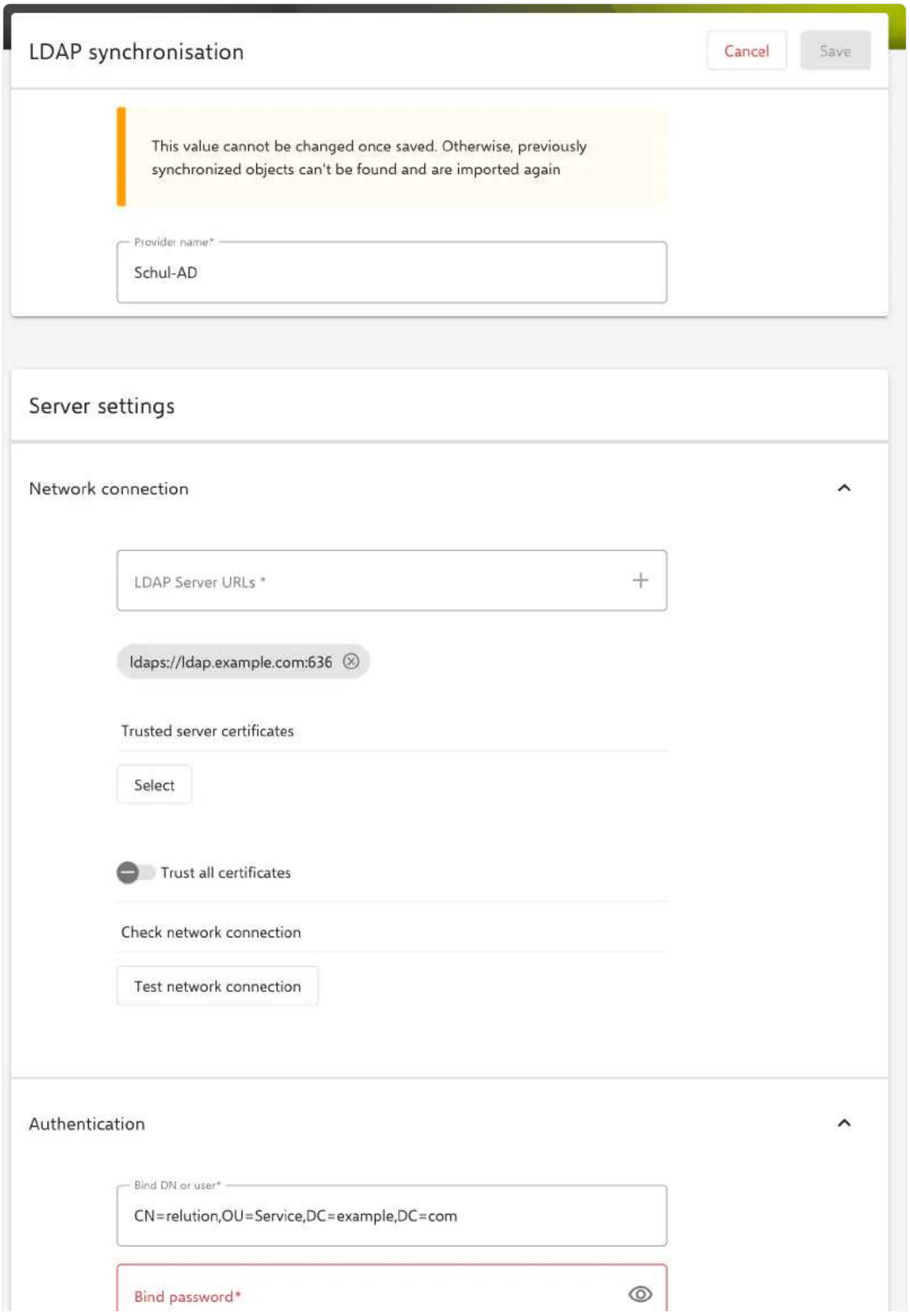
Server settings

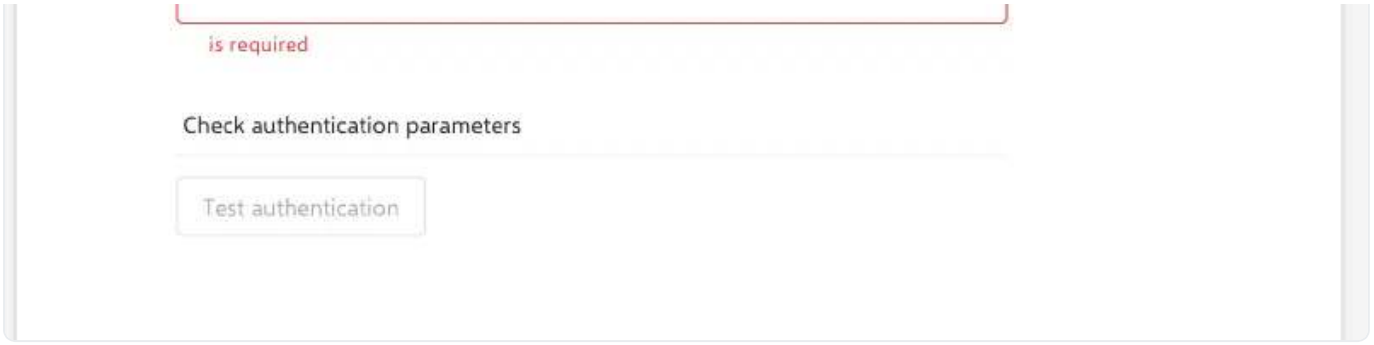
- LDAP Server URLs: The URL of the LDAP server is entered and confirmed with `Enter`.

If LDAPS is used and the server does not have a trusted certificate, the certificate can be stored under Trusted server certificates so that Relution classifies it as trusted. Alternatively, Trust all certificates makes Relution accept any server certificate. The portal points out the security risk; explicitly stored certificates are preferable.

The connection is checked with Test network connection. The connection attempt should be successful before continuing with the configuration.

For version 26.4.0


LDAP synchronisation
Cancel
Save
This value cannot be changed once saved. Otherwise, previously synchronized objects can't be found and are imported again
Provider name*
Schul-AD
Server settings
Network connection
LDAP Server URLs *
ldaps://ldap.example.com:636
Trusted server certificates
Select
Trust all certificates
Check network connection
Test network connection
Authentication
Bind DN or user*
CN=relution,OU=Service,DC=example,DC=com
Bind password*



Authentication

- Bind DN or user: Username with read permissions in LDAP. Ideally, the Distinguished Name (DN) is used here.
- Bind password: The corresponding password.

The credentials are checked with Test authentication.

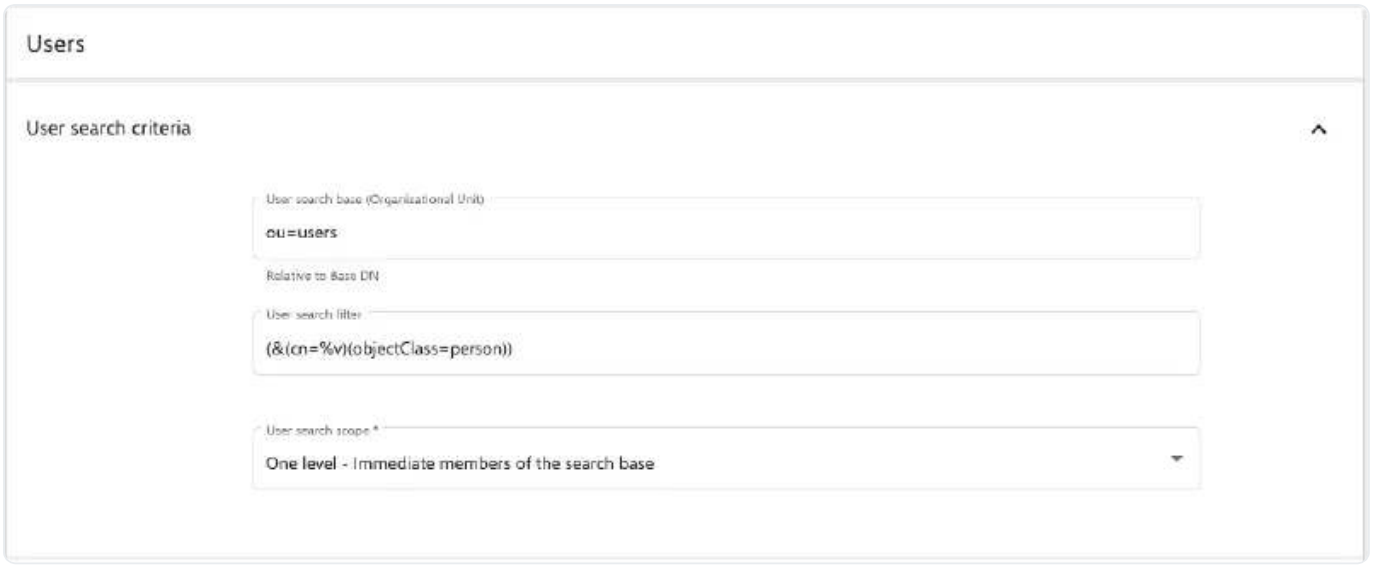
Base DN

After a successful Test authentication, the base DNs reported by the server are offered in the Discovered base DNs selection; the first entry is preselected. Use discovered base DN as base DN copies the selected entry into the Base DN field. Any necessary changes can be made at any time.

For version 26.4.0

Search criteria for users

- User search base (Organizational Unit): The search base for users, relative to the base DN, for example `OU=users`.
- User search filter: Conventional LDAP search filters are used here. Relution always uses the placeholder `%v` for user input. For example, a simple search filter for users could be `(&(cn=%v)(objectClass=person))`.
- User search scope: Configures how deep in the path user accounts are searched with the corresponding search filter. Selecting Subtree may result in a large number of hits.



Manual mapping for users

After the connection is established, Relution checks which type of LDAP it is, for example OpenLDAP or an Active Directory. The appropriate fields are then preconfigured via an auto-mapping. This function can be partially or completely overridden by enabling Manual user attribute mapping.

For example, setting a foreign key is recommended. This is useful when users change their name: the user account can still be identified, and the name and mail address are just updated without creating a new account in Relution.

The objectSID field is not suitable here. It causes errors as it sometimes contains uninterpretable characters.

User synchronization

Test user import checks whether the users can be imported and whether the filters return the correct results.

- In addition, Periodic user import can be enabled. This is an automatic synchronization that runs every 24 hours at the selected Synchronization time. If periodic import is disabled, users matching the search filter are still imported when they log in or when they are assigned to an enrollment.
- A manual synchronization can be started at any time (see Basics →).
- Synthetic group: This is a group that is automatically created by the LDAP sync. All users imported via the LDAP provider – during the scheduled synchronization or at their first login – become members of this group.
    - The group name consists of the organization's Unique name in uppercase letters and the entered value. With the default value `LDAP`, this results, for example, in the group `MYORG LDAP`.
    - If the field is left empty, no synthetic group is created.
    - Since permissions can be assigned to LDAP groups, the synthetic group is suitable for assigning a role to all LDAP users together, e.g. for Multi-factor authentication →.
- The option When an LDAP user is not found can only be edited while Periodic user import is enabled (default: Do nothing). It also applies when a user still exists in LDAP but no longer matches the search criteria. Three reactions are available:
    1. Do nothing: The user remains in Relution. However, the account can no longer be used for login because the LDAP provider refuses authentication.
    2. Disable the user in Relution: This is the recommended setting, as user accounts remain associated with devices and no data is lost if the accounts are accidentally no longer found, for example after renaming a group in LDAP that a filter then no longer finds.
    3. Delete the user from Relution: Users that are no longer found by the importer are removed directly from the database, regardless of any links to devices, groups or classes.

Caution: Deletion is irreversible — affected users are removed from the database immediately, regardless of any links to devices, groups or classes.

For version 26.4.0

Search criteria for groups

- Group search base (Organizational Unit): The search base for groups, relative to the base DN, for example `OU=groups`.
- Group search filter: Conventional LDAP search filters are used here. Relution always uses the placeholder `%v` for user input. For example, a simple search filter for groups could be `(&(cn=%v)(objectClass=groupOfNames))`.
- Group search scope: Configures how deep in the path groups are searched with the corresponding search filter. Selecting Subtree may result in a large number of hits.



Manual mapping for groups

The manual mapping (Manual group attribute mapping) behaves for groups as it does for users. Often, the `entryUUID` field is used for the Foreign key (UID) and the `member` field for Member. The attributes can be checked with one of the LDAP tools recommended above or via the console with `ldapsearch`.

Group synchronization

Test group import checks whether the groups are found.

For LDAP groups to be imported, Import groups of imported users must be enabled. Relution then imports all groups in which synchronized users are members and that match the group filter, including the groups these groups in turn belong to. If the toggle is disabled, only synthetic groups are created.

In addition, Periodic group import can be enabled: every 24 hours at the selected Synchronization time, all groups matching the group filter are imported, even without imported members. Periodic group import and the time can only be set once Import groups of imported users is enabled.

The import is always user-centric: groups do not pull in additional users. Members of a group are only imported if they match the user search criteria themselves.

Groups that are no longer found during a successful synchronization, for example after the group filter has been changed, are deleted in Relution.

Education

LDAP synchronization can also be used to create classes that are displayed in the Education section of the menu and can be used for the Relution Teacher Console or in Apple Classroom. Classes to be created in Relution are group objects in LDAP. They must contain at least one teacher or teacher group and at least one student or student group.

Search criteria for classes

The configuration here is similar to that for users and groups: a search base containing the classes and a corresponding search filter are defined. The search scope is configured as usual via the drop-down menu.

The configuration can be checked with Test class import. Classes are only created later if they contain at least one teacher or teacher group and at least one student or student group. Groups only count if they are found via the search criteria for teacher and student groups.

Search criteria for teachers and students

Here, the configuration also consists of the search base and a corresponding filter. Often, the individual user types are defined by group memberships. Search filters can look like this, for example:

- Teachers: `(&(memberOf=CN=all-teachers,OU=groups,DC=school,DC=local)(objectClass=person))`
- Students: `(&(memberOf=CN=all-students,OU=groups,DC=school,DC=local)(objectClass=person))`

The filters can be checked with Test teacher import and Test student import.

Search criteria for teacher and student groups

As of Relution 5.31, groups can be imported as members of classes. For this, one filter each is configured for teacher groups and student groups. These filters can be used in addition to or instead of the filters for teachers and students. If the automatic import of education data is enabled, at least one of the two filters (user or group filter) must be set for each role. Search filters can look like this, for example:

- Teachers: `(&(cn=teacher*)(objectClass=groupOfNames))`
- Students: `(&(cn=students*)(objectClass=groupOfNames))`

The filters can be checked with Test teacher group import and Test student group import.

Synchronization of education data

The automatic import of education data is configured here as well: with Periodic education import, classes are synchronized every 24 hours at the selected Synchronization time. Classes that are no longer found during a successful synchronization are deleted in Relution.

Organization mapping (Global and Meta)

In the Global Organization and in meta organizations, LDAP providers can be configured to synchronize users, groups and classes into individual organizations via mappings (Map objects to organizations). For each target organization, filters can be set for users, groups, classes, teachers, teacher groups, students and student groups, each as an LDAP filter or a DN filter. The result can be checked with Test organization mapping.

The filters of a mapping only distribute objects that are already found via the import filters. By default, only objects that match a mapping are synchronized; all others are not imported and are reported as synchronization errors. If the option Sync unmapped objects to this organization is enabled under Organization mapping settings, the remaining objects end up in the organization in which the provider is created. If an object matches the filters of several organizations, it is skipped with an error.

For version 26.4.0

Meta Organizations

Meta Organizations form a hierarchy below the global organization. A Meta Organization bundles several sub-organizations that inherit the items it shares, such as apps, policies and scripts. Creating organizations in general is described under Create organizations →.

Organization Type

When an organization is created in the global organization, the Organization Type is defined:

- Standalone: A standalone organization is created directly under the global organization. It can be assigned to a Meta Organization later.
- Meta: A Meta Organization is created directly under the global organization. Other organizations can be assigned to it after creation and inherit the items it shares.
- Sub: A sub-organization is assigned to the selected Meta Organization and inherits the items it shares. The Meta Organization is selected via Select Meta as Parent; this selection is mandatory. This assignment cannot be undone.

The organization type can only be selected when an organization is created in the global organization. Organizations created within a Meta Organization automatically become its sub-organizations. The organization type of an existing organization cannot be changed when editing it. A standalone organization can only be placed under a Meta Organization afterwards via Assign to Meta Organization (see below).

For version 26.4.0

The following restrictions also apply to Meta Organizations:

- A Meta Organization cannot be converted back into a standalone organization.
- Meta Organizations cannot be nested: a Meta Organization cannot be placed under another Meta Organization.
- The global organization cannot be a Meta Organization.
- A Meta Organization that has sub-organizations cannot be deleted.

Inheritance to sub-organizations

Sub-organizations adopt the items that the Meta Organization shares with all sub-organizations, for example apps, policies, scripts, device groups and roles. In the Meta Organization, these items are marked Shared; in the sub-organizations, they are marked From Meta. In lists, they can be found on the Shared (Meta) or From Meta tab. Items marked Local only remain limited to the Meta Organization. Inherited items can only be changed in the Meta Organization.

If apps that already exist in other organizations are made available meta-wide, the portal points out this conflict. For the selected apps, the existing apps in the other organizations are replaced and deleted.

Assigning an existing organization

A standalone organization can be placed under a Meta Organization afterwards. This action is only available in the global organization and requires the permission to edit organizations. It is not available in a Meta Organization.

Under `Organizations`, one or more standalone organizations are selected and Assign to Meta Organization is chosen in the context menu. Alternatively, the action is available in the detail view of a standalone organization. In the Assign to Meta Organization dialog, the target Meta Organization is selected first. After Next, the dialog shows the selected Meta Organization and, under New Sub-Organizations, the organizations to be assigned; Confirm carries out the assignment.

> Assigning an organization to a Meta Organization is permanent and cannot be undone. Only standalone organizations can be assigned.

For version 26.4.0

Link Microsoft Entra ID

Linking `Microsoft Entra ID` with Relution creates the foundation for Microsoft-based integrations in the organization. This includes, for example, connecting Windows devices and using other Microsoft services together with Relution.

As a result, users and groups from `Microsoft Entra ID` can be synchronized with Relution. This allows user accounts to be managed centrally in Microsoft and automatically provisioned in Relution.

To allow synchronized users to sign in to Relution, OIDC authentication → must also be configured. If access is to be secured using Conditional Access →, both the link to `Microsoft Entra ID` and the configuration of OIDC → are required.

The required settings are configured partly in Relution and partly in the Microsoft Entra admin center.

Requirements

To link `Microsoft Entra ID` with Relution, the following requirements must be met when only synchronizing users from `Microsoft Entra ID` to Relution:

- an existing `Microsoft Entra ID` environment
- sufficient permissions in Microsoft Entra, usually the `Global Administrator` role
- an accessible Relution Server
- an app registration in Microsoft Entra

If `Windows Autopilot` or `Entra Join` is also to be used, the following additional requirements must be met:

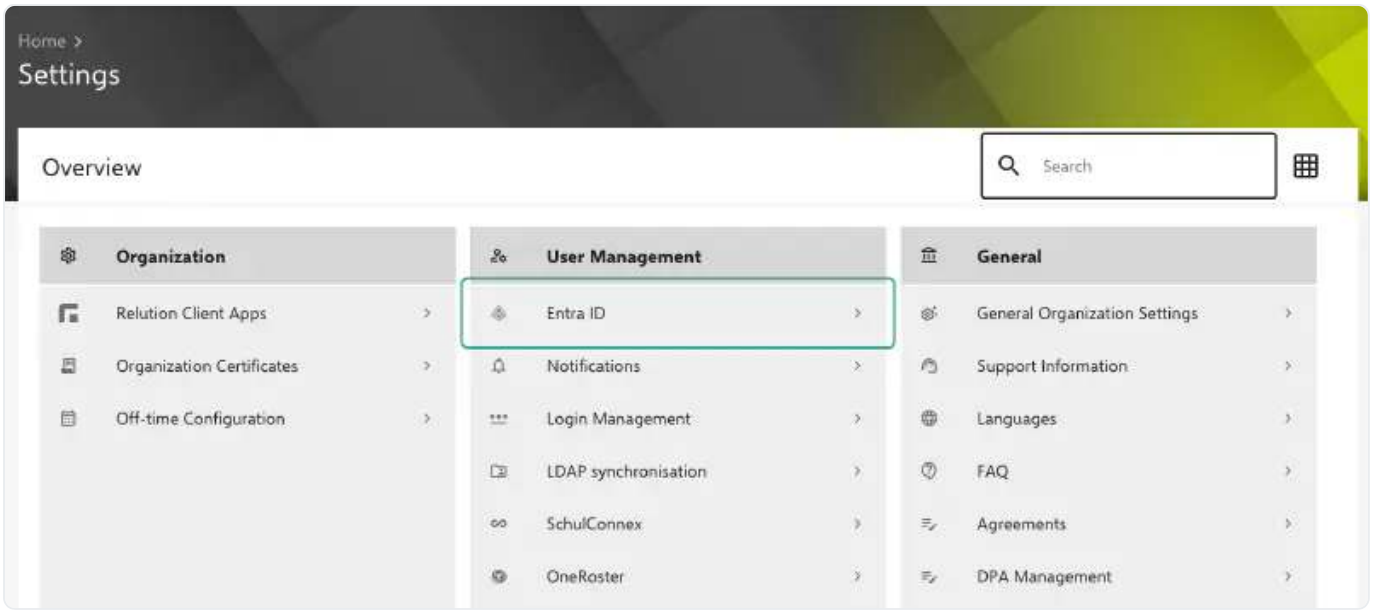
- the server URL of the Relution Server, which will later be stored in Microsoft Entra
- a created MDM application

For version 26.4.0

Open the link configuration in Relution

In the Relution portal, the setup area is found under `Settings` → `User Management` → `Entra ID`.

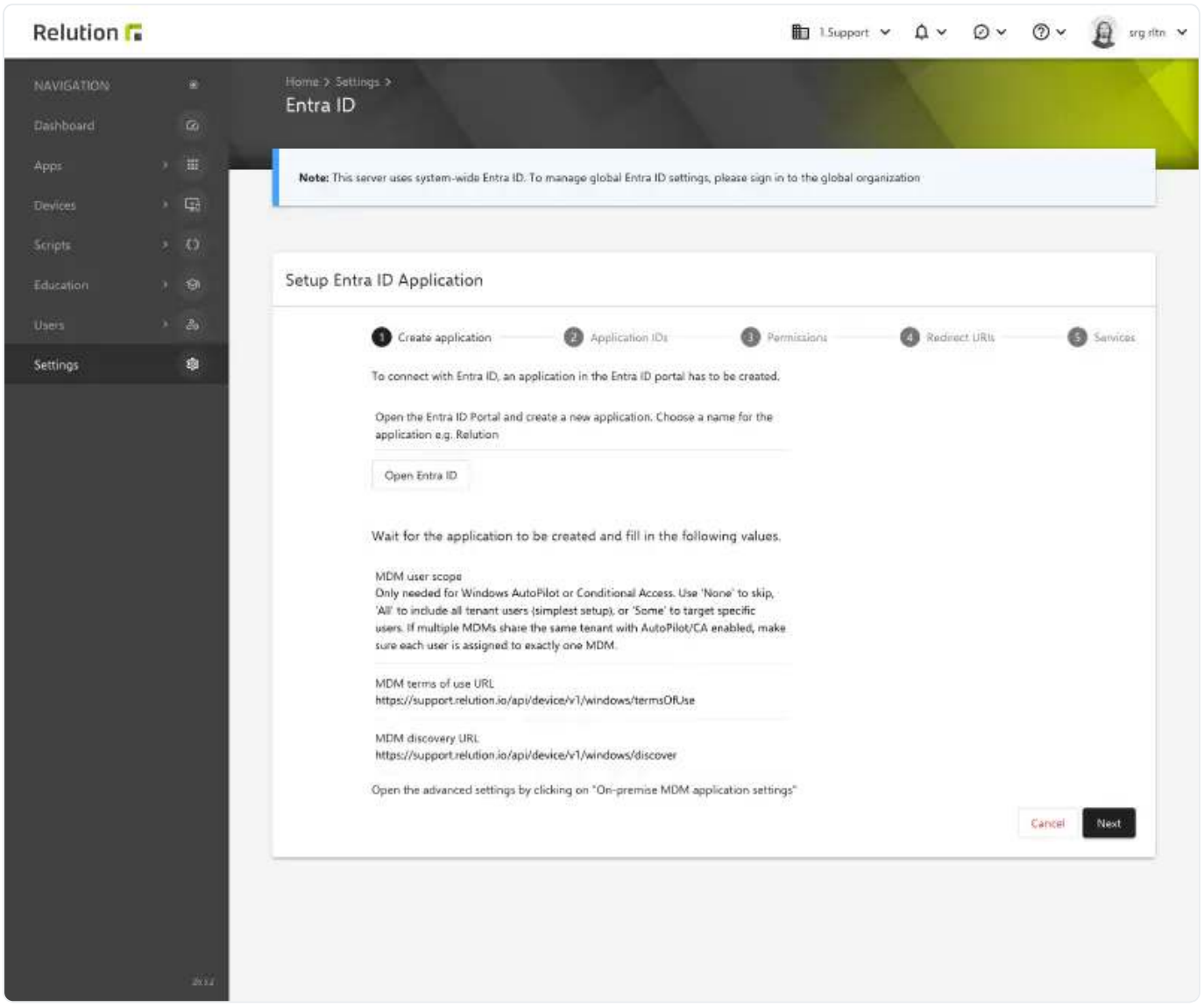
There, a guide provides support for configuring and linking Microsoft Entra. It covers the steps Create application, Application IDs, Permissions, Redirect URIs and Services.



Create the application

The first step, Create application, points out that the connection requires an application in the Entra portal. The Open Entra ID button opens the `Mobility (MDM and MAM)` area in Microsoft Entra. Below it, the Relution guide shows the values that are entered in the MDM application:

For version 26.4.0



- MDM user scope: only required for Windows Autopilot or Conditional Access. `None` skips the scope, `All` includes all users of the tenant, `Some` targets selected users only. If several MDM solutions share the same tenant with Autopilot or Conditional Access, each user must be assigned to exactly one MDM solution.
- MDM terms of use URL: `https://<host>/api/device/v1/windows/termsOfUse`
- MDM discovery URL: `https://<host>/api/device/v1/windows/discover`

The MDM application is required for `Windows Autopilot` and `Entra Join` and, according to the note in the portal, also for Conditional Access. How it is created and configured (on-premises MDM application, custom domain, URLs) is described in the Windows Autopilot → article.

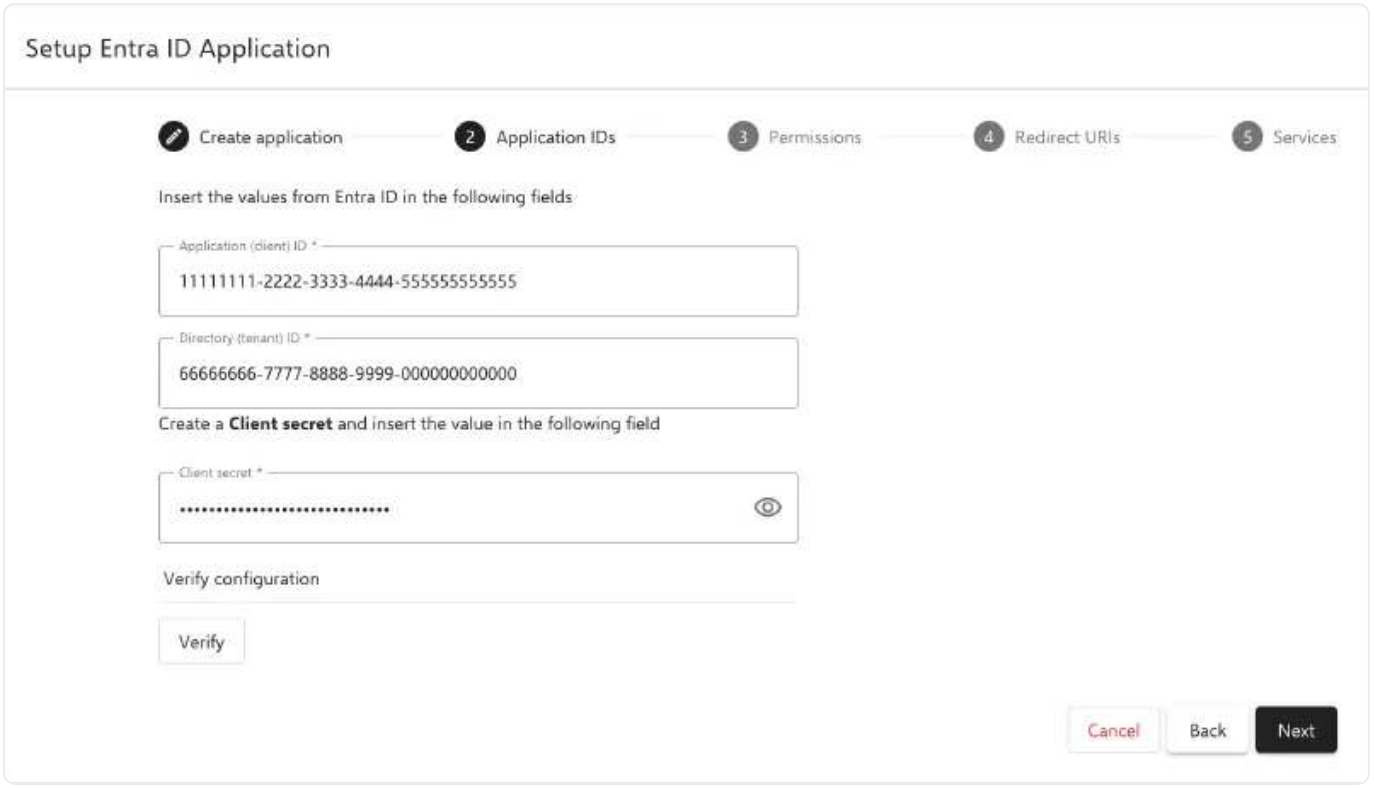
To only synchronize users and groups from Microsoft Entra with Relution, a standard app registration is sufficient and this step is skipped with Next. The app registration can be created using the following link:

Create new app registration in Entra →

Configure the application settings

In the Application IDs step, the following information from Microsoft Entra is transferred to the Relution guide. It applies both to the MDM application and to a standard app registration:

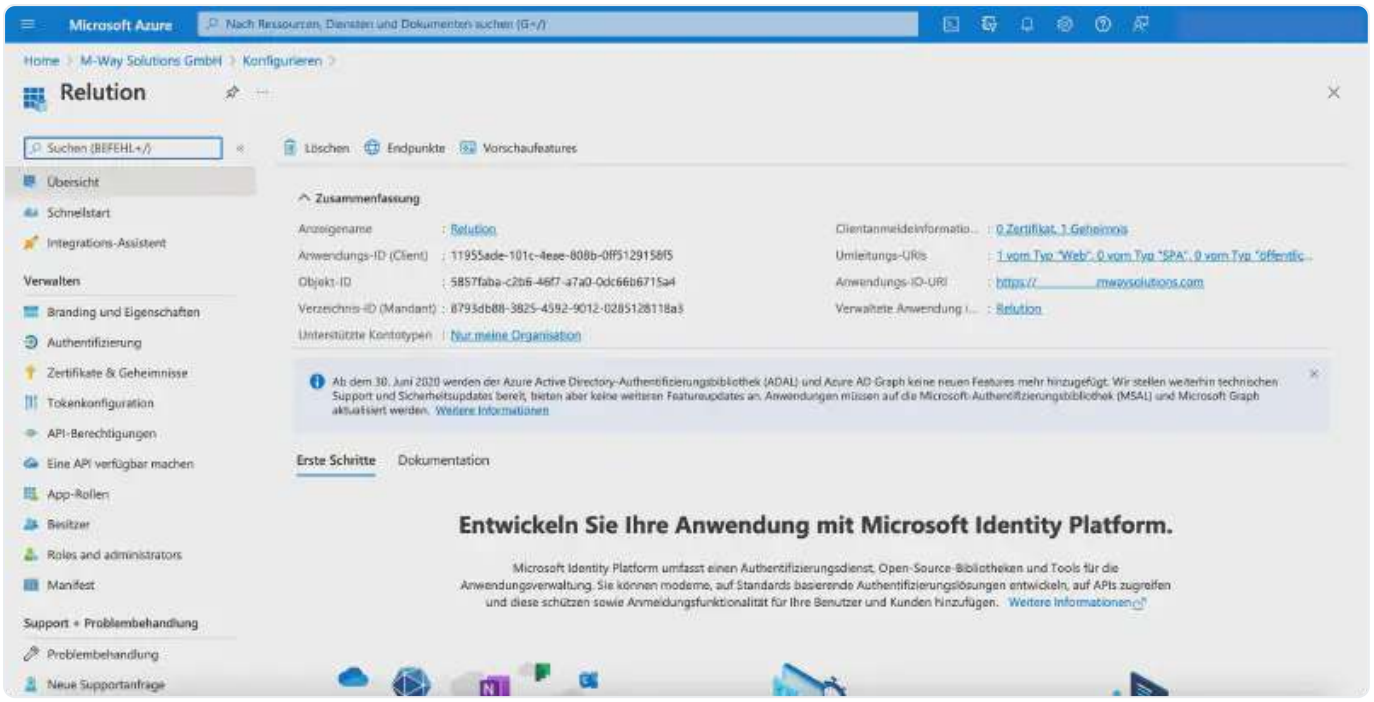
1. Application (client) ID
2. Directory (tenant) ID
3. the value of the Client secret (same field name in Relution)



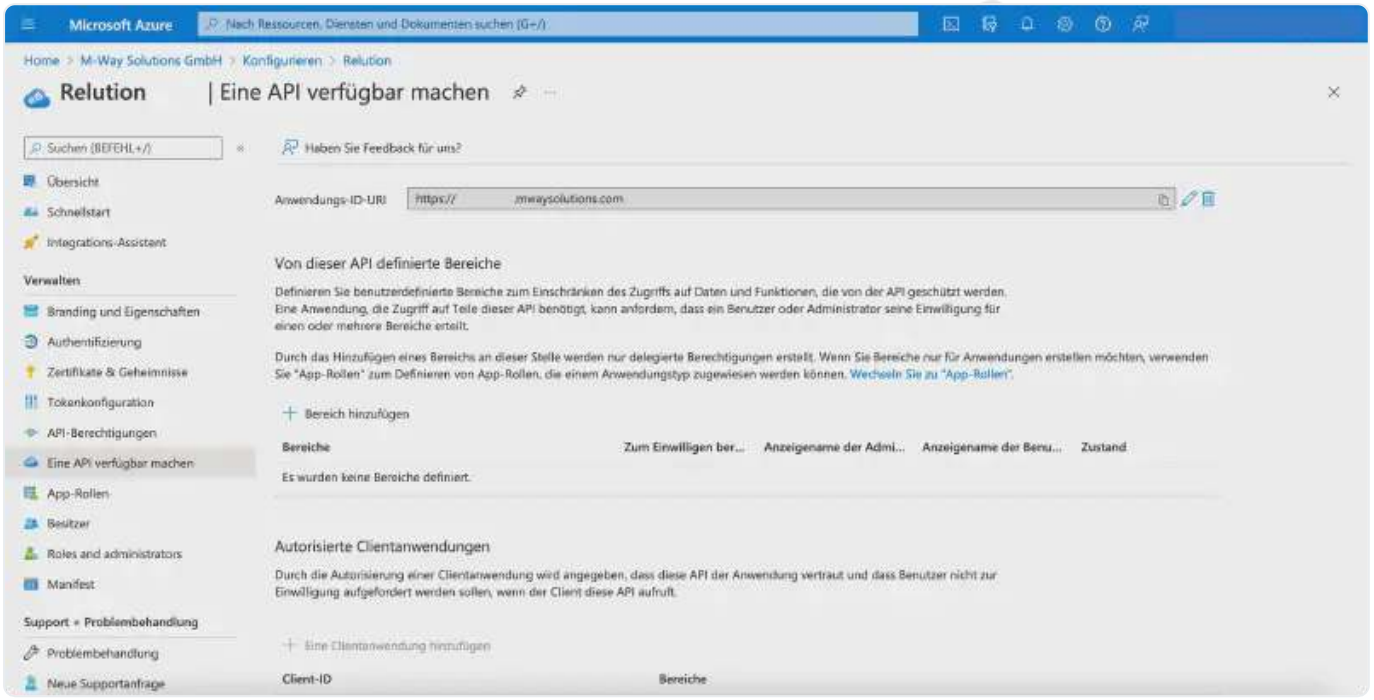
Verify in the Verify configuration row tests right away whether Relution can sign in to Microsoft Entra with this information.

If Conditional Access is already configured for the organization, Relution points out when the Directory (tenant) ID is changed that the new tenant also affects the Conditional Access setting. The app ID and secret in that setting should be checked again afterwards.

Only for an MDM application (Windows Autopilot, Entra Join): to edit the Application ID URI, it is then selected in the local MDM application settings. For a standard app registration, this and the following step are omitted.



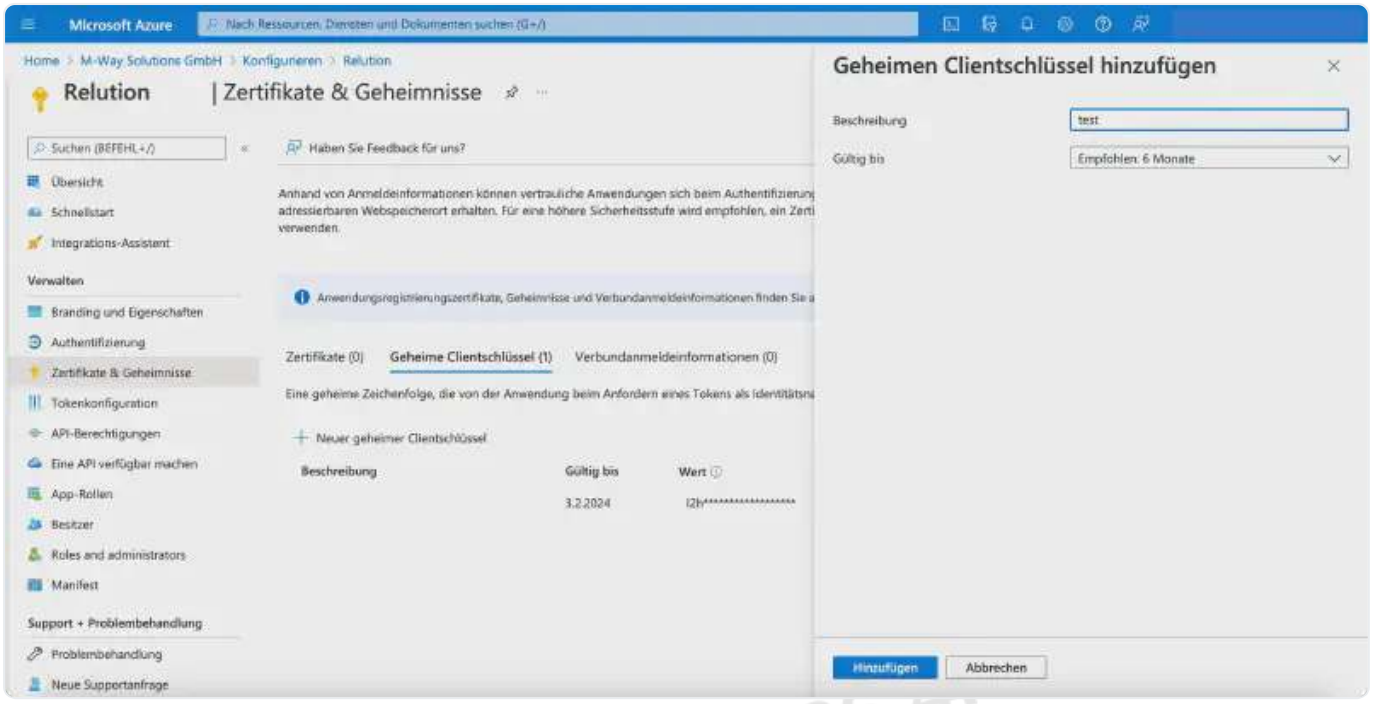
In the following view, the corresponding server URL is entered as the `Application ID URI`.



Next, a Client secret is added under Certificates & secrets:

1. In the Client secrets tab, New client secret is clicked.
2. In the `Add a client secret` dialog, a description and the validity period are entered.
3. The entry is confirmed with Add.

If the validity period expires, the connection is no longer available and Relution can no longer communicate with Microsoft Entra. In this case, a new `Client secret` must be created for the application in Microsoft Entra and stored again in Relution.

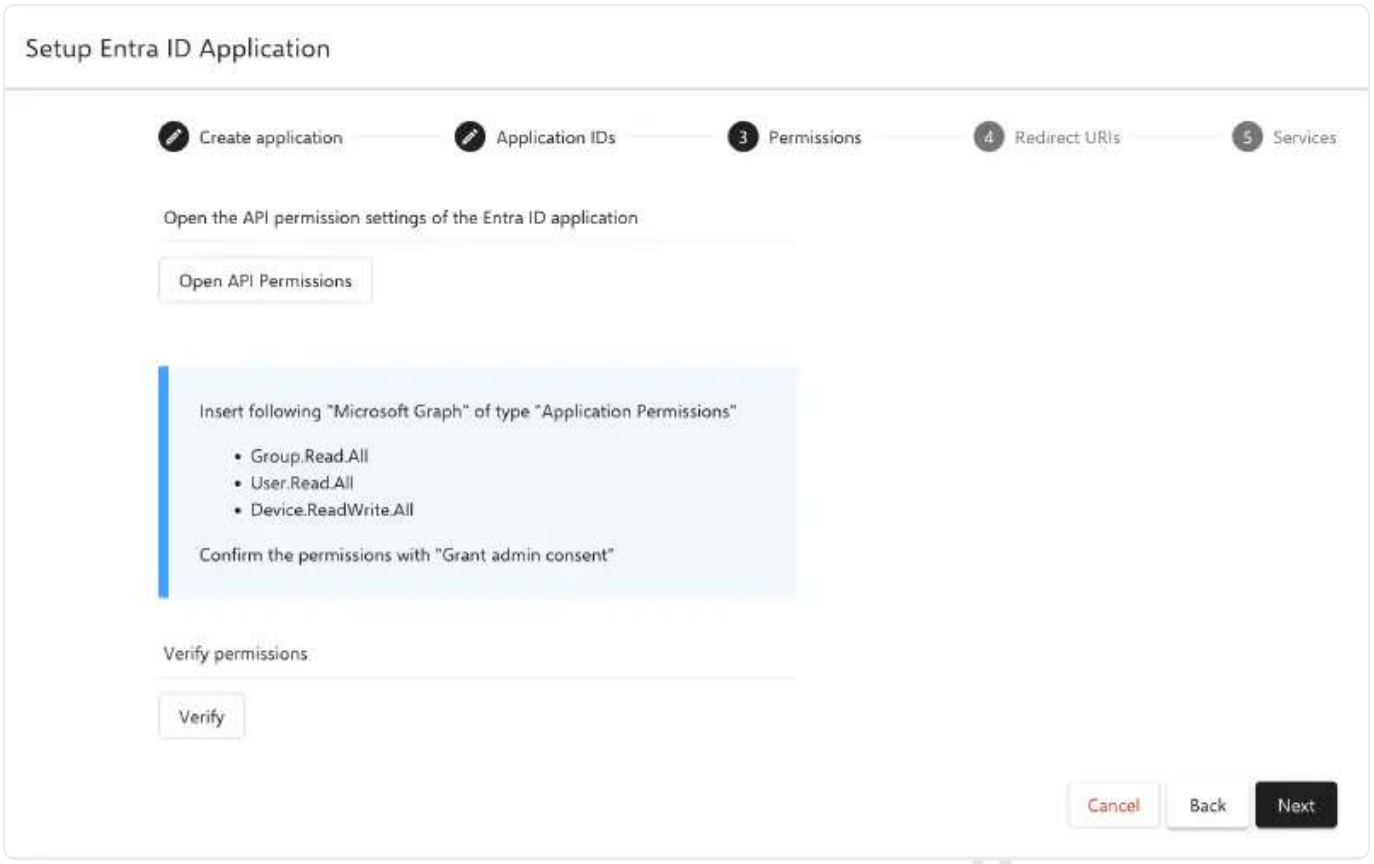


The new entry is then displayed in the overview under the `Client secrets` tab.

The corresponding `Value` is shown only once and must therefore be copied immediately and transferred to Relution.

Configure the API permissions

In the next step, Permissions, the API permissions are configured. The Open API Permissions button opens the API permissions of the application directly in Microsoft Entra:



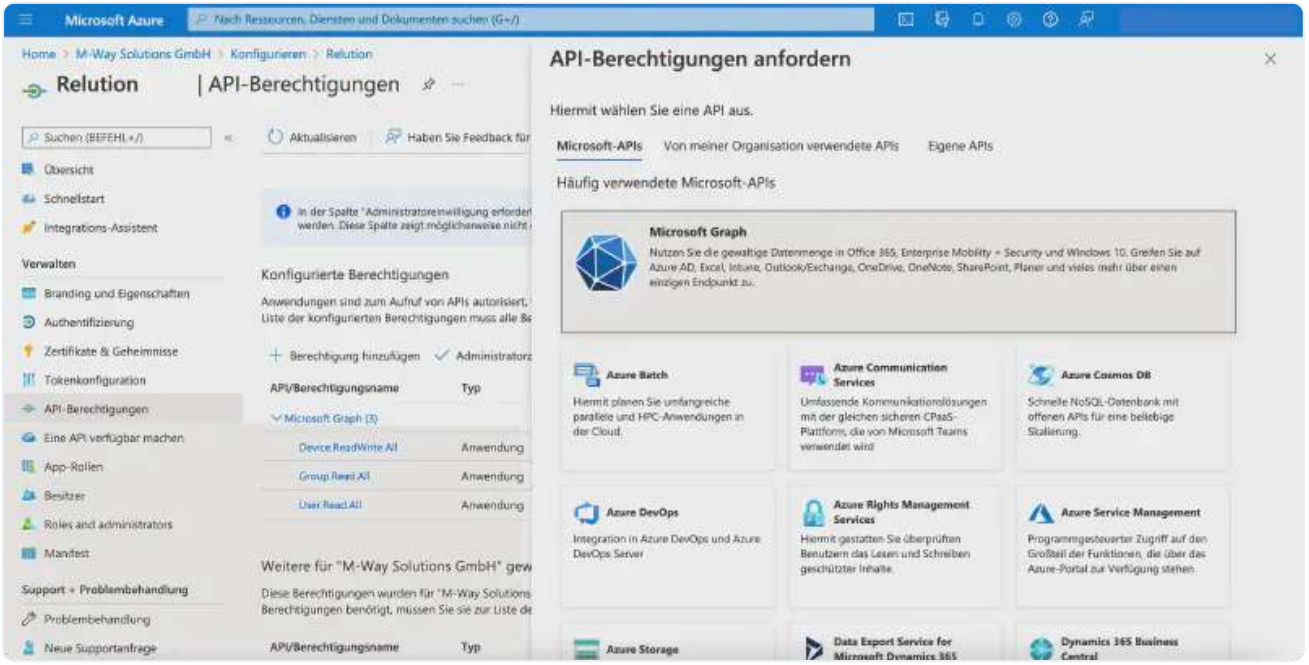
Depending on which Microsoft features are used in the future, additional permissions may need to be added later.

The following settings must be configured in Microsoft Entra:

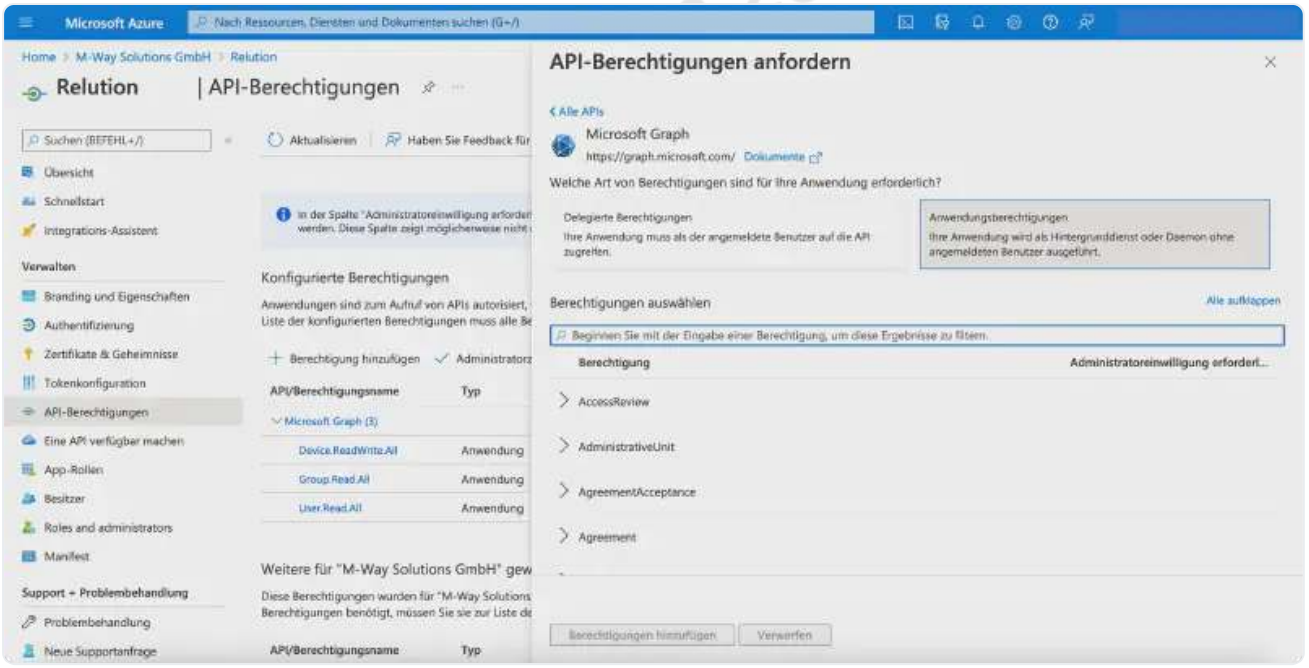
For version 26.4.0

1. Under `API permissions` → `Configured permissions`, Add a permission is clicked.

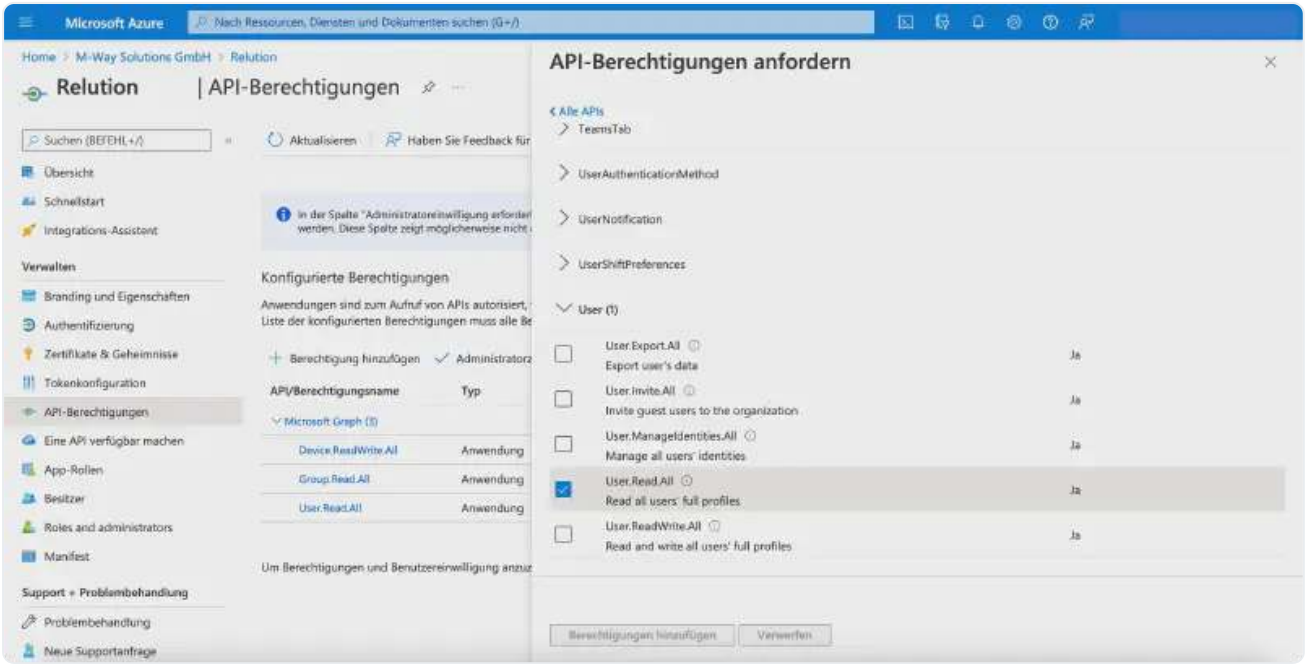
2. In the Request API permissions dialog, Microsoft Graph is selected under Microsoft APIs.



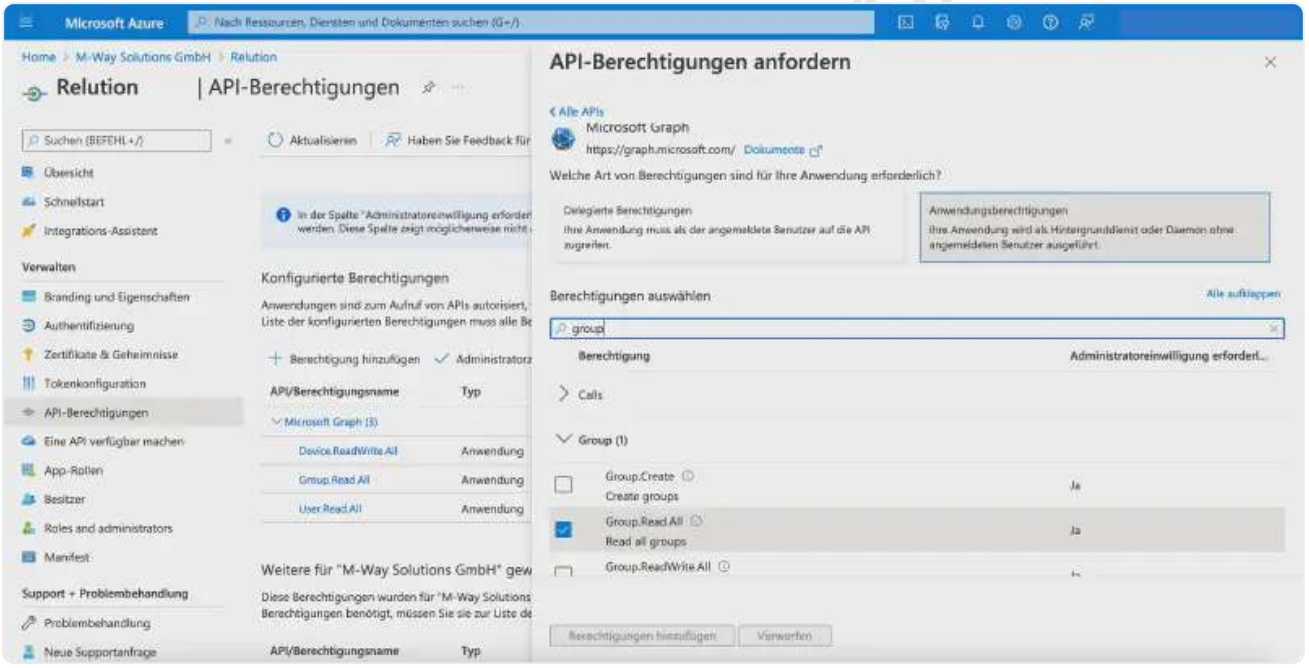
3. In the next step, the Application permissions tile is selected.



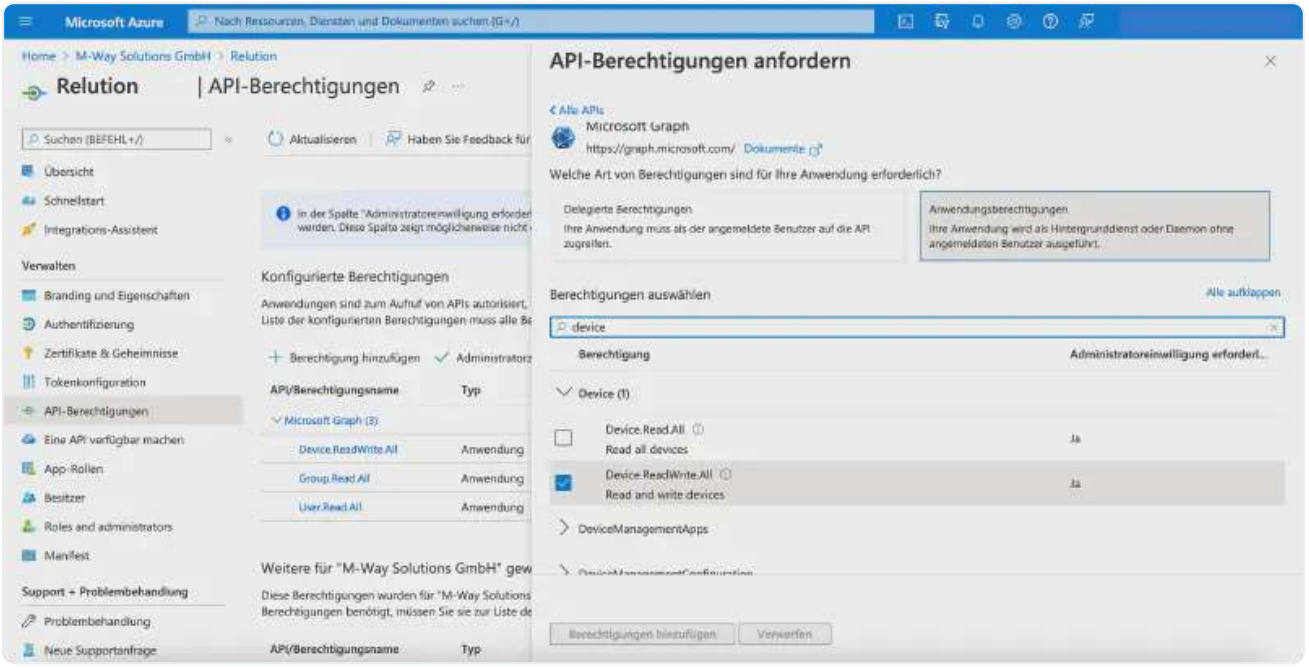
4. For User, the `User.Read.All` permission is selected.



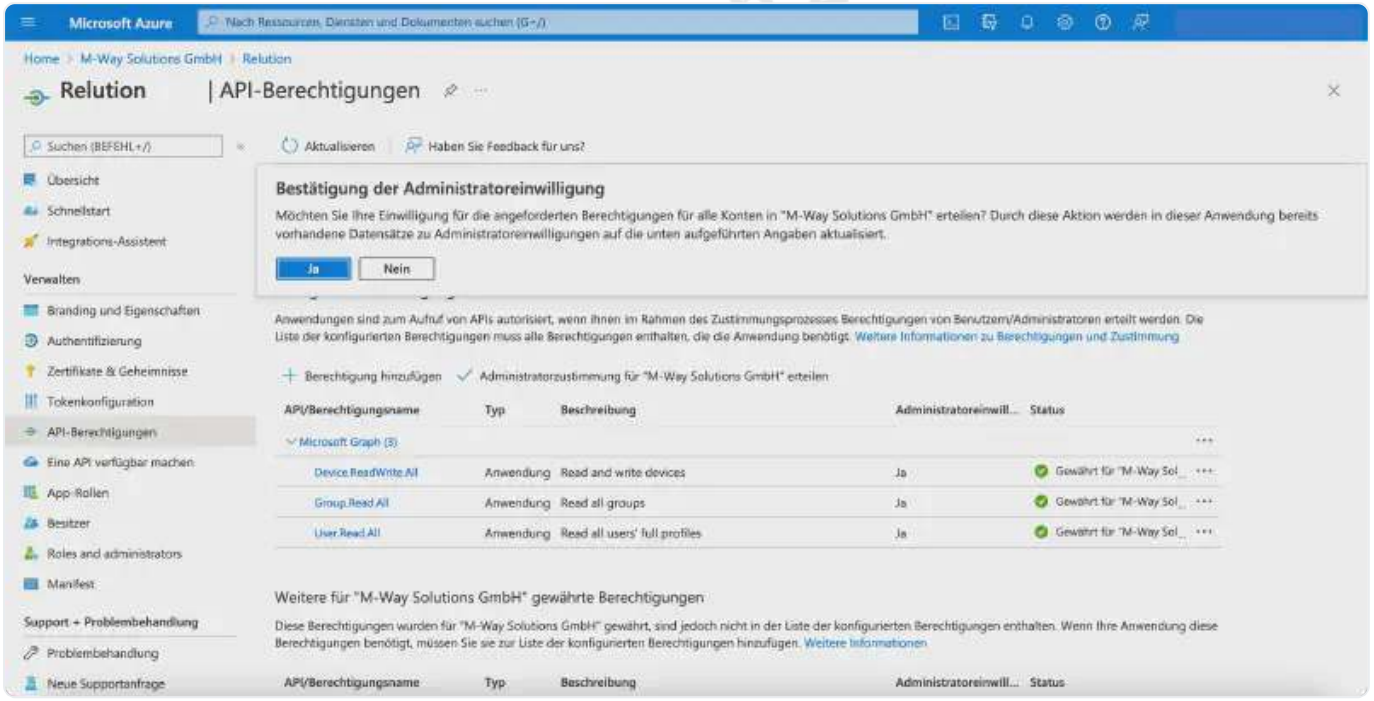
5. For Group, the `Group.Read.All` permission is selected.



6. For Device, the `Device.ReadWrite.All` permission is selected and the selection is confirmed with Add permissions.



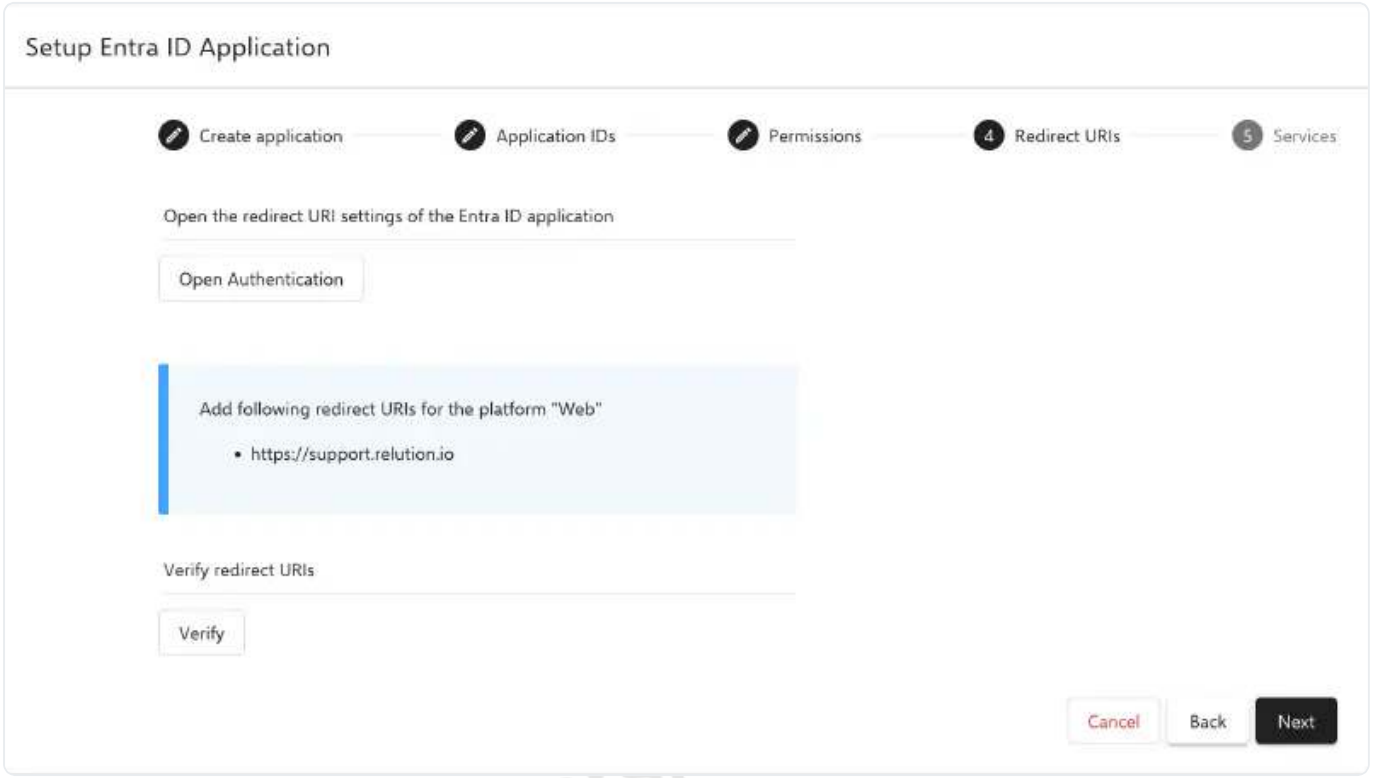
For newly added API permissions, an exclamation mark is initially displayed as the status. For the application to receive the permissions, administrators must confirm them once using Grant admin consent for “”. The status is then shown as `Granted` with a green check mark.



Verify in the Verify permissions row checks whether the permissions have been granted. Without consent, the check reports Permission not granted.

Define the redirect URI

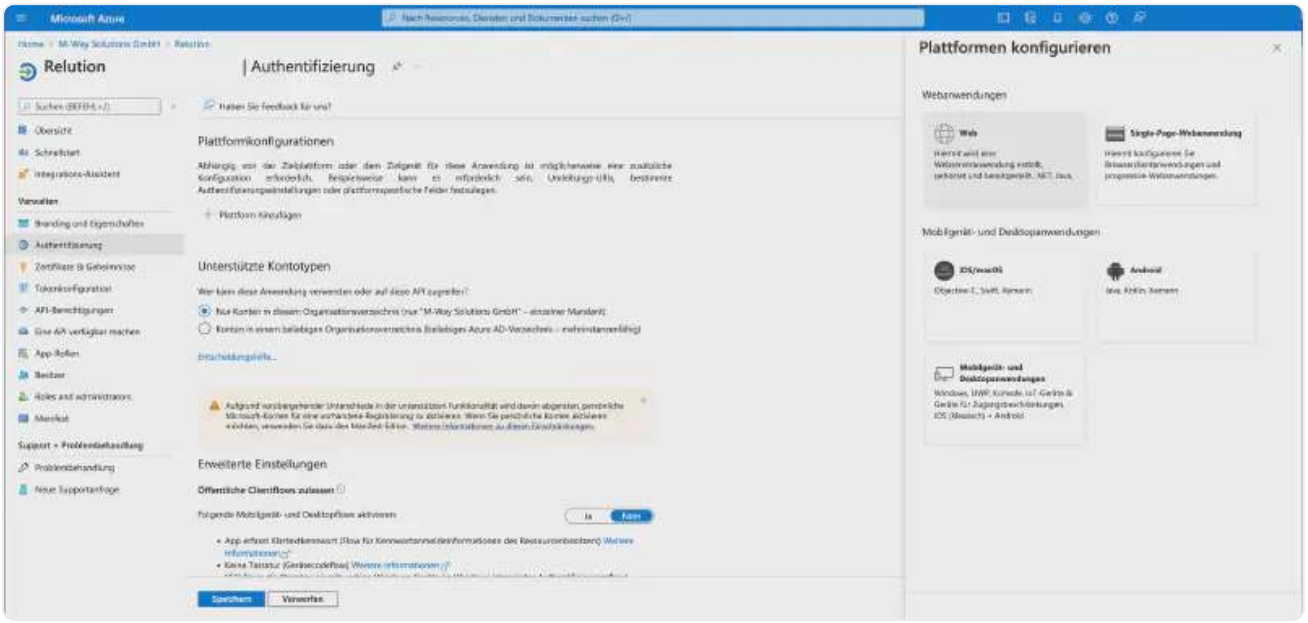
In the Redirect URIs step, the Relution guide shows the `Redirect URI` that is then entered in Microsoft Entra for the `Web` platform. The Open Authentication button opens the corresponding page of the application in Microsoft Entra:



For vers

1. Under Authentication, Add a platform is clicked.

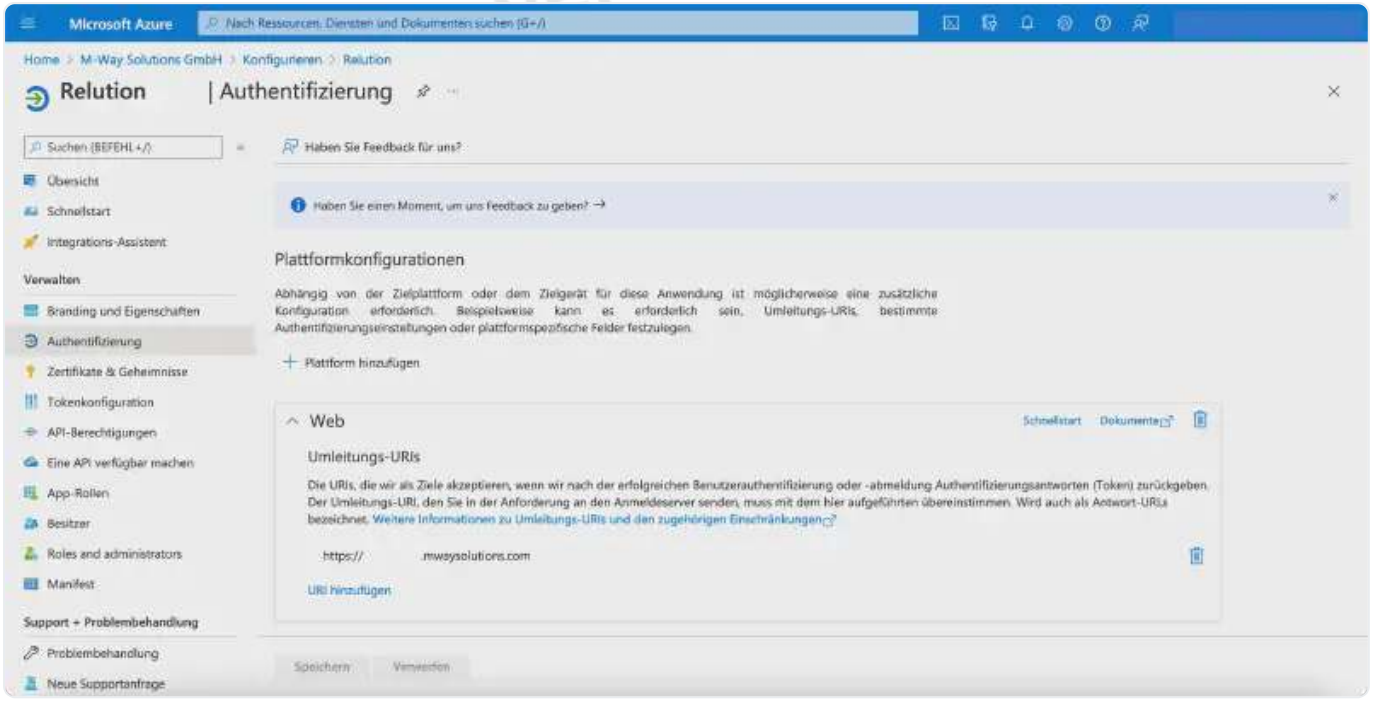
2. In the Configure platforms dialog, the Web tile is selected.



3. In the Web section, the server URL is entered under Add a Redirect URI.

4. The ID tokens checkbox is disabled.

5. The settings are saved with Save.

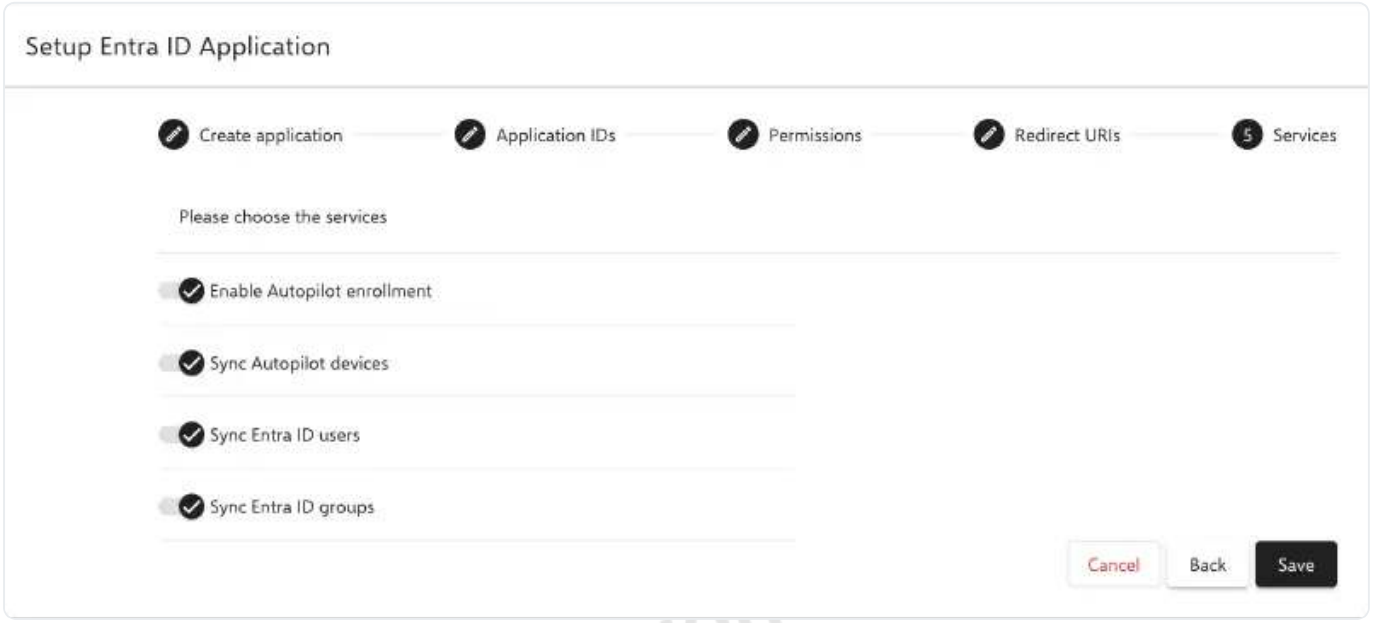


Verify in the Verify redirect URIs row checks whether the server URL is registered in the application. The registered URI must match the displayed server URL exactly, otherwise the check reports `Redirect URI … not present`.

This completes the configuration in Microsoft Entra.

Select the Relution service options and complete the setup

The Services step defines which services Relution uses. The available switches are Enable Autopilot enrollment, Sync Autopilot devices, Sync Entra ID users and Sync Entra ID groups. For a new connection, all four switches are already enabled. If only users and groups are to be synchronized (without `Windows Autopilot` or `Entra Join`), Enable Autopilot enrollment and Sync Autopilot devices are disabled.



Clicking Save completes the setup and linking of `Microsoft Entra ID` in Relution.

Manage and synchronize the connection

After saving, `Settings` → `User Management` → `Entra ID` shows the overview of the Entra ID connection with the application ID and directory ID. The following functions are available there:

- Edit connection: opens the guide again, for example to enter a new value in the Client secret field after the client secret has expired.
- Verify connection: checks sign-in, permissions and redirect URI in one step.
- Delete connection: removes the link to Microsoft Entra.
- Services section: the four switches from the setup can be changed here later and applied with Save.

The Synchronisation section shows the Last Synchronisation, the New entries, any errors and the Next Synchronisation for each synchronization. By default, users and groups are synchronized once a day and Autopilot devices every 24 hours.

A synchronization can also be started manually:

- Sync Autopilot devices synchronizes the devices registered in Windows Autopilot.
- Sync users and groups (in the menu of the action bar) is only available if both user and group synchronization are enabled. The dialog offers a Synchronization mode: Changes only (Recommended) only fetches users and groups changed since the previous synchronization. Full synchronization re-imports all users and groups and can take a long time. It is only useful if synchronizing the changes does not provide the expected result.

In the global organization the link applies system-wide, in a meta organization meta-wide. The overview shows this under Account scope as System-wide or Meta-wide. There, Organization mapping assigns Entra ID groups to individual organizations. In this case, the switches for user and group synchronization are coupled and are always switched on or off together.

Summary

After completing these steps, `Microsoft Entra ID` is linked with Relution. This allows users and groups from Microsoft Entra ID to be synchronized with Relution and enables the use of additional Microsoft-related features.

To allow synchronized users to sign in to Relution, OIDC authentication → must also be configured. This also applies when using `Conditional Access`.

For version 26.4.0

OIDC with Entra

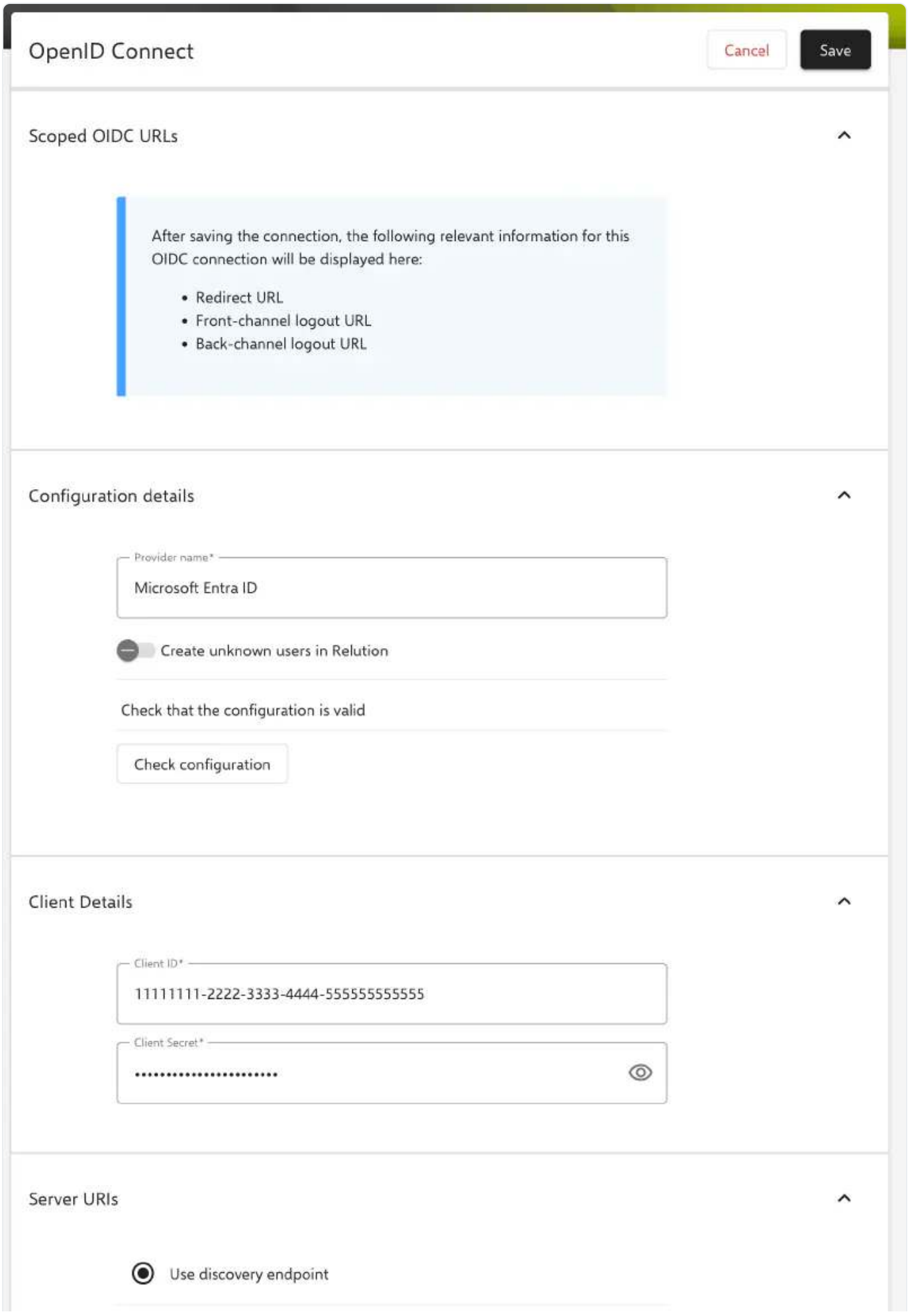
OpenID Connect `OIDC` is an identity protocol built on top of OAuth 2.0 that enables secure authentication and authorization for web and mobile applications. It allows users to log in securely to various services while enabling service providers to access verified identity information. This guide describes how to configure OpenID Connect in Relution using Microsoft Azure as the identity provider.

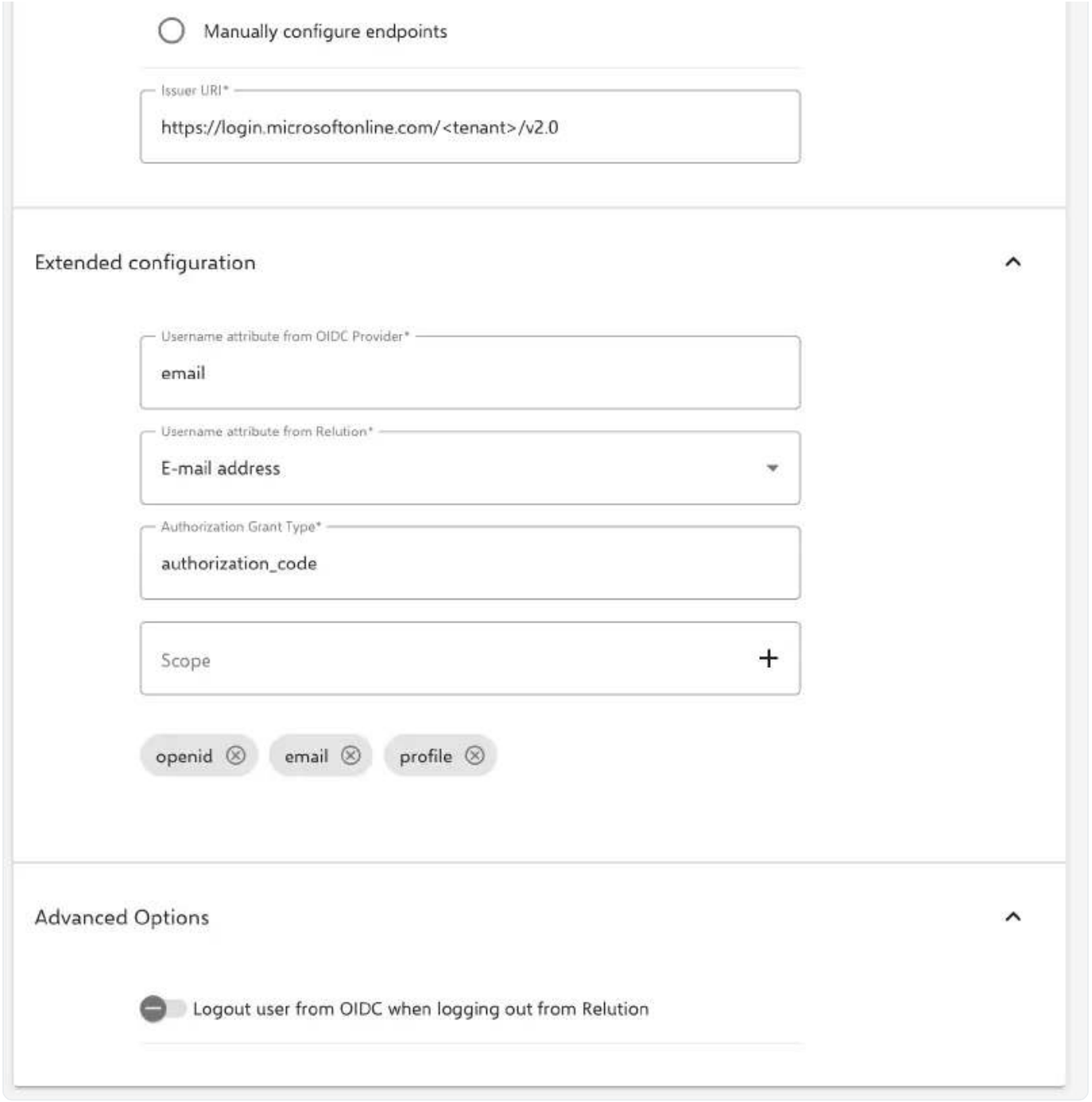
> When using OIDC, no classes or groups are synchronized. A user is only created in Relution on their first successful login, and only if Create unknown users in Relution is enabled. Relution automatically adds newly created users to the group `<Provider name> Users` and creates this group in the organization if necessary. This group can be used to assign permissions.

Settings in Relution

OIDC can be configured in the Relution portal under `Settings` → `User Management` → `OpenID Connect`. The following screenshots include a working configuration example with Microsoft Azure.

For version 26.4.0


OpenID Connect
Cancel
Save
Scoped OIDC URLs
After saving the connection, the following relevant information for this OIDC connection will be displayed here:
Redirect URL
Front-channel logout URL
Back-channel logout URL
Configuration details
Provider name*
Microsoft Entra ID
Create unknown users in Relution
Check that the configuration is valid
Check configuration
Client Details
Client ID*
11111111-2222-3333-4444-555555555555
Client Secret*
Server URIs
Use discovery endpoint



Configuration details

Provider name: Required. Displayed as the label on the login button in the Relution portal. It cannot be changed after saving. Create unknown users in Relution: Relution creates new users automatically upon successful login with valid OIDC credentials. The switch is disabled by default. In that case, only users who already exist in Relution can log in. Check configuration: Checks whether the configuration is valid before it is saved.

If a login is done with an unknown user on the store organization with OIDC configured, it will be created in the store organization. In the case of multiple clients with OIDC configuration, the login must be made via the organization URL so that the unknown user is created in the corresponding organization. This URL is displayed in the portal in the OIDC connections.

Client Details

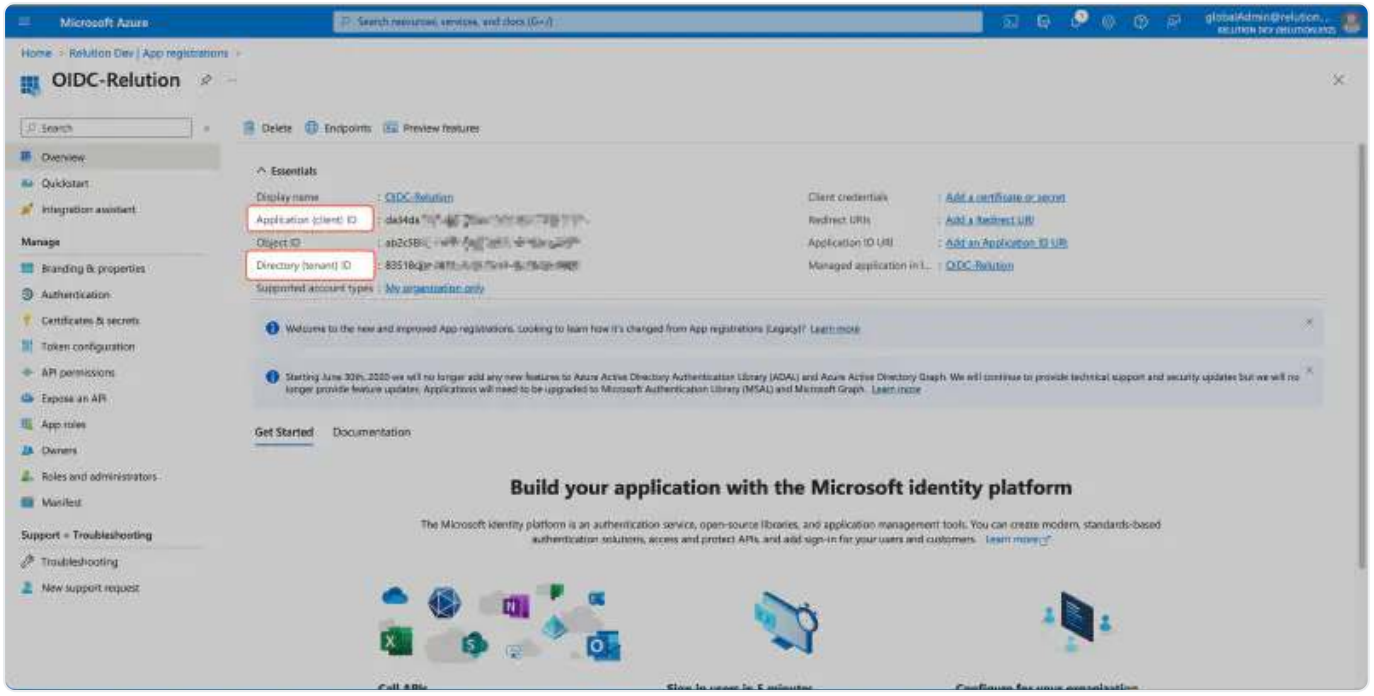
Client ID: Corresponds to the application ID in Azure. Client Secret: Corresponds to the client secret of the application ID in Azure. When a saved configuration is edited, the field stays empty. If no new value is entered, the existing secret remains unchanged.

For version 26.4.0

Server URIs

Use discovery endpoint: If supported by the provider, an automatic configuration of the required URIs is performed. Manually configure endpoints: Necessary as soon as automatic discovery does not work.

If using Microsoft Azure, endpoints must be entered manually.



- Authorization URI:
  `https://login.microsoftonline.com/$-your-tenant-ID/oauth2/v2.0/authorize`
- JWK Set URI:
  `https://login.microsoftonline.com/common/discovery/keys`
- Token URI:
  `https://login.microsoftonline.com/$-your-tenant-ID/oauth2/v2.0/token`
- End session endpoint (optional, for signing out at the IdP, see Logout verification):
  `https://login.microsoftonline.com/$-your-tenant-ID/oauth2/v2.0/logout`

For version 26.4.0

Extended configuration

Username attribute from OIDC Provider: Specifies the attribute that contains the unique user ID from the identity provider (default: `email`).

Username attribute from Relution: Defines which Relution user property (User name, E-mail address, UUID or Foreign key (UID); default: E-mail address) is matched against the value of the username attribute from the OIDC provider. With UUID, unknown users are not created even if Create unknown users in Relution is enabled.

Authorization Grant Type: The Authorization Grant Type is an OAuth mechanism that specifies how an application obtains access permissions from a user (default: `authorization_code`).

Scope: Specifies the identity information or resources the application can request from the OIDC provider (default: `openid`, `email`, `profile`).

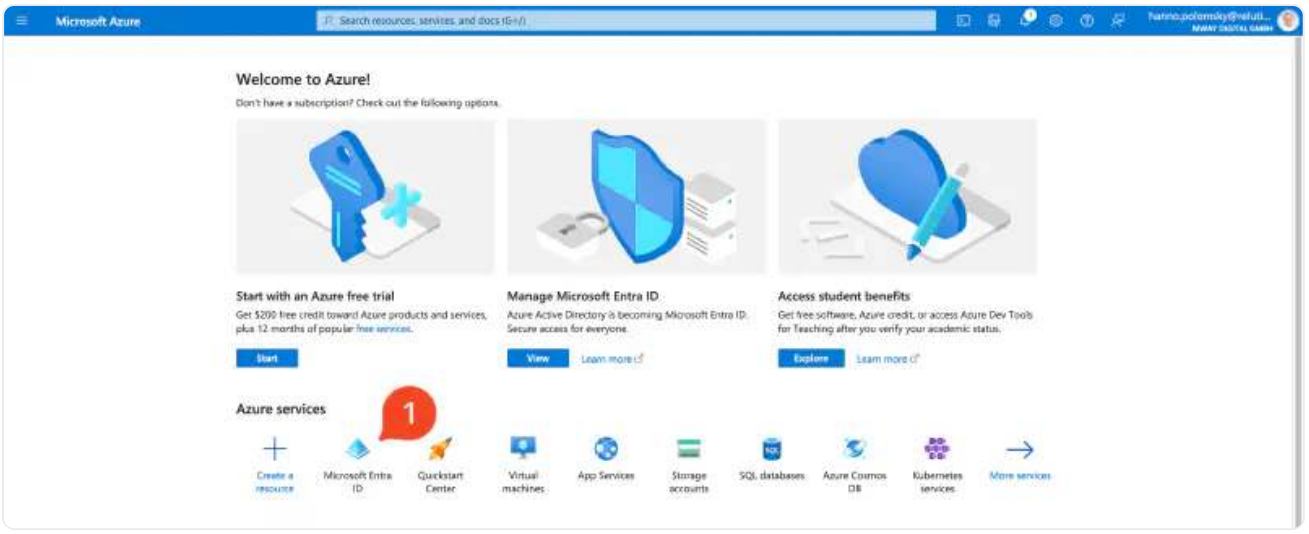
Advanced Options

Logout user from OIDC when logging out from Relution: When logging out of Relution, the browser is additionally redirected to the logout endpoint of the IdP (default: disabled). Details are described under Logout verification.

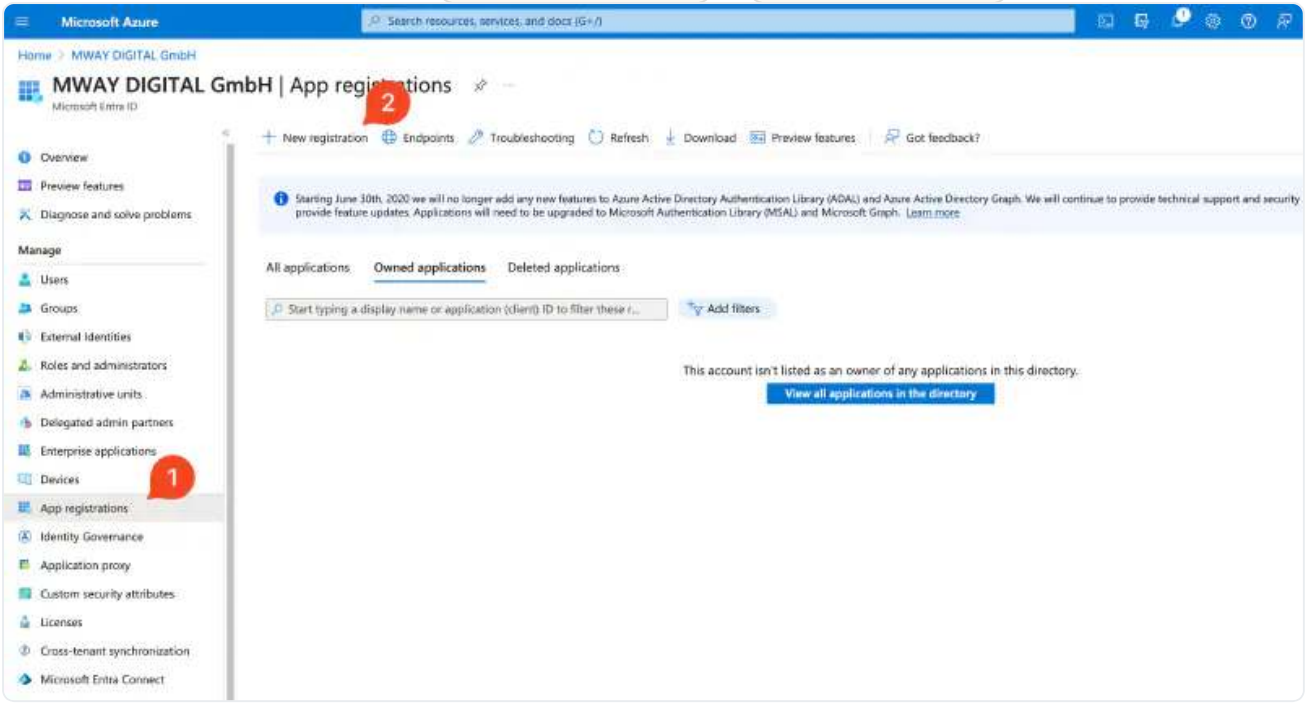
For version 26.4.0

Creating a new app registration

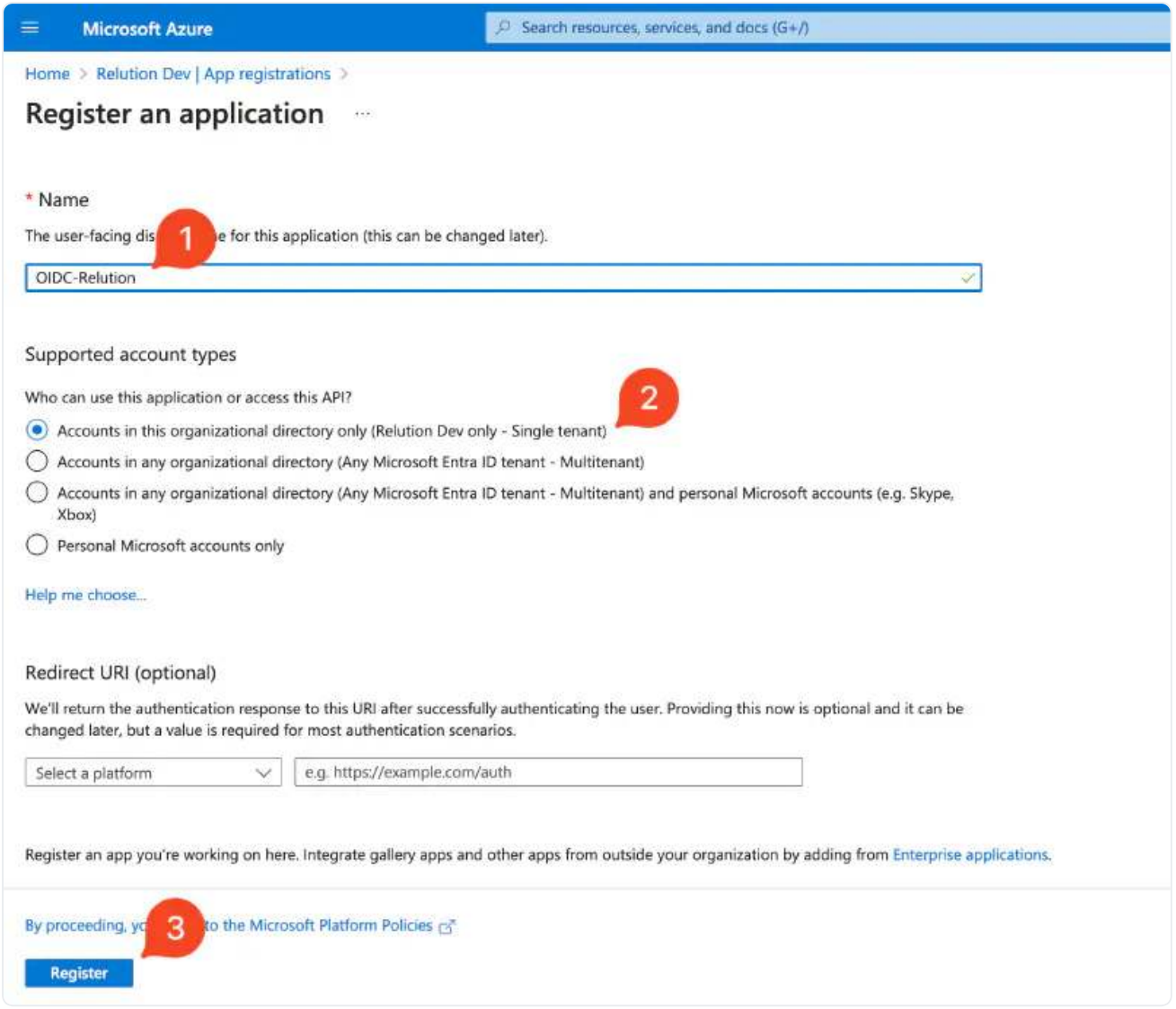
1. After signing in to the Azure portal, Microsoft Entra ID is opened.



2. A new registration for OIDC is created via `App registrations` → `New registration`.



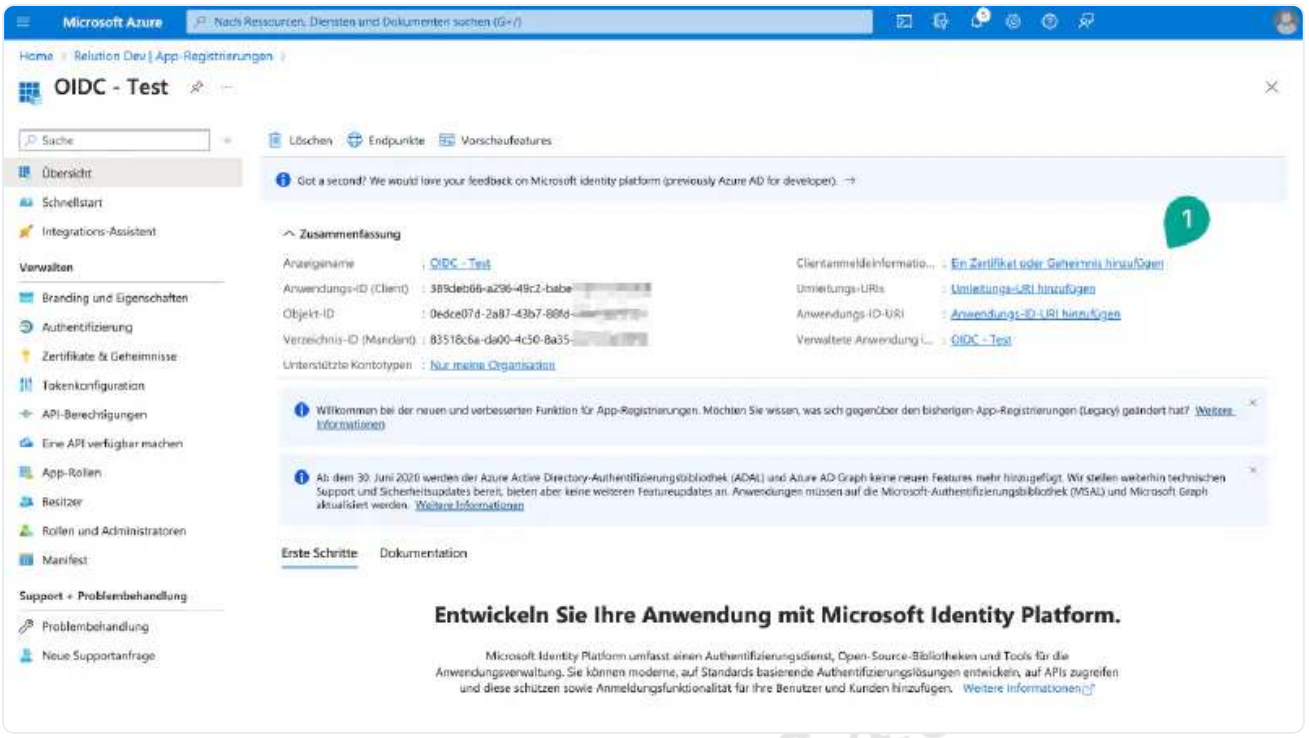
3. A name is entered, the account type Only accounts in this organization directory is selected and the app is registered.



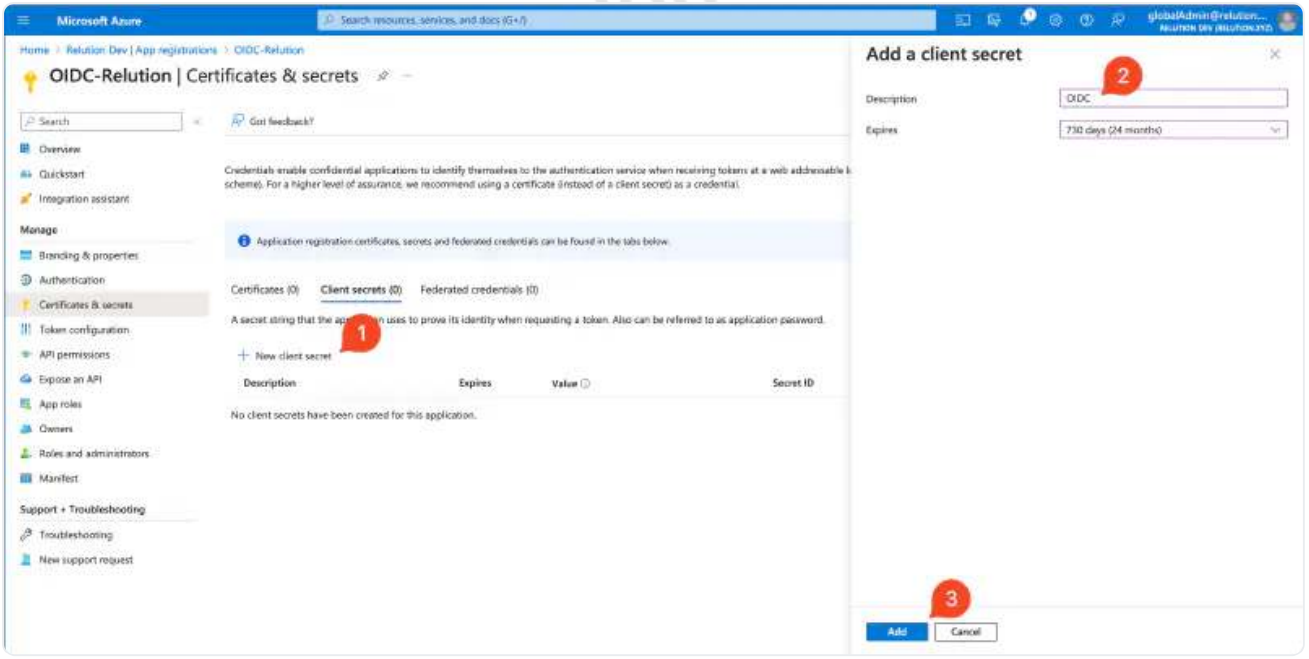
Signing in via OIDC alone requires no additional API permissions and no admin consent. The application permissions for Microsoft Graph (e.g. `User.Read.All`) are only needed for linking Microsoft Entra ID → and are configured there.

Adding a client secret under Certificates & secrets

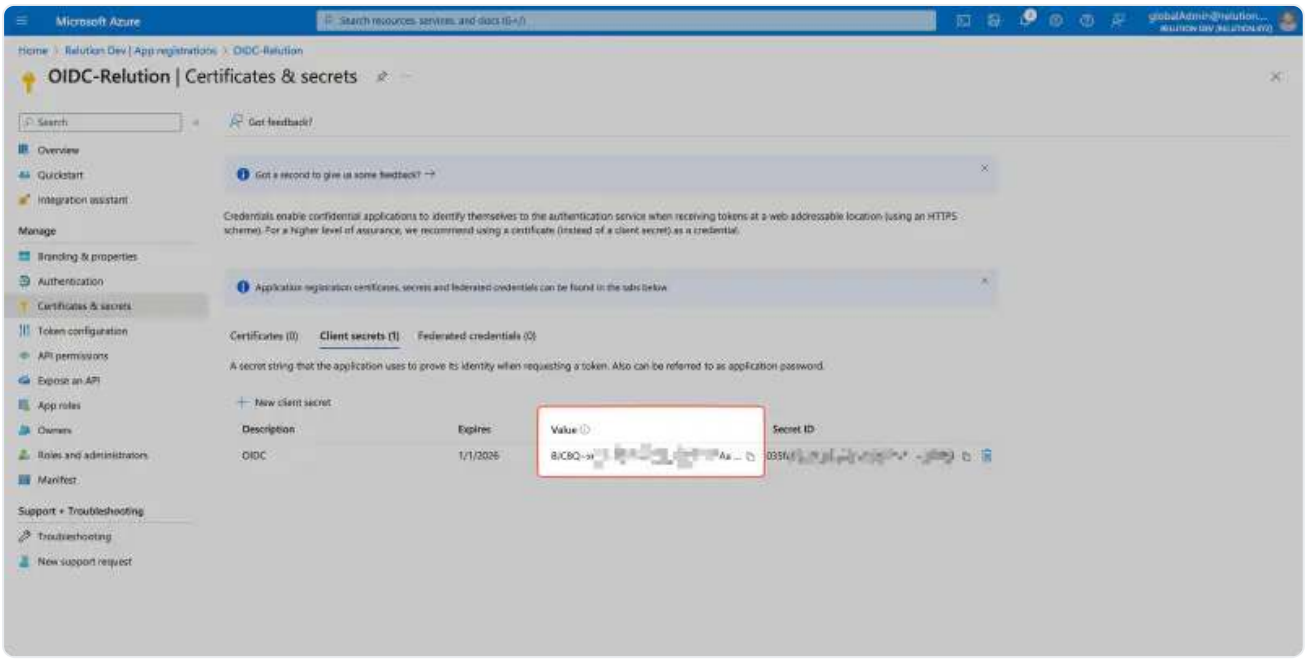
1. The required client secret is created under Add a certificate or secret.



2. Via New client secret, the Description and expiration Expires can be set.



3. The client secret can be copied directly.



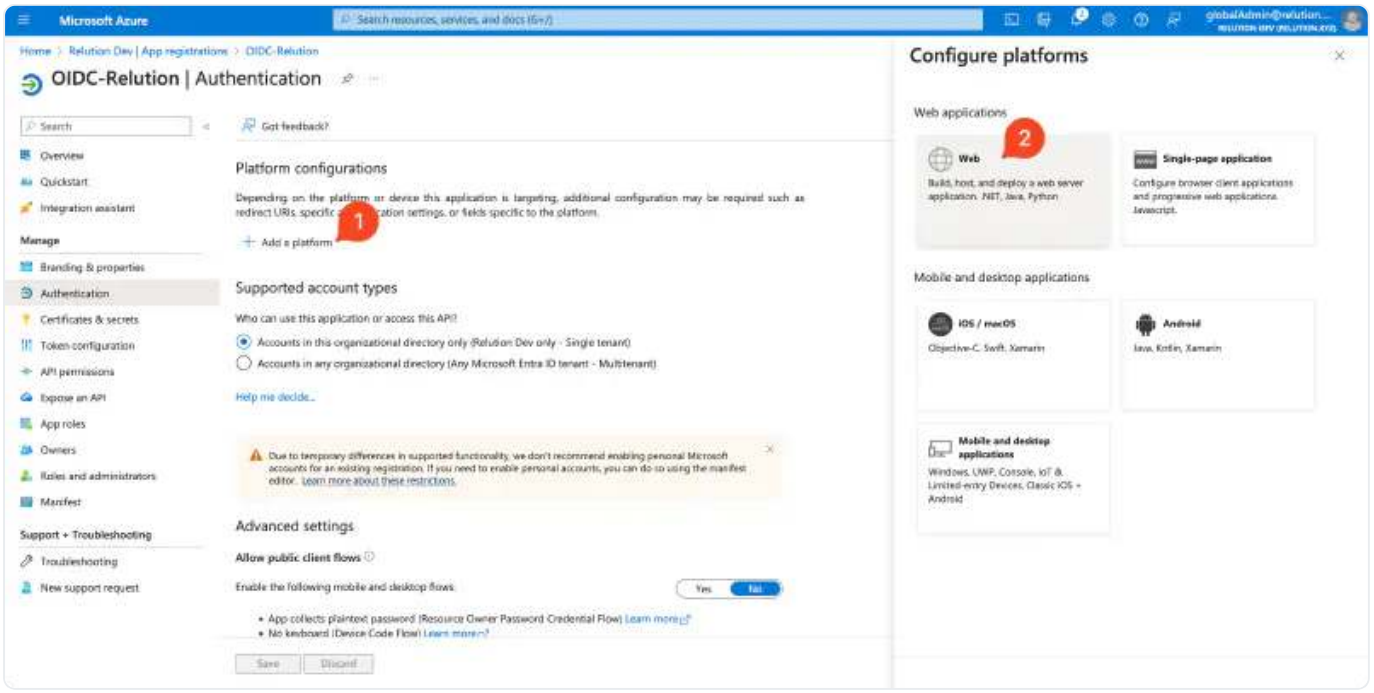
Important: The client secret is shown only once after creation. If it expires, Relution will no longer be able to connect to Azure. In this case, a new client secret must be created for the application in Azure and re-transmitted to Relution.

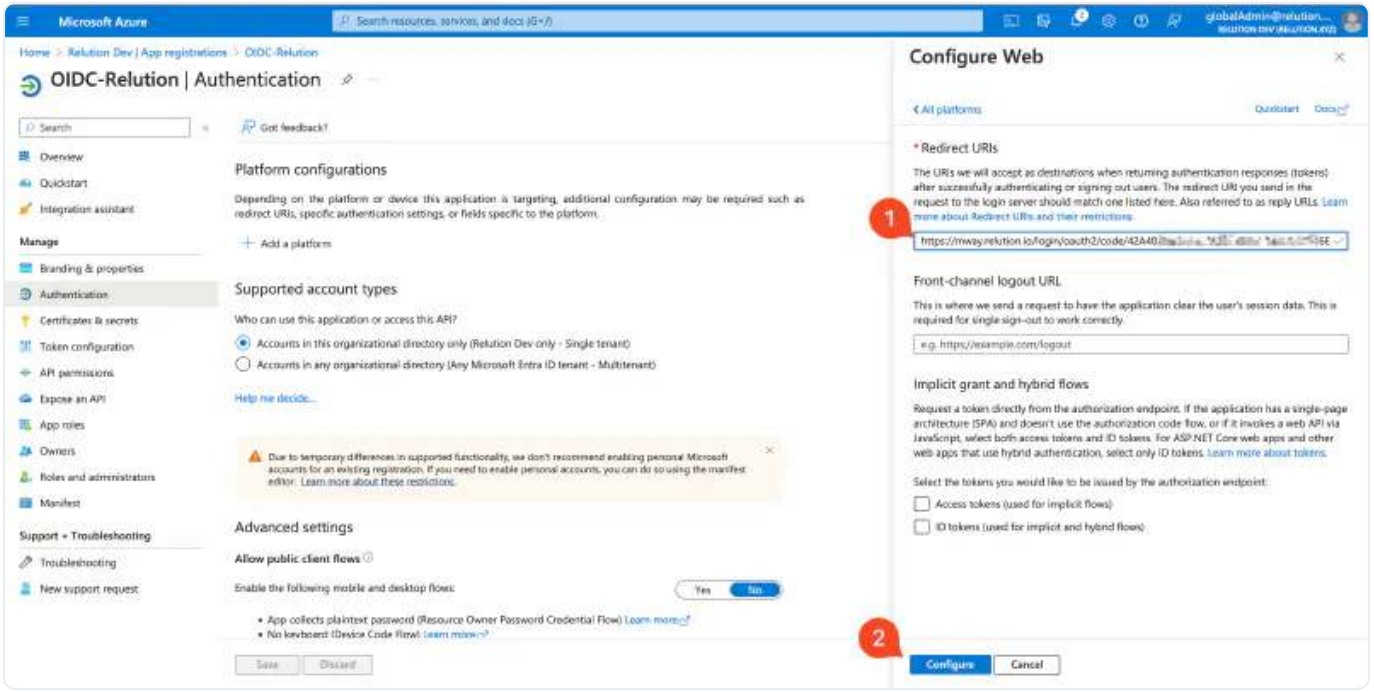
For version 26.4.0

Add redirection URI

New in 26.4

The redirection URI will be displayed in the Relution portal once the connection is configured and saved.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Relution Dev | App registrations > OIDC-Relution
OIDC-Relution | Authentication
Search
Got feedback?
Overview
Quickstart
Integration assistant
Manage
Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest
Support + Troubleshooting
Troubleshooting
New support request
Platform configurations
Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.
+ Add a platform
1
Supported account types
Who can use this application or access this API?
Accounts in this organizational directory only (Relution Dev only - Single tenant)
Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
Help me decide...
Due to temporary differences in supported functionality, we don't recommend enabling personal Microsoft accounts for an existing registration. If you need to enable personal accounts, you can do so using the manifest editor. Learn more about these restrictions.
Advanced settings
Allow public client flows
Enable the following mobile and desktop flows:
Yes
No
App collects plaintext password (Resource Owner Password Credential Flow) Learn more
No keyboard (Device Code Flow) Learn more
Save
Discard
Configure platforms
Web applications
2
Web
Build, host, and deploy a web server application. .NET, Java, Python
Single-page application
Configure browser client applications and progressive web applications. Javascript.
Mobile and desktop applications
iOS / macOS
Objective-C, Swift, Xamarin
Android
Java, Kotlin, Xamarin
Mobile and desktop applications
Windows, UWP, Console, IoT & Limited-entry Devices, Classic iOS + Android


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Relution Dev | App registrations > OIDC-Relution
OIDC-Relution | Authentication
Got feedback?
Platform configurations
Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.
+ Add a platform
Supported account types
Who can use this application or access this API?
Accounts in this organizational directory only (Relution Dev only - Single tenant)
Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
Help me decide...
Due to temporary differences in supported functionality, we don't recommend enabling personal Microsoft accounts for an existing registration. If you need to enable personal accounts, you can do so using the manifest editor. Learn more about these restrictions.
Advanced settings
Allow public client flows
Enable the following mobile and desktop flows:
Yes
No
App collects plaintext password (Resource Owner Password Credential Flow) Learn more
No keyboard (Device Code Flow) Learn more
Save
Discard
Configure Web
All platforms
Quickstart
Docs
* Redirect URIs
The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. The redirect URI you send in the request to the login server should match one listed here. Also referred to as reply URLs. Learn more about Redirect URIs and their restrictions
1
https://mway.relution.io/login/oauth2/code/42A40
Front-channel logout URL
This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.
e.g. https://example.com/logout
Implicit grant and hybrid flows
Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. Learn more about tokens.
Select the tokens you would like to be issued by the authorization endpoint:
Access tokens (used for implicit flows)
ID tokens (used for implicit and hybrid flows)
2
Configure
Cancel

> Migration notice — Scoped redirect URIs (from 26.4.0). With 26.4.0 Relution changed the redirect URI scheme: login callbacks are now scoped so they can in future be gated per path on a reverse proxy. The redirect URIs that must be registered depend on the respective OIDC configuration: configurations created from 26.4 onward always use the scoped redirect URIs. Configurations created before 26.4 keep using the previous redirect URI (`/login/oauth2/code/`) until they are switched to scoped paths (see Switching existing configurations).
>
> From 26.5.0, logins during a device enrollment (`enrollment`), in the Relution Agent (`agent`), in Relution Assets (`assets`) and in the Self-Service Portal (`selfService`) additionally run through dedicated scopes. If the configuration uses scoped paths and these logins are used with OIDC, the corresponding URIs must be registered at the identity provider.

Where to find them: the redirect URIs for the instance are shown in the Relution portal under `Settings` → `User Management` → `OpenID Connect` in the configuration's Scoped OIDC URLs section once the connection is saved, and they can be copied from there. However, the portal only shows the entries Redirect URL (management), Redirect URL (device) and, with an Education license, Redirect URL (teacher). It currently does not show the URIs for device enrollment (`/api/enrollment/`), the Relution Agent (`/api/agent/`), Relution Assets (`/api/assets/`), the Self-Service Portal (`/api/selfService/`) and Relution as Identity Provider → (`/api/idp/`). These are added manually following the scheme below, as far as the respective function is used with OIDC.

Previous paths (configurations created before 26.4, one redirect URI):

```
https://<host>/login/oauth2/code/<registrationId>
```

Scoped paths (configurations created from 26.4 or switched, register all that apply):

```
https://<host>/api/management/login/oauth2/code/<registrationId>       # Relution
portal
https://<host>/api/enrollment/login/oauth2/code/<registrationId>       # device
enrollment (ADE, User Enrollment, Android Enterprise), from 26.5
https://<host>/api/teacher/login/oauth2/code/<registrationId>          # Education
license only
https://<host>/api/agent/login/oauth2/code/<registrationId>            # Relution
Agent, from 26.5
https://<host>/api/assets/login/oauth2/code/<registrationId>           # Relution
Assets, from 26.5
https://<host>/api/selfService/login/oauth2/code/<registrationId>      # Self-Service
Portal, from 26.5
https://<host>/api/idp/login/oauth2/code/<registrationId>              # Relution as
Identity Provider (beta), from 26.5
https://<host>/api/device/login/oauth2/code/<registrationId>           # 26.4.x only,
no longer used by any login from 26.5
```

`<registrationId>` is the OIDC configuration UUID shown in Relution.

Logout URLs: The portal additionally shows two logout URLs in the same section. They are not redirect URIs:

- Front-channel logout URL: `https://<host>/api/management/v1/logout/connect/front-channel/<registrationId>`
- Back-channel logout URL: `https://<host>/api/management/logout/connect/back-channel/<registrationId>`

Switching existing configurations

Configurations created before 26.4 keep using the previous redirect URI after the update. Such a configuration additionally shows the Legacy OIDC URLs section with the currently active redirect URL and the previous back-channel logout URL. The switch is done in two steps:

1. All applicable scoped URIs are added to the existing Entra app registration. The previous URI remains registered for now.
2. In Relution, the configuration is opened under `Settings` → `User Management` → `OpenID Connect`, Enable Scoped OIDC Paths is clicked in the Legacy OIDC URLs section and the following dialog is confirmed.

> The switch cannot be undone. Afterwards, Relution only uses the scoped URIs for this configuration. If one of them is missing at the identity provider, the affected logins fail.

Newly created configurations do not show this section, because they use the scoped URIs from the start. The previous URI is deprecated and may be removed in a future release.

Redirect URI for device enrollment

New in 26.5

For version 26.4.0

From Relution 26.5.0, all logins during an enrollment use a dedicated `enrollment` scope. This applies to Apple Automated Device Enrollment (ADE, DEP in the portal), Apple Account-Driven User Enrollment, Android Enterprise enrollment and the Android Enterprise DPC sign-in. For configurations with scoped paths, these logins only work if the `/api/enrollment/` URI listed above is registered at the identity provider. Configurations with the previous paths keep using the previous URI for enrollments as well.

Symptom of a missing URI: logging in to the Relution portal keeps working, because it uses the `/api/management/` URI. Only the device enrollment fails, for example the ADE enrollment of a Mac with the message `AADSTS50011: The redirect URI ... does not match`. If this error occurs during an enrollment with a configuration that uses scoped paths, the `/api/enrollment/` URI is missing from the Entra app registration.

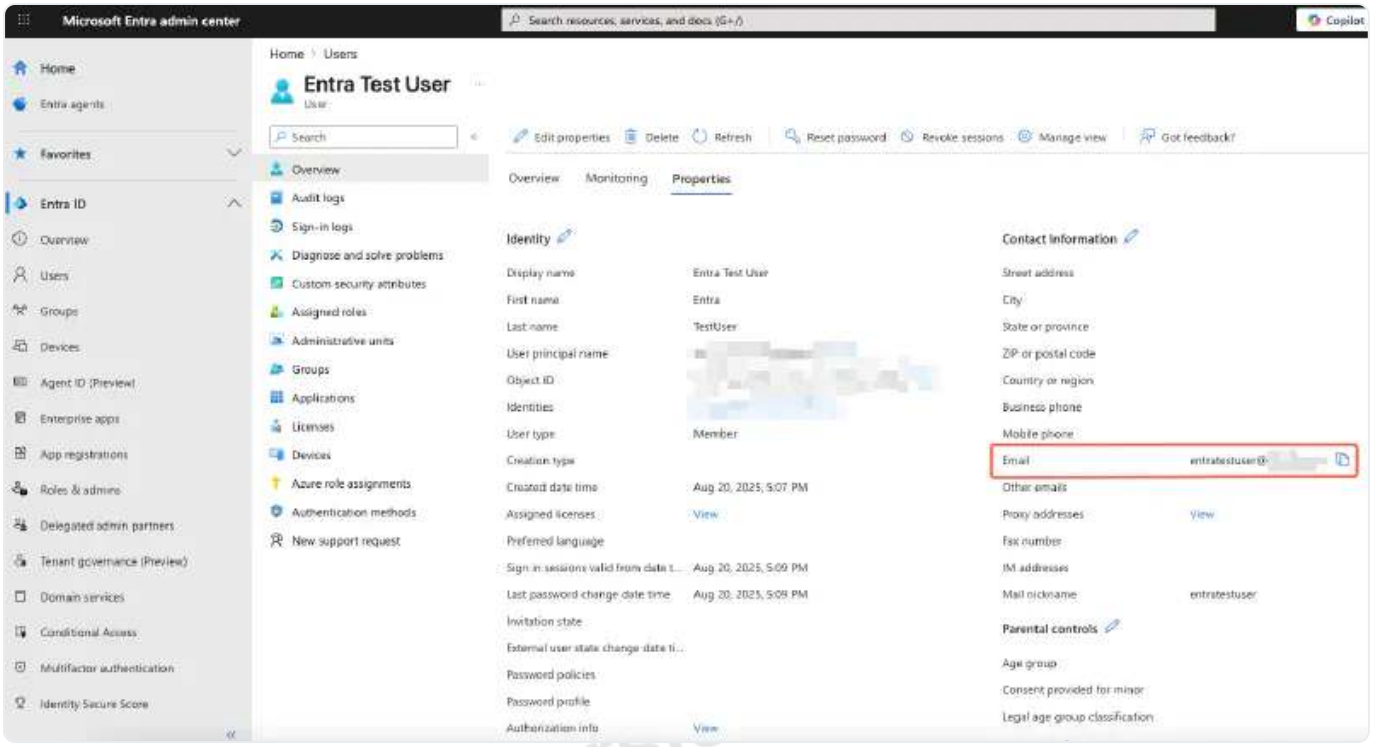
Backchannel Logout

Backchannel Logout is supported in Relution starting with Server version 5.32.0.

Example use case: A user is signed in to a central SSO service and multiple applications. When the user logs out of the SSO service, the backchannel logout ensures that all connected applications also terminate their sessions—even if running in the background.

Entra User Requirements for OIDC

For login via OIDC with an Entra user to work, an email address must be configured for the Entra user.



Logout Verification

Before go-live, the logout paths should be verified:

- Signing out at the IdP when logging out of Relution: clicking Logout in Relution revokes the session. The browser is only additionally redirected to the logout endpoint of the IdP if the Logout user from OIDC when logging out from Relution switch is enabled under Advanced Options and an end session endpoint is known. Since the endpoints for Entra are configured manually, the End session endpoint field must be filled in for this.
- Front-channel logout: when the user signs out at the IdP, the IdP calls the Front-channel logout URL shown in the portal and Relution revokes the session. This requires the URL to be registered at the IdP.
- Back-channel logout: the IdP sends a logout notification to the Back-channel logout URL — the session is revoked without user interaction.

Testing these paths ensures that IdP-initiated session termination (e.g. from the IdP admin console) propagates correctly to Relution.

Relution as Identity Provider

From version 26.5.0, Relution can act as its own OpenID Connect / OAuth2 Identity Provider — client applications are registered directly in Relution, allowing users to sign in with their existing Relution account across all connected applications.

The configuration is located under `Settings` → `Identity Provider`. The page is only visible with the permission to read IdP clients; registering, editing and deleting clients requires the respective permissions.

> This feature is currently in a beta phase and is subject to change. Feedback, questions, and suggestions are welcome.

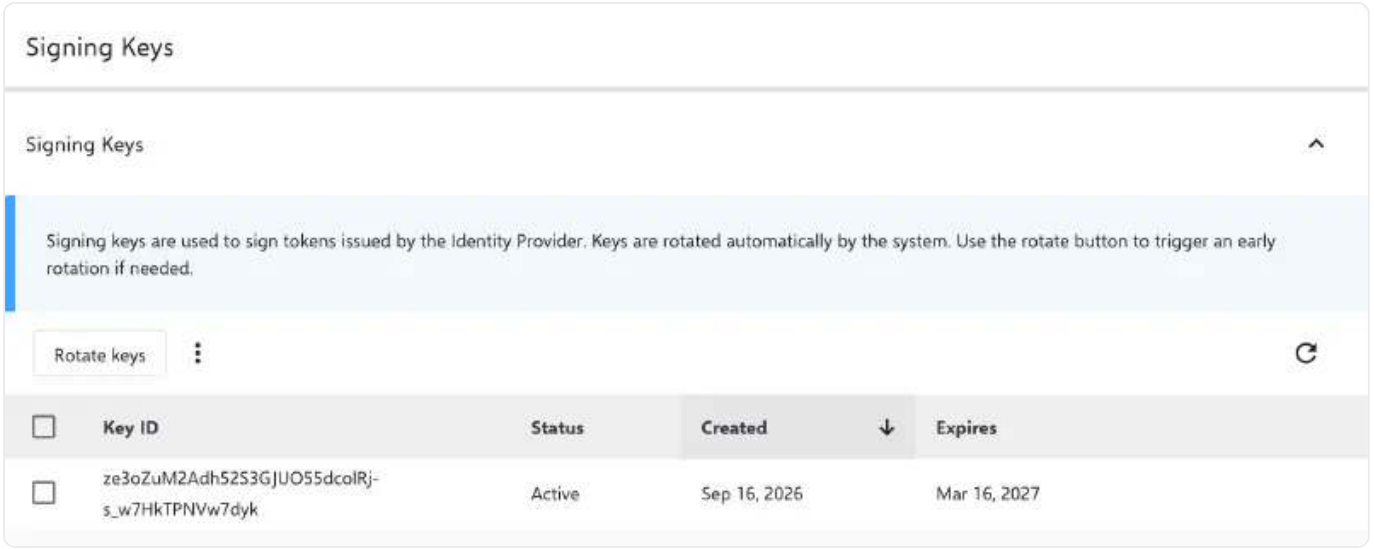
> Only confidential OIDC clients are currently supported — public clients (e.g. single-page apps or native apps without a client secret, such as those used by Zammad) will follow in a later release.

Feature overview

- Standard OIDC login flow using the Authorization Code flow with PKCE; refresh tokens are supported.
- Per-client configurable scopes (`profile` , `email` , `phone` , `relution`), including a consent screen shown to users. The `relution` scope provides Relution-specific data (e.g. organization membership). The `phone` scope can be enabled but currently provides no additional claims (e.g. no phone number).
- Single sign-out: both RP-initiated logout and OIDC Back-Channel Logout 1.0 are supported.
- Signing keys (JWK): The keys used to sign tokens are automatically managed and regularly renewed by Relution (an active key is replaced by a new one after four months) — no action is required.

Rotating and revoking signing keys

Signing keys are managed in the Signing Keys section of the `Settings` → `Identity Provider` page. This section is only available in the global organization; it is not displayed in meta organizations and suborganizations.

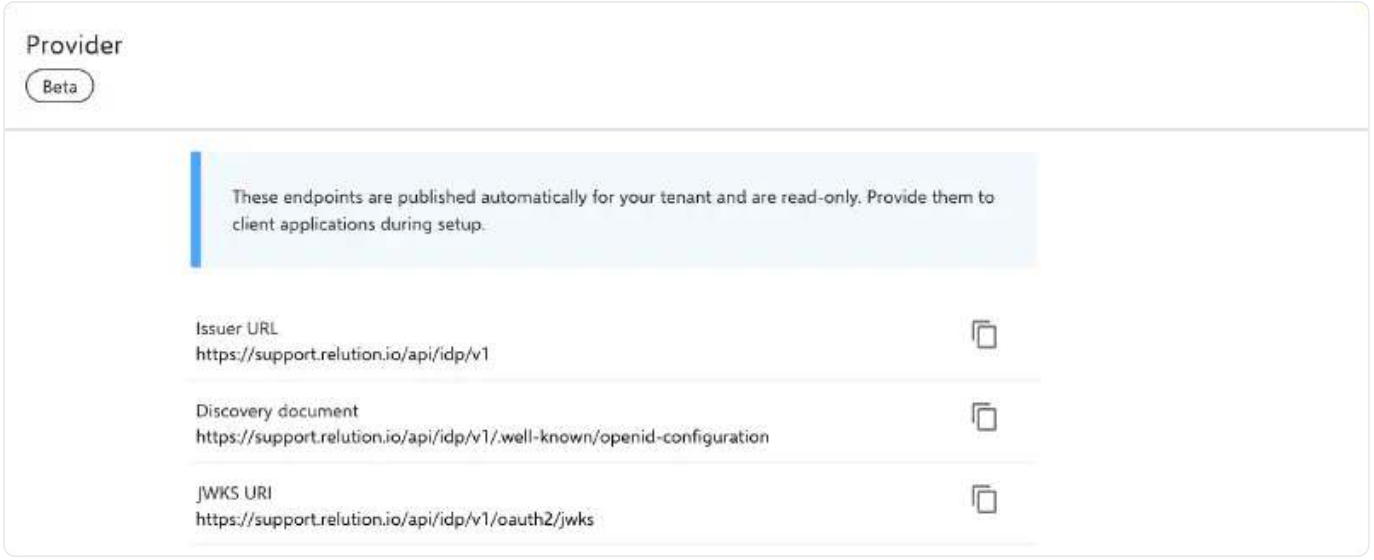


Automatic rotation fully covers normal operation. For exceptional cases (e.g. a security incident), two manual actions are available:

- Rotate keys: A new active key is created and the previous one is retired (status Retiring). Tokens already issued remain valid until they expire. Another rotation is possible no earlier than five minutes after the last one.
- Revoke: The selected key is immediately removed from the published key set. Note that connected applications (relying parties) may still have the previous key cached for a while, so tokens signed with it may not be recognized as invalid until that cache expires.

Endpoints for integration

In the Provider section at the top of the `Settings` → `Identity Provider` page, the Issuer URL, the Discovery document (`.well-known/openid-configuration`) and the JWKS URI are displayed and can be copied directly. Further technical endpoints (e.g. the token endpoint) can be looked up in the discovery document if needed.



IdP chaining

Relution can also be chained behind an upstream identity provider (e.g. Microsoft Entra ID → Relution → connected application).

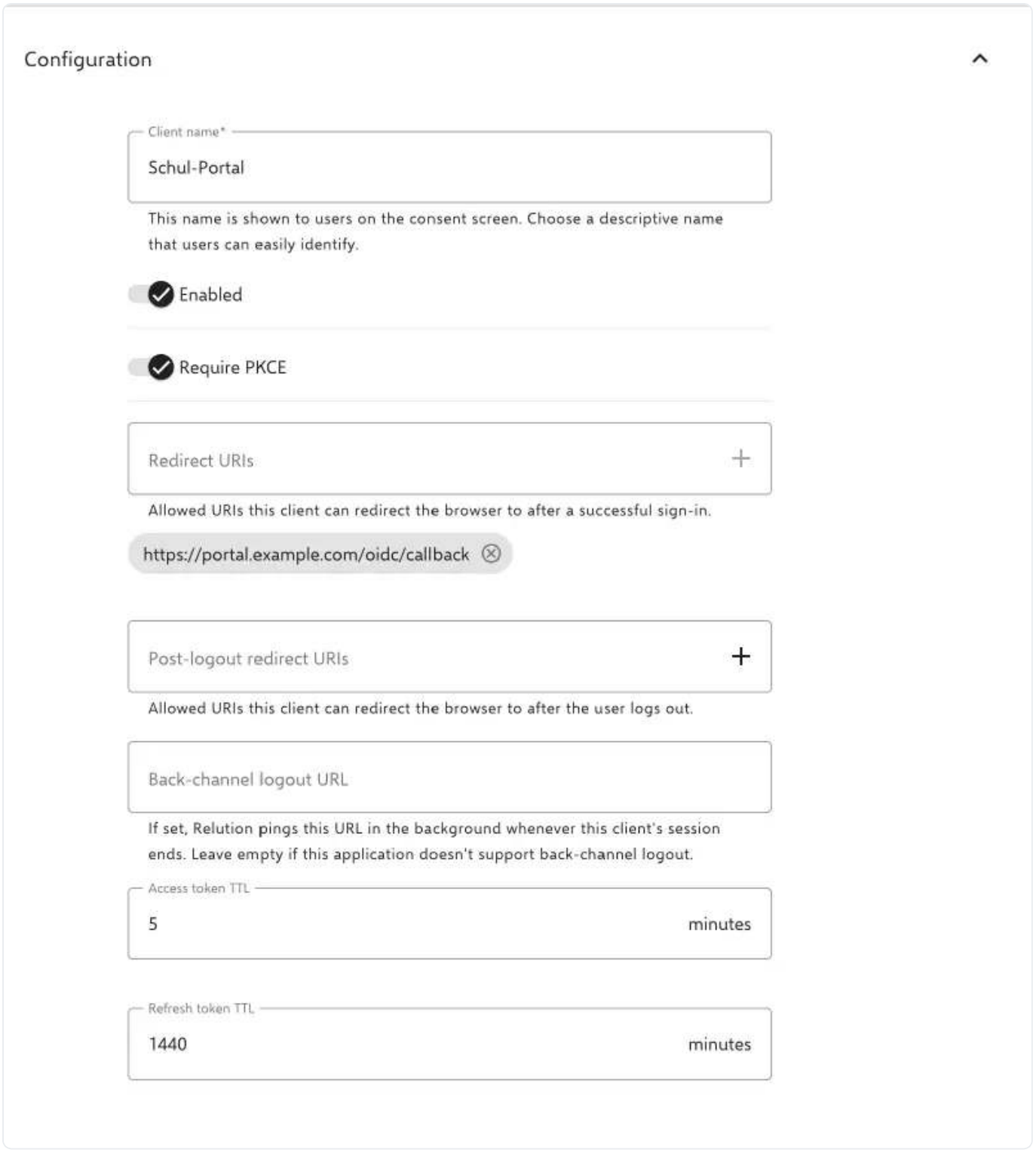
Registering a client

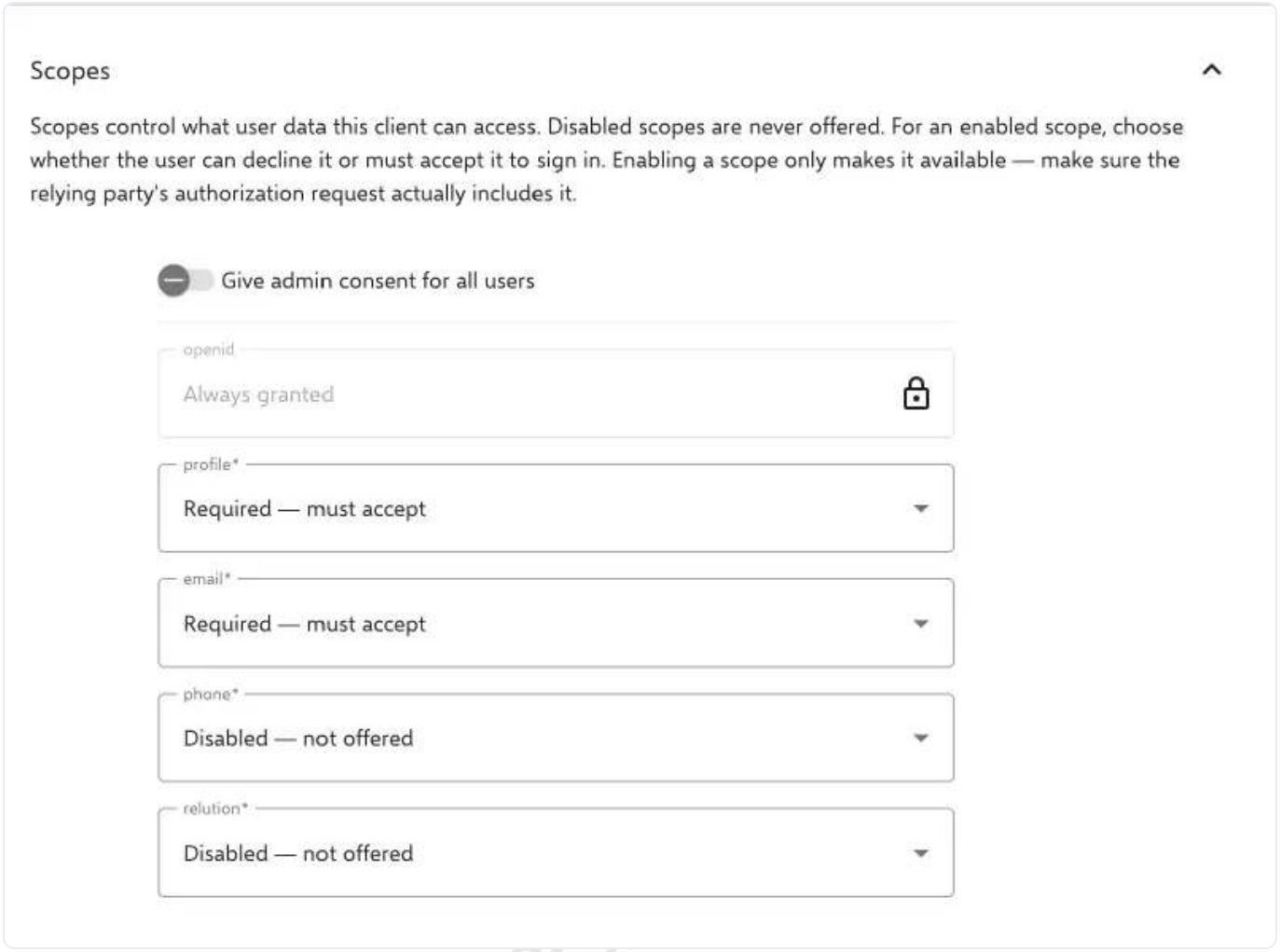
A dedicated client is created for each connected application via Register client:

- Client name: Freely chosen, shown to users on the consent screen, and used by administrators to distinguish multiple clients.
- Client ID and Client secret: Generated automatically and required by the connecting application (relying party). The application authenticates with them using `client_secret_basic` or `client_secret_post`. The client secret is displayed only once, directly after the client is created, and must be copied at that point; it cannot be retrieved later. If it is lost, a new secret can be generated in the Registered Clients list via Regenerate secret (also displayed only once). This invalidates the previous secret and revokes all existing tokens for the client.
- Enabled: A disabled client rejects new sign-ins and token renewal via refresh token.
- Require PKCE: Enabled by default. If the connecting application does not support PKCE, the option can be disabled for the respective client.
- Redirect URIs: Provided by the connecting application and must be entered accordingly.
- Post-logout redirect URIs: Addresses to which the application may redirect the browser after an RP-initiated logout.
- Back-channel logout URL: If set, Relution notifies the application in the background as soon as the client's session ends. Left empty if the application does not support back-channel logout.
- Access token TTL and Refresh token TTL: Lifetime of the issued tokens. For new clients, the form is prefilled with 5 minutes and 1 day respectively; permitted values are 1 to 60 minutes for access tokens and 1 to 90 days for refresh tokens.
- Scopes: Each scope is set to Disabled, Optional or Required. By default, `profile` and `email` are required, `phone` and `relution` are disabled. `openid` is always active (Always granted). Enabling a scope only makes it available; the connecting application must also request it during the login flow. If the request lacks `openid` or a required scope, the sign-in is rejected with the error `invalid_scope`. Optional scopes are only granted if the application requests them and they are not declined on the consent screen.
- Give admin consent for all users (admin consent): Consent for all of a client's scopes can be pre-approved by administrators (all-or-nothing, not per individual scope) — users are then not prompted to accept them on the consent screen the first time they log in to the application. While this option is enabled, scopes can only be configured as Disabled or Required. Scopes previously set to Optional are automatically reset to their default value (`profile` and `email`: Required; `phone` and `relution`: Disabled).

Clients that are no longer needed are deleted in the Registered Clients list.

For version 26.4.0


Configuration
Client name*
Schul-Portal
This name is shown to users on the consent screen. Choose a descriptive name that users can easily identify.
Enabled
Require PKCE
Redirect URIs
Allowed URIs this client can redirect the browser to after a successful sign-in.
https://portal.example.com/oidc/callback
Post-logout redirect URIs
Allowed URIs this client can redirect the browser to after the user logs out.
Back-channel logout URL
If set, Relution pings this URL in the background whenever this client's session ends. Leave empty if this application doesn't support back-channel logout.
Access token TTL
5
minutes
Refresh token TTL
1440
minutes



Visibility by organization level

The organization level at which a client is registered determines which users can sign in through it:

- Global: All users across the entire system can sign in.
- Meta organization: All users of the meta organization and its suborganizations can sign in.
- Suborganization: Only users of that specific suborganization can sign in.

Token preview

A preview of the resulting token claims can be viewed for a client's current scope configuration — making it possible to check in advance which information a connected application would receive in the token.

The scopes provide the following claims:

Scope	Claims
`openid`	`sub` (user ID), `amr` (authentication method), additionally `idp` with an upstream identity provider
`profile`	`name`, `given_name`, `family_name`, `preferred_username`, `locale`, `updated_at`
`email`	`email`
`relution`	UUID, name and unique name of the user's organization
`phone`	currently none

Granted consents

In their profile, users see on the Authorized apps tab which applications they have granted which scopes to, and can revoke access there. Administrators with the corresponding permission find the same section in a user's details. Revoking also removes the application's existing authorizations for that user, so the application can no longer obtain new tokens via refresh token; consent is requested again at the next login.

For version 26.4.0

Logging

Logins through the Identity Provider are recorded both in the audit log and in the respective user's login history. In the login history, the IdP Client column shows which client the login was made through.

OIDC with Workspace

OpenID Connect `OIDC` is an identity protocol built on top of OAuth 2.0 that enables secure authentication and authorization for web and mobile applications. It allows users to log in securely to various services while service providers can simultaneously access verified identity information.

This guide explains the step-by-step configuration of OIDC in Relution using Google Workspace as an example.

> When using OIDC, no classes or groups are synchronized. Users are only created in Relution on their first successful login, and only if the Create unknown users in Relution switch is enabled in the OIDC configuration. If it is disabled (default), only users who already exist in Relution can log in. Relution automatically adds newly created users to the group `<Provider name> Users`, which can be used to assign permissions.

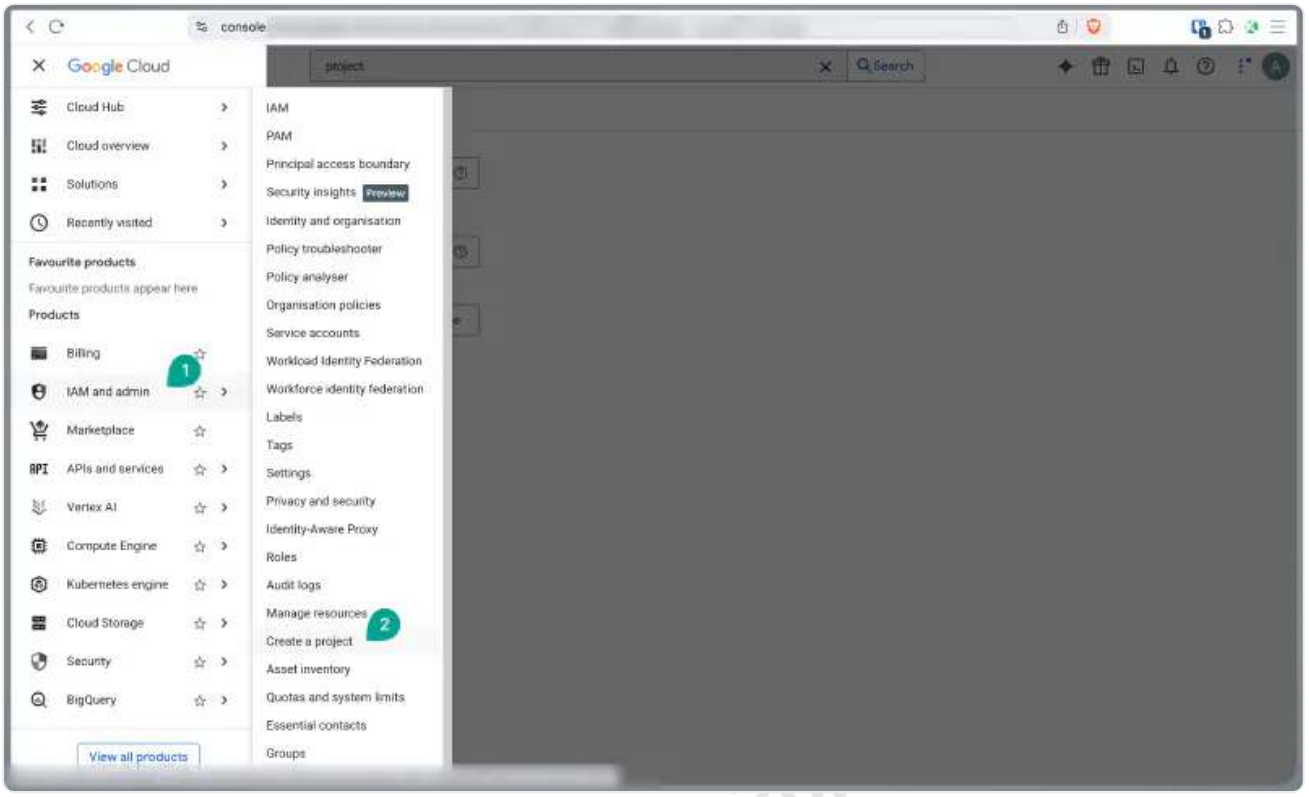
Project and Client Setup (Google Cloud Console)

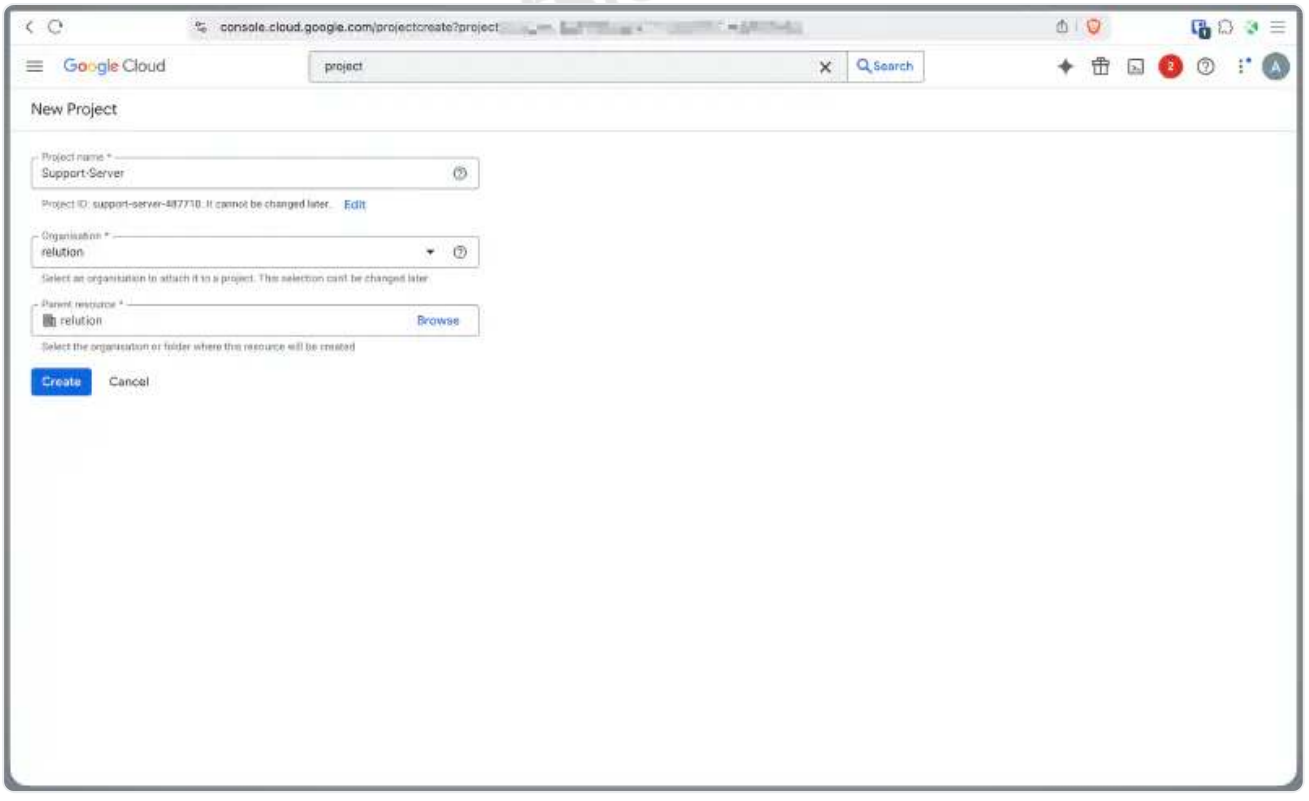
First, an application must be registered in the Google Cloud Console to obtain the necessary credentials.

For version 26.4.0

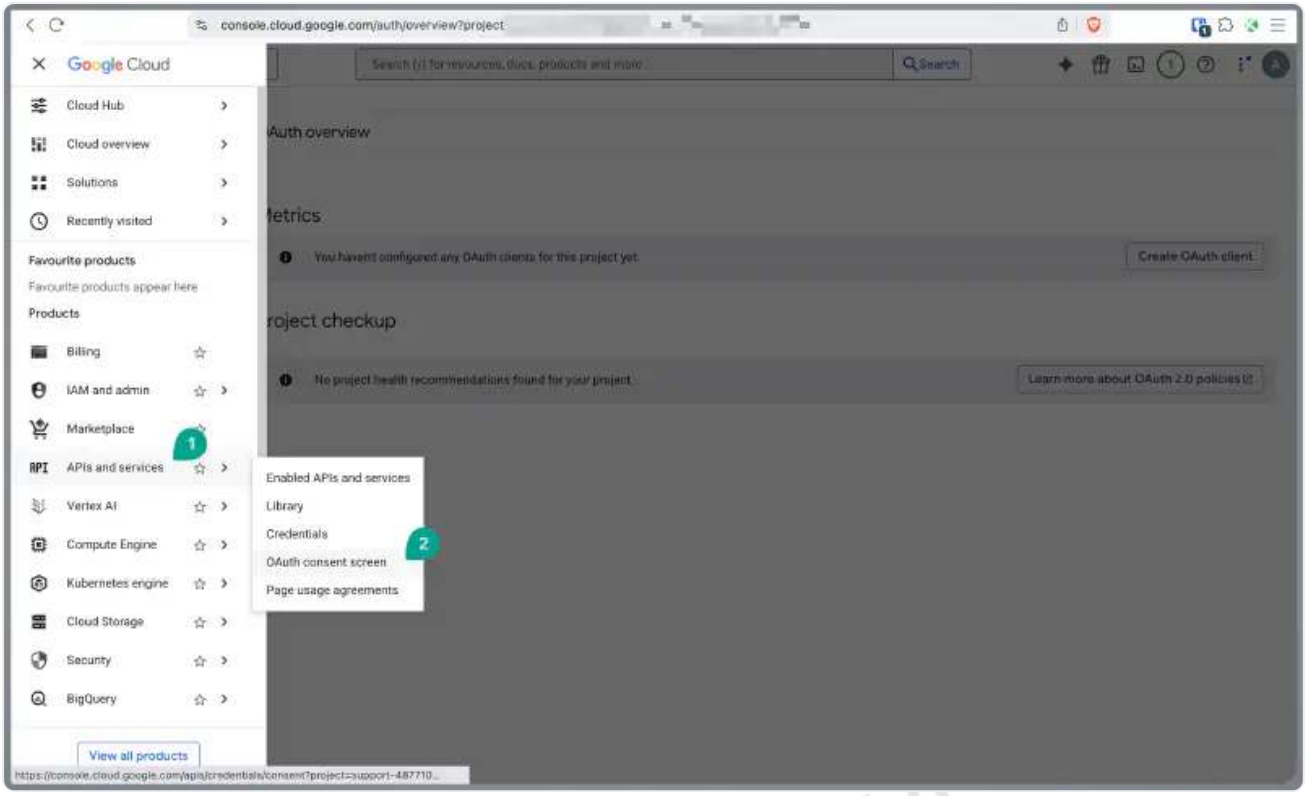
1. The sign-in takes place at console.cloud.google.com →.

2. A new project is created or an existing one is selected.

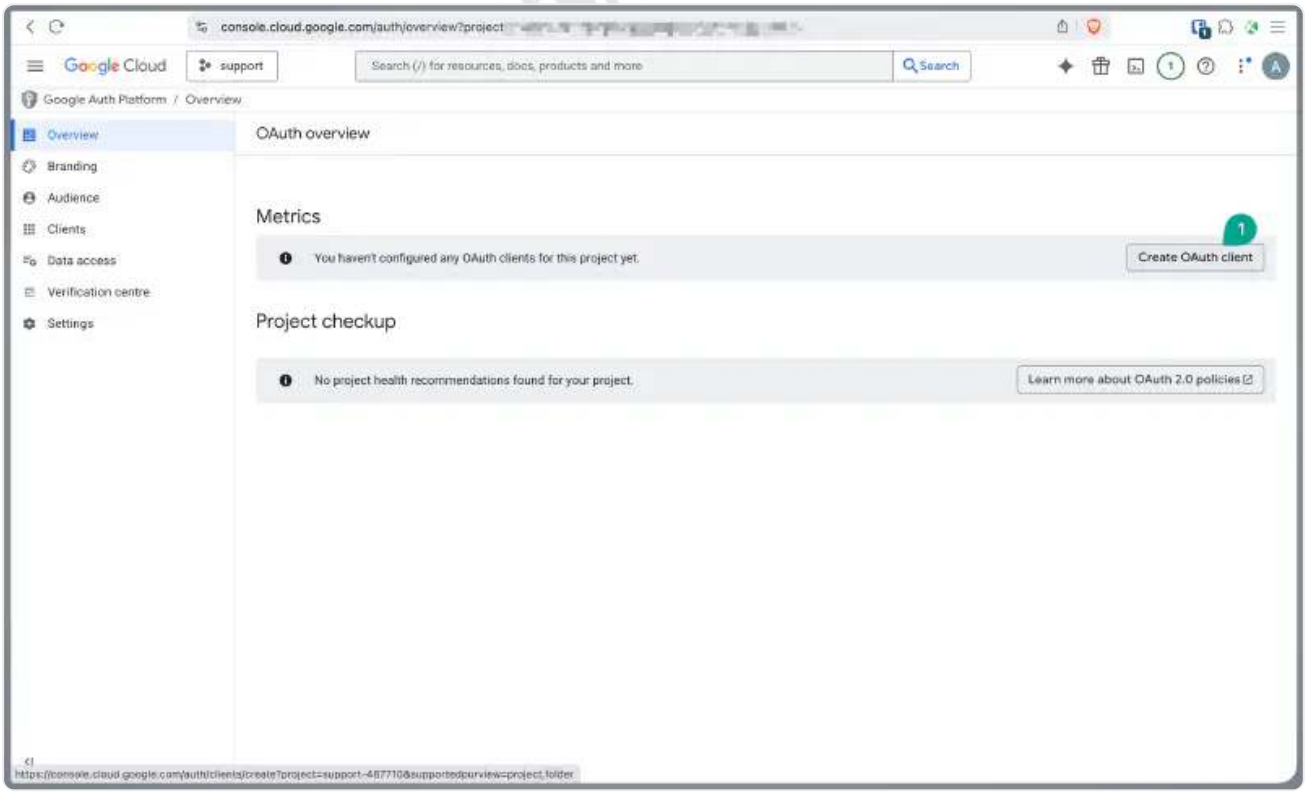




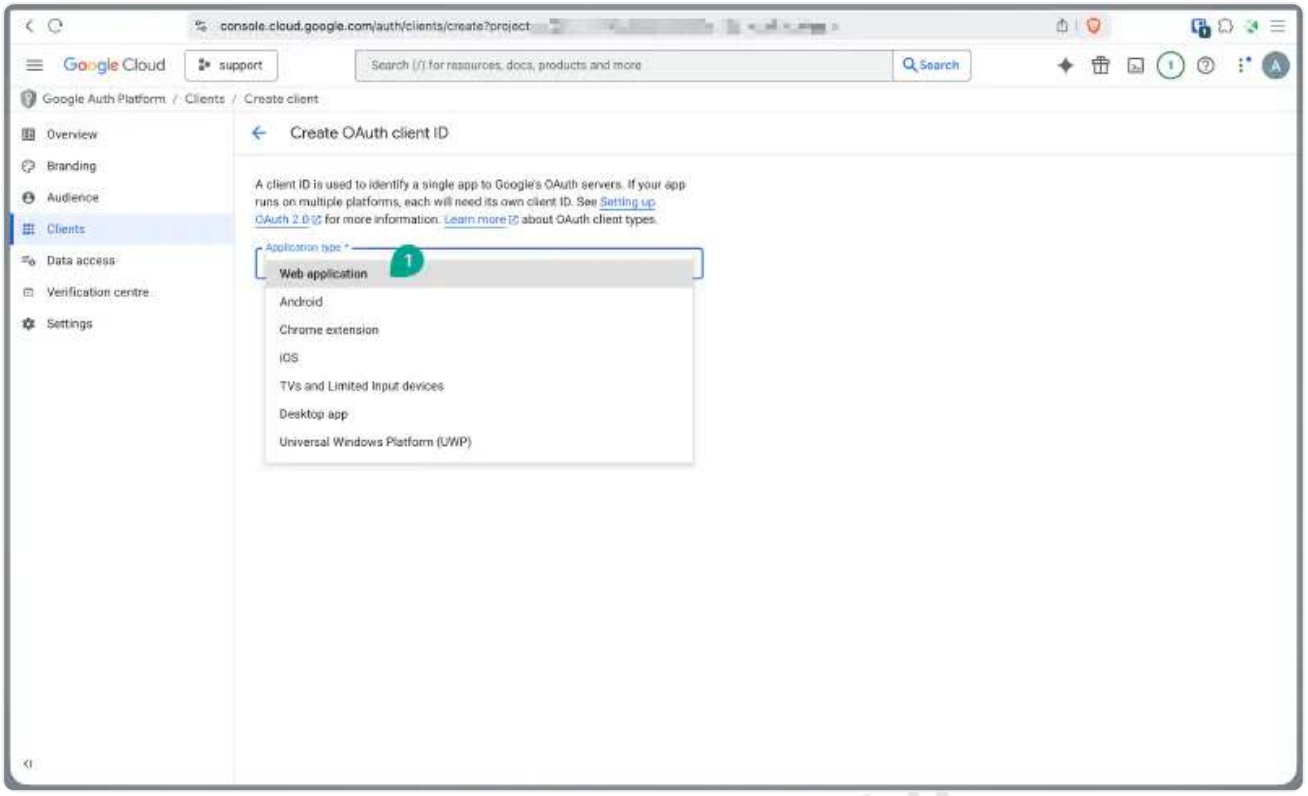
3. In the navigation menu, `APIs & Services` → `OAuth consent screen` is opened and configured if necessary.



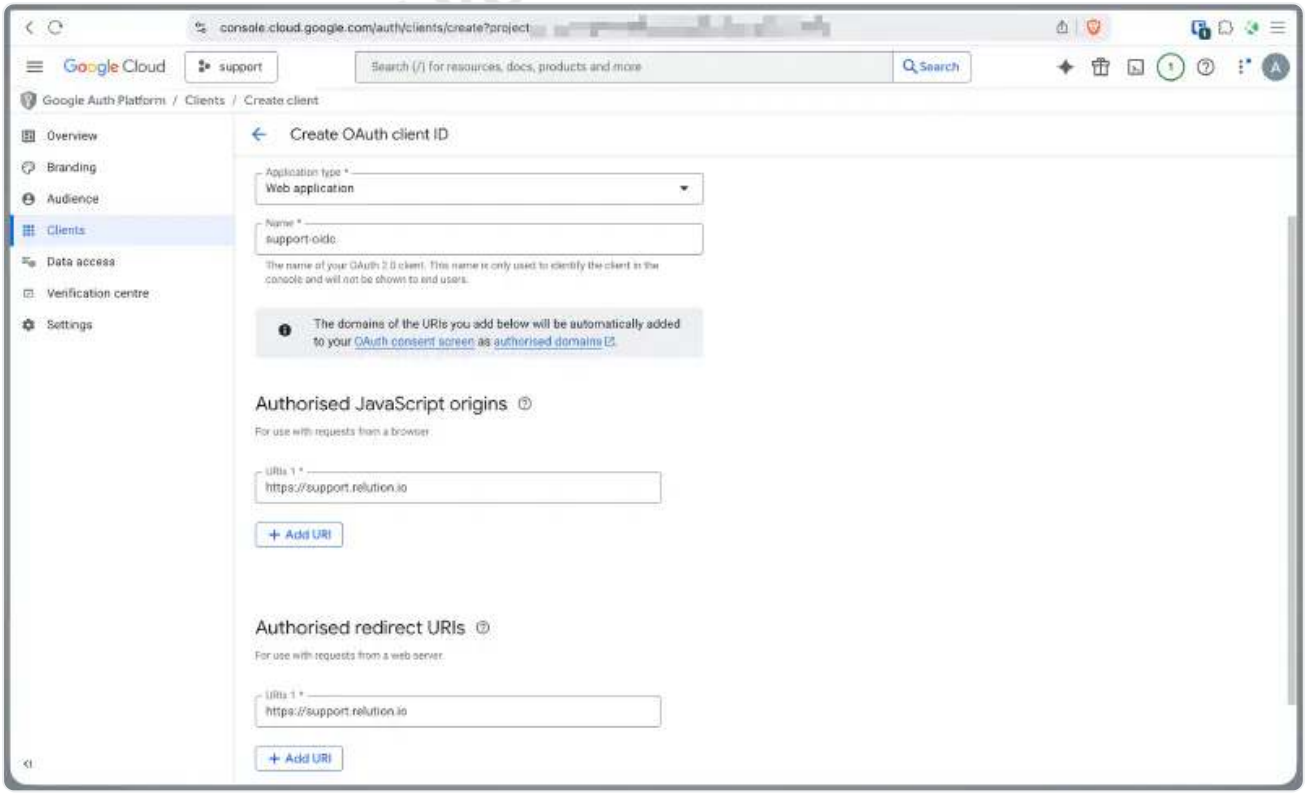
4. Under Credentials, Create Credentials is clicked and OAuth client ID is selected.



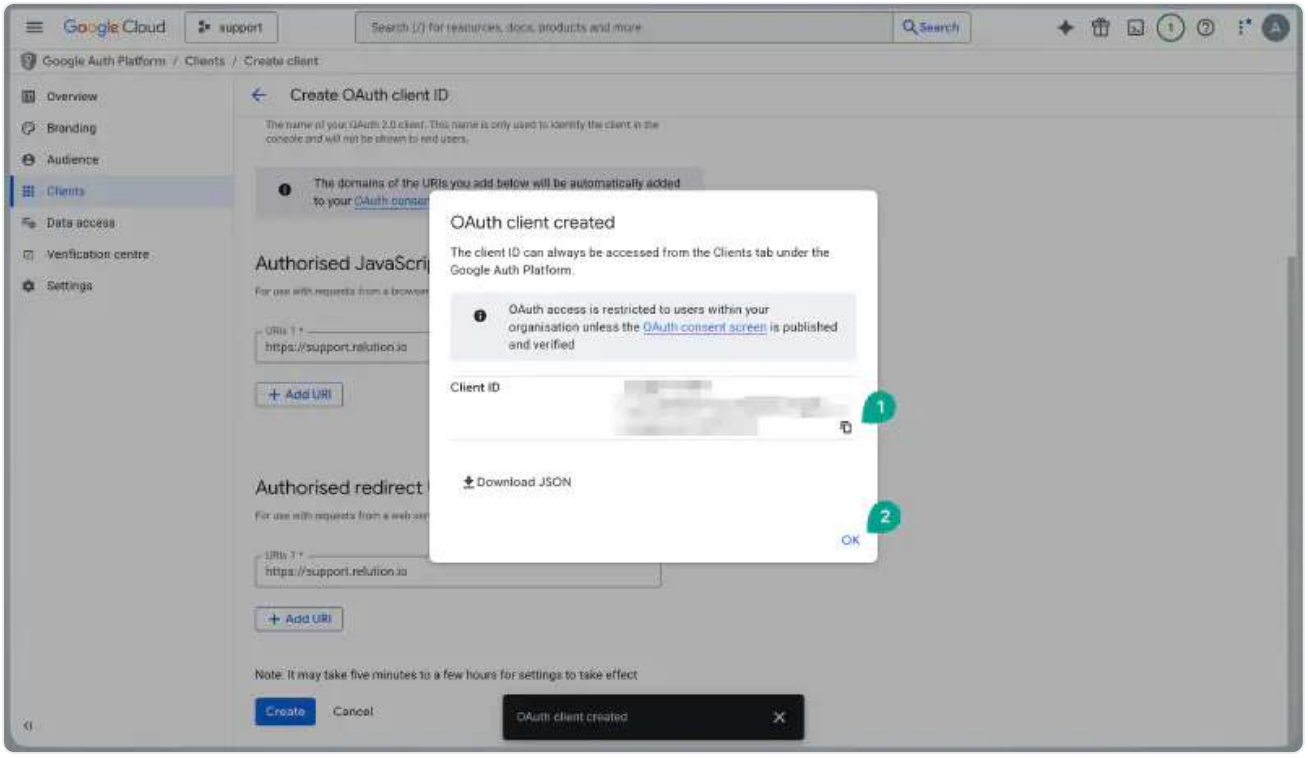
5. For Application type, `Web application` is selected.



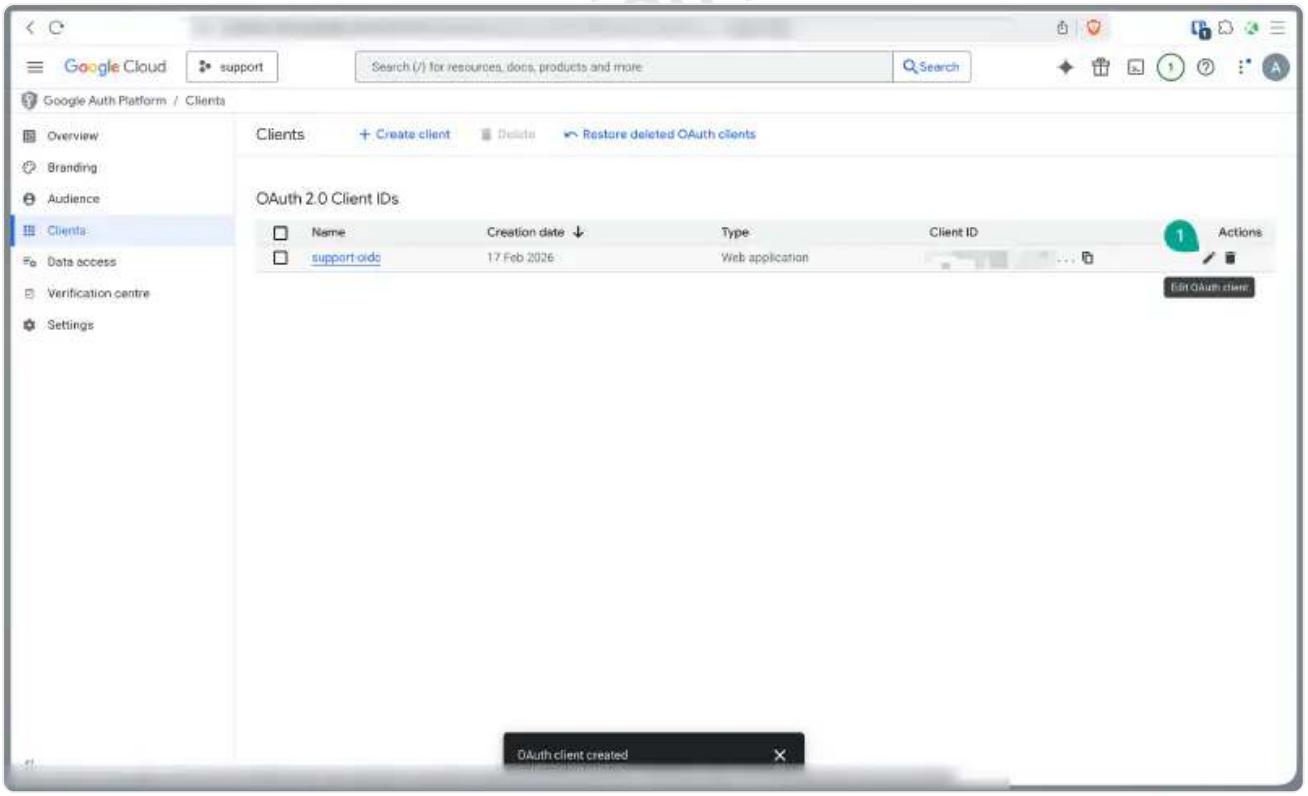
6. Under Authorized JavaScript origins, the server URL is entered (e.g., `https://support.relution.io`). *Note: The Authorized redirect URIs field can be left open for now; it will be updated later with the redirect URIs from Relution.*



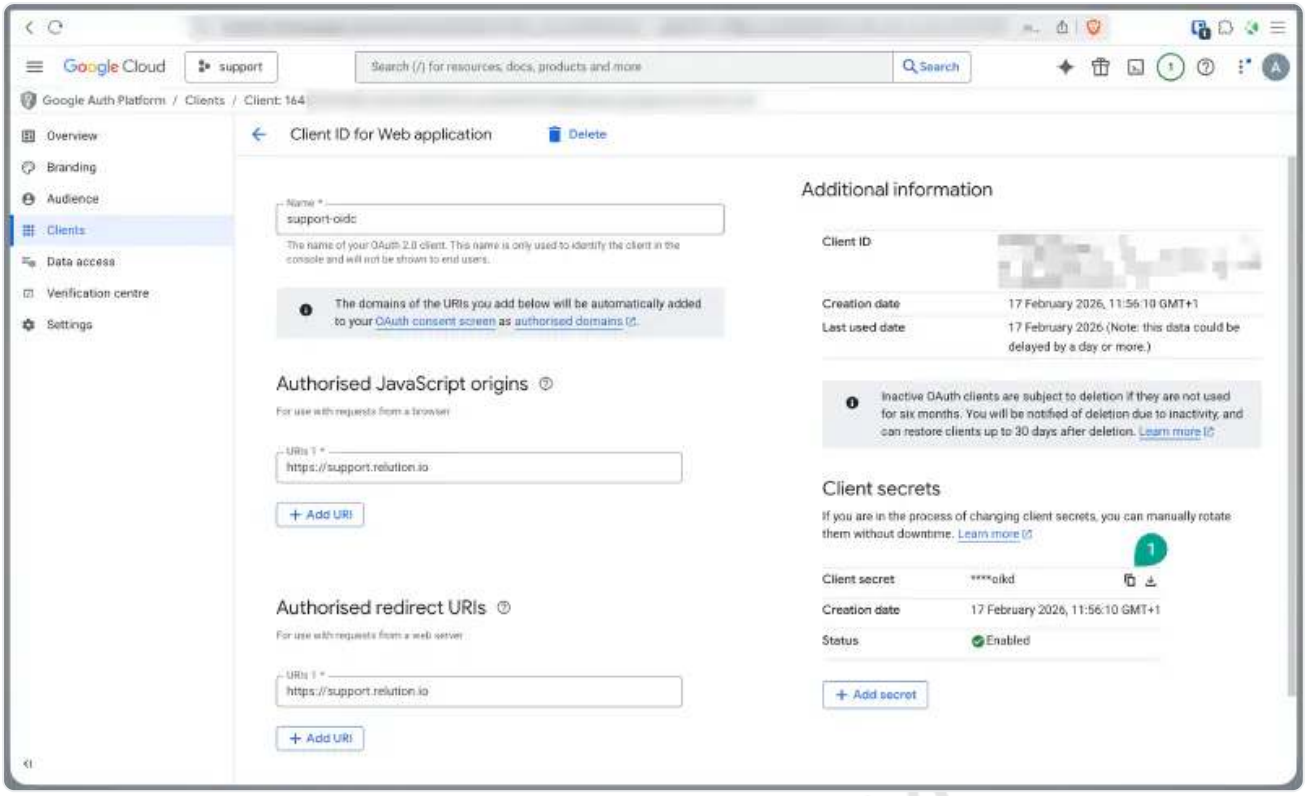
7. The Client ID displayed after saving is copied.



8. The newly created client is edited again to view the details.



9. The Client Secret is copied. Both the ID and Secret are kept secure for later use in Relution.

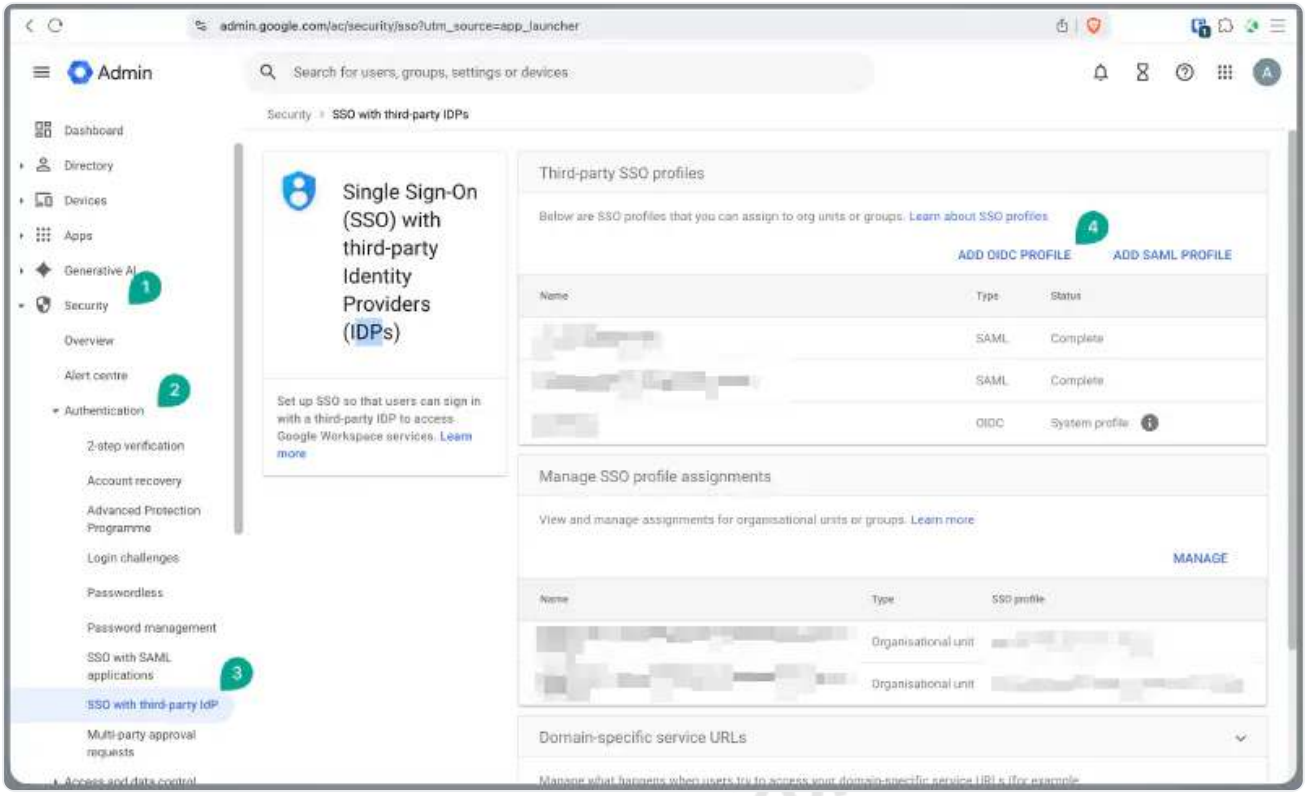


For version 26.4.0

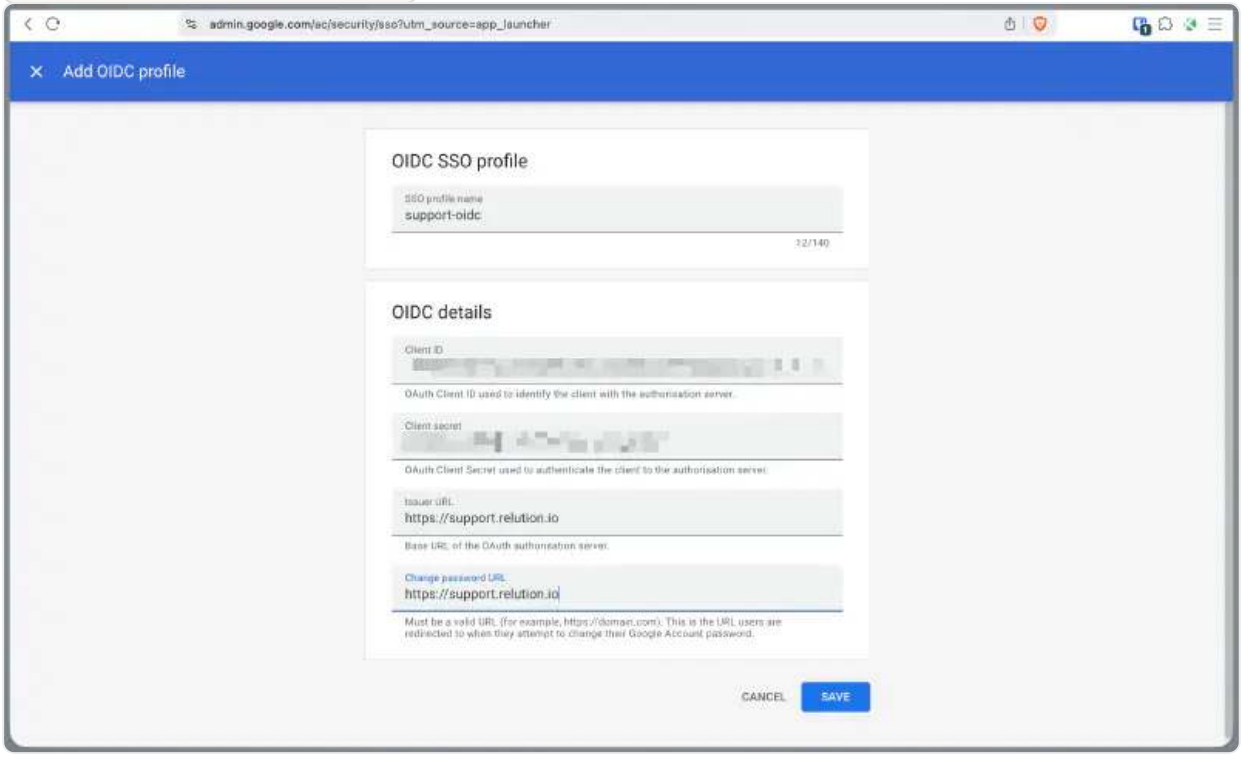
SSO Setup (Google Admin Console)

In parallel, the Single Sign-On (SSO) profile must be stored in the Google Admin Console.

1. admin.google.com → is opened.
2. A new OIDC profile is created under `Security` → `Authentication` → `SSO with third-party IdP`.



3. The Client ID and Client Secret obtained in the previous steps are entered.
   - For the Issuer URL and Change password URL, the Relution server URL is used (e.g., `https://support.relution.io`).



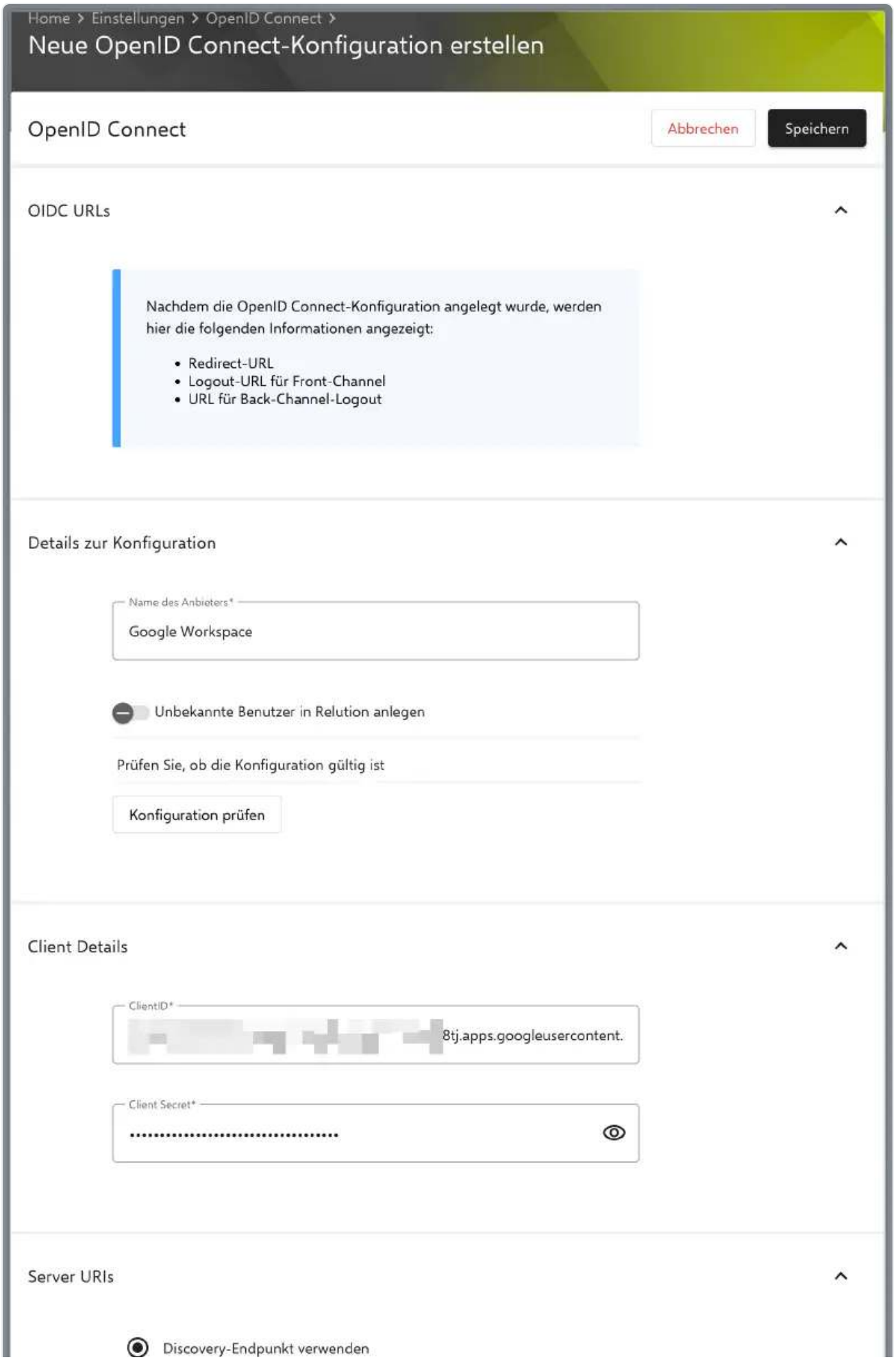
OIDC Configuration in Relution

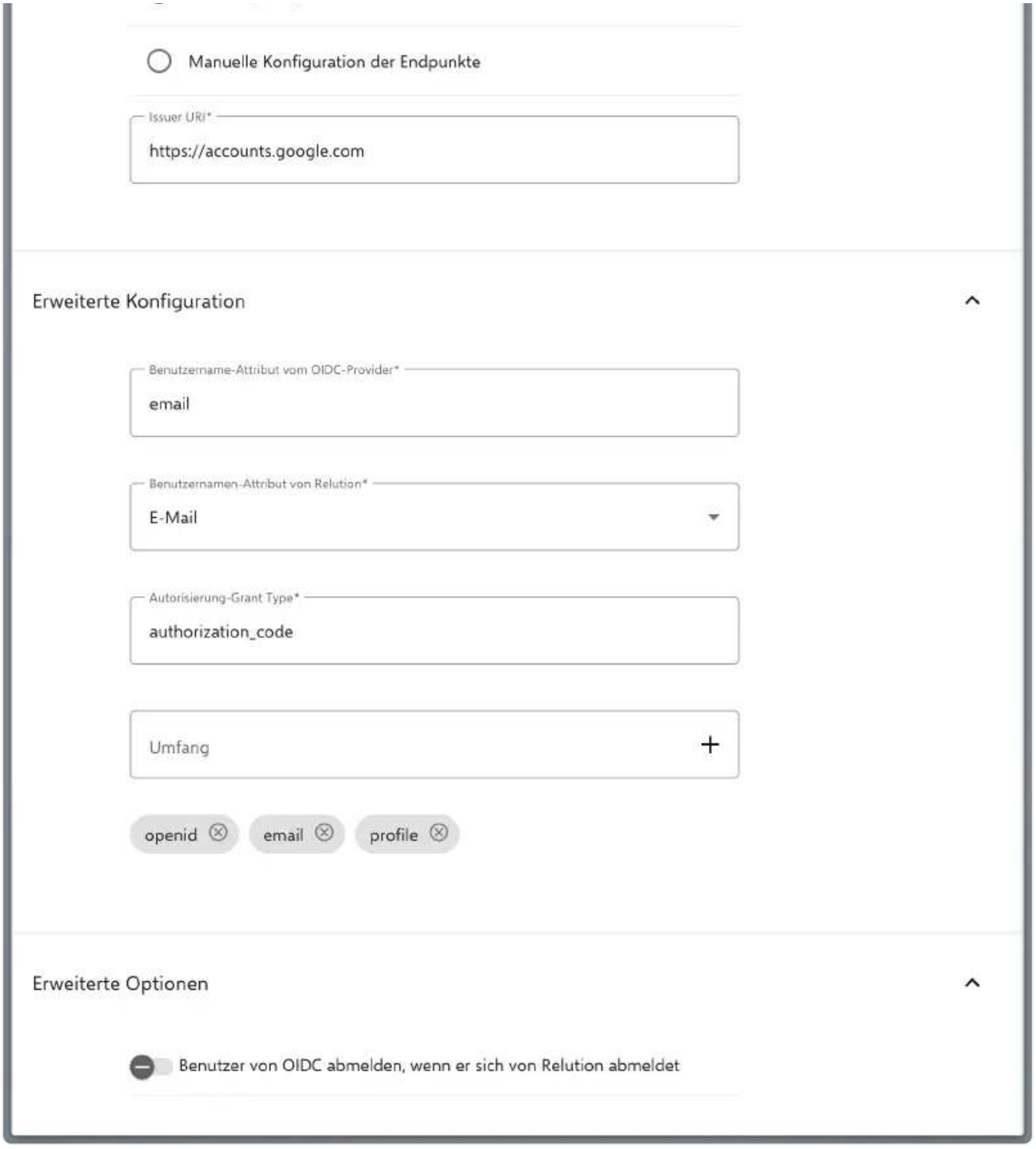
Now, the collected data is entered into Relution to establish the connection with Google.

For version 26.4.0

1. The OIDC settings are opened in Relution under `Settings` → `User Management` → `OpenID Connect`.

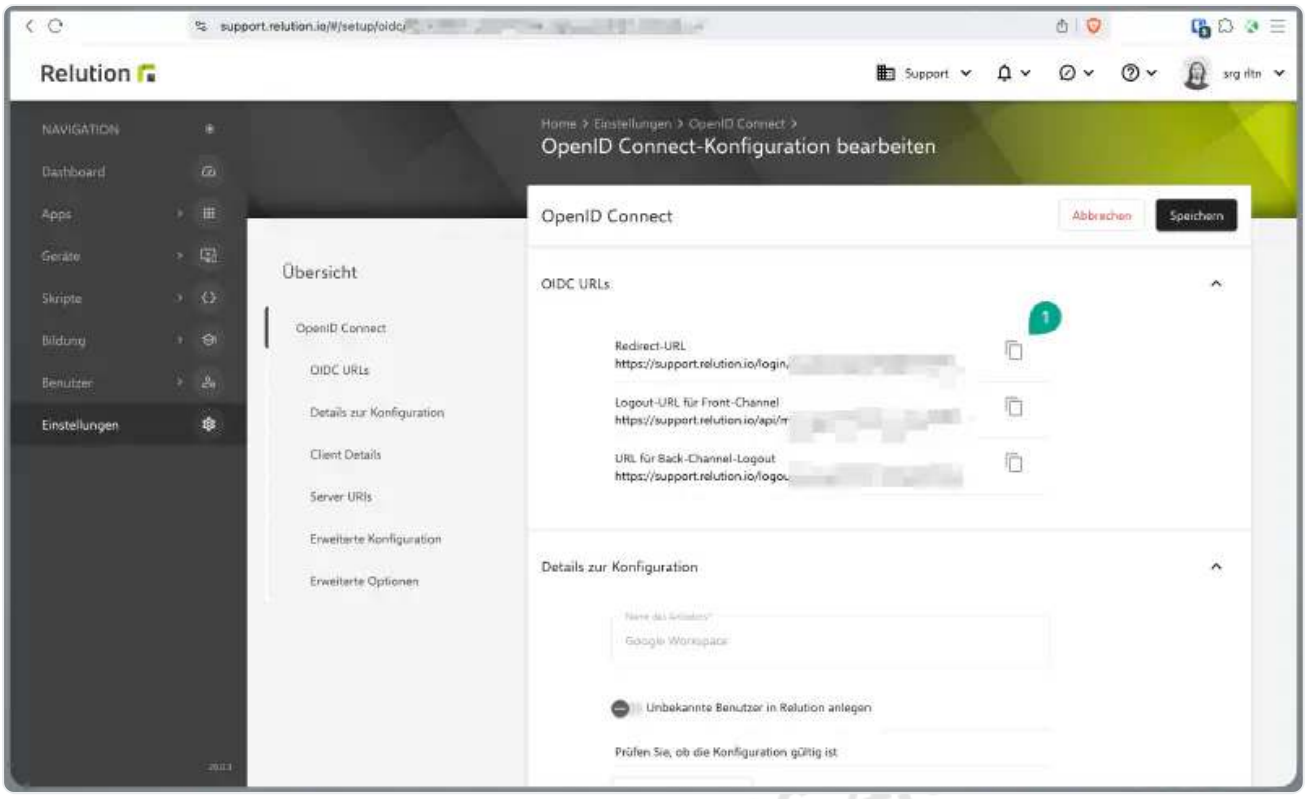
For version 26.4.0


Home > Einstellungen > OpenID Connect >
Neue OpenID Connect-Konfiguration erstellen
OpenID Connect
Abbrechen
Speichern
OIDC URLs
Nachdem die OpenID Connect-Konfiguration angelegt wurde, werden hier die folgenden Informationen angezeigt:
Redirect-URL
Logout-URL für Front-Channel
URL für Back-Channel-Logout
Details zur Konfiguration
Name des Anbieters*
Google Workspace
Unbekannte Benutzer in Relution anlegen
Prüfen Sie, ob die Konfiguration gültig ist
Konfiguration prüfen
Client Details
ClientID*
8tj.apps.googleusercontent.
Client Secret*
Server URIs
Discovery-Endpunkt verwenden



2. Under Provider name, a unique name is entered (e.g. “Google Workspace”). The name appears on the login button and cannot be changed after saving.
3. If required, Create unknown users in Relution is enabled so that new users are created automatically on their first login.
4. The Client ID and Client Secret from the Google Cloud Console are entered in the Client ID and Client Secret fields.
5. In the Server URIs section, Use discovery endpoint is selected and `https://accounts.google.com` is entered in the Issuer URI field.
6. The configuration is saved and then opened again to see the generated fields.

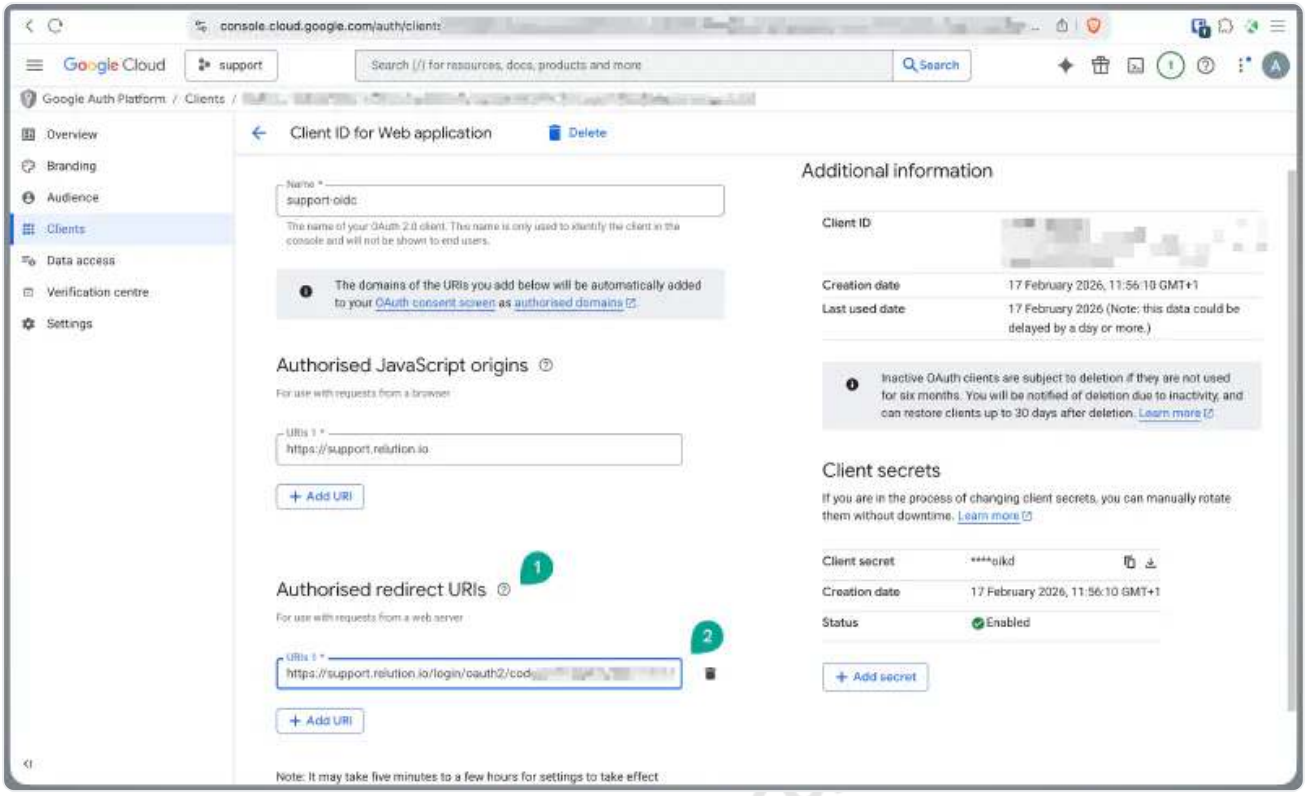
7. In the Scoped OIDC URLs section, all Redirect URL entries shown are copied (one each for `management` and `device`, plus `teacher` with an Education license).



8. console.cloud.google.com → is opened again.

For version 26.4

9. The OAuth client is edited and all URLs just copied from Relution are added under Authorized redirect URIs. In addition, the redirect URIs that the portal does not display are added, at least the one for device enrollment (`/api/enrollment/`), see Scoped redirect URIs.



Extended configuration defines how Relution assigns the signed-in user: the Username attribute from OIDC Provider (default: `email`) is matched against the user property selected under Username attribute from Relution (User name, E-mail address, UUID or Foreign key (UID); default: E-mail address). With UUID, unknown users are not created. The Scope defaults to `openid`, `email`, `profile`. Check configuration validates the configuration before saving.

Scoped redirect URIs

New in 26.4

> Migration notice — Scoped redirect URIs (from 26.4.0). With 26.4.0 Relution changed the redirect URI scheme: login callbacks are now scoped so they can in future be gated per path on a reverse proxy. Which redirect URIs are used depends on whether the OIDC configuration still uses the previous paths: configurations created from 26.4 onward always use the scoped redirect URIs. Configurations created before 26.4 keep using the previous redirect URI (`/login/oauth2/code/`) until they are switched to scoped paths (see Switching existing configurations).
>
> From 26.5.0, logins during a device enrollment (`enrollment`), in the Relution Agent (`agent`), in Relution Assets (`assets`) and in the Self-Service Portal (`selfService`) additionally run through dedicated scopes. If the configuration uses scoped paths and these logins are used with OIDC, the corresponding URIs must be registered at the identity provider.

Where to find them: the redirect URIs for the instance are shown in the Relution portal under `Settings` → `User Management` → `OpenID Connect` in the configuration's Scoped OIDC URLs section once the connection is saved, and they can be copied from there. However, the portal only shows the entries Redirect URL (management), Redirect URL (device) and, with an Education license, Redirect URL (teacher). It currently does not show the URIs for device enrollment (`/api/enrollment/`), the Relution Agent (`/api/agent/`), Relution Assets (`/api/assets/`), the Self-Service Portal (`/api/selfService/`) and Relution as Identity Provider → (`/api/idp/`). These are added manually following the scheme below, as far as the respective function is used with OIDC.

Previous paths (configurations created before 26.4, one redirect URI):

```
https://<host>/login/oauth2/code/<registrationId>
```

Scoped paths (configurations created from 26.4 or switched, register all that apply):

```
https://<host>/api/management/login/oauth2/code/<registrationId>       # Relution
portal
https://<host>/api/enrollment/login/oauth2/code/<registrationId>       # device
enrollment (ADE, User Enrollment, Android Enterprise), from 26.5
https://<host>/api/teacher/login/oauth2/code/<registrationId>          # Education
license only
https://<host>/api/agent/login/oauth2/code/<registrationId>            # Relution
Agent, from 26.5
https://<host>/api/assets/login/oauth2/code/<registrationId>           # Relution
Assets, from 26.5
https://<host>/api/selfService/login/oauth2/code/<registrationId>      # Self-Service
Portal, from 26.5
https://<host>/api/idp/login/oauth2/code/<registrationId>              # Relution as
Identity Provider (beta), from 26.5
https://<host>/api/device/login/oauth2/code/<registrationId>           # 26.4.x only,
no longer used by any login from 26.5
```

`<registrationId>` is the OIDC configuration UUID shown in Relution.

Logout URLs: The portal additionally shows two logout URLs in the same section. They are not redirect URIs:

- Front-channel logout URL: `https://<host>/api/management/v1/logout/connect/front-channel/<registrationId>`
- Back-channel logout URL: `https://<host>/api/management/logout/connect/back-channel/<registrationId>`

Switching existing configurations

Configurations created before 26.4 keep using the previous redirect URI after the update. Such a configuration additionally shows the Legacy OIDC URLs section with the currently active redirect URL and the previous back-channel logout URL. The switch is done in two steps:

1. All applicable scoped URIs are added to the existing Google OAuth client. The previous URI remains registered for now.
2. In Relution, the configuration is opened under `Settings` → `User Management` → `OpenID Connect`, Enable Scoped OIDC Paths is clicked in the Legacy OIDC URLs section and the following dialog is confirmed.

> The switch cannot be undone. Afterwards, Relution only uses the scoped URIs for this configuration. If one of them is missing at the identity provider, the affected logins fail.

Newly created configurations do not show this section, because they use the scoped URIs from the start. The previous URI is deprecated and may be removed in a future release.

Redirect URI for device enrollment

New in 26.5

From Relution 26.5.0, all logins during an enrollment use a dedicated `enrollment` scope. This applies to Apple Automated Device Enrollment (ADE, DEP in the portal), Apple Account-Driven User Enrollment, Android Enterprise enrollment and the Android Enterprise DPC sign-in. For configurations with scoped paths, these logins only work if the `/api/enrollment/` URI listed above is registered at the identity provider. Configurations with the previous paths keep using the previous URI for enrollments as well.

Symptom of a missing URI: logging in to the Relution portal keeps working, because it uses the `/api/management/` URI. Only the device enrollment fails, with an error about an invalid redirect URI (`invalid_redirect_uri`, at Google `Error 400: redirect_uri_mismatch`). If this error occurs during an enrollment with a configuration that uses scoped paths, the `/api/enrollment/` URI is missing from the Google OAuth client.

For version 26.4.0

Backchannel Logout

Relution supports Backchannel Logout starting with server version 5.32.0.

Example Scenario: A user is simultaneously logged into multiple applications via SSO. When logging out of the central SSO service, Backchannel Logout ensures that the sessions in Relution and other connected applications are also terminated securely in the background.

Logout Verification

Before go-live, the logout paths should be verified:

- Signing out at the IdP when logging out of Relution: clicking Logout revokes the session in Relution. If the Logout user from OIDC when logging out from Relution switch is enabled under Advanced Options (default: off) and an end session endpoint is known (entered manually in the End session endpoint field or reported by the IdP via discovery), the browser is additionally redirected to the logout endpoint of the IdP.
- Front-channel logout: when the user signs out at the IdP, the IdP calls the Front-channel logout URL shown in the portal and Relution revokes the session. This requires the URL to be registered at the IdP.
- Back-channel logout: the IdP sends a logout notification to the Back-channel logout URL — the session is revoked without user interaction.

Testing these paths ensures that IdP-initiated session termination (e.g. from the IdP admin console) propagates correctly to Relution.

For version 26.4.0

Off-Time Configuration

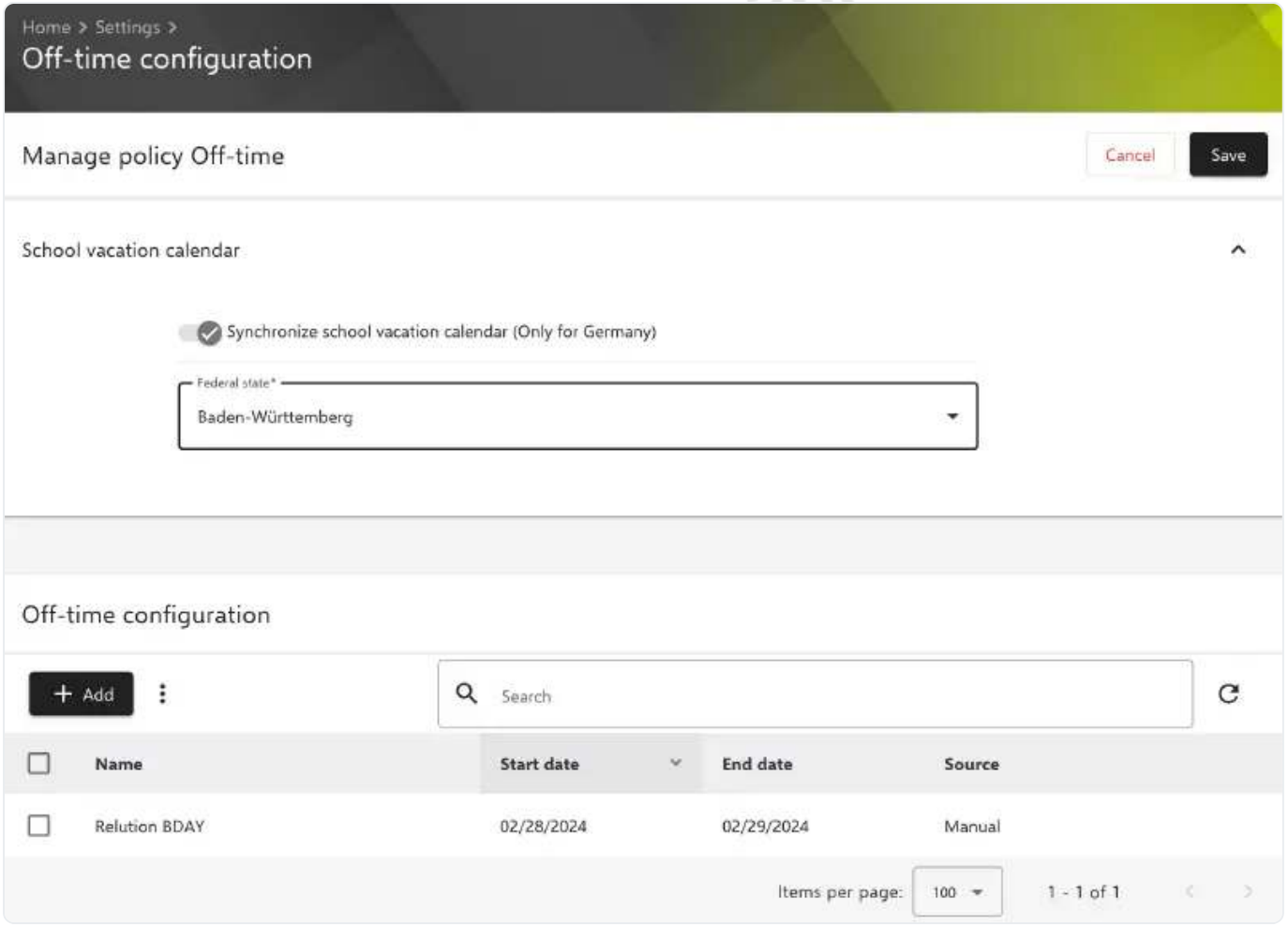
In version 5.23 and beyond, the off-time configuration in Relution allows users with the corresponding permissions (by default the Administrator and Device Manager roles of an organization) to enter school holiday calendars for federal states and to add their own dates, either manually or by uploading an existing calendar file. Policies in which off-time is enabled are disabled during these periods.

Configuration

The off-time configuration is located within an organization under `Settings` → `Off-time Configuration`. It is not available in the global organization.

Synchronizing school holiday calendars

Synchronization is enabled using the Synchronize school vacation calendar (Only for Germany) switch and the Federal state selection, and applied with Save. The holidays of the current and the following year are imported; after that, the server updates the entries automatically. The synchronization can be started manually using the button next to Last Off-time sync. If synchronization is disabled, all synchronized entries are deleted.

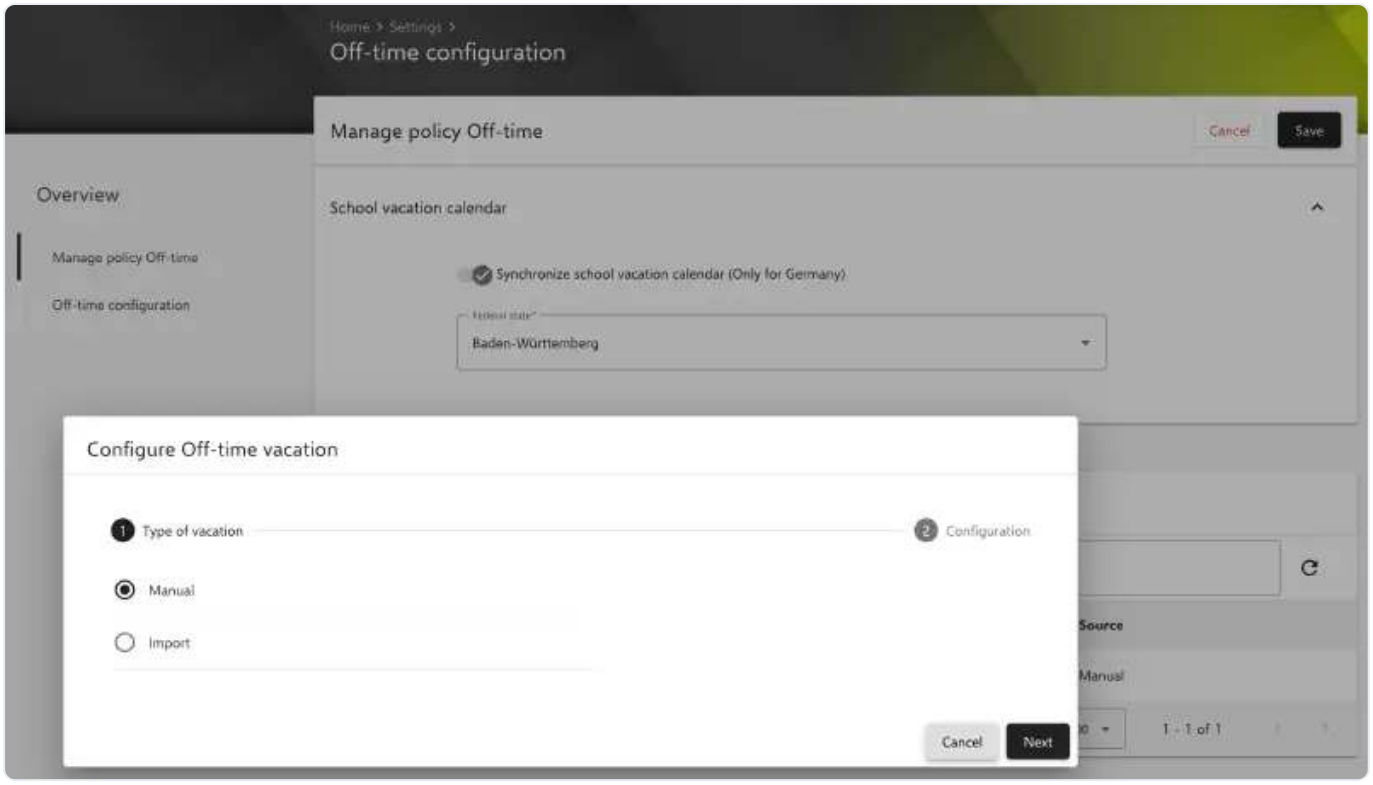


School holiday calendars are only available for Germany.

Adding or importing custom periods

Add opens the Configure Off-time vacation dialog. In the Type of vacation step, Manual or Import is selected:

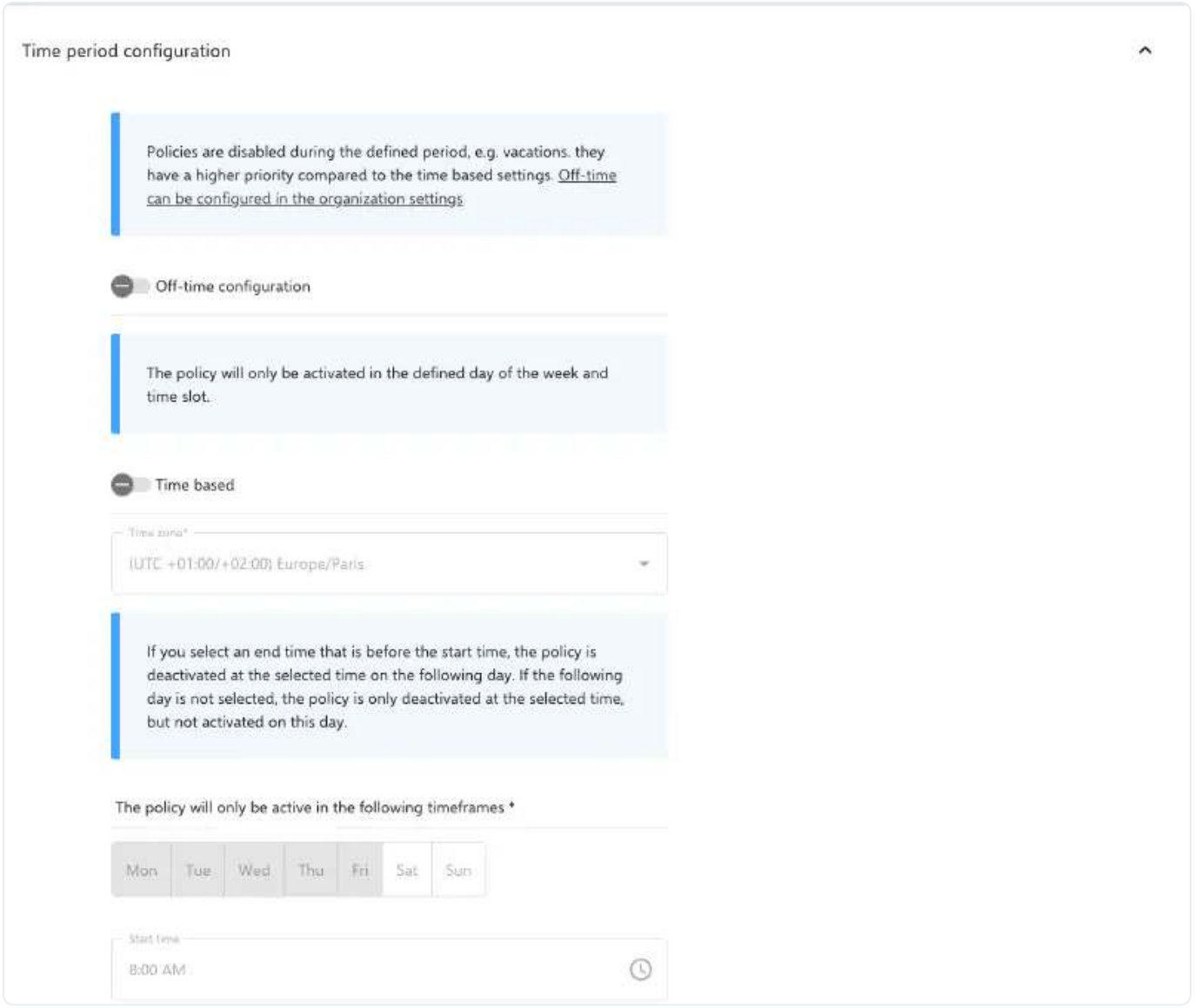
- Manual: A Name and the Off-time custom period with start and end date are entered.
- Import: A calendar file is uploaded. The following formats are supported: `.ical`, `.ics`, `.ifb`, `.icalendar`. Only all-day events with a title are imported; the title becomes the name of the off-time.



For each entry, the list shows the name, start date, end date and source (manual, imported with the name of the calendar, or Synced for a federal state). Past entries are shown greyed out. Entries can be edited and deleted; via the context menu, the off-times can be exported as an iCalendar file (Export Off-times to iCalendar) or as CSV. Expired off-times are removed automatically two years after their end by default.

Application in policies

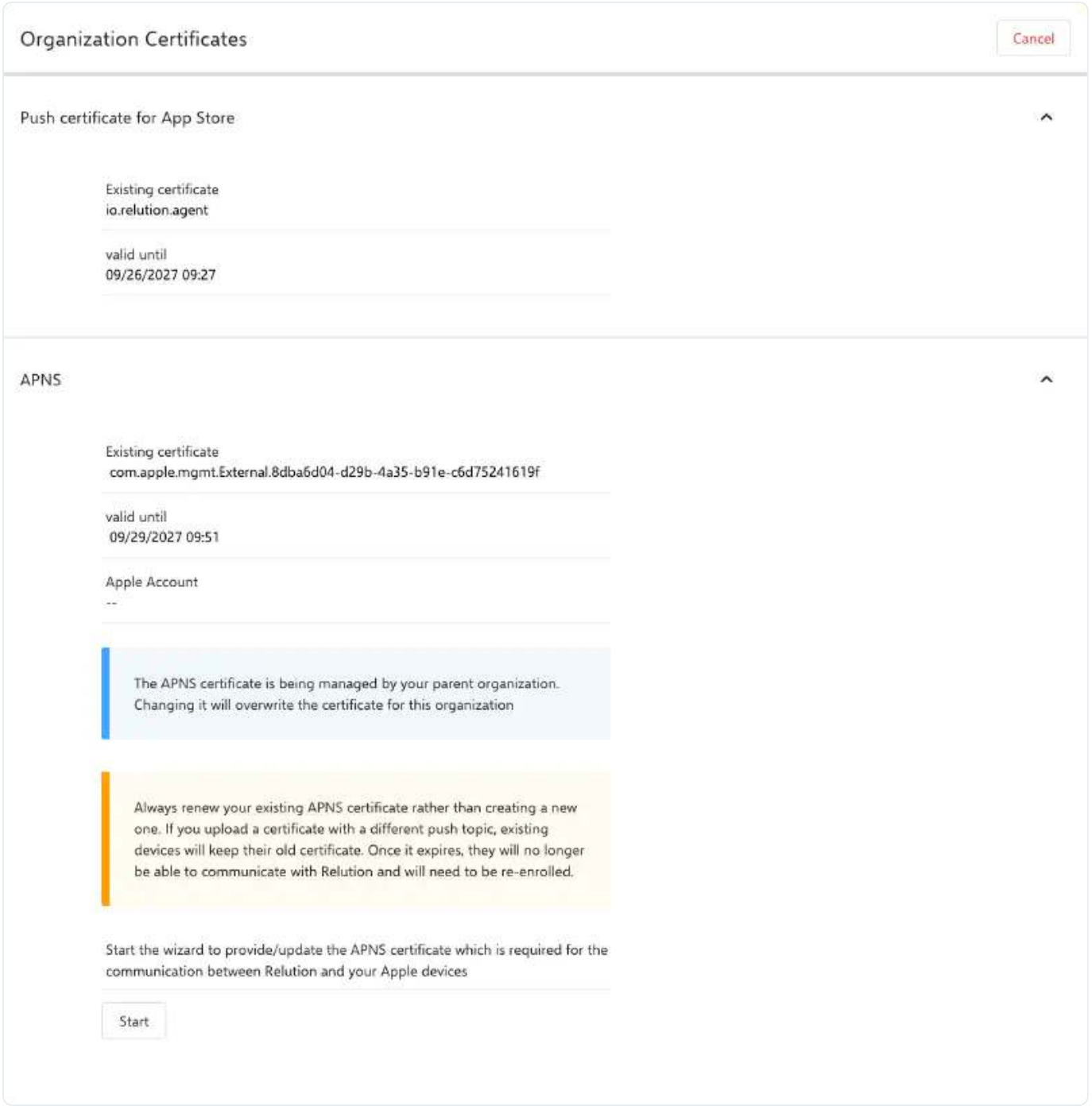
When creating or changing a policy, the Off-time configuration switch can be enabled. When it is enabled, the policy is disabled during all periods defined in the off-time configuration (e.g. school holidays) and is not applied to devices. This also applies if no time-based schedule is set up. The periods are evaluated in the Time zone of the policy, which can also be set without a time-based schedule when off-time is enabled; if no time zone is set, the server's time zone applies.



The off-time configuration has a higher priority than a time-based policy: during an off-time, the policy remains disabled even within its time-based window.

Organization Certificates

To work with the Apple APNS service — responsible for push notifications and submitting profiles to enrolled Apple devices — Relution requires a signed MDM push certificate. If no APNS certificate is configured, the enrollment of Apple devices is disabled and the notification center reports APNS certificate missing. Before and after the certificate expires, the notices APNS certificate will expire soon and APNS certificate has expired are shown.



An existing APNS certificate should always be renewed rather than newly created. If a certificate with a different push topic is uploaded, already enrolled devices keep their old certificate; once it expires, they can no longer communicate

with Relution and must be re-enrolled. When switching from the Relution default certificate to a custom certificate, existing devices continue to use the default certificate until they are re-enrolled.

Information on the page

In the APNS area, the page under `Settings` → `Organization Certificates` shows the push topic (Existing certificate), the expiration date (valid until) and the associated Apple Account for the stored certificate. If no certificate is stored, the notice No certificate configured appears. The Start button opens the Edit APNS Certificate wizard.

In regular organizations, the Push certificate for App Store area additionally shows the push certificate for the App Store with its expiration date; this area is for display only.

An APNS certificate stored in the global organization or a meta organization applies to all sub-organizations that do not have their own APNS certificate defined. If a custom certificate is stored in a sub-organization, it overrides the inherited certificate for this organization. A notice on the page indicates whether the certificate is inherited or managed by the parent organization.

Default certificate (existing installations)

Existing Relution installations may use the Relution default certificate (`com.apple.mgmt.mway.mwaysolutions`). This certificate is updated automatically with each Relution update — no manual action is required. See Update →.

As of Relution 26.3.0, new installations no longer use the Relution default certificate. New instances must provide their own certificate via the self-service wizard.

For existing installations still using the default certificate, switching to the self-service wizard is recommended — especially when setting up new organizations — as the Relution default certificate is planned to be phased out in a future release.

For version 26.4.0

Setting up a custom certificate

The self-service wizard in `Settings` → `Organization Certificates` covers the full process: Relution generates a signed CSR automatically, the CSR is uploaded to Apple, and the resulting certificate is brought back to Relution — no support ticket required.

Set up or renew APNS push certificates →

Migration from the previous workflow

If the installation previously used a certificate provided via the Relution Helpdesk, a migration notice appears on this page, followed by the entry Migrate your old APNS certificate with a Migrate button. Migration is a single-click operation and does not affect enrolled devices. As long as the migration is pending, the wizard (Start) is not available.

After migrating, the self-service wizard is available for all future renewals.

Full migration and setup guide →

Secure Mail Gateway

With the Secure Mail Gateway (SMG), Relution offers the possibility to connect to an Exchange server without making it available on the internet. Relution works as a proxy for the communication via Exchange Active Sync (EAS). The use of SMG requires the availability of basic auth on the Exchange server. Modern auth is not supported.

> The SMG service must be reachable by devices on port 443. To do this, the reverse proxy forwards the path `/Microsoft-Server-ActiveSync` to the SMG service (port 8093). The SMG service must be able to reach the Exchange server (Exchange URL) and the Relution server. A connection from the Exchange server to the Relution server is not required.

It is recommended to configure the restrictions options only after the connection has been successfully tested to exclude possible errors. Once the connection has been successfully tested and one can work with the endpoints, the permissions can be configured accordingly.

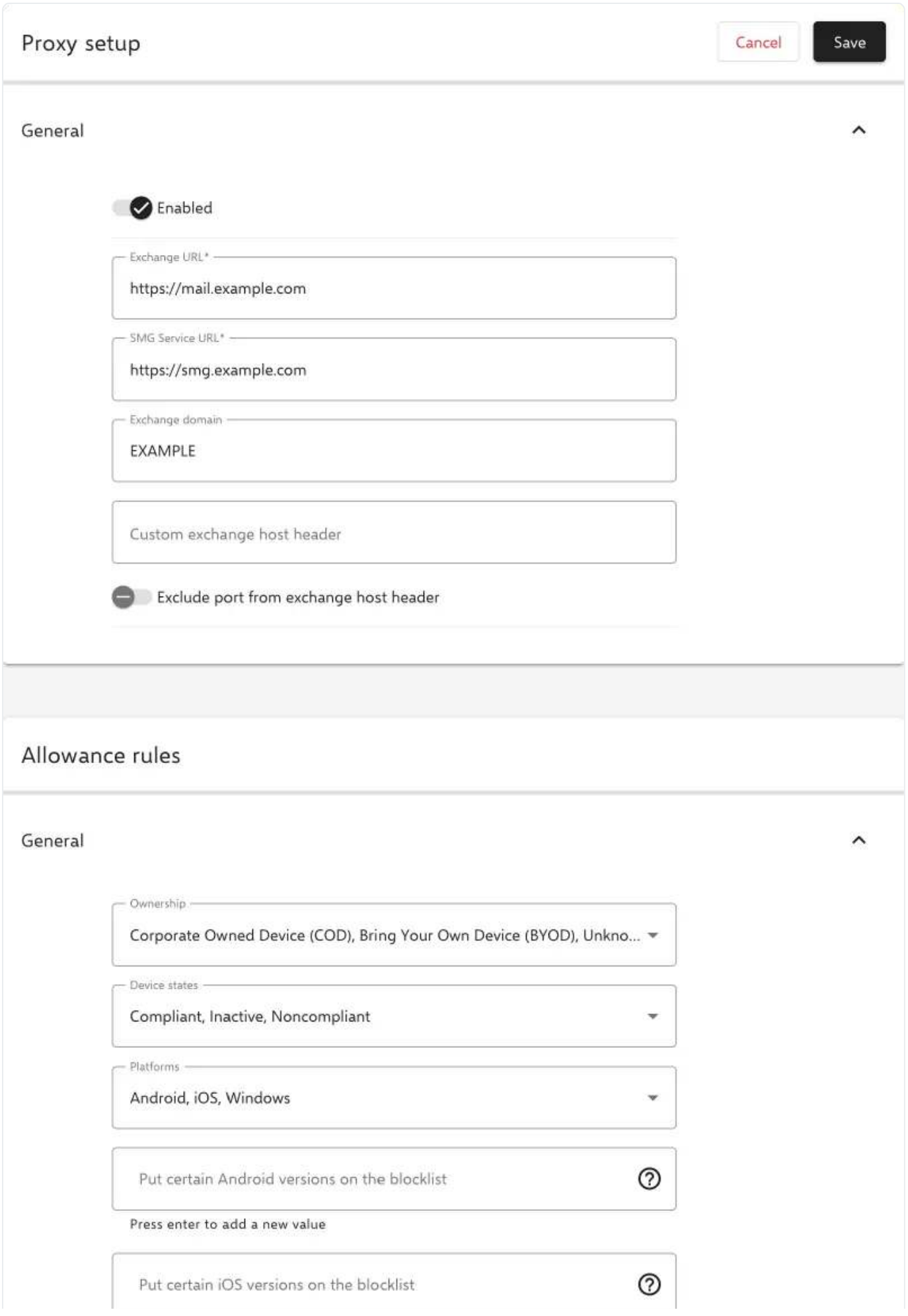
> Breaking change with Relution 26.4.0: From version 26.4.0, the SMG feature requires a dedicated standalone service. Setup instructions: Secure Mail Gateway →.

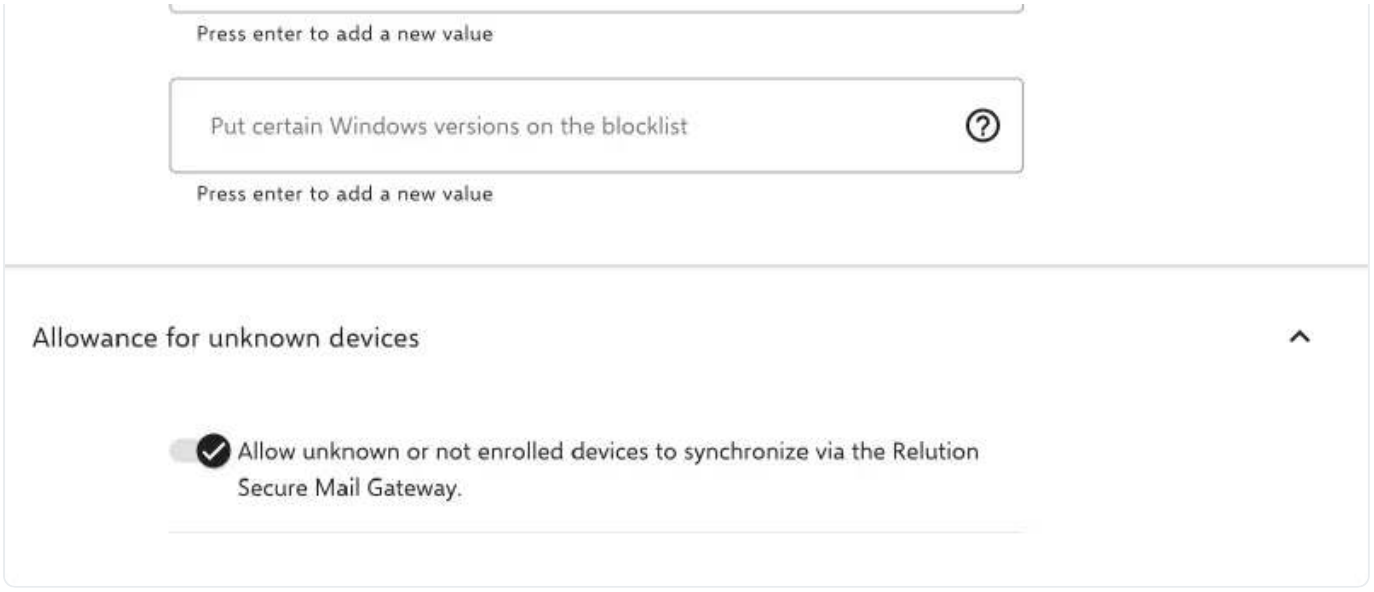
Configuration of the Secure Mail Gateway

New in 26.4

The settings are located under `Settings` → `Device Management` → `Secure Mail Gateway`. They apply per organization; the tile is not available in the global organization.

For version 26.4.0


Proxy setup
Cancel
Save
General
Enabled
Exchange URL*
https://mail.example.com
SMG Service URL*
https://smg.example.com
Exchange domain
EXAMPLE
Custom exchange host header
Exclude port from exchange host header
Allowance rules
General
Ownership
Corporate Owned Device (COD), Bring Your Own Device (BYOD), Unkno...
Device states
Compliant, Inactive, Noncompliant
Platforms
Android, iOS, Windows
Put certain Android versions on the blocklist
Press enter to add a new value
Put certain iOS versions on the blocklist



Proxy setup

- Enabled Turns on the SMG for the organization. If the toggle is off, the other fields are locked, and the option Use Secure Mail Gateway cannot be turned on in the Exchange configurations of policies.
- Exchange URL The address where the Exchange server can be reached. Mandatory field.
- SMG Service URL The publicly reachable URL of the SMG service. This can be a dedicated subdomain (e.g. `https://smg.yourserver.example.com`) or the same URL as the Relution server — provided the reverse proxy forwards `/Microsoft-Server-ActiveSync` to the SMG service correctly.

  This field is available as of Relution 26.4.1 and is mandatory. If a URL is entered that differs from the Relution server URL, existing Exchange configurations do not adopt the new host automatically. A new version must be created in every policy containing an Exchange configuration. In the Exchange configuration, the option Use Secure Mail Gateway must be enabled so that the host is set to the new SMG Service URL. The policy must then be published.
- Exchange domain The corresponding domain of the Exchange server to be accessed. Optional; if set, the SMG uses this domain when forwarding requests to the Exchange server (see Technical overview →).
- Custom exchange host header Optional value for the host header used when communicating with the Exchange server. If a value is entered, it replaces the host header that is otherwise derived from the Exchange URL.

Allowance rules

The allowance rules define which devices enrolled in Relution may synchronize with the Exchange server via the SMG. A request is only forwarded if the device meets all rules.

For version 26.4.0

- Ownership Allowed ownership types: Corporate Owned Device (COD), Bring Your Own Device (BYOD) and Unknown. By default, all are selected.
- Device states Allowed device states: Compliant, Inactive and Noncompliant. By default, only Compliant is selected; inactive and noncompliant devices are rejected.
- Platforms Allowed platforms: Android, iOS and Windows. By default, all are selected.
- Put certain ⋯ versions on the blocklist A separate field appears for each selected platform, e.g. Put certain iOS versions on the blocklist. Devices running one of the listed operating system versions are rejected.

A connection should be established first and the function tested before any restrictions are configured.

Allowance for unknown devices

The toggle allows unknown or non-enrolled devices to synchronize via the SMG, e.g. notebooks or PCs that cannot be enrolled in Relution. A device counts as unknown if Relution cannot match the request to an enrolled device. The option is enabled by default. If it is disabled, enrolled devices may also be rejected during the initial account setup as long as Relution cannot yet identify them.

Use in policies

For devices to use the SMG, the option Use Secure Mail Gateway is enabled in the Exchange configuration of a policy, e.g. for iOS → or Windows →. Exchange Host and Exchange Domain are then set automatically. If the platform or an operating system version is blocked in the SMG settings, the configuration shows a warning.

For version 26.4.0

Technical overview

For Exchange configurations using SMG, the SMG Service URL without the protocol (`https://`) is set as the server address on the device, so the device connects to the EAS endpoint `<SMG Service URL>/Microsoft-Server-ActiveSync`. The domain is set to the unique name of the organization. Relution uses the domain to identify the corresponding SMG settings.

If SMG is enabled and configured in these settings, the request headers `DeviceId` and `DeviceType` are evaluated to identify the device triggering the request. Depending on the SMG settings, if the device could be identified at all, and the properties and status of the device (see section Allowance rules), the request is denied or forwarded to the Exchange host configured in the SMG settings and the response is delivered back to the device. The domain is adjusted to the one configured in the SMG settings if present.

Password

Exchange and SMG use BasicAuth, here it is possible that account errors may occur on the end device when using special characters such as `$ # / * ü ö ä` and `space`.

To check this, a simple password consisting of letters and numbers should be used for testing.

---

macOS

MacOS uses the Exchange connection via EWS. However, the SecureMailGateway can only forward ActiveSync. Therefore, it is currently not possible to use macOS devices with SMG.

For version 26.4.0

Data Processing Agreement (DPA)

To ensure full GDPR compliance, the controller must conclude a Data Processing Agreement (DPA) with the operator of the Relution environment (the processor). The Create new DPA area allows this agreement to be configured and signed entirely digitally.

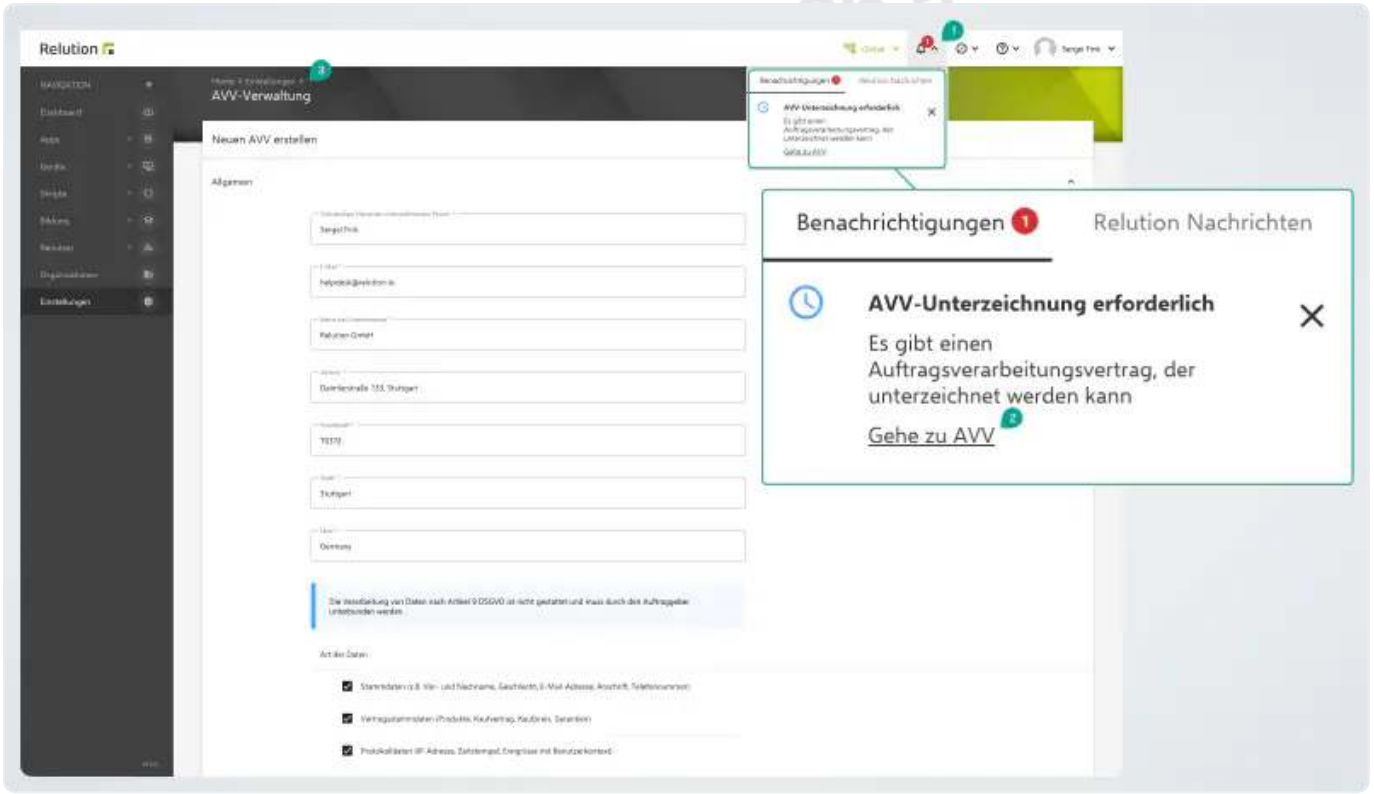
Relution thereby supports an efficient, transparent, and legally compliant conclusion of Data Processing Agreements between Relution GmbH and the customer.

As long as the current DPA version has not been signed in an organization, the message DPA signing required appears in the notification area (1). It is shown to users with the DPA Management → Update permission. When a new DPA version is provided, the message appears again; the form is then prefilled with the details of the last signed version.

The DPA can be concluded individually for each tenant. Alternatively, it can be concluded for all subordinate organizations in the global organization or in a meta organization using the Sign for all sub-tenants option. In these organizations, the message and the DPA settings are then no longer shown.

The DPA settings can be accessed in two ways:

1. Directly via the notification (1 + 2) in the notification area.
2. Via the menu path (3): `Settings` → `General` → `DPA Management`



1. General Information

This section serves to clearly identify the signatory and the legal entity concluding the agreement. The person completing this section must be authorized to sign on behalf of the organization.

Field	Description
Full name of the signing person	The name of the person who signs the agreement in a legally binding manner.
Email	The email address of the signing person.
Company name	The official name of the organization (the controller).
Address, postal code, city, country	The official address of the organization.

Name and email are prefilled with the data of the signed-in user, company name and address with the details from the general organization settings. The values can be adjusted before signing.

---

2. Important Note on Art. 9 GDPR

For version 26.4.0

The highlighted blue notice applies:

> The processing of data pursuant to Article 9 GDPR is not permitted and must be prevented by the Controller.

Background: Article 9 GDPR governs special categories of personal data (e.g., health data, ethnic origin, political opinions). Since Relution is an MDM system that primarily processes technical and administrative data, the processing of these highly sensitive data categories is not permitted in standard operation and must be prevented by the controller.

---

3. Type of Data

This section defines which categories of personal data are processed on behalf of the organization as part of using Relution. All applicable categories whose data occurs in the Relution instance are checked:

- Master data (e.g., first and last name, gender, email address, address, phone number)
- Contract master data (products, purchase contract, purchase price, warranties)
- Log data (IP address, timestamp, events with user context)
- User-generated content (e.g., forum posts, feature requests, support requests)
- Device data (device type, device number, IP address, operating system information, installed apps)
- Location data (iBeacons, GPS position, cellular network, WiFi networks)

If needed, further data categories not listed here can be added via Add other.

At least one data category must be selected or added via Add other, otherwise Preview and Sign DPA remain disabled.

4. Group of People Affected

This section specifies which groups of people are affected by the data processing in the Relution instance:

- Parents and parent representatives
- End customers and suppliers
- Employees (e.g., workers, teachers, trainees, administrative staff)
- Students

Here too, further groups not included in the list can be added via Add other. At least one group must be selected or added here as well.

5. Emergency Contact

This section contains the contact details of the person in the organization who can be contacted immediately in the event of a data breach or other security-relevant emergencies. Name and email are mandatory, the phone number is optional.

- Name
- Email
- Phone

For version 26.4.0

6. Conclusion and Signature

Before concluding the agreement, the signing authority must be confirmed:

- Confirmation of signing authority: Confirms that the signer is authorized to conclude the agreement on behalf of the organization.

In the global organization and in meta organizations, the optional Sign for all sub-tenants selection is also available. It is relevant if the parent instance (e.g., a school authority) also concludes the agreement for subordinate, managed units (e.g., individual schools). If it is set, the DPA also applies to all subordinate organizations; no separate DPA is offered there anymore.

The following actions are available for concluding the agreement:

- Preview: Shows the complete agreement text in advance. Available as soon as the general information as well as type of data and group of people affected are filled in.
- Sign DPA: Concludes the agreement digitally. The DPA is thereby legally valid. The button only becomes active once the emergency contact (name and email) has also been entered and the signing authority has been confirmed.

The signed document should be kept carefully as part of the documentation obligations (accountability under GDPR).

When the DPA is signed, the agreement details are automatically transmitted to the Relution license server. The following is transmitted:

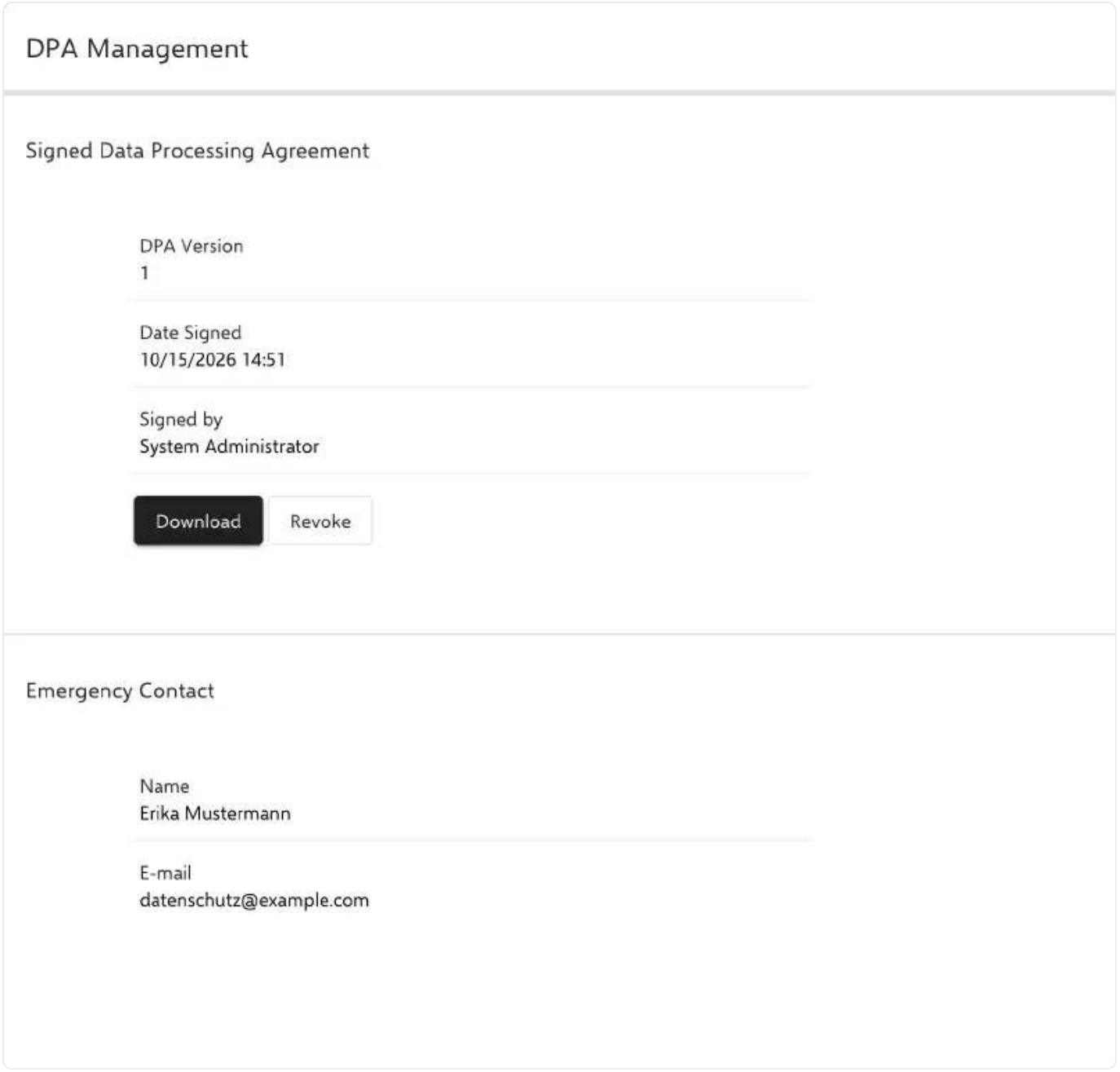
- the details from the form: signing person and email, company name and address, type of data, group of people affected, emergency contact, and the Sign for all sub-tenants selection
- the time of signing, the IP address and the Relution user name used for signing

The PDF documents of the DPA are not transmitted to the license server. Without this transmission, the DPA cannot be signed.

After signing, the DPA is sent as a PDF in German and English by email to the email address entered for the signing person. If sending fails, the signature remains valid.

Signed DPA

After signing, DPA Management shows the Signed Data Processing Agreement area with DPA Version, Date Signed, Signed by and the Emergency Contact. In the global organization and in meta organizations, Signed for sub-tenants is shown as well.



- Download: Downloads the signed DPA as a PDF, in German if the portal language is German, otherwise in English.
- Revoke: Revokes the signed DPA. The time and user of the revocation are transmitted to the Relution license server. The DPA is then offered for signing again.

Permissions

The DPA permissions are found in the roles in the DPA Management permission group:

- Read: Shows the overview of the signed DPA.
- Update: Shows the message and the signing form.
- Delete: Allows revoking a signed DPA.

The Administrator role contains all three permissions. As long as no DPA has been signed, users without the Update permission only see the note No DPA has been signed yet instead of the form.

Notes on Signing the DPA

If the signatory is not authorized to sign the Data Processing Agreement (DPA), the following procedure applies:

- Account creation: A separate account is created for the colleague who is authorized to sign, in the organization for which the DPA is concluded. The account requires a role with the DPA Management → Update permission (e.g. the Administrator role); without this permission, neither the DPA notification nor the signing form is shown.
- Signing: The colleague can then log in to the portal and sign the DPA independently.

Relution 26.0.0

For version 26.4.0

Language Settings

In Relution, the interface language can be set for each user, and the languages in which content such as app descriptions and notifications is maintained can be configured.

Organization languages and default language

Under `Settings` → `General` → `Languages`, the languages in which content is maintained in Relution are defined. Each added language provides additional localized fields, for example app names and descriptions, texts for enrollment and app notifications, and support information. These languages are independent of the language of the Relution interface, which each user sets individually (see User Language).

German and English are available in every organization by default. A new organization adopts the default language of the global organization as its default language; out of the box, this is English.

- Additional languages can be added using Add. Numerous languages and regional variants (locales) are available, for example Dutch, Polish or German (Austria), regardless of the interface languages. Missing content for a new language is copied from the default language.
- A language is set as the default via the 3-dot menu → Make default. Before the change, a confirmation dialog appears: translations for existing apps, enrollment notifications and app notifications should be available in the new language beforehand, as missing translations may lead to errors during enrollment.
- A language is removed using Delete. The default language cannot be deleted.

The default language is used for push notifications, for example app notifications sent via push or push messages from a device group action of the type Notification action, and for emails to additionally entered email addresses without a Relution user account. In addition, newly created users without their own language setting receive the default language as their user language if it is one of the supported interface languages, otherwise English.

Emails to Relution users, for example for resetting the password or about apps, are sent in the recipient's user language. If no translation exists for it, they are sent in English.

User Language

The user language can be set individually by each user and affects the entire interface in Relution. This means, for example, the dashboard, policies, and tables will be displayed in the selected language. Emails that Relution sends to the user also follow this language.

The setting can be found in the user menu at the top right under `Profile`. On the User information tab, the Preferences card contains the Language entry. The language is changed using the pencil icon (Edit Language).

Supported languages

Relution currently supports the following languages in its graphical user interface:

For version 26.4.0

- German
- English
- French
- Italian
- Spanish
- Turkish

For version 26.4.0

REST API

All of Relution's functionality is available through an extensive REST API. This API can be used to control Relution from any other application or via scripts.

API Documentation

Every Relution server ships the complete API specification, matching exactly the installed server version. It documents all endpoints with their parameters, request and response bodies, and the returned status codes.

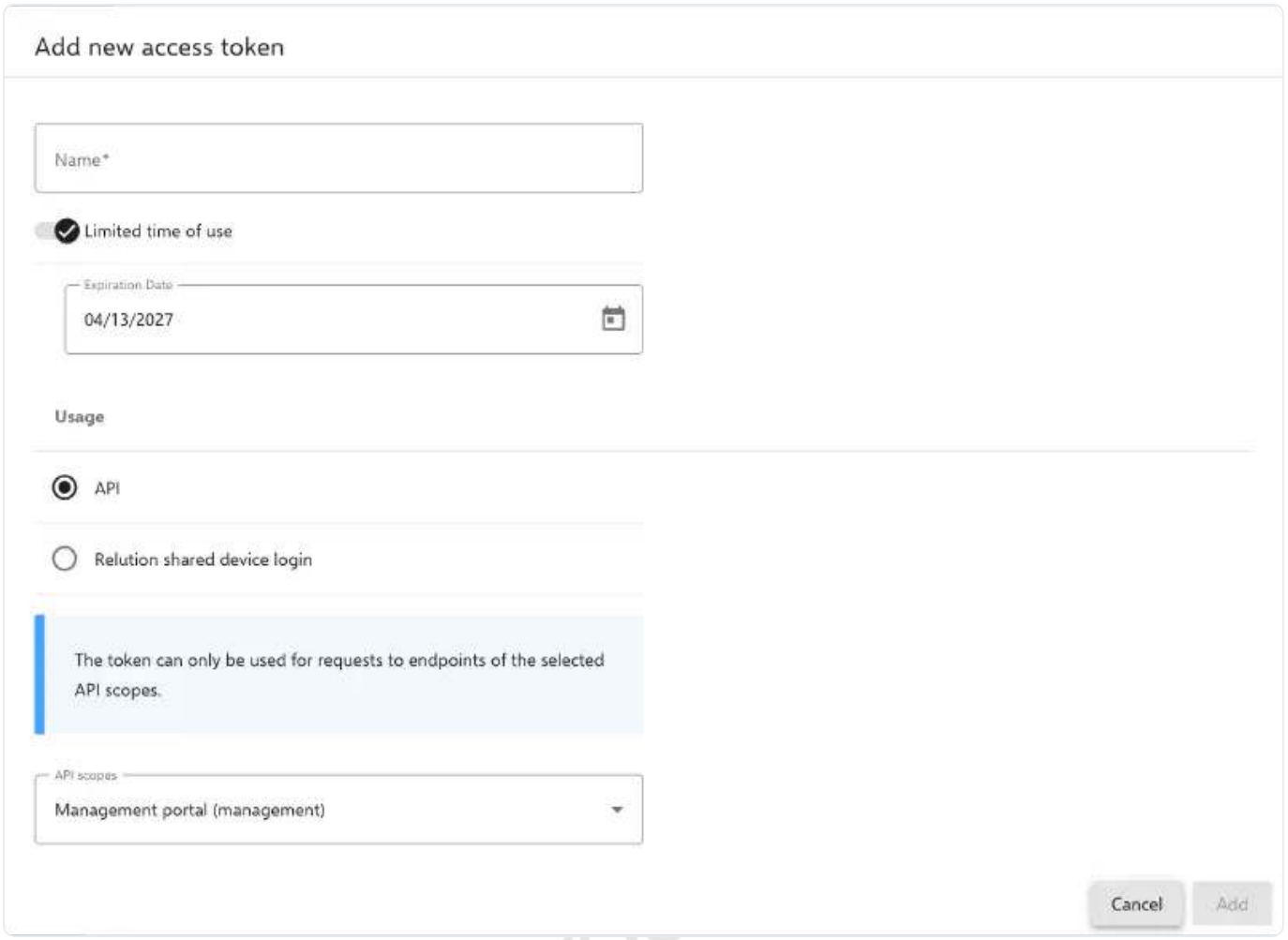
The specification is opened from the Relution portal: the entry Web API in the support menu (top right corner) opens the interactive documentation. Alternatively, it is available directly at `https://<server>/web-api/index.html`.

Requests to the REST API are subject to the same permission checks as actions performed in the portal, and security-relevant actions are recorded in the Audit Log →.

Create API Access Tokens

To access Relution from third-party systems or scripts, an API Access Token is required.

For version 26.4.0



1. Clicking the username in the upper right corner of the Relution portal opens the user menu.
2. The token is created under `Profile` → `Access tokens` → `Add`.
3. The token is given a name and copied.

The following options are also available when creating a token:

- Limited time of use: enabled by default. The Expiration Date is preset to today plus 180 days and can be changed later via Edit Access Token. If the option is disabled, the token does not expire.
- API scopes: The token can only be used for requests to endpoints of the selected scopes (multiple selection, default: Management portal). The examples in this article use endpoints under `/api/management/` and require this scope.

The token is passed in the `X-User-Access-Token` HTTP header to authenticate requests.

Administrators with the permission to create API access tokens can also create a token for another user, for example for a service account. To do so, exactly one user is selected under `Users` → `Users` and the action Add Access Token is called from the context menu.

> The token will only be displayed once when it is created.

---

1. Users in CSV File Format

- The first line of the `.csv` file contains a header line with the desired property names.
- The order of the columns is not relevant.
- Properties that are not needed can be omitted.
- Mandatory fields: The header line must contain the `email` column, and every row needs a user name in the `name` column. The portal template starts with the following columns:

```
name,email,givenName,surname,password
```

Column names are not case-sensitive. Passwords must follow the policy under `Settings` → `Login Management`. Phone numbers must be in international format, e.g. `+4912345`.

Up to 15 custom properties can be added, named: `custom1` – `custom15`

The portal template contains further columns, such as `disablePasswordAuthentication`, `locale`, `permissions`, `memberOfGroups`, `teacherOfClasses` and `studentOfClasses`. Their meaning is described in the article CSV Import →.

👉 A template can be downloaded in the Relution portal: `Users` → `Users` → `Three dots menu` → `Import users via CSV`. In the dialog, it is available via the template link in the description text.

Example CSV:

For 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. Uploading Users via the Relution Portal

1. The import is opened via `Users` → `Users` → `Three dots menu` → `Import users via CSV`.
2. The CSV file and the separator are selected. The option Automatically create groups and classes creates groups and classes that are named in the file but do not exist yet.
3. The imported users can be assigned to one or more groups.
4. Imported users will then appear in the overview.

3. Creating Users via the Relution API

Relution 5.34 change:

- User import is now a background job with the states CREATED, RUNNING, FINISHED and FAILED.
- Each job stores a report per line.
- Legacy import was removed.
- Some column names changed:
  - `first name` → `givenName`
  - `last name` → `surname`
  - `managed apple id` → `managedAppleId`
  - `phone number` → `phone`
  - `userId` → `name`

For version 26.4.0

Steps

1. A `users.csv` file is prepared.
2. The bash script below is copied into a file, e.g. `uploadUserCSV.sh`.
3. The file is made executable:

```
chmod +x ./uploadUserCSV.sh
```

4. The script is then run:

```
./uploadUserCSV.sh -f 'FILEPATH' -h 'HOST' -a 'YOUR-ACCESS-TOKEN'
```

Arguments

Argument	Meaning	Example	Default	Required
`-f`	Path to the `users.csv`	user.csv		✅
`-h`	Relution host	https://relution.io		
`-a`	API access token	xxxxxxxx		
`-r`	Group (name or UUID) the imported users are assigned to; spaces as `%20`	School%20Teachers	`Organame%20Device%20User`	❌
`-s`	Separator for parsing	SEMICOLON	COMMA	
`-w`	Overwrite existing users	true	false	❌

- Users are imported into the organization of the account that owns the API access token. This account needs the permissions to create and update users.
- Without `-r`, the script uses the group `Organame Device User`. “Organame” has to be replaced in the script with the name of the own organization; otherwise no group is assigned.
- With `-w true`, existing users are overwritten; they are matched by the `name` column. Users that originate from an external directory such as LDAP are skipped.
- The API additionally supports the parameter `createMissingGroupsAndClasses=true`. It corresponds to the portal option Automatically create groups and classes and is not set by the script.

For version 26.4.0

Output Example

```
============
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. Bash Script: Upload Users via CSV

Show full configuration example

5. Create a New Organization

The following script creates a new organization including an organization administrator. The token used belongs to a user with the permission to create organizations or sub-organizations, for example the system administrator. The short name `orgaName` is required; the administrator details (`orgaAdminUser`, `orgaAdminGivenName`, `orgaAdminSurName`, `orgaAdminPwd`) are required as long as `skipAdminCreation` is not set to `true`. The administrator password must meet the default password policy. On success, the server responds with HTTP status 202 and returns the UUID of the organization, its name and the UUID of the administrator.

Show full configuration example

6. Query Devices in an Organization

Show full configuration example

API Token Best Practices

- API access tokens should always have an expiration date. Tokens without expiration remain valid indefinitely.
- Tokens should be revoked immediately when the associated account's role changes, the account is deactivated, or the account holder leaves the organization.
- Token secrets are stored only as hashes (SHA-256, or HMAC-SHA-256 if an HMAC key is configured) and cannot be recovered after creation. When needed, a new token is generated rather than attempting to retrieve an existing one.

Related Topics

- Create API access tokens in Relution → — Instructions for generating tokens.
- LDAP / Active Directory connection → — Synchronize users and groups.

For Version 26.4.0

Audit Log

The audit log makes it possible to track activities in Relution without having to search through logs.

Audit log

The audit log is available under `Settings` → `Audit Log`. Access is controlled by two permissions:

- Audit Log: all records.
- Device Management Audit Log: only records in the device management category.

Organization administrators have both permissions by default. The records of the current organization are shown; in a Meta organization, the records of its sub-organizations are included as well. In the Global organization, the audit log covers the records of all organizations.

The data is saved for 180 days by default and can be searched and filtered within the Relution portal.

The following columns are available for information:

- Date
- Username
- Authenticated device
- Client
- Impersonator
- Method (POST, GET, PUT, DELETE)
- Description
- Endpoint (hidden by default, can be shown via the column selector)
- HTTP Status
- Organization (only in the Global organization and in Meta organizations)
- IP
- Category (only with the Audit Log permission)
- Result
- Event type

For version 26.4.0

Filters are available for method, HTTP status (2xx, 4xx, 5xx), username, authenticated device, client, organization, category, result and event type; the same restrictions as for the columns apply to organization and category.

This allows changes on the server to be tracked; which events are recorded is determined by the server configuration (see Scope of Logging →).

Export

In the three dots menu, Export full Audit Log opens the Audit Log export dialog. Start new export creates a CSV file in the background, which can then be downloaded in the same dialog. Only one export is stored at a time; a new export replaces the previous one. A running export can be stopped via Abort.

Storage Limit Behaviour

Audit records are automatically purged when they exceed the retention period. The default is 180 days; in the server configuration (`application.yml`), the period can be adjusted in days via `relution.cleanup.audit-log.remove-after` (e.g. `365d`, at least 1 day). The cleanup runs roughly every 17 minutes between 18:00 and 07:00 and deletes at most 10,000 records per run in batches of 1,000 to avoid database locks. Every run that deletes records or fails is itself recorded as an Audit Logs cleaned up event in the audit log.

If disk space is exhausted before cleanup runs, new audit records may fail to write. The System Administrator must monitor disk usage and ensure sufficient storage is available for the configured retention period. There is no automatic low-storage notification — this is a System Administrator responsibility.

Scope of Logging

Activation and scope of the audit log are controlled via the `relution.audit-log` block in the `application.yml`; the audit log is enabled by default. In the default configuration, some very frequent device events are not recorded: device identification, changed device settings, and changes to installed apps and certificates. Individual high-volume endpoints are excluded as well, for example device actions and queries of the current device. In the configuration for operation according to Common Criteria (CC-EAL4), full logging is active; these values must not be changed there.

Server start and stop are also recorded as Relution server start and Relution server stop events, each with the server version and cluster node.

For version 26.4.0

nginx Access Logs

The nginx reverse proxy logs incoming HTTP/HTTPS requests. These logs complement the Relution application audit log for the network channel layer. In the configuration template for operation according to Common Criteria (CC-EAL4), the TLS protocol and cipher suite negotiated for HTTPS requests are recorded as well. The standard template of the Docker installation → does not log these two fields.

Accessing the logs:

```
docker logs nginx
```

Or for real-time monitoring:

```
docker logs -f nginx
```

In the CC-EAL4 template `relution-nginx.conf`, each access log line of the HTTPS ports (443 and 8443) has the following format:

```
<remote_addr> - <user> [<time>] "<request>" <status> <bytes> "<referer>" "<user_agent>"
"<x_forwarded_for>" <request_time> <upstream_time> <pipe> <ssl_protocol> <ssl_cipher>
```

The `$ssl_protocol` and `$ssl_cipher` fields at the end of each line record the TLS version and cipher suite used for that connection (e.g. `TLSv1.3 TLS_AES_256_GCM_SHA384`). Requests on port 80, which are redirected to HTTPS, are logged in the default format of the nginx image without these fields.

The error log is written to `stderr` and is also accessible via `docker logs nginx`.

Audit Event Reference



Device Management Events



General Events

Server Log References

For version 26.4.0

Encryption/Decryption integrity failures:

```
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="{}"
```

Cryptographic key derivation (the `TLS_KEY_DERIVATION` line is written once at server startup):

```
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 channels:

```
TLS_CHANNEL_ATTEMPT host={} port={} tls={} cipher={} cert_subject="{}"
cert_fingerprint={}
TLS_CHANNEL_SUCCESS host={} outcome=SUCCESS
TLS_CHANNEL_FAILURE host={} outcome=FAILURE reason="{}"
```

The messages about TLS connection attempts and successful connections can be suppressed via `logging.level.io.relution.security.audit.tls.channel: WARN`; error messages (`TLS_CHANNEL_FAILURE`) are still logged.

For version 26.4.0

License Management

Device licenses are required to configure devices in Relution. These licenses can be obtained either directly from the sales team or from a partner. Once purchased, the licenses are assigned either to the server or to the organizations.
If a dedicated server (OnPrem / dedicated cloud server) is used, a limit can also be assigned to the number of licenses for individual organizations (e.g. sites or schools).

This limitation restricts the number of devices registered in an organization according to the number of licenses. The limitation is set per license type that is limited in the server license, e.g. Devices, Users or Native Apps. Each of these license types has its own tab in the license information.
This function ensures that organizations do not use more licenses than are actually required. By default, organizations do not have a limit unless the licenses are explicitly assigned by the sales team.

Prerequisites

- A paid license model; with the free license, the Organization limits section is not displayed.
- Signed in as system administrator in the Global organization. The permissions for license allocations only exist in the Global organization; changing and clearing limits requires the update permission.

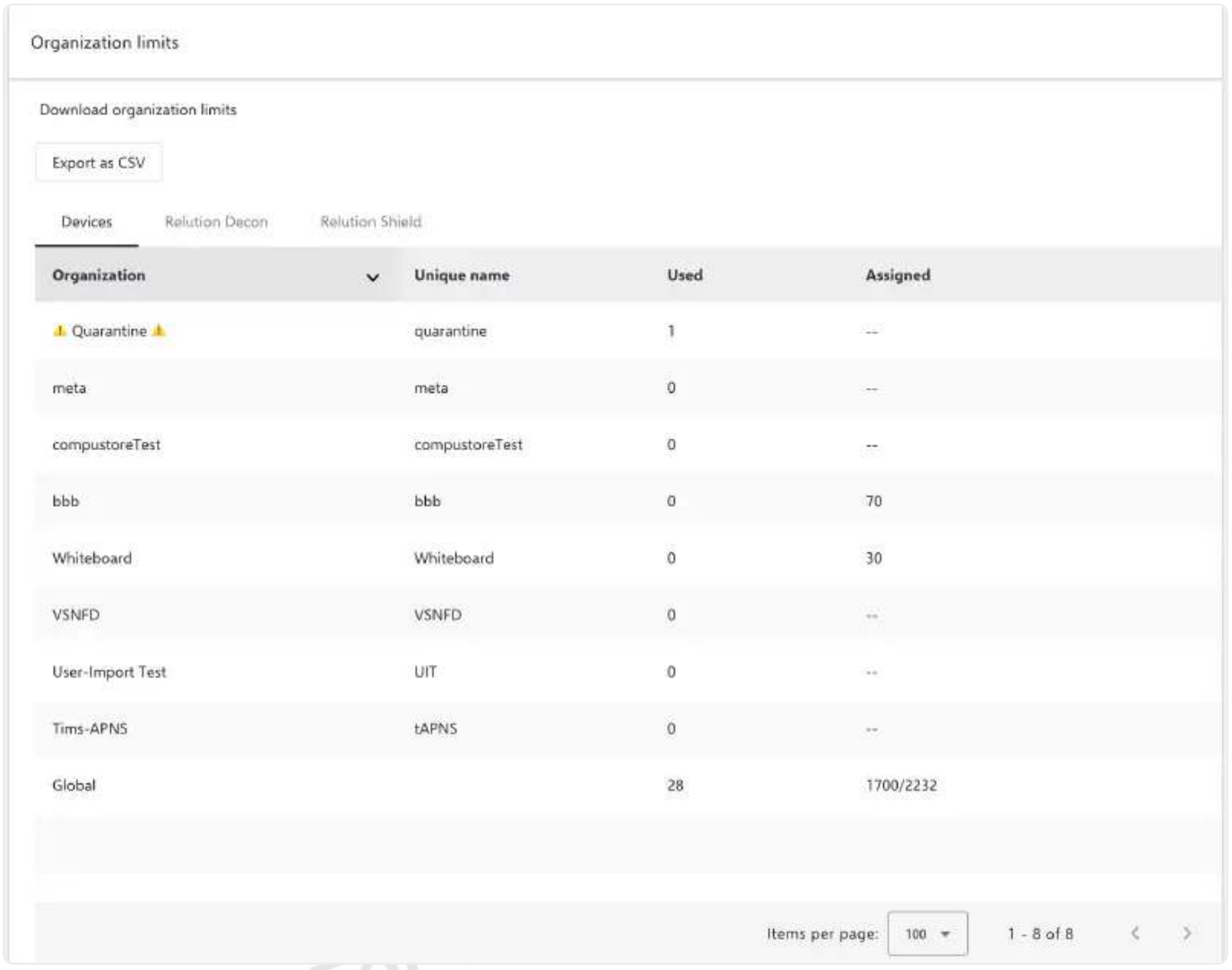
for version 26.4.0

Adjust limitation

1. The system administrator signs in to the Relution portal in the Global organization.
2. In the top right corner, the support menu (question mark icon) is opened and License information is selected. The limits are listed in the Organization limits section.
3. The tab of the desired license type (e.g. Devices) is selected, the organization is located in the list and the button with the three dots is clicked.
4. Edit is selected in the menu. In the Edit organization limit dialog, the desired number is entered in the limit field and applied with Confirm.

The value cannot be lower than the number of licenses already used by the organization (column Used). The column Assigned shows the limit that has been set. The Global row at the end of the table sums up the licenses used by all organizations and compares the total of the assigned limits with the overall limit of the server license.

> The total of the organization limits can exceed the overall limit of the server license; the dialog points this out. Once the overall limit is reached, no organization can consume any more licenses, regardless of its own limit.



Clear limitation

Via the button with the three dots and Clear, the limit of an organization is removed once the Clear organization limit dialog has been acknowledged with Confirm. Afterwards, the organization can use all available licenses.

Export limitations

The Export as CSV button (Download organization limits) in the Organization limits section downloads the limits of the organizations as a CSV file.

Limitation when creating an organization

The limit can be set directly when creating an organization: after the organization has been created, the Allocate licenses button in the Summary step leads to the optional Limits step. This step only appears with a paid license model with limited license types and with the permission to update license allocations. More information under Create organizations →.

For version 26.4.0

Lifetime Licenses

Lifetime licenses are valid permanently for exactly one device. This eliminates recurring annual license costs.

A lifetime license is permanently claimed to the device's serial number (SN) and cannot be transferred to another device.

Binding to the Serial Number

Lifetime licenses must be claimed to a serial number to take effect for a device. Devices whose serial number is claimed to a lifetime license are enrolled even if the device quota of the other licenses is exhausted.

Devices and auto enrollments without a serial number cannot be claimed. The number of claims is limited by the device limit of the lifetime license; once it is reached, further claims are rejected.

> Important: If lifetime licenses are not claimed to serial numbers, enrollment may be limited in mixed environments using lifetime and perpetual/subscription licenses.

For version 26.4.0

Requirement for Use

For lifetime license functionality to be available, at least one lifetime license must be assigned either on the Global organization or on a tenant.

> Assignment can only be made on Global or on one tenant — not on both levels at the same time.

The applicable level is shown in the Assignment type field of the license information: with global-based, the lifetime licenses and their claims are kept in the Global organization, with tenant-based in the respective tenant.

All ways of claiming require the permission to update the License information. Without a lifetime license, the buttons are locked (hint The organization has no Lifetime license).

Supported Platforms

Currently, lifetime licenses are only available for the following platforms:

- iOS / iPadOS
- Android Enterprise

Unsupported platforms continue to be licensed using other license types, e.g.:

- Perpetual – remains valid until cancellation
- Subscription – remains valid until the defined end of life (EoL)

No Revocation Possible

It is not possible to withdraw lifetime licenses that have already been assigned.

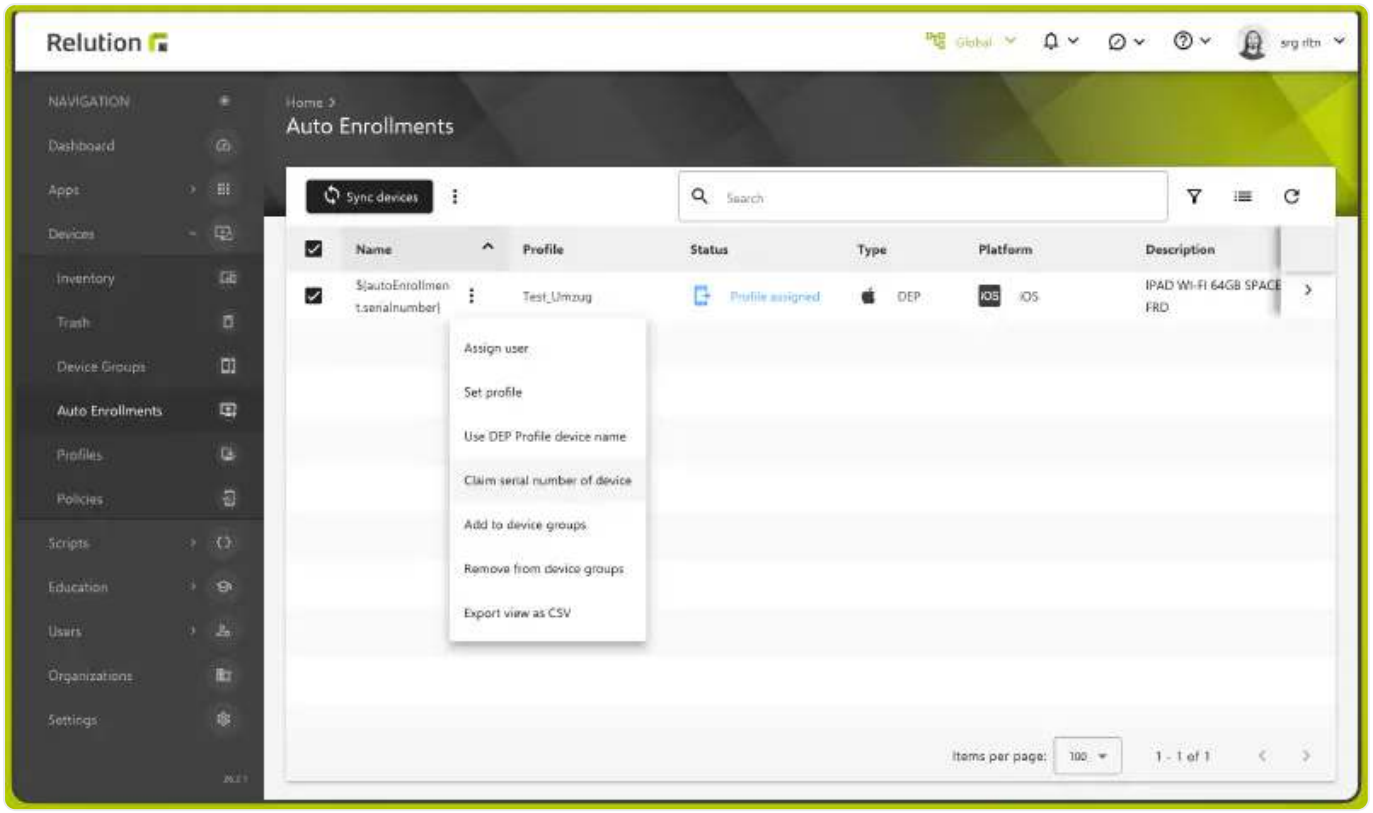
Ways to Assign Lifetime Licenses

There are currently 4 ways to assign lifetime licenses:

1. Via Auto-Enrollments

Lifetime licenses can be assigned on the Global / Tenant level via auto-enrollments. To do so, the desired entries are selected under `Devices` → `Auto Enrollments`. Then the action Claim serial number to lifetime license is chosen and the dialog is confirmed with Claim serial numbers to lifetime license. The claim cannot be undone.

The action is only available if a lifetime license exists and all selected entries have a serial number and belong to the same organization.

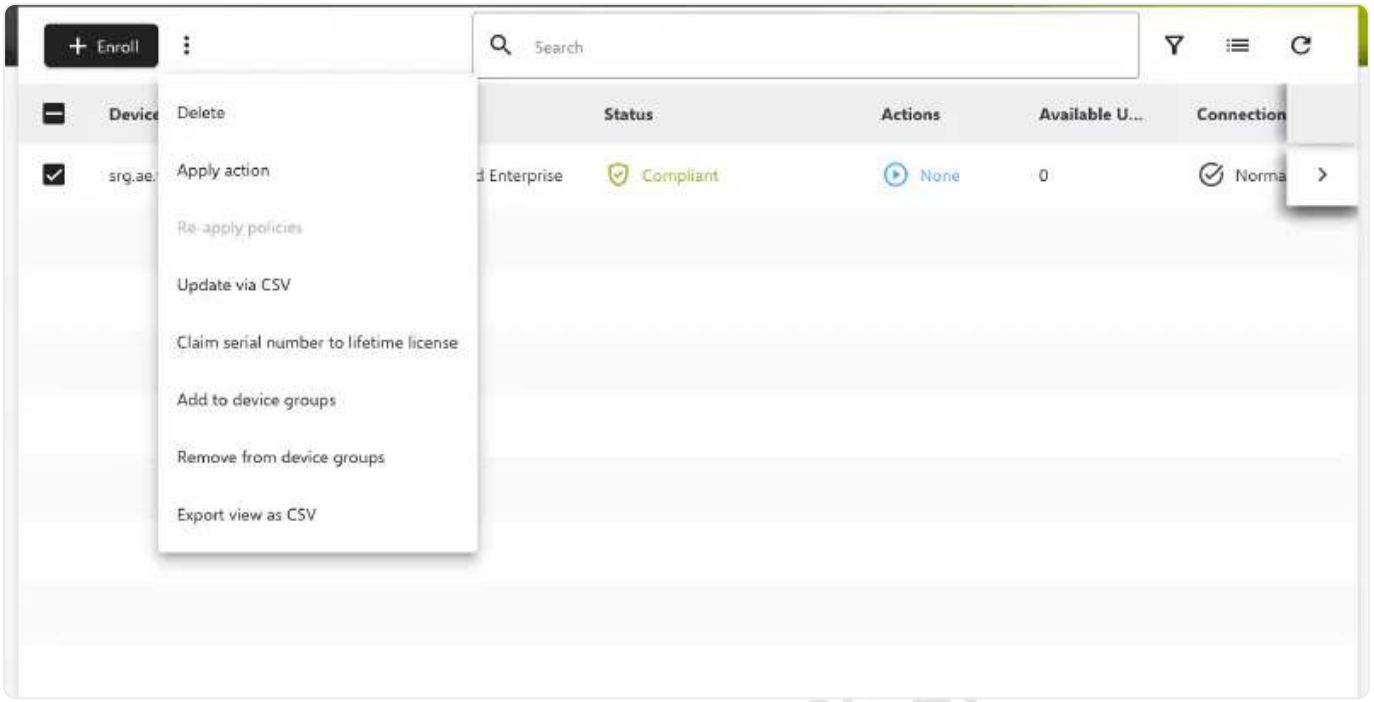


2. Directly in the Inventory for a Device

Assignment can be made directly in the inventory on the device. To do so, the desired devices are selected under `Devices` → `Inventory`, the action Claim serial number to lifetime license is chosen and the dialog is confirmed with Claim serial numbers to lifetime license.

Requirements:

- the assignment is made on the tenant
- the device has a serial number
- all selected devices belong to the same organization

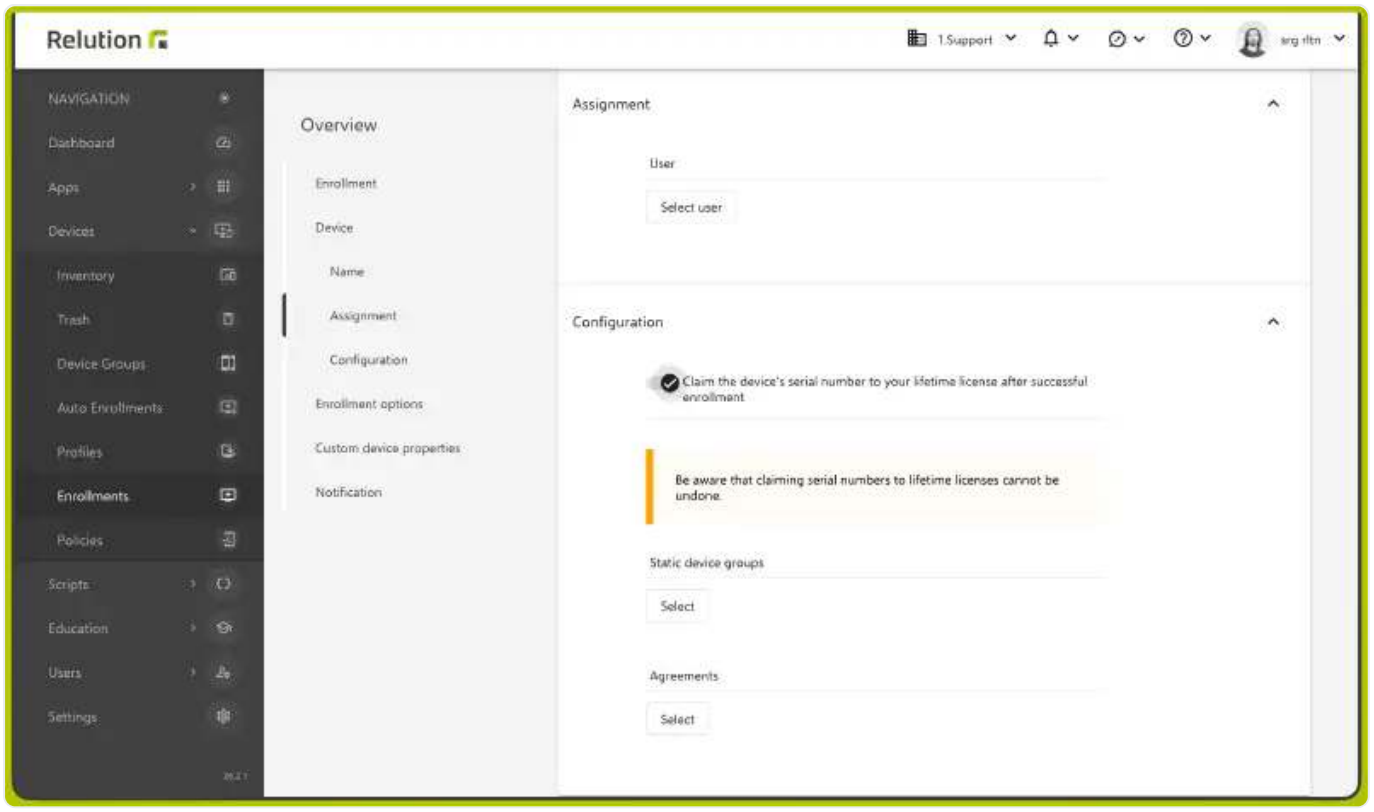


3. During Manual Enrollment on a Tenant

Lifetime licenses can be assigned as part of a manual enrollment on a tenant. When an enrollment for iOS / iPadOS or Android Enterprise is created under `Devices` → `Enrollments`, the Configuration section contains the toggle Claim the device's serial number to your lifetime license after successful enrollment.

The toggle is only displayed if a lifetime license is available to the organization. It can only be set when the enrollment is created, not when it is edited later. Relution claims the serial number to the lifetime license only after successful enrollment. This claim cannot be undone.

> For iOS / iPadOS, Relution checks the device license before enrollment. If no perpetual or subscription licenses are left in a mixed environment, the enrollment fails. In this case, the serial number is claimed beforehand via auto-enrollments or a CSV upload (ways 1 or 4).



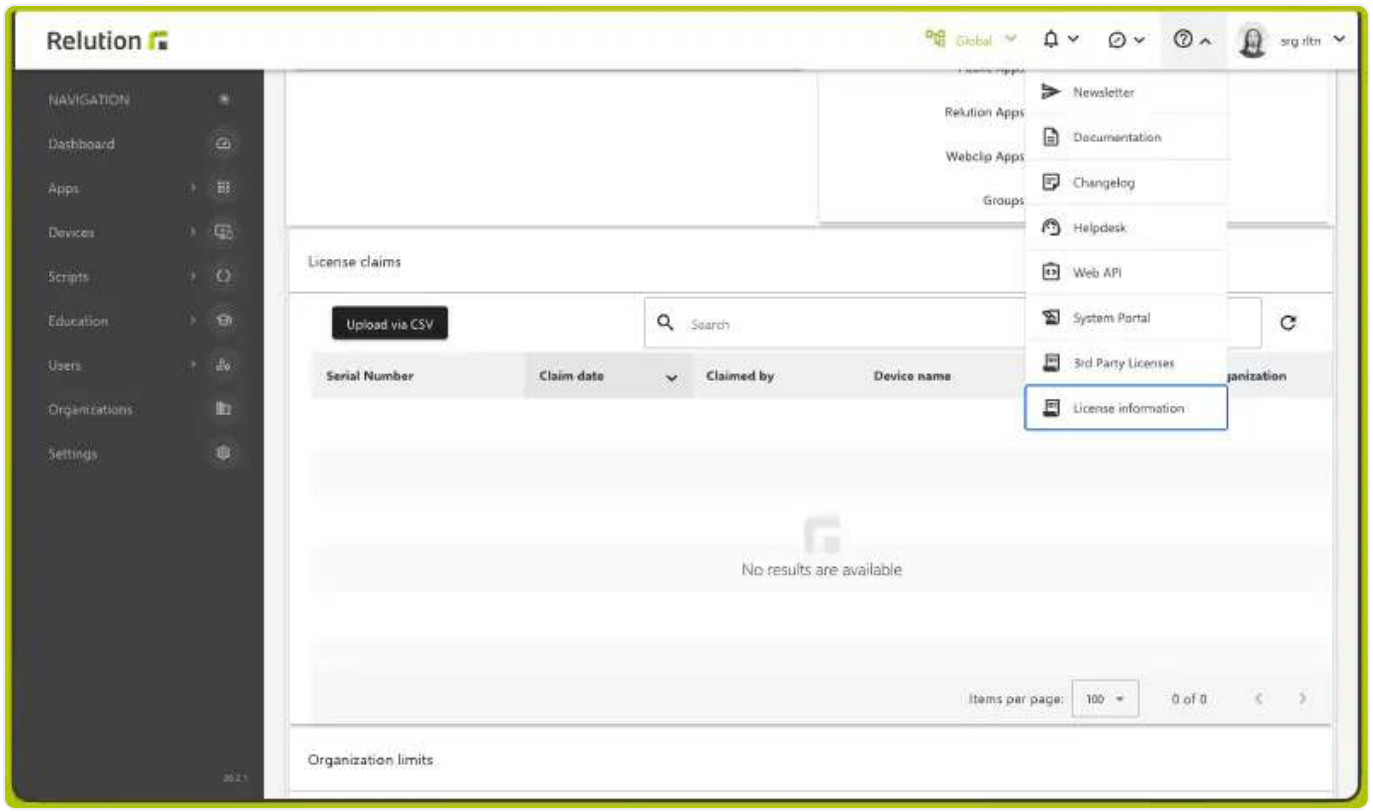
4. Via CSV Upload

Assignment is also possible via CSV upload. To do so, the support menu (question mark icon) in the top right corner is opened and License information is selected. In the License claims section, the Upload via CSV button opens the import. The CSV file contains a `serialNumber` column with one serial number per line.

The License claims section only exists if a lifetime license is available. Where it appears depends on the Assignment type: with global-based only in the Global organization, with tenant-based only on the tenant where the lifetime licenses are stored.

Serial numbers that have already been claimed are skipped during the import. Once the device limit of the lifetime license is reached, the remaining lines are reported as failed.

For Version 26.4.0



Overview of Claims

The License claims section of the license information lists all serial numbers claimed to the lifetime license, regardless of how they were claimed. Among other things, Claim date, Claimed by, Device name and Organization are shown for each entry.

Summary

- Lifetime licenses are valid for the lifetime of a single device
- they are permanently claimed to the serial number
- transfer to another device is not possible
- lifetime licenses that have already been assigned cannot be revoked
- currently, only iOS / iPadOS and Android Enterprise are supported
- unsupported platforms still require other license types (e.g. perpetual or subscription)

For version 26.4.0

License Management by Partners

The management of licenses can be handed over to a partner or service provider. To do so, the connection key shown in Relution is passed on to the partner. Relution receives this key from the license server during the license check. Using this key, the partner connects to the organization via the license server and can then manage its licenses.

This connection can be established not only for the Global organization but also for individual tenants that are managed by the partner.

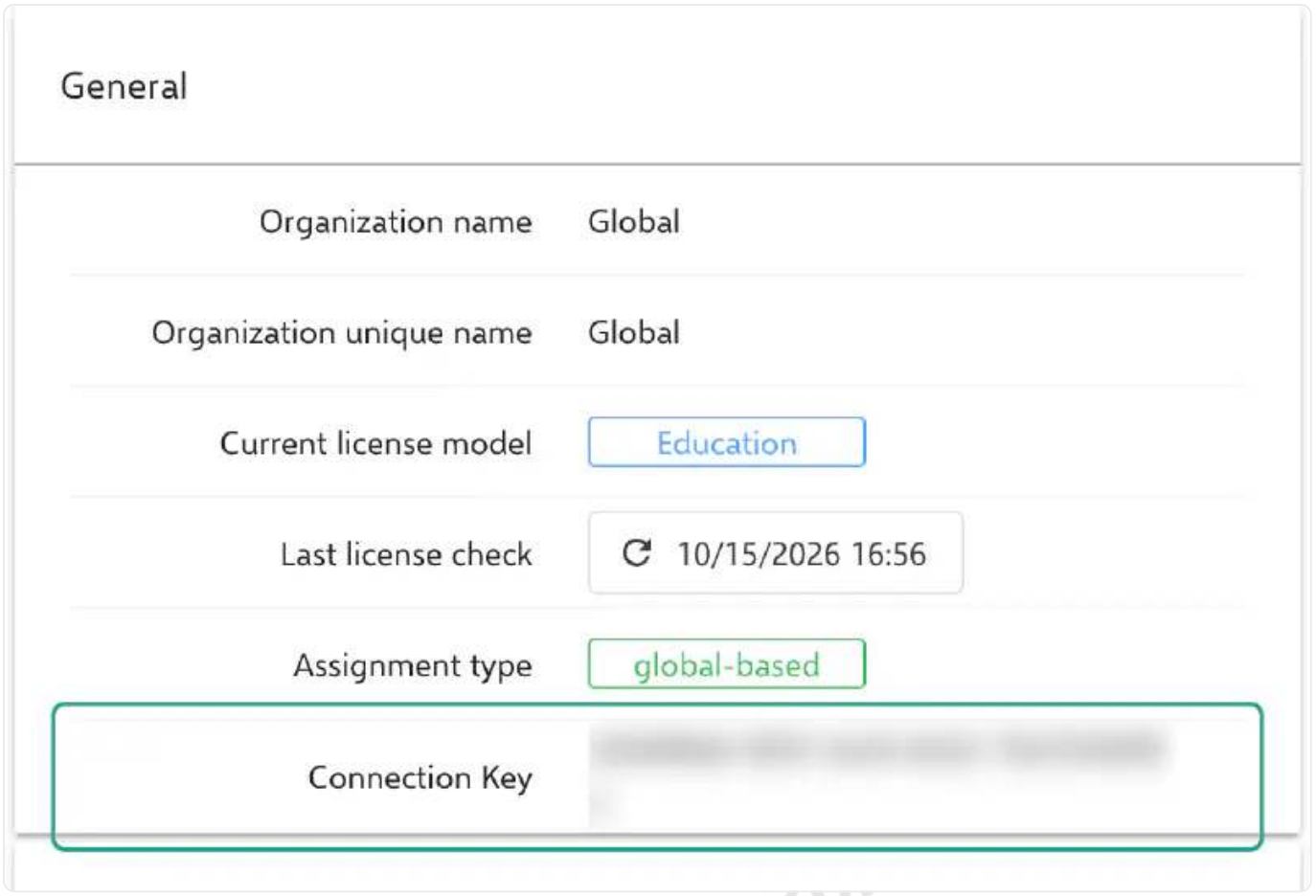
> The connection key grants access to the organization's license management. It should only be shared through a trusted, secure channel.

Copy the connection key (customer)

1. The customer signs in to Relution and switches to the Global organization or to the tenant whose licenses are to be managed.
2. In the top right corner, the support menu (question mark icon) is opened and License information is selected. The entry only appears with the read permission for License information.
3. In the General section, the value of the Connection Key field is copied, e.g. using the copy button next to the value.

The connection key is only displayed after a successful license check. If the field is empty, for example because there was no connection to the license server, the license check can be triggered again in the same section using the button next to Last license check.

For version 26.4.0

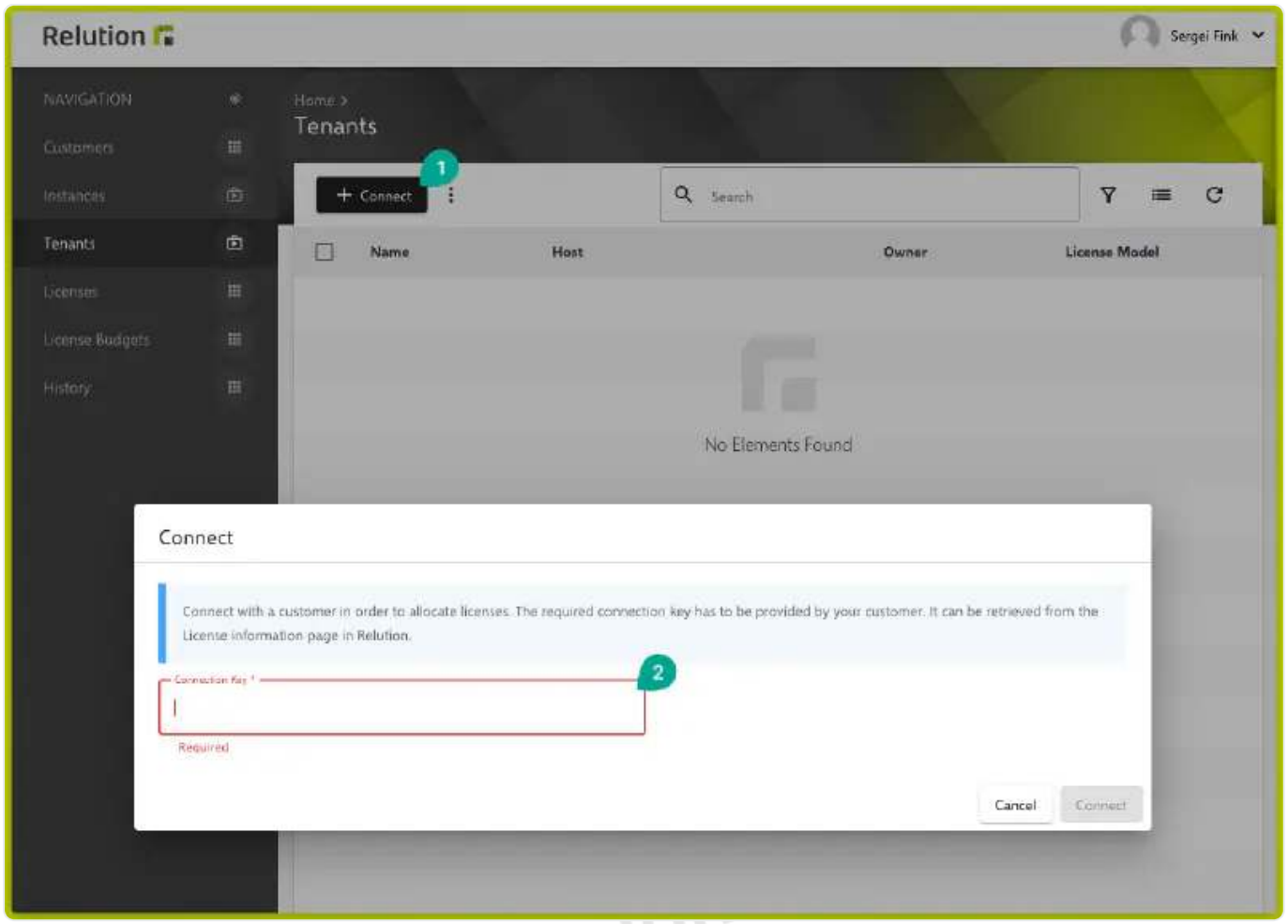


Share the connection key

The copied connection key is sent to the partner or service provider who is to take over license management for the organization.

Connect the organization (partner)

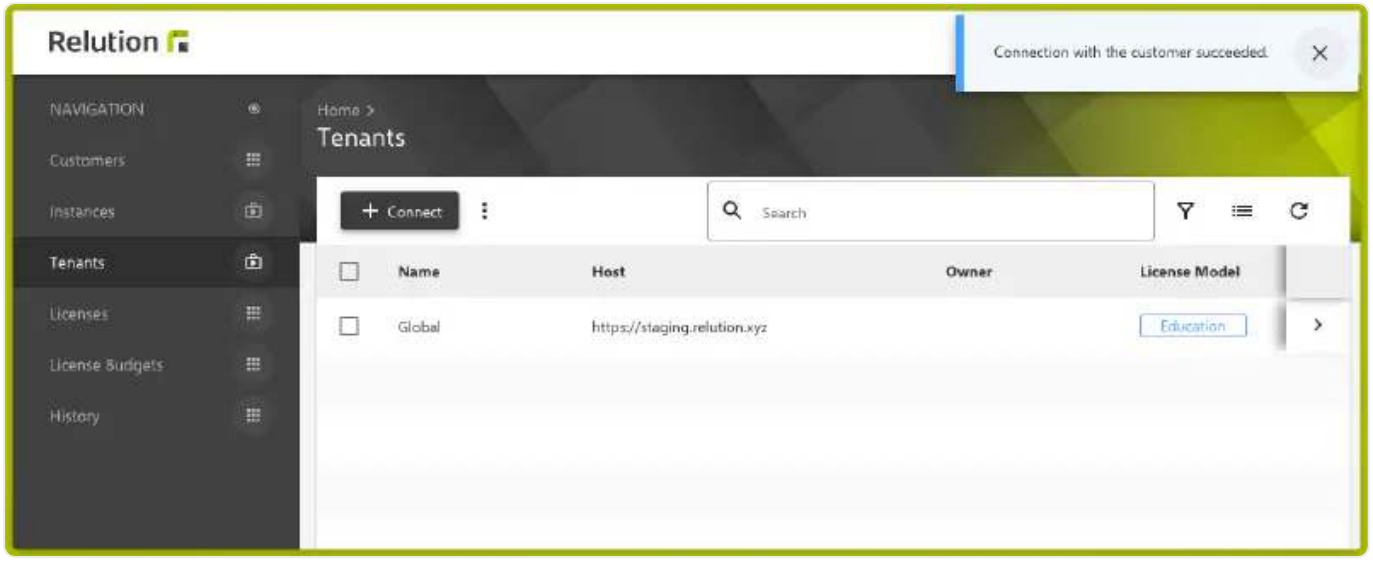
1. The partner signs in to the license server: https://license.relution.io →
2. In the sidebar navigation, Tenants is opened and Connect is clicked.
3. The connection key is pasted into the input field and confirmed with Connect.



For version

Result

The organization is now connected to the partner and appears in their Tenants list. From now on, the partner can manage the licenses of the connected organization.



Summary

- License management can be delegated to a partner or service provider.
- The basis for this is the connection key, found under License information.
- The connection is possible for both the Global organization and individual tenants.
- The connection key should only be shared through a secure channel.

For version 26.4.0

Configure TeamViewer

With the Relution license add-on for TeamViewer remote support, the TeamViewer license is included in the Relution license. In this case, an existing TeamViewer account without its own TeamViewer license can be linked directly to Relution.

With Relution, the TeamViewer app can be distributed directly to managed devices, and remote support sessions can be started via the Relution portal.

Requirements

> TeamViewer integration in the License included license mode requires an additional license for this add-on. It can be purchased through the Relution sales team.

Supported platforms

After successful connection, remote support sessions can be initiated via Relution on the following platforms:

- Android Enterprise
- macOS
- Windows

For version 26.4.0

For further information on how to register the device see Remote support sessions →.

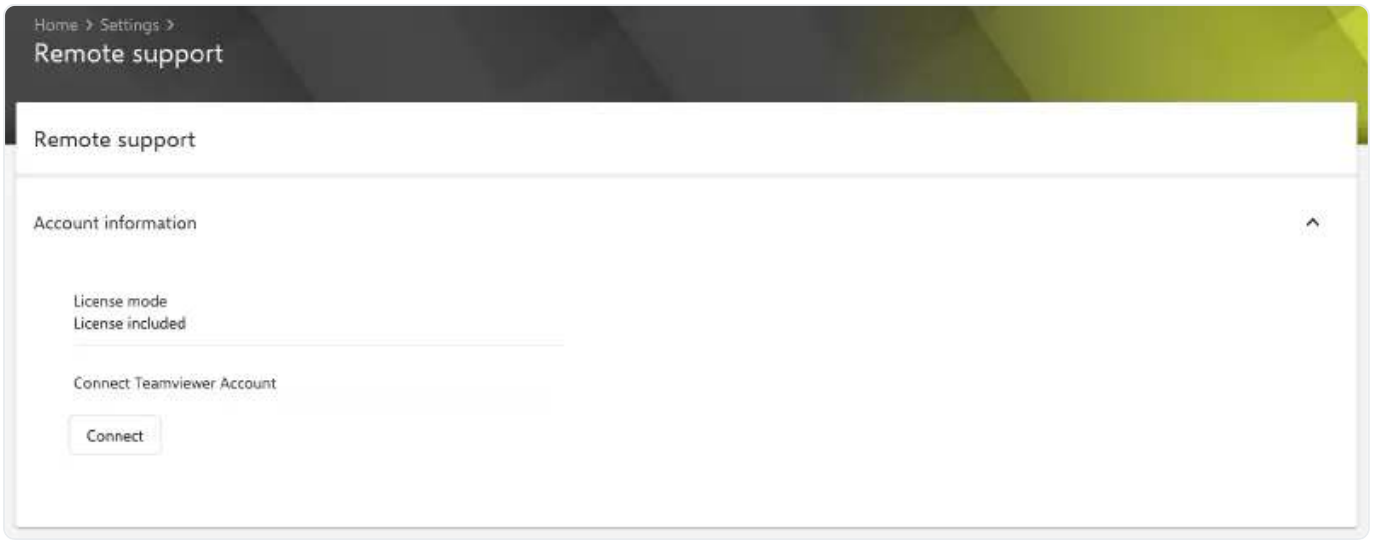
Setup account

The account is linked in the Relution portal under `Settings` → `Remote support` : Connect is clicked next to Connect Teamviewer Account. The setup is then completed by logging in with the TeamViewer account credentials. The buttons on this page are only available with the permission to change the remote support settings.

Once connected, the TeamViewer account is linked to the Relution organization as a tenant account under the Relution vendor. The page then shows Account (email address), Name and Description of the TeamViewer account under Account information. The connection can be tested at any time via Check connection. If any issues arise, the account can be linked again via the Connect button next to Reconnect Teamviewer Account to re-establish the integration.

The setup requires the add-on for the included TeamViewer license (in the license information: Teamviewer Remote Support). License mode must show License included. Relution sets the mode automatically based on the license; it cannot be selected. If an incorrect mode is displayed, a license check updates the available functions. It is triggered in the License information (via the support menu (question mark icon) in the top right corner) using the button next to Last license check. If the add-on is missing while License included is active (e.g. after the license has expired), the page shows a warning.

A TeamViewer account can only be linked to one organization. If it is already linked to another organization, the connection is rejected with a corresponding error message.



Multiple organizations

The connection is set up either in a superior organization (global or meta organization) or in individual sub-organizations, not in both. If it is already set up in a superior organization, it also applies to its sub-organizations; a notice is shown there and the buttons are hidden. If it is set up in a sub-organization, it can only be configured in the superior organization after it has been removed from all sub-organizations.

For version 26.4.0

Remove account

In the Remove account section, the Disconnect button next to Disconnect Teamviewer Account removes the connection. This deactivates the TeamViewer tenant and removes the TeamViewer credentials of the organization’s devices from Relution. Switching back to the Bring your own license license mode is only possible after disconnecting.

Remote support sessions

The TeamViewer integration with Relution enables efficient remote support to managed devices via the Relution Portal. Once the TeamViewer account has been configured in the Remote support settings and the TeamViewer Host app is installed on the device, both attended and unattended remote support sessions can be initiated.

This guide outlines how to set up and distribute the TeamViewer Host app across Android Enterprise, macOS, and Windows devices, register the device for remote support, and start remote support sessions via Relution.

Device registration

To register a device, the TeamViewer Host app must be installed. The Register for remote support action then retrieves the TeamViewer login data required for remote support sessions. It is executed by the Relution companion app of the respective platform (Android Enterprise: Relution app, macOS: macOS companion, Windows: Windows Companion). If the companion app is not active, the device is not registered.

- Android Enterprise: The action is triggered automatically as soon as the device reports the TeamViewer Host app as installed.
- macOS: The action is triggered automatically after installation, provided the macOS companion is enabled (`Settings` → `Relution Client Apps`, switch Enable macOS companion). User-enrolled Macs (User Enrollment) are not supported.
- Windows and all cases without automatic registration: The action can be sent manually via the remote support dialog (see Initiate remote support sessions →).

If the TeamViewer Host app is uninstalled from the device, Relution removes the device registration automatically.

The following explains how the TeamViewer apps are distributed via Relution and installed on the devices depending on the platform.

Android Enterprise

In the Relution portal, a Manage apps → configuration is created, to which the TeamViewer Host app → as well as the manufacturer-specific TeamViewer add-on or the TeamViewer Universal Add-On from the Managed Google Play Store are added. No further configuration is required here.

> After installation, the TeamViewer Host app must be launched to complete the displayed steps and grant all required permissions.
>
> If the Register for remote support action fails with the error verify failed, it is likely that not all required permissions were granted in the TeamViewer Host app.

For version 26.4.0

macOS

The TeamViewer Host app is downloaded from the TeamViewer website, and the .dmg file is added as a native app in the Relution App Store. A detection rule is defined by specifying the bundle identifier of the TeamViewer Host (`com.teamviewer.TeamViewerHost`).

The app is distributed to the devices using an app compliance configuration or a Deploy Relution store app action.

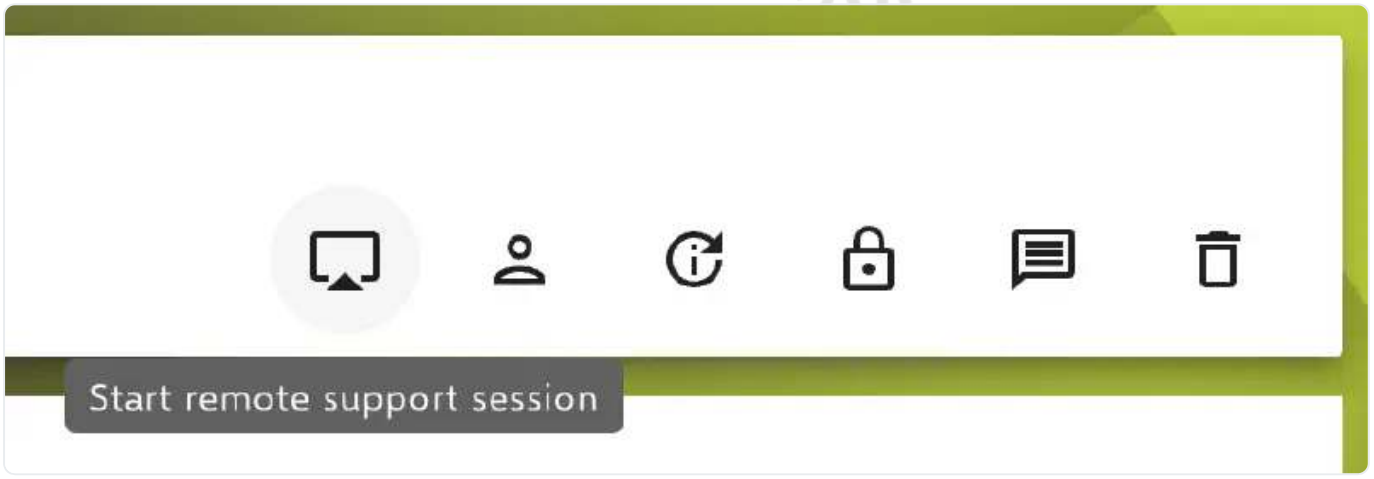
To complete the installation, the installed app is opened on the macOS device and the displayed steps are followed.

Windows

The TeamViewer Host app is deployed to the devices from the WinGet → store. The WinGet package ID is `TeamViewer.TeamViewer.Host`.

Initiate remote support sessions

A remote support session is started from the detail view of the device in the Relution portal, using the Start remote support session icon in the header. Alternatively, the device list provides the Start remote support session button as soon as exactly one device is selected. Both require the permission to request remote support sessions.



A dialog opens, offering a choice between Attended and Unattended; Unattended is preselected. The main difference between the session types is the need for user interaction:

- Attended: Requires a user at the device to approve the connection.
- Unattended: No user interaction is needed to start the connection.



Links for the TeamViewer web app and the TeamViewer desktop application are generated. Administrators can use one of the two links to start a remote support session.

To open the desktop link, a TeamViewer desktop app, such as the TeamViewer Full Client, is required.

In attended mode, the link is valid for 24 hours; in unattended mode, for 5 minutes. After that, a new request is required. If the device is offline or not reachable via TeamViewer, the dialog shows a corresponding error message.



If the TeamViewer credentials for the device have not yet been transmitted to Relution, the dialog shows a corresponding notice. Under Register device, the Send action button sends the Register for remote support action to the device; the dialog then closes. Once the action has been completed successfully, the remote support session can be started again.



After successfully completing all steps for the remote support session, approval may be required on the desired end device.

For version 26.4.0

Configure TeamViewer

With Relution, a TeamViewer account can be connected with its own license to enable seamless integration. Additionally, the TeamViewer Host can be distributed and configured on managed devices, allowing for uncomplicated remote support directly through the Relution portal.

Requirements

To use the integration, a TeamViewer (Classic) Corporate or Tensor license is required. Furthermore, the user account must have access to the TeamViewer portal to perform the necessary configurations.

Supported platforms

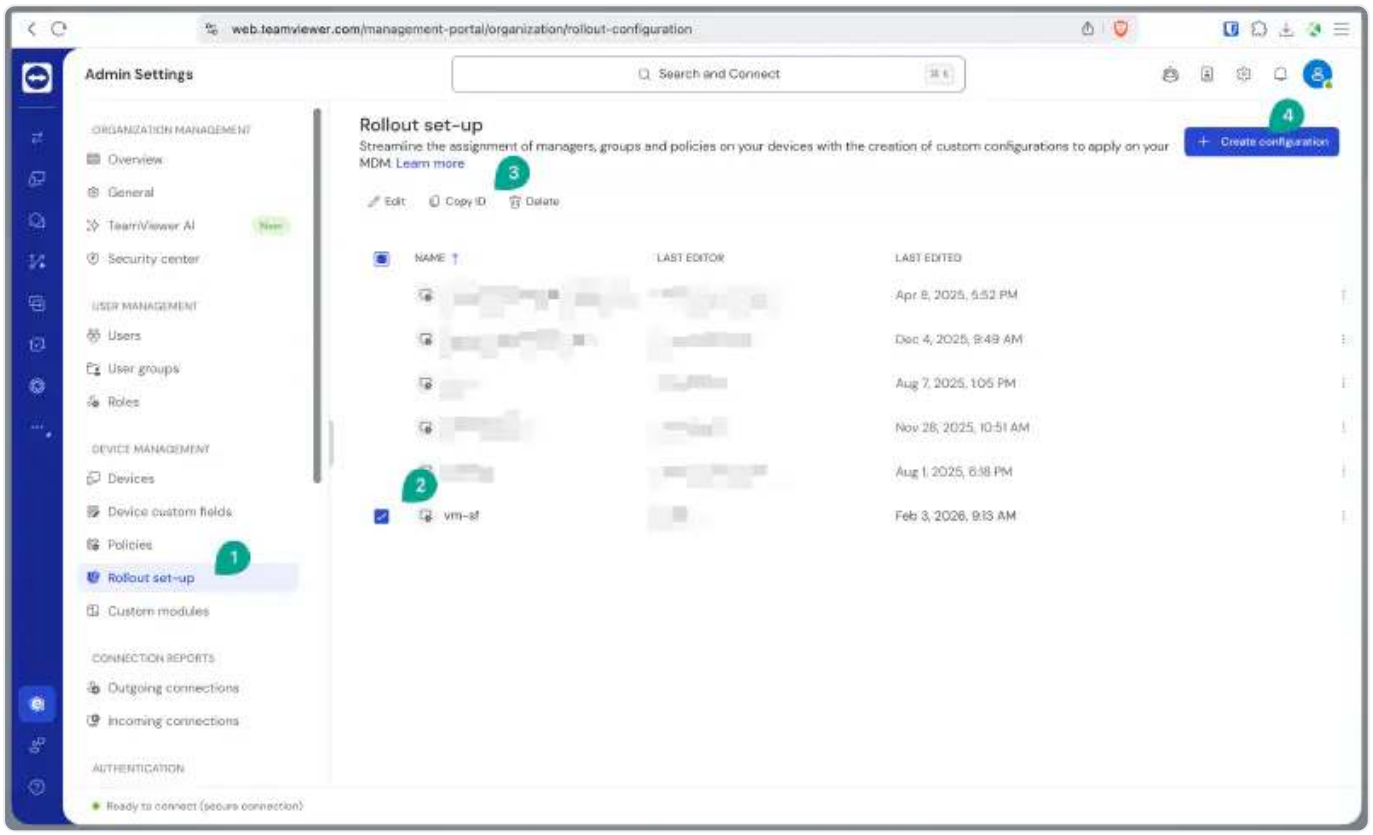
The TeamViewer app can be distributed and configured via Relution on the following platforms:

- Android Enterprise →
- iOS →
- macOS →
- Windows →

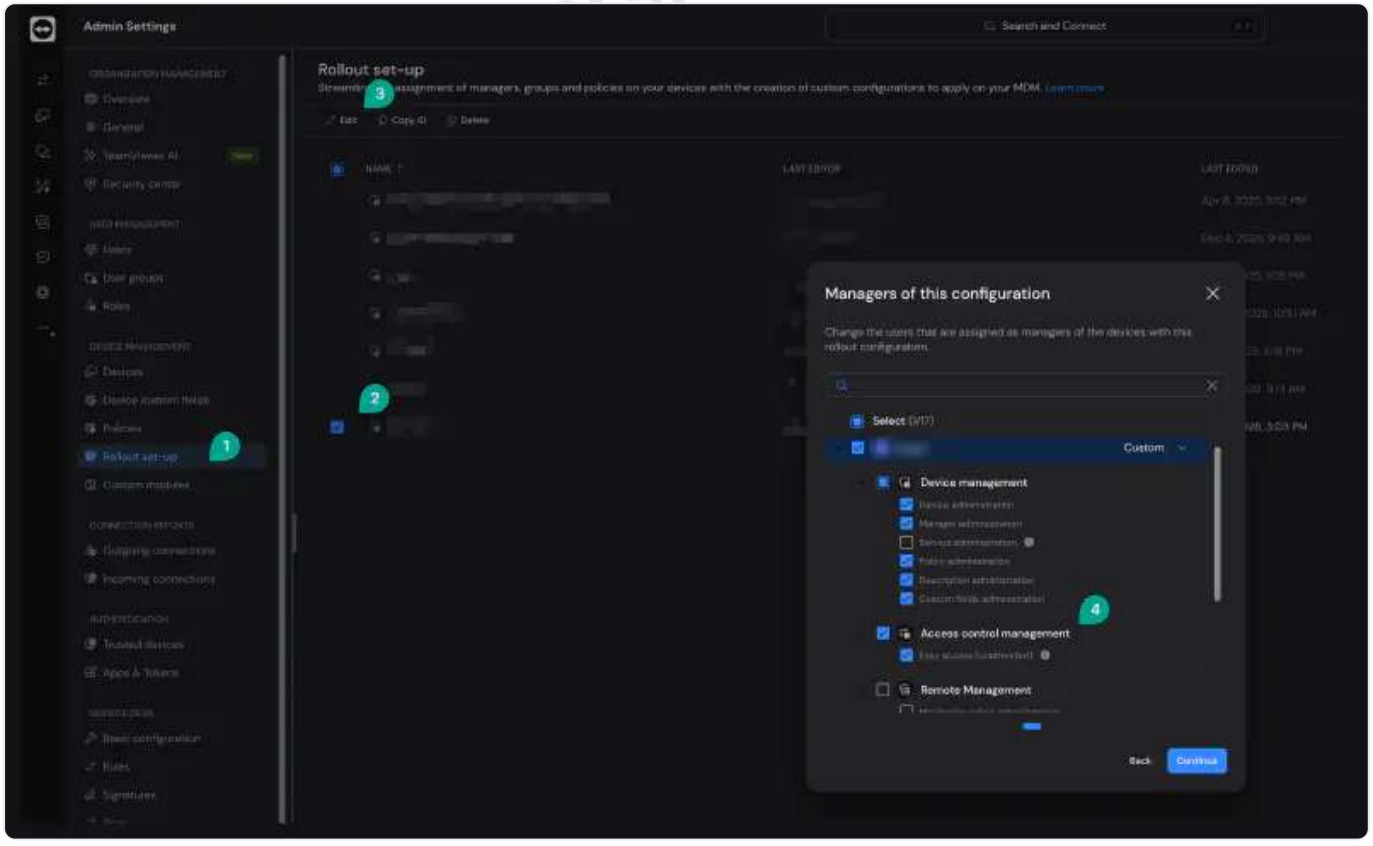
For version 26.4.0

Creating the Rollout Configuration

To configure devices, an *Assignment ID* is required. It is obtained by creating a rollout configuration in the TeamViewer Portal → as described in the Rollout Configuration Guide →.



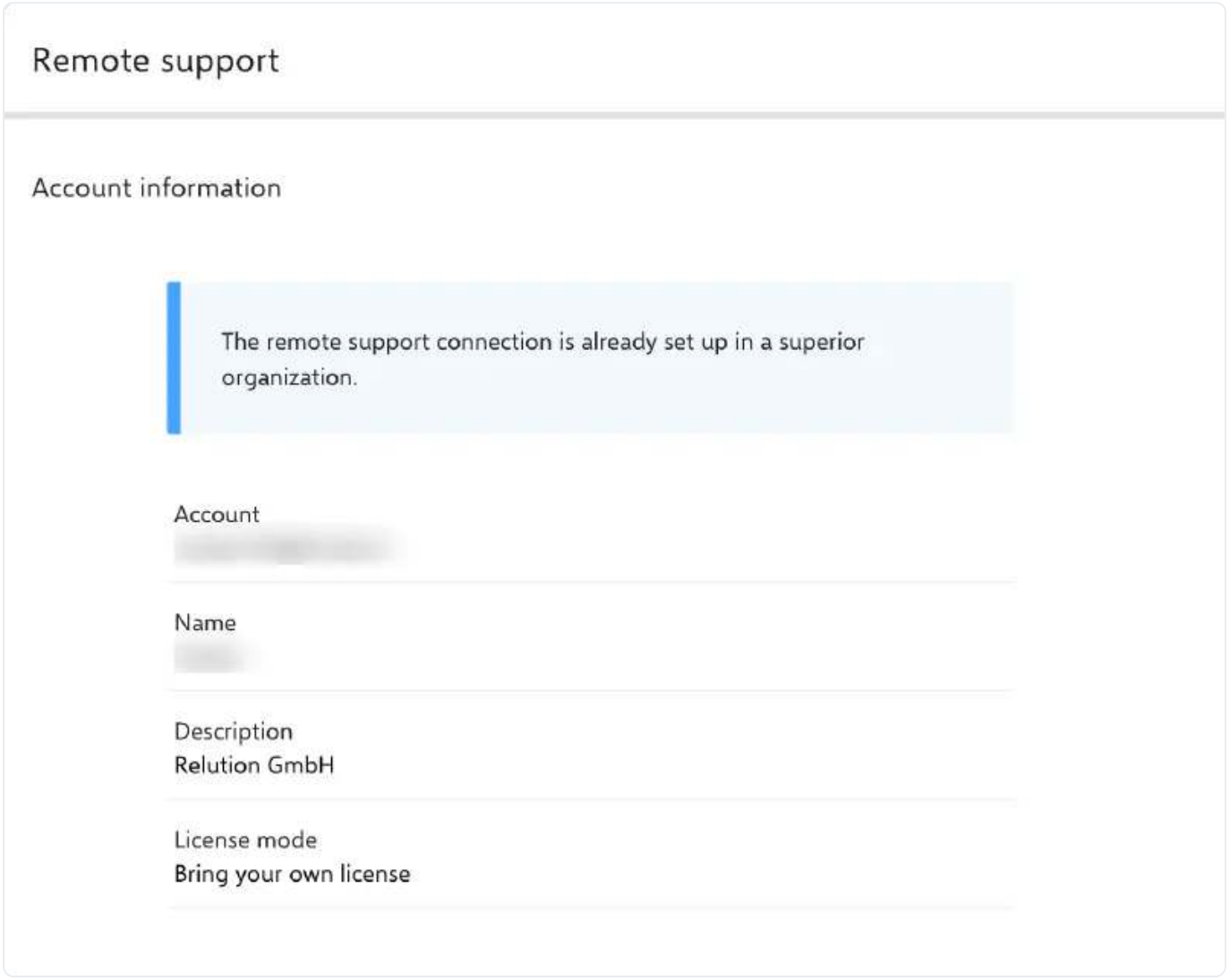
To enable remote sessions with unattended access to devices, users are assigned the Easy Access permission in the Access Rights Management section.



Connecting a TeamViewer account in Relution

The account is connected in the Relution portal under `Settings` → `Remote support`. In the Account information section, the Connect button next to Connect Teamviewer Account leads to the TeamViewer login page. Logging in with the TeamViewer account completes the integration; Relution then shows the details of the connected account.

The License mode is derived automatically from the Relution license: without the add-on for the included TeamViewer license, it is Bring your own license.



After successful authentication, the connection can be verified with Check connection under Test remote support connection. If connection issues occur, the account is re-authorized via Connect next to Reconnect Teamviewer Account to re-establish the integration with TeamViewer. In the Remove account section, the Disconnect button removes the connection.

Restrictions

The following restrictions apply to the connection:

- A TeamViewer account can only be connected to one organization. If the account is already connected to another organization, Relution rejects the connection.
- If the connection is set up in a superior organization (global or meta organization), it also applies to the subordinate organizations and cannot be changed there. If it is already set up in a sub organization, it can only be configured globally after the setup has been removed in all sub organizations.

For version 26.4.0

Android Enterprise

This article describes how to configure the TeamViewer Host App in Relution to enable automatic device assignment within the TeamViewer portal.

Configuring the TeamViewer Host App

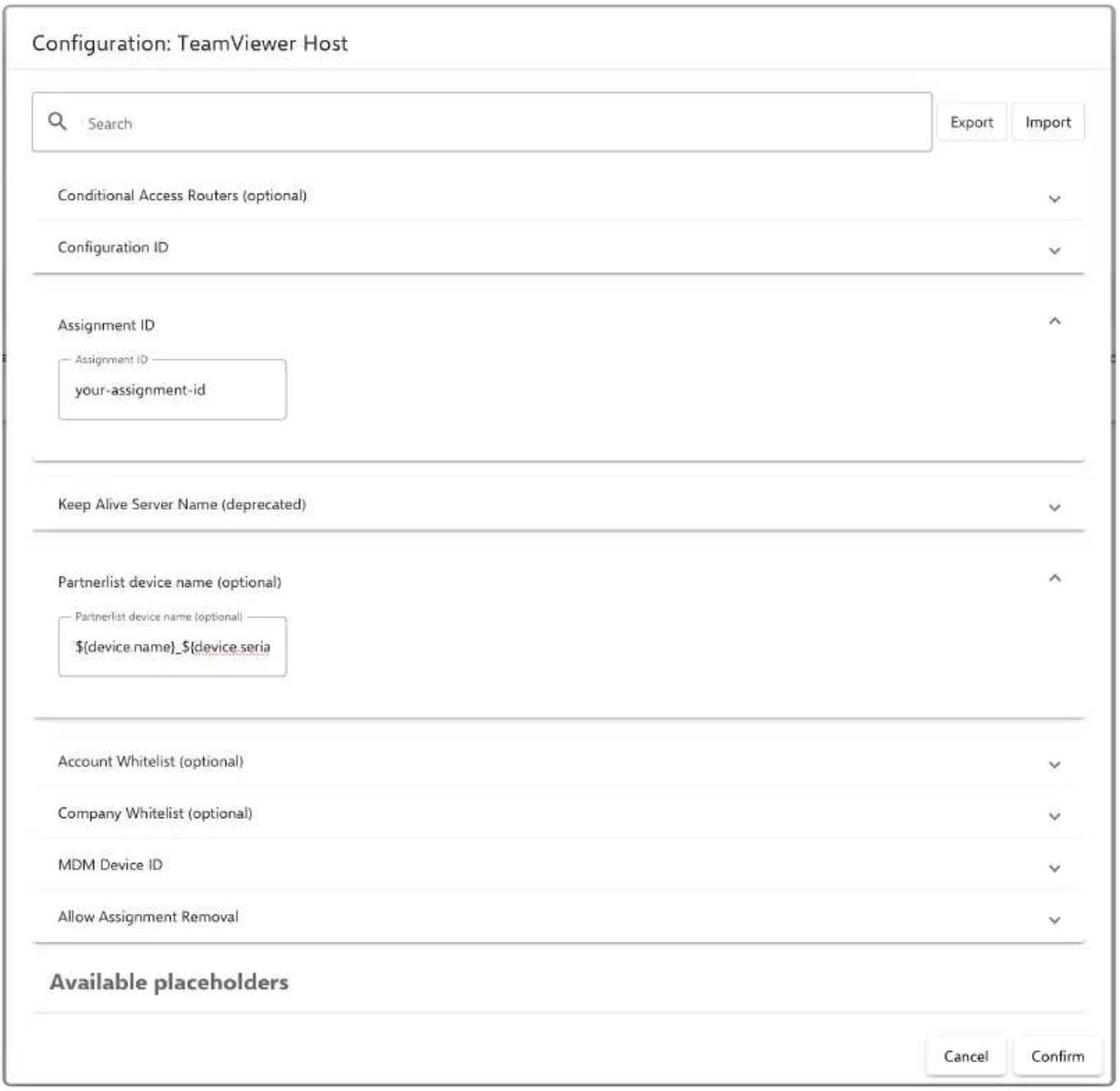
In the Relution portal, a Manage apps → configuration is created and the following two apps are added from the Managed Google Play Store:

1. TeamViewer Host
2. TeamViewer Universal

Afterwards, the app configuration is adjusted and the following relevant settings are defined:

Name	Description
Assignment ID	For automatic device assignment as a managed device in TeamViewer.
Partner List Device Name	The display name in the TeamViewer web interface.

For ve



Configuration Details

- Assignment ID The Assignment ID from the TeamViewer portal, received during the setup step →, is entered here.
- Partner List Device Name The name consists of the device name and serial number and is configured using the placeholders listed under Available placeholders in the configuration dialog:

```
${device.name}_${device.serialnumber}
```

To ensure a clear correlation between devices in Relution and TeamViewer, the serial number must be included in the device name. This is ensured by using the `${device.serialnumber}` placeholder.

Completion

Newly added apps receive the Installation type Force-installed by default and are therefore installed automatically. The configuration is applied to the Android Enterprise devices. As soon as the installation is complete, the assignment will be performed automatically, and the devices will appear correctly in the TeamViewer portal.

Notes

> Login Canceled or Authentication Denied

Important Information on User Interaction

The behavior during remote access varies depending on the Android version:

- Android 13 and older: On many devices (especially those with manufacturer-specific TeamViewer Add-ons), access often works completely in the background without any user interaction.
- Android 14 and newer: Due to stricter security policies from Google (Media Projection API), a system pop-up will inevitably appear when a remote access session starts. The user must manually confirm the screen sharing. Currently, this cannot be bypassed on standard Android Enterprise devices.

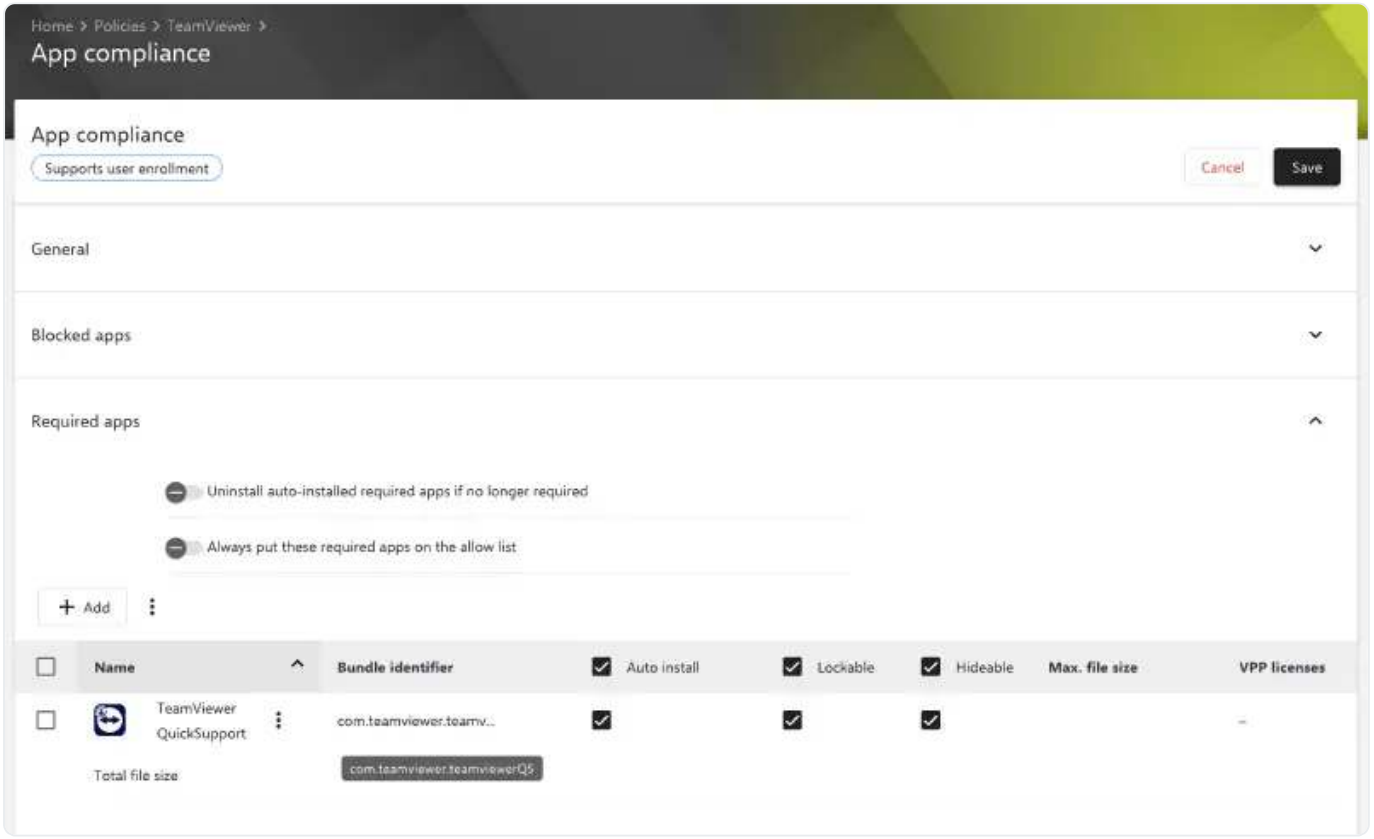
For version 26.4.0

iOS

This article describes how to deploy and configure the TeamViewer QuickSupport App on iOS devices using Relution.

Deploy TeamViewer QuickSupport App

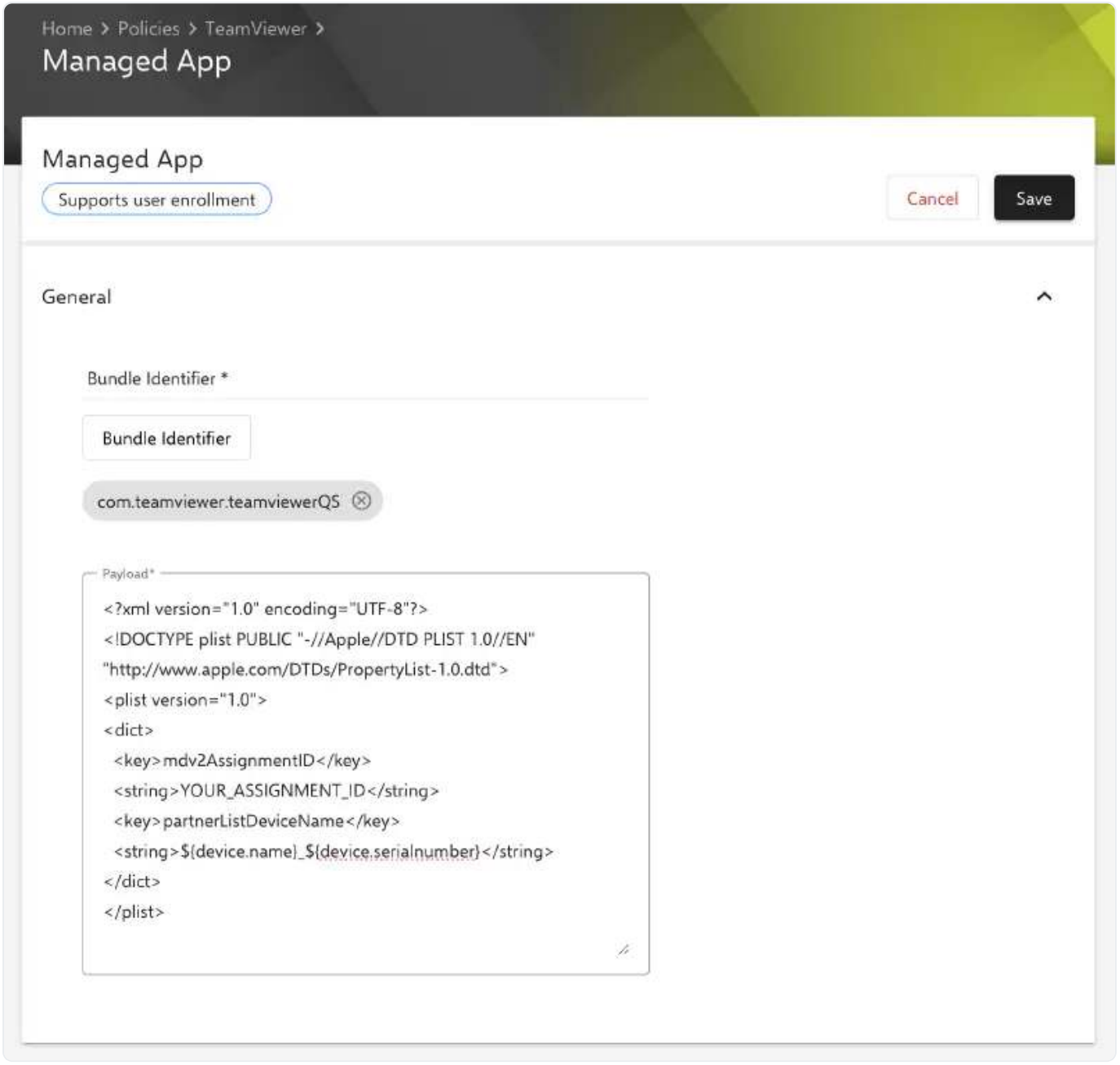
A policy with an App compliance → configuration is created. The TeamViewer QuickSupport app (bundle identifier: `com.teamviewer.teamviewerQS`) from the App Store is added to the required apps list.



Configure app for device registration

A Managed App → configuration is added and the TeamViewer QuickSupport app from the App Store is selected. In the Payload field, the following keys are added inside the predefined `<dict>` element (between `<dict>` and `</dict>`); outside of it, the XML is considered invalid and the configuration cannot be saved:

```
<key>mdv2AssignmentID</key>
<string>YOUR_ASSIGNMENT_ID</string>
<key>partnerListDeviceName</key>
<string>${device.name}_${device.serialnumber}</string>
```



- mdv2AssignmentID: Used for automatic device assignment as a managed device in TeamViewer. The Assignment ID from the TeamViewer portal is entered here, received during the setup step →.
- partnerListDeviceName: Display name of the device in the TeamViewer web interface. The name consists of the device name and serial number and is configured as follows using the available placeholders: `${device.name}_${device.serialnumber}`

To establish a link between devices in Relution and TeamViewer, the serial number must be part of the device name. This is ensured by using the placeholder `${device.serialnumber}`. The name can be composed differently as long as it still contains the serial number; when a session is started, Relution searches TeamViewer for a device whose name contains the serial number.

The configurations are applied to the iOS devices. Once the installation is complete, the assignment will be carried out automatically, and the devices will appear in the TeamViewer portal.

Remote support sessions on iOS devices

In Relution, remote support sessions for iOS devices, including iOS User Enrollment, are only available with Bring your own license. They are started as described under Remote support sessions →. On the iOS device, the session must be confirmed by the user in the TeamViewer QuickSupport app.

For version 26.4.0

macOS

This article describes how to deploy and configure the TeamViewer Host on macOS devices using Relution.

Downloading the TeamViewer client

The macOS installer is downloaded in the TeamViewer portal under `Admin Settings` → `Rollout Configuration`. The package includes both the *TeamViewer Full Client* and the *TeamViewer Host*. For integration with Relution, only the *TeamViewer Host* is required.

Distributing the TeamViewer client

In the Relution portal, a new native app is created under `Apps` → `App Store` using the previously downloaded PKG file. A detection rule of the type Package Name (the only rule type available for macOS apps) is added, containing the bundle identifier of the TeamViewer Host (`com.teamviewer.TeamViewerHost`).

The app can be distributed to the macOS devices either through an App compliance configuration or by using the action Deploy Relution store app.

For version 26.4.0

Performing assignment via script

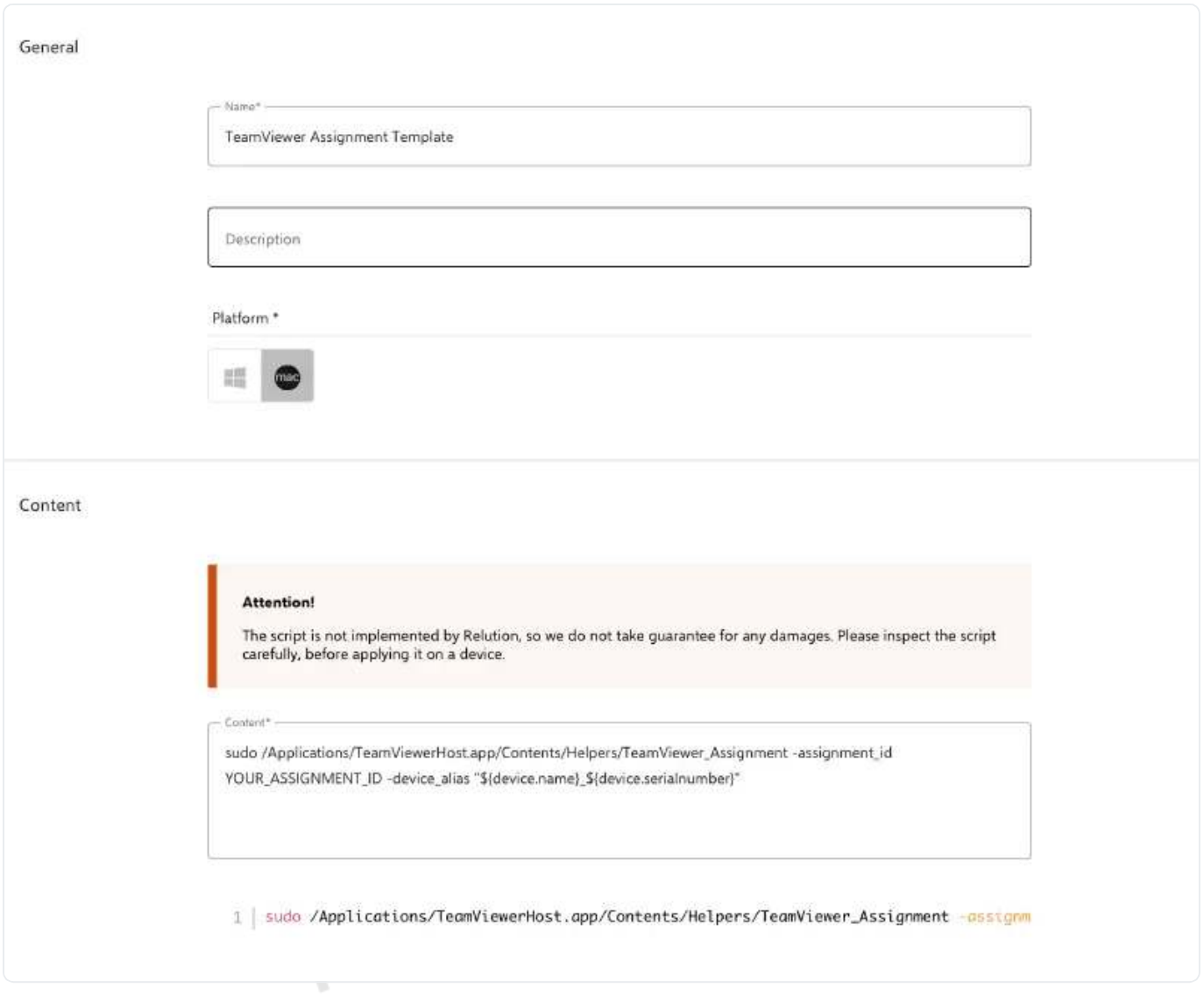
In the Relution portal, a script for the macOS platform is created containing the following command:

Script for TeamViewer Host:

```
sudo /Applications/TeamViewerHost.app/Contents/Helpers/TeamViewer_Assignment -
assignment_id 'YOUR_ASSIGNMENT_ID' -device_alias
"${device.name}_${device.serialnumber}"
```

`YOUR_ASSIGNMENT_ID` is replaced with the Assignment ID from the TeamViewer portal, received during the setup step →.

To establish a link between devices in Relution and TeamViewer, the serial number must be included in the device name. This is ensured by using the placeholder `${device.serialnumber}` in the script. The combined name will be displayed in the TeamViewer portal after successful registration.



Running the script requires the macOS companion to be enabled (`Settings` → `Relution Client Apps`, switch Enable macOS companion). The macOS companion is only deployed on Macs running macOS 12 or later and not on user-enrolled Macs; scripts cannot be executed there. Unlike on Windows, the script cannot be attached to the app. It is therefore executed after the TeamViewer Host has been installed, in one of the following ways:

- once via the Execute shell script action (see macOS actions →) or on the `Scripts` → `Scripts` page via Execute on device,
- on a schedule via a Script configuration in a macOS policy; this also covers Macs added later.

Once the assignment is complete, the devices should appear in the TeamViewer portal.

Windows

The following guide outlines the steps to configure TeamViewer Host for Windows via Relution, including the distribution of the TeamViewer Host as a Relution Store App and the creation of a script to configure the application.

Downloading the MSI package

First, the appropriate MSI package for the target architecture is downloaded from TeamViewer. The MSI package is available in the TeamViewer portal under `Admin Settings` → `Rollout Configuration`. The downloaded installer includes both the *TeamViewer Full Client* and the *TeamViewer Host*. For integration with Relution, only the *TeamViewer Host* is required. Detailed information on downloading the MSI package can be found in the TeamViewer Documentation →.

Creating the Relution Store App

After the TeamViewer MSI package has been downloaded, a new native app is created in the Relution portal under `Apps` → `App Store` using the previously downloaded MSI file. At least one detection rule is required for the app; otherwise it cannot be saved. Installation and script execution on the devices are handled by the Relution Companion, which must therefore be installed on the target devices: Windows Companion →. Further details can be found under Windows App Installation →.

For version 26.1.0

Creating the assignment script

To configure the TeamViewer Host on the devices, a new script for the Windows platform is created in the Relution portal under `Scripts` → `Scripts`. Depending on the architecture of the target device, one of the following scripts is used:

Script for devices with a 64-bit operating system:

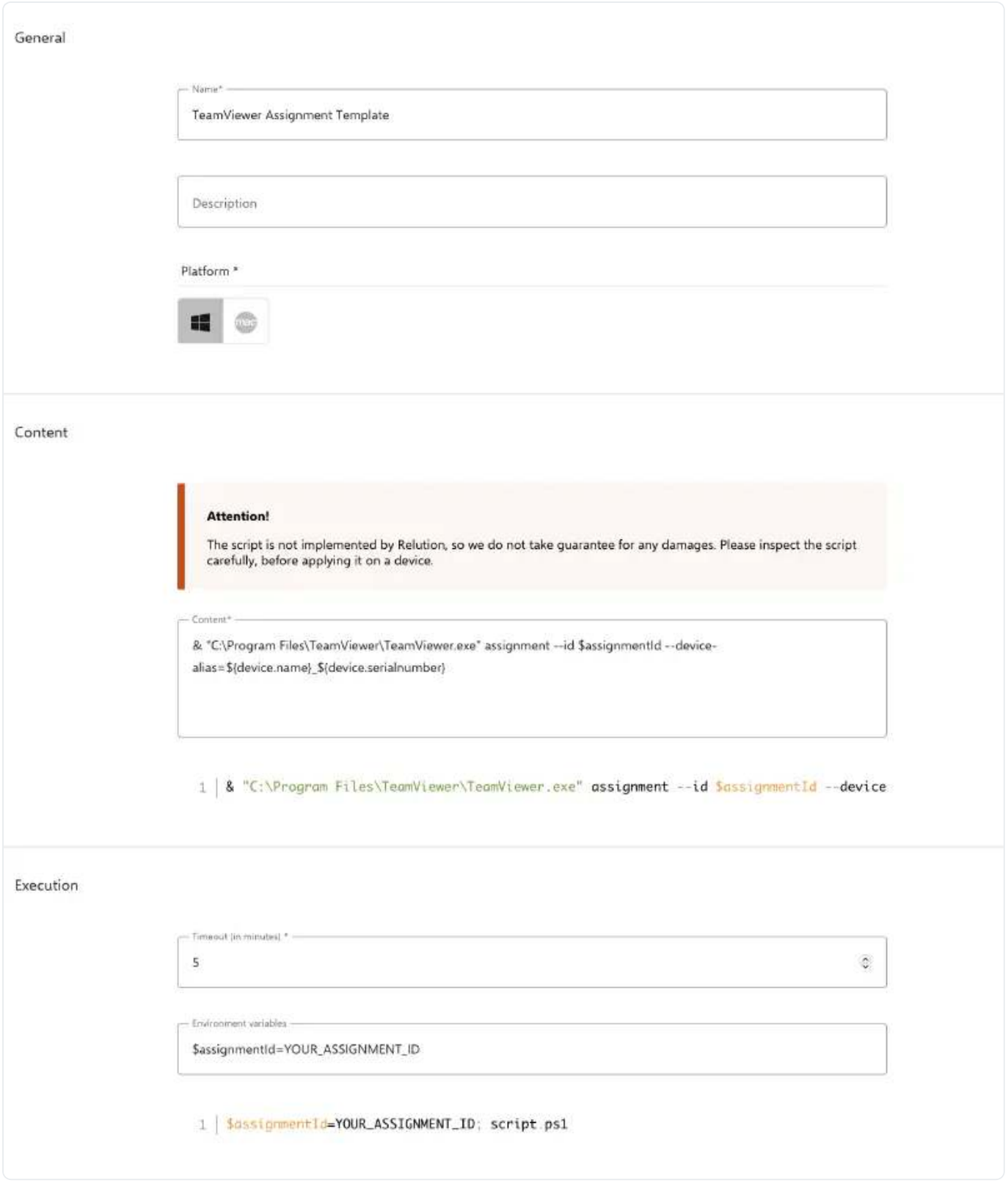
```
& "C:\Program Files\TeamViewer\TeamViewer.exe" assignment --id $assignmentId --device-alias=${device.name}_${device.serialnumber}
```

Script for devices with a 32-bit operating system:

```
& "C:\Program Files (x86)\TeamViewer\TeamViewer.exe" assignment --id $assignmentId --device-alias=${device.name}_${device.serialnumber}
```

In the Execution section, the variable `$assignmentId` is set in the Environment variables field to the Assignment ID from the TeamViewer portal, received during the setup step →: `$assignmentId='YOUR_ASSIGNMENT_ID'`. The content of this field is inserted at the beginning of the script when it is executed.

To establish a link between devices in Relution and TeamViewer, the serial number must be included in the device name. This is ensured by using the placeholder `${device.serialnumber}` in the script. The combined name will appear in the TeamViewer portal after successful registration.



Executing the script after installation

To execute the script, the TeamViewer Host MSI app created earlier is opened in Relution. In the Scripts tab, the previously created configuration script is added under Post install scripts. Multiple scripts can be arranged there in their execution order via drag and drop. The tab only appears for classic Windows apps of the own organization and only with read permission for scripts.

The application is installed on the desired Windows devices via an App compliance configuration or the Deploy Relution store app action.

Once the TeamViewer Host has been installed, the script will automatically run. After the configuration is complete, the devices should appear in the TeamViewer portal.

For version 26.4.0

Remote support sessions

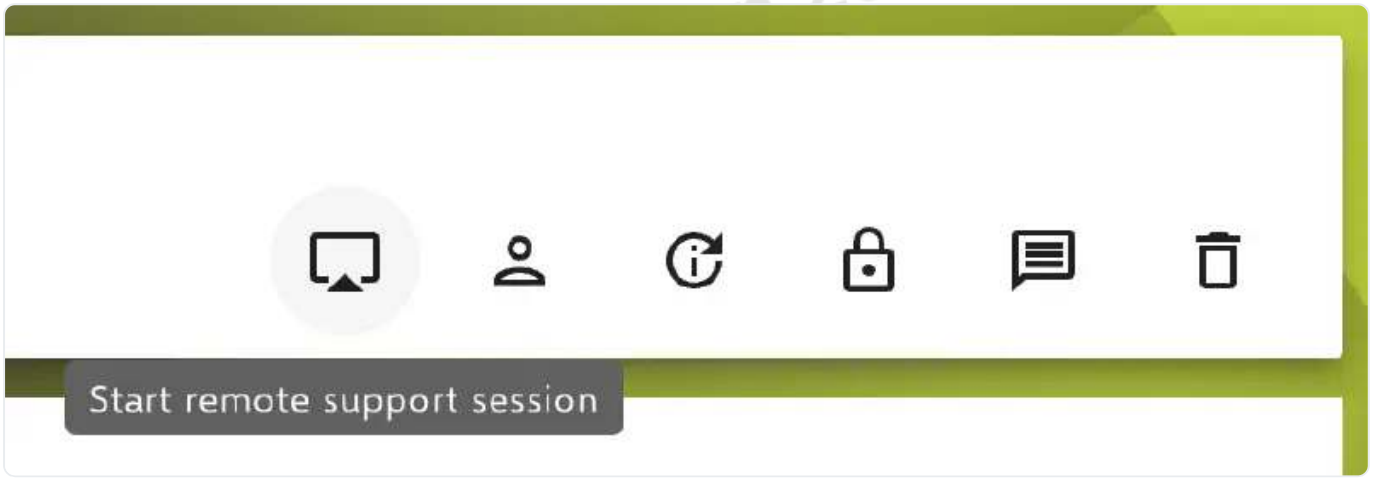
Once a TeamViewer account with a valid license is configured in the Relution settings, and the device is successfully registered in the TeamViewer portal, unattended remote support sessions can be initiated. This applies to Android Enterprise (fully managed devices and work profiles), macOS and Windows. With Bring your own license, iOS devices are supported as well, including iOS User Enrollment. For iOS, the TeamViewer QuickSupport app only allows attended sessions that require active user interaction.

The matching TeamViewer client must be installed on the managed device and registered in the TeamViewer portal (see Android Enterprise →, iOS →, macOS → and Windows →). Opening the session via the administrator link requires a TeamViewer desktop app, such as the full TeamViewer client, on the administrator's computer.

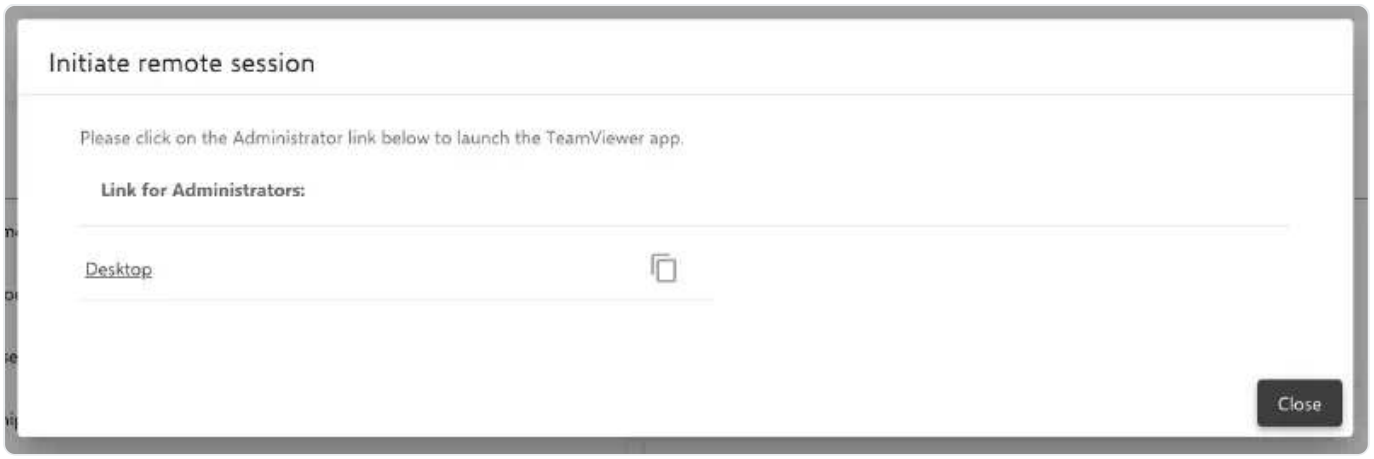
Relution identifies the device by its serial number: it searches TeamViewer for a device whose name contains the serial number from Relution. The device name configured in the rollout articles must therefore contain the `${device.serialnumber}` placeholder.

Start remote support session

A remote support session is started from the device's detail view in Relution by selecting the Start remote support session icon in the header section. The icon only appears if a TeamViewer account is connected, the device's enrollment type is supported and the logged-in user is permitted to request remote support.



With Bring your own license, there is no choice of session type; Relution immediately generates a link for an unattended remote session. The Initiate remote session dialog shows it under Link for Administrators: as the Desktop link, and the icon next to it copies it to the clipboard. The generated link can only be opened with an installed TeamViewer desktop app.



After successfully completing all steps for the remote support session, approval may be required on the desired end device.

Messages in the dialog

If no session can be created, the dialog shows one of the following messages instead of the link:

- “The device could not be found on TeamViewer.” TeamViewer contains no device whose name includes the device’s serial number. The assignment and the device name are checked as described in the respective rollout article.
- “The device is currently offline or not available via TeamViewer” The device cannot be reached or the request to TeamViewer failed. The attempt can be repeated later.

For version 26.4.0

Microsoft Conditional Access

Microsoft Conditional Access → is Microsoft's Zero Trust policy engine that enforces access controls based on device and user signals. In this documentation, it is referred to as `MSCA`. If Relution users are synced via `Microsoft Entra ID`, Conditional Access can additionally be enabled to enforce compliance-based restrictions. When a Relution-managed device changes its compliance status (e.g., from compliant to non-compliant), this information is automatically synced with Microsoft. Depending on the Conditional Access policies →, it is possible to restrict access to specific applications when a device is marked as non-compliant.

Supported Platforms

- Android Enterprise
- iOS
- macOS
- Windows
  - Devices must be Entra ID joined or enrolled via Autopilot

Preconditions

For version 26.4.0

To use Microsoft Conditional Access with Relution, the following requirements must be met:

- Available from Relution Server 5.33.1
- Microsoft Entra ID P1 licenses. See more details →.
- `Entra ID` configured with users sync active, see Linking Entra ID and Relution →
- Entra users can log in to Relution only after OIDC → has been configured.

For Android Enterprise, iOS and macOS, the following additionally applies:

- Relution has been added in Intune as a compliance partner for the respective platform, see Set up platforms →.
- The affected users have an Intune license. If it is missing, the device is listed on the Conditional Access settings page with the status The intune license is missing.
- The `Conditional Access` configuration must be applied to the affected devices through an appropriate policy (on iOS and macOS only for device enrollment). Optionally, the configuration marks a device as non-compliant as long as the user has not yet registered it, and asks the user to register it via push notification, see Conditional Access (policy) →.
- The device is linked with `Entra ID` via the Relution Agent →.
- `Broker app` for authentication must be available on the device:
  - Android Enterprise & iOS - `Microsoft Authenticator` - is installed automatically as soon as Relution has been added in Intune as a compliance partner for the platform and the `Conditional Access` configuration has been assigned to the device through a policy
  - macOS - `Company Portal App` - has to be installed on the device. It is available as a download from Microsoft →.

Windows has neither the `Conditional Access` configuration nor a broker app or a compliance partner in Intune. Conditional Access for Windows is turned on on the Conditional Access settings page via Enable next to Enable Conditional Access for Windows, see Set up platforms →.

Limitations

- `Conditional Access` as of now can't be configured per global organization in Relution.
- Users must have been imported via Entra Sync; users previously synchronized through LDAP, for example, cannot be used.
- Users imported via Entra Sync must exist in the same organization as their associated devices.
- On iOS and macOS, User Enrollment (BYOD) is not supported; the `Conditional Access` configuration is only available for device enrollment.
- `Shared iPad` has various restrictions with CA configurations; for example, the requirement that the device must be marked as compliant is not supported. As a result, Relution shows the message Microsoft Conditional Access is not connected on the device's Microsoft Entra ID card. More information can be found in the Microsoft documentation details →.

For version 26.4.0

Set up platforms

This setup guide explains how to connect `Relution` with `Microsoft Entra/Intune` to support Conditional Access for Android Enterprise, iOS, macOS, and Windows. Before starting, all requirements → must be fulfilled.

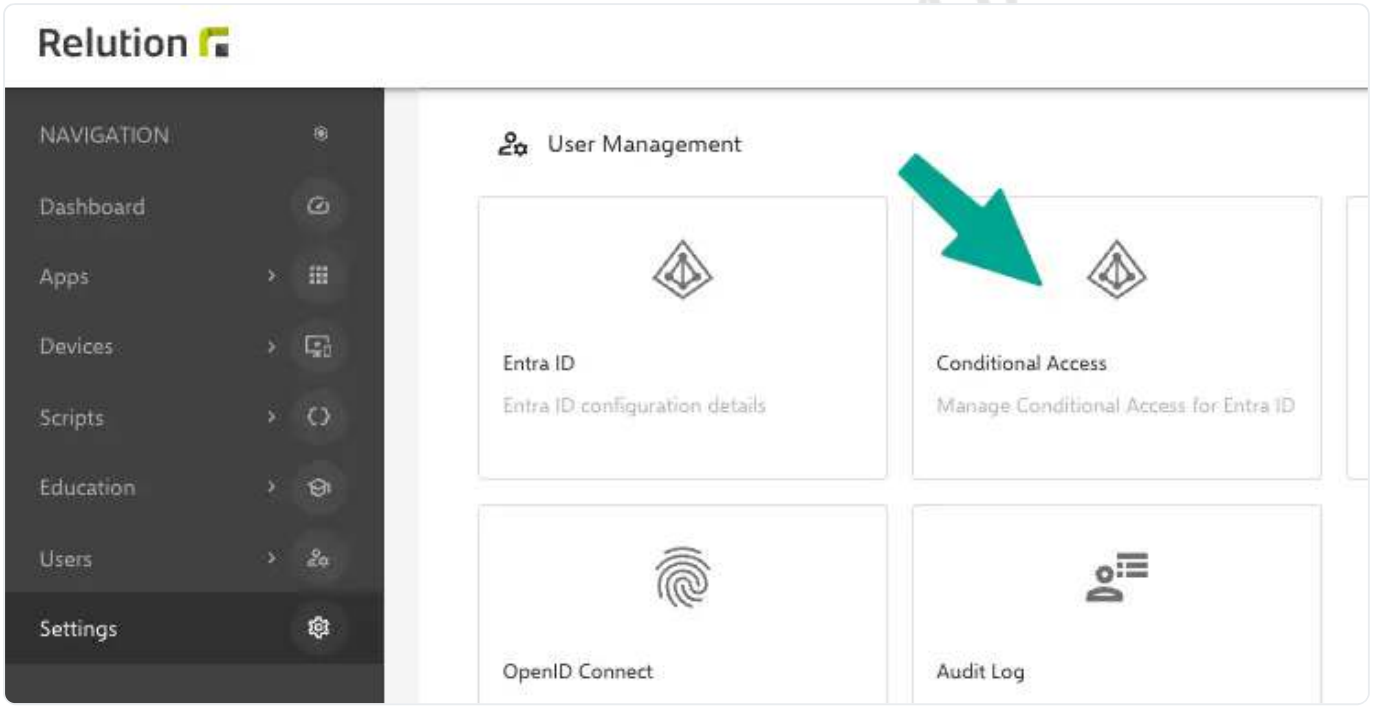
This setup consists of the following steps:

1. `Create an Entra ID application` to authenticate the server with Relution's microservice.
2. `Give consent to the multi-tenant Relution app` to report compliance states to `Entra ID`.
3. Add `Relution` as compliance partner in `Intune`
4. Verify successful setup via synchronization and status checks.

Each step builds on the previous one. The steps are carried out carefully one after the other; whenever a verification is requested, it must report Validation succeeded (when synchronizing, Synchronisation succeeded).

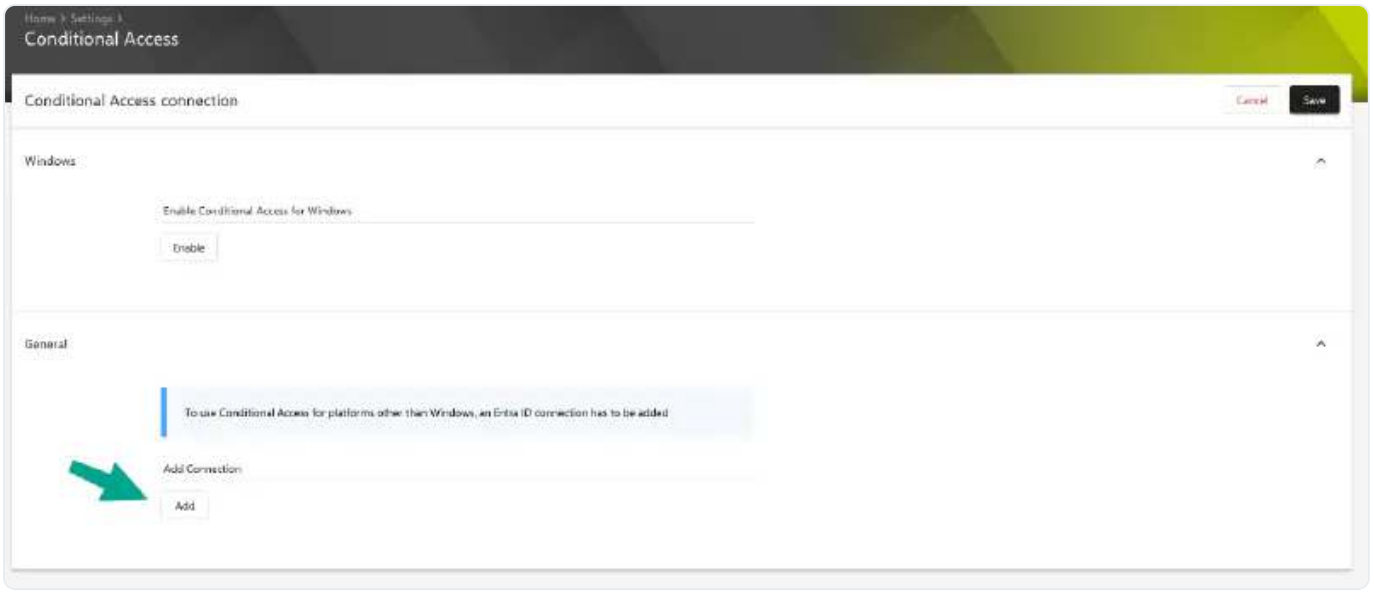
Navigate to Conditional Access

Once Entra ID → is configured and user synchronization is complete, `Conditional Access` can be opened in the settings.



Support for Android Enterprise, iOS and macOS

The wizard for enabling platform-specific support is started in the General section via Add next to Add Connection.



Wizard (1): Create application

The app from the Entra ID setup may be reused, but Relution recommends creating a separate app for clarity and security.

A new `Entra ID application` is created to authenticate with Relution's backend. Contrary to the `Entra ID` setup, no MDM-specific app is needed — a basic App Registration is sufficient. The application has to be in the same tenant as the configured Entra ID.

Open Entra ID in the wizard leads to the Entra ID app registrations →. After creating the app, Next leads to the next step, where the Application (client) ID is entered.

For version 26.4.0

Wizard (2): Application IDs

A client secret is generated for the app; the Application (client) ID and the Client secret are then entered in the respective input fields of the wizard. Once verification via Verify succeeds, the wizard continues with the next step.

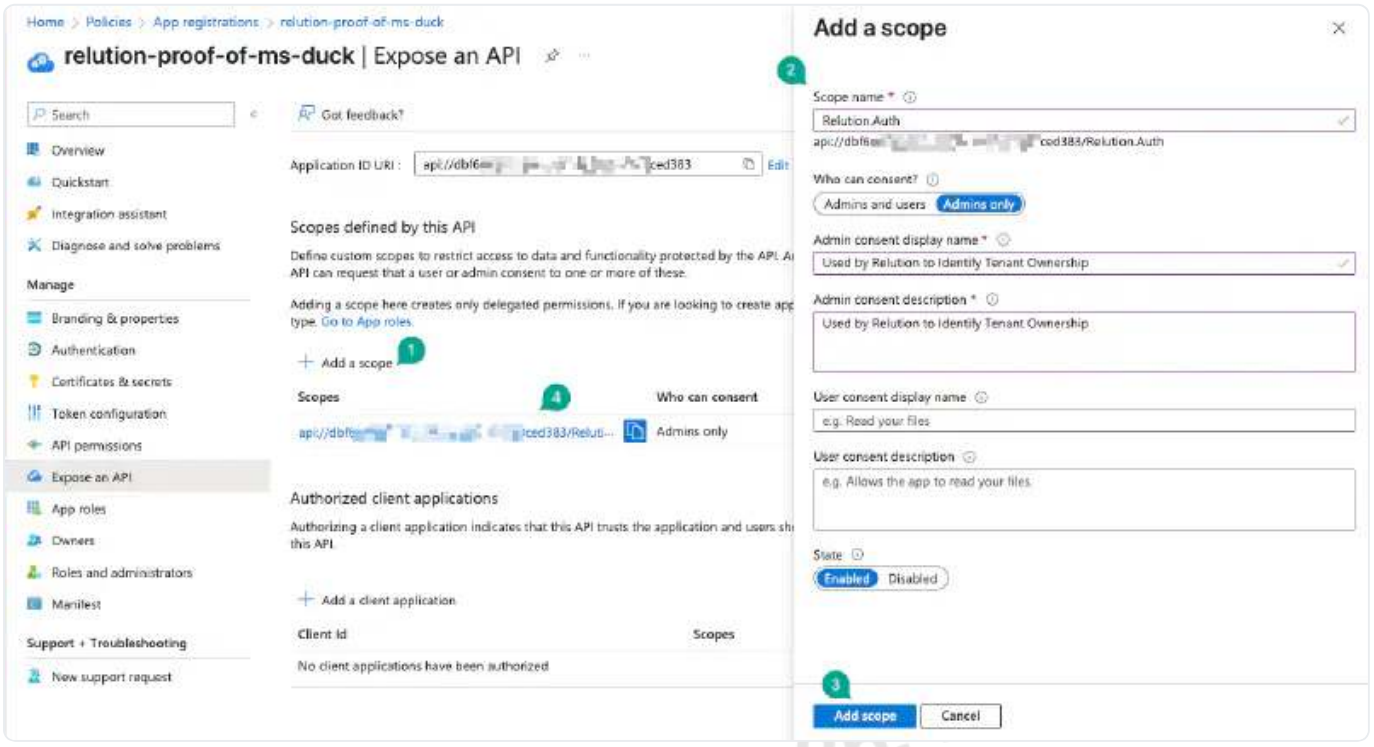
Wizard (3): Expose API

Due to Microsoft token validation limitations, an API needs to be exposed and a custom scope added. Open Expose API in the wizard opens the corresponding settings page of the Entra app directly.

In the Expose an API setting page of the Entra app, the following steps are carried out:

1. Add a scope is clicked.
2. The necessary information is filled in:
    - Scope name: `Relution.Auth`
    - Consent: Admins only
    - Display name and description can be chosen freely, for example: `Used by Relution to identify Tenant Ownership`.
3. Add scope is clicked.
4. The scope should now appear in Scopes defined by this API.

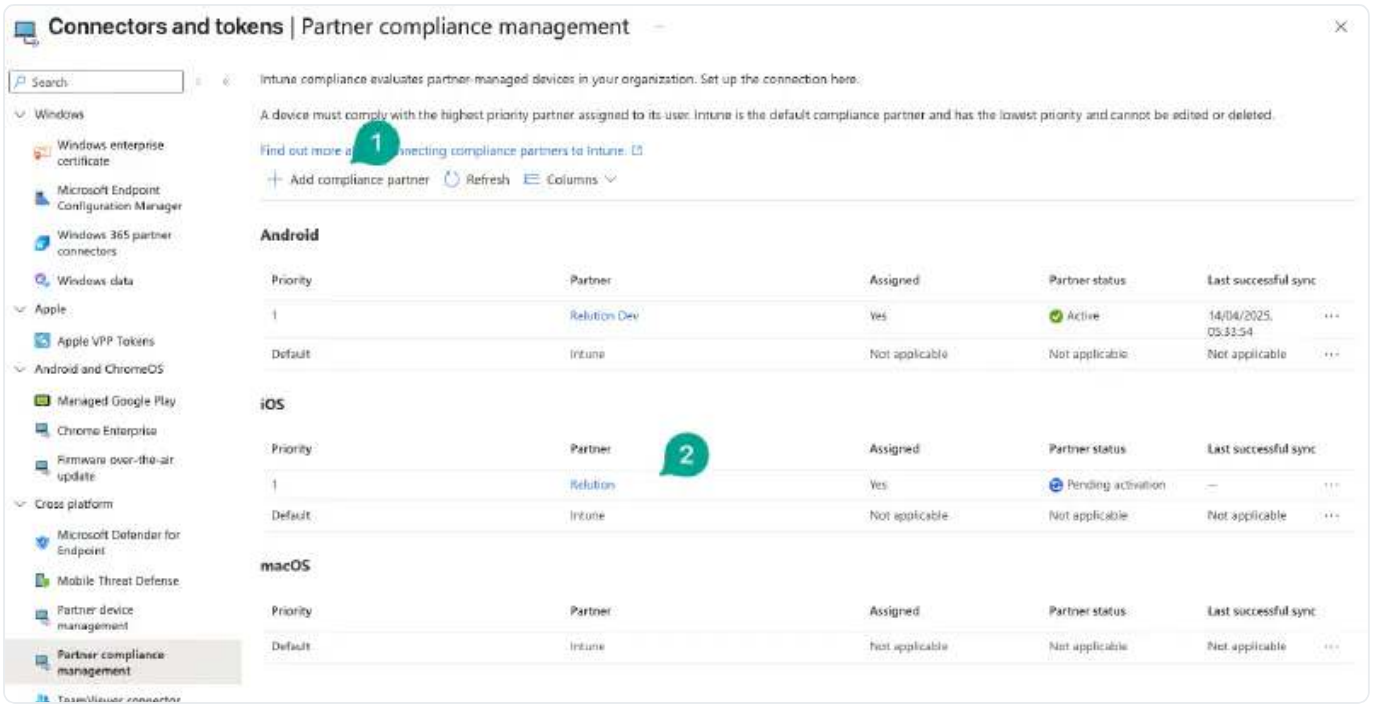
On the top of the Expose an API view in Entra, an Application ID URI is shown. The matching value is selected in the wizard under Scope type: `api://<Application ID>` for a newly created app (step 1), or the Relution server URL (`https://<Relution host>`) if the app from the Entra ID setup is reused. If the Application ID URI differs from both, Custom is selected and the Application ID URI is entered in the Custom scope field.

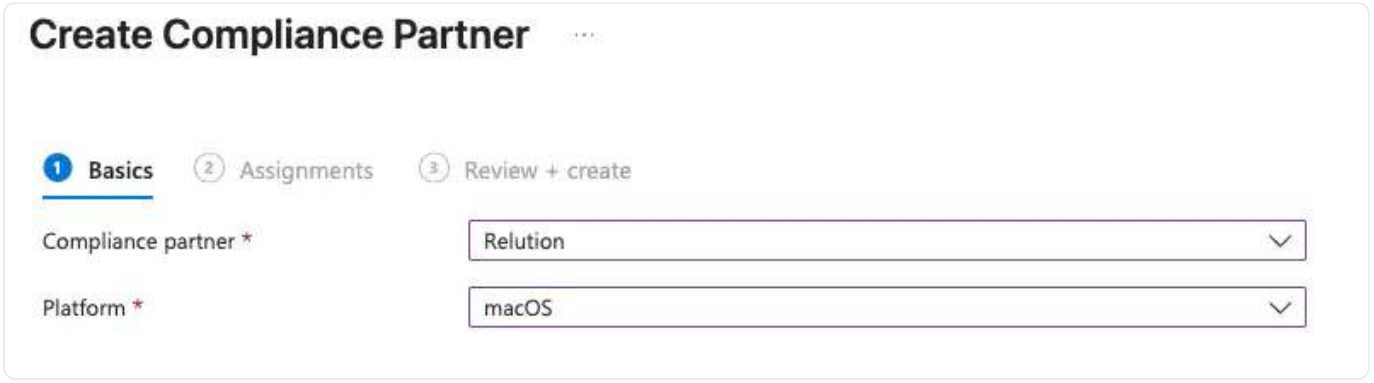


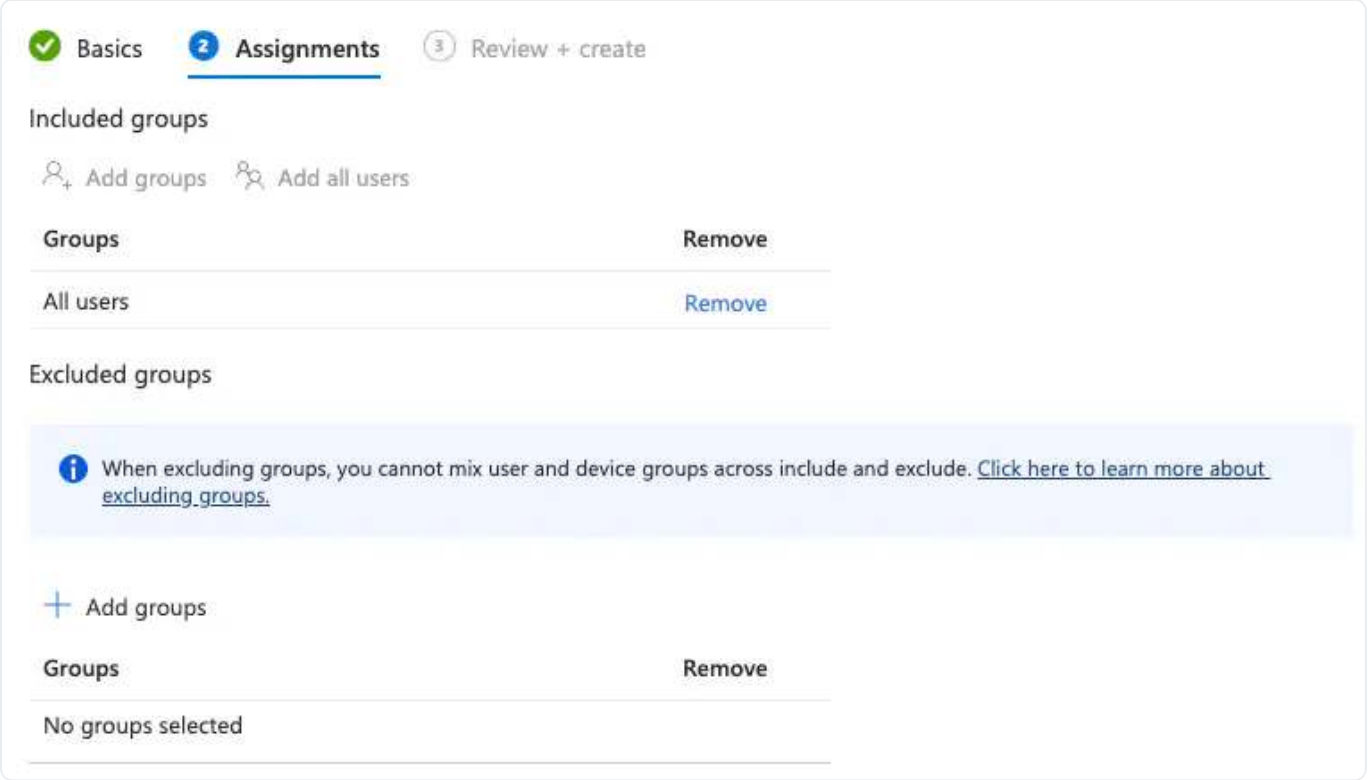
It should now be possible to successfully verify this step in the wizard via Verify.

Wizard (4): Add Compliance Partner

In Intune Partner Compliance Management →, `Relution` is added as a compliance partner for every platform that should be synced. Open Partner settings in the wizard opens this page directly.


Connectors and tokens | Partner compliance management
Search
Windows
Windows enterprise certificate
Microsoft Endpoint Configuration Manager
Windows 365 partner connectors
Windows data
Apple
Apple VPP Tokens
Android and ChromeOS
Managed Google Play
Chrome Enterprise
Firmware over-the-air update
Cross platform
Microsoft Defender for Endpoint
Mobile Threat Defense
Partner device management
Partner compliance management
Intune compliance evaluates partner-managed devices in your organization. Set up the connection here.
A device must comply with the highest priority partner assigned to its user. Intune is the default compliance partner and has the lowest priority and cannot be edited or deleted.
Find out more a nnecting compliance partners to Intune.
1
Add compliance partner
Refresh
Columns
Android
Priority
Partner
Assigned
Partner status
Last successful sync
1
Relution Dev
Yes
Active
14/04/2025, 05:33:54
Default
Intune
Not applicable
Not applicable
Not applicable
iOS
Priority
Partner
2
Assigned
Partner status
Last successful sync
1
Relution
Yes
Pending activation
Default
Intune
Not applicable
Not applicable
Not applicable
macOS
Priority
Partner
Assigned
Partner status
Last successful sync
Default
Intune
Not applicable
Not applicable
Not applicable


Create Compliance Partner
1 Basics
2 Assignments
3 Review + create
Compliance partner *
Relution
Platform *
macOS



Steps:

1. Add compliance partner is clicked.
2. The platform to sync is selected (these steps can be repeated for all platforms): Android, iOS or macOS. Windows is not enabled via the compliance partner but in the section Support for Windows →.
3. A group of users that should be synced is assigned. Add all users can also be selected; in this case, care must be taken not to get locked out later.
    - As of now, excluding groups won't have any effect.
4. After reviewing that everything was selected correctly, Create is clicked.
5. `Relution` should now be shown with a status of `🔄 Pending activation` for that platform. Status might differ if this is not the first setup.

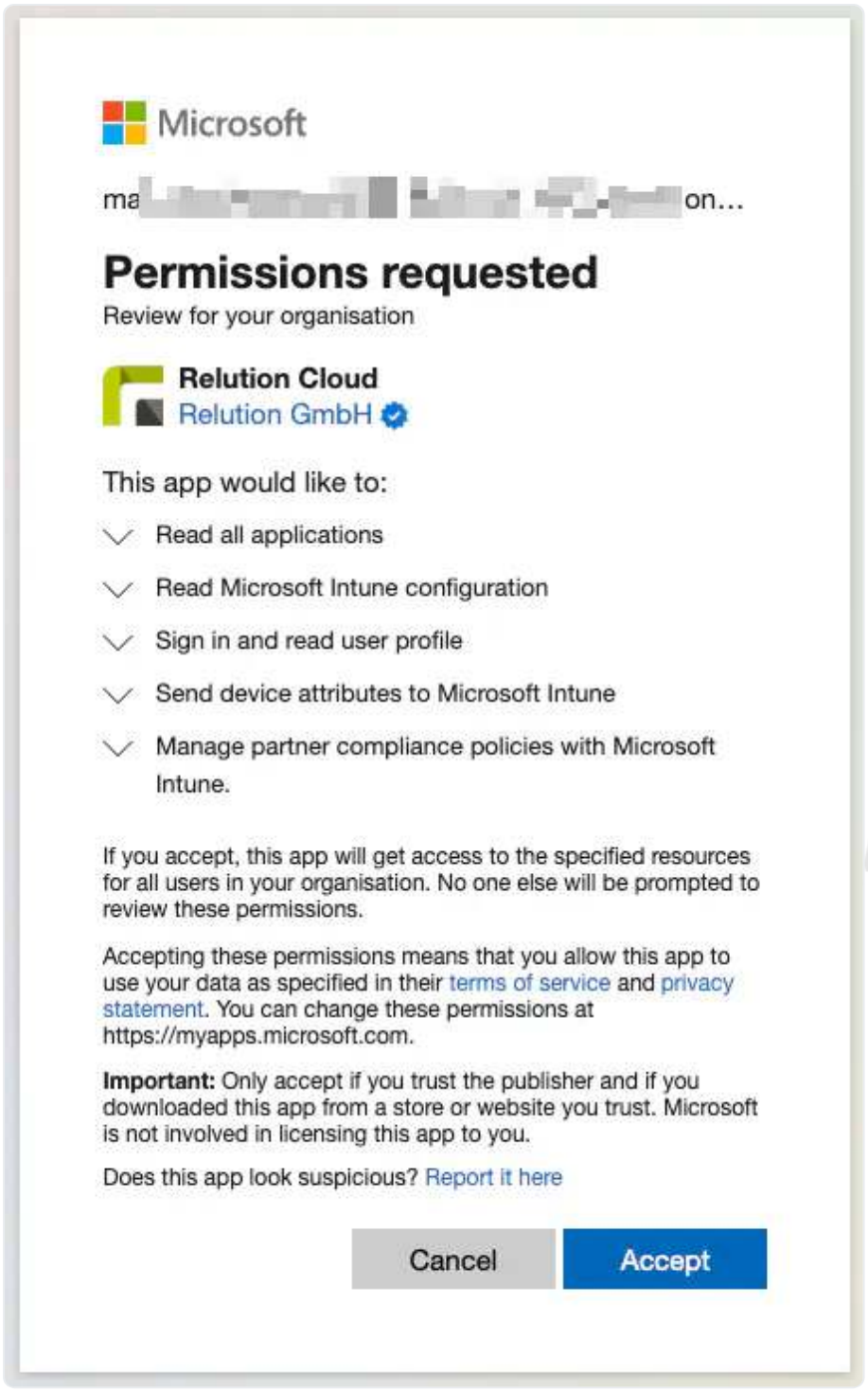
For Android Enterprise and iOS, Relution distributes the broker app `Microsoft Authenticator` itself. For macOS, the `Company Portal App` has to be distributed to the devices separately, e.g. via the Relution Store and a policy, see Preconditions →.

Wizard (5): Grant Consent

> This step will only work if at least one platform was linked in the previous step.

In this step, `admin consent` is granted to the `multi-tenant app Relution`. This step is necessary so that `Relution` is allowed to actually manipulate compliance states of the `Entra ID devices`. Clicking Open Consent saves the wizard data entered so far and opens the consent page in a new tab (the browser may block it as a pop-up). After successfully granting consent, a confirmation page appears: `Success! You can now close this tab`. This extra tab can now be closed. In the wizard, the consent can be checked via Verify before continuing. If consent has already been granted, Open Consent is disabled.

For Version 26.4.0



Wizard (6): Synchronize

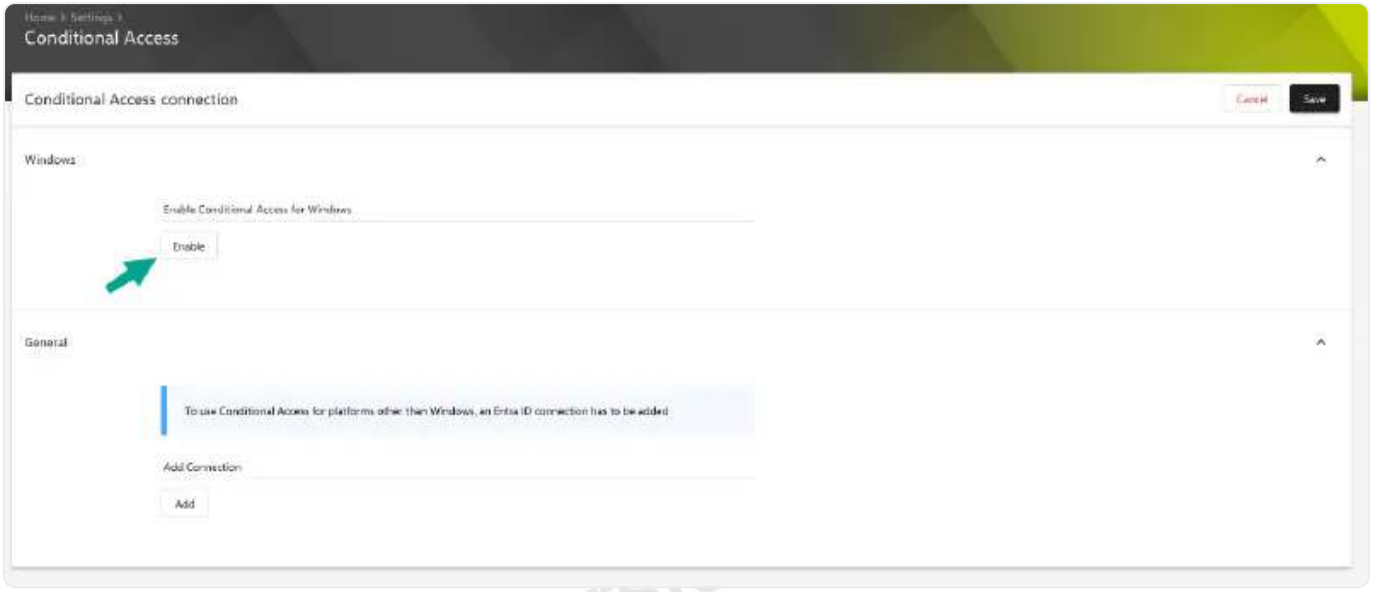
Lastly, the `Entra ID groups` are synchronized. In the Synchronize wizard step, the configuration is first checked via Verify. Only after a successful check can Sync Entra ID groups be clicked; until then, the button is disabled and a notice points to the missing check. During this synchronization, `Relution` ensures a correct setup and syncs the groups assigned in Intune during step 4. Finally, the wizard is completed via Save.

In the Intune Partner Compliance Management → setting, `Relution` should now be shown as `✅ Active`.

If changes are made to groups or platforms in Intune, a sync has to be triggered manually in Relution.

Support for Windows

Windows devices require neither the wizard nor a compliance partner in Intune. On the Conditional Access settings page, Enable is clicked next to Enable Conditional Access for Windows in the Windows section. The change takes effect immediately.



Windows devices should now sync their compliance status successfully.

Managing the Connection

After the setup, the Conditional Access settings page shows the following areas:

- General: Edit connection opens the wizard again, Delete connection removes the connection. Disable Conditional Access stops sending compliance updates to Microsoft, Enable Conditional Access turns them back on. Verify checks the configuration at any time.
- Partner details: Sync Entra ID groups starts the synchronization manually, e.g. after changes to groups or platforms in Intune. Last Heartbeat, Last Synchronisation and the platforms (Android, iOS, macOS) whose groups were synchronized are shown as well.
- Devices that encountered issues during their last sync: list of the affected devices with user, state (e.g. The intune license is missing) and Last error message. After the cause has been fixed, e.g. by assigning an Intune license, the transfer is triggered again via Sync.

If the connection is faulty, e.g. due to missing admin consent, invalid credentials (expired client secret), a missing `Relution.Auth` scope or no platform linked in Intune, the page shows a warning. After fixing the problem, the partner details have to be synchronized again via Sync Entra ID groups.

Related Topics

- Conditional Access Overview → — Requirements and fundamentals for Conditional Access.
- Link Microsoft Entra ID → — Linking Entra ID and synchronizing users, a precondition for Conditional Access.
- OIDC with Entra → — Sign-in of Entra users to Relution via OpenID Connect.

For version 26.4.0

Setup Intune Policies

This guide explains how to configure and test `Conditional Access Policies` in `Microsoft Intune`. These policies define how access is granted or denied for users based on the compliance state of their devices. Further information is available in the official Microsoft Conditional Access documentation →.

> Misconfigured Conditional Access policies can unintentionally block users from signing in. Relution is not liable for any damages resulting from improper configuration.
>
> Targeting All cloud apps in the Target resources with strict policies will also block users from registering their devices.

Recommendations from Relution

To ensure a smooth rollout, `Relution` recommends the following:

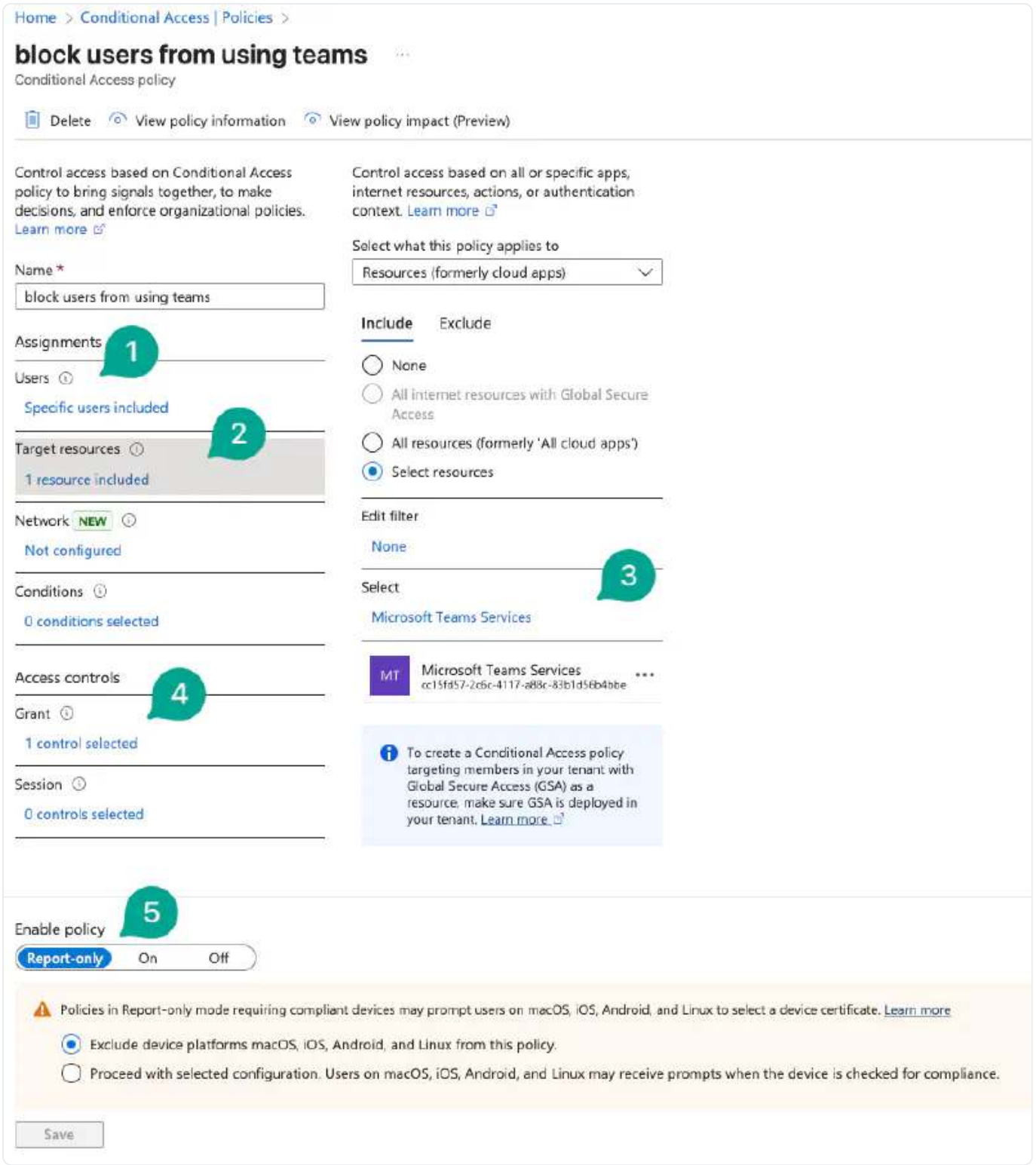
- Initially, either
  - policies are run in Report-only mode to simulate their effect before enforcement
  - OR the policy is applied to a limited group of test users first
- Selecting All cloud apps in the Target resources should be avoided. Selecting All cloud apps with strict policies will block users from being able to register their device. As of today, the `Microsoft Broker app` can't be selected in the Exclude filter, which always needs to be enabled.
  - A good starting point is to target Office 365 →.

For Version 26.4.0

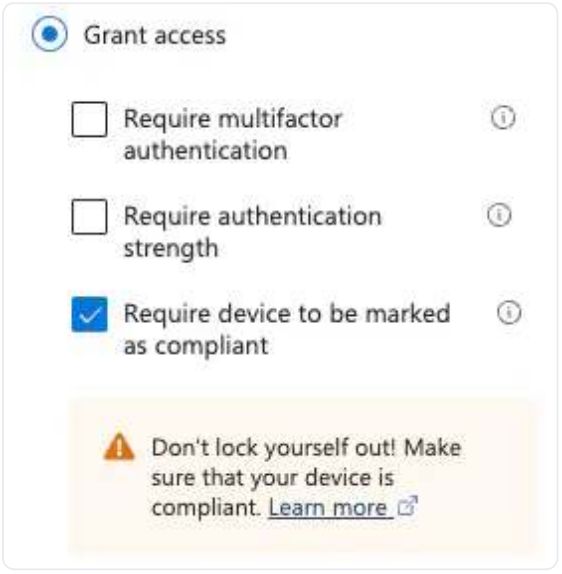
Example Policy Setup

Policies can be configured in Intune > Endpoint security > Conditional Access > Policies →.

The following screenshot shows an example:



Example configuration:

1. Under Users, the users the policy applies to are selected.
2. Under Target resources, the policy is set to apply to selected resources.
3. In this example, Microsoft Teams is selected as the resource.
4. Under Grant, the access requirement is defined, e.g. only devices marked as compliant are allowed.
   - 

5. The policy is set to Report-only to test it without impact.

On Android Enterprise, iOS and macOS, the requirement that the device must be marked as compliant only takes effect for devices to which the `Conditional Access` configuration has been assigned in Relution through a policy and whose users are synchronized in Intune via the Relution compliance partner. The affected users also need an Intune license; if it is missing, the device is listed on the Conditional Access settings page with the status The intune license is missing. After the license has been assigned, the transfer is triggered again there via Sync. More information: Preconditions → and Set up platforms →.

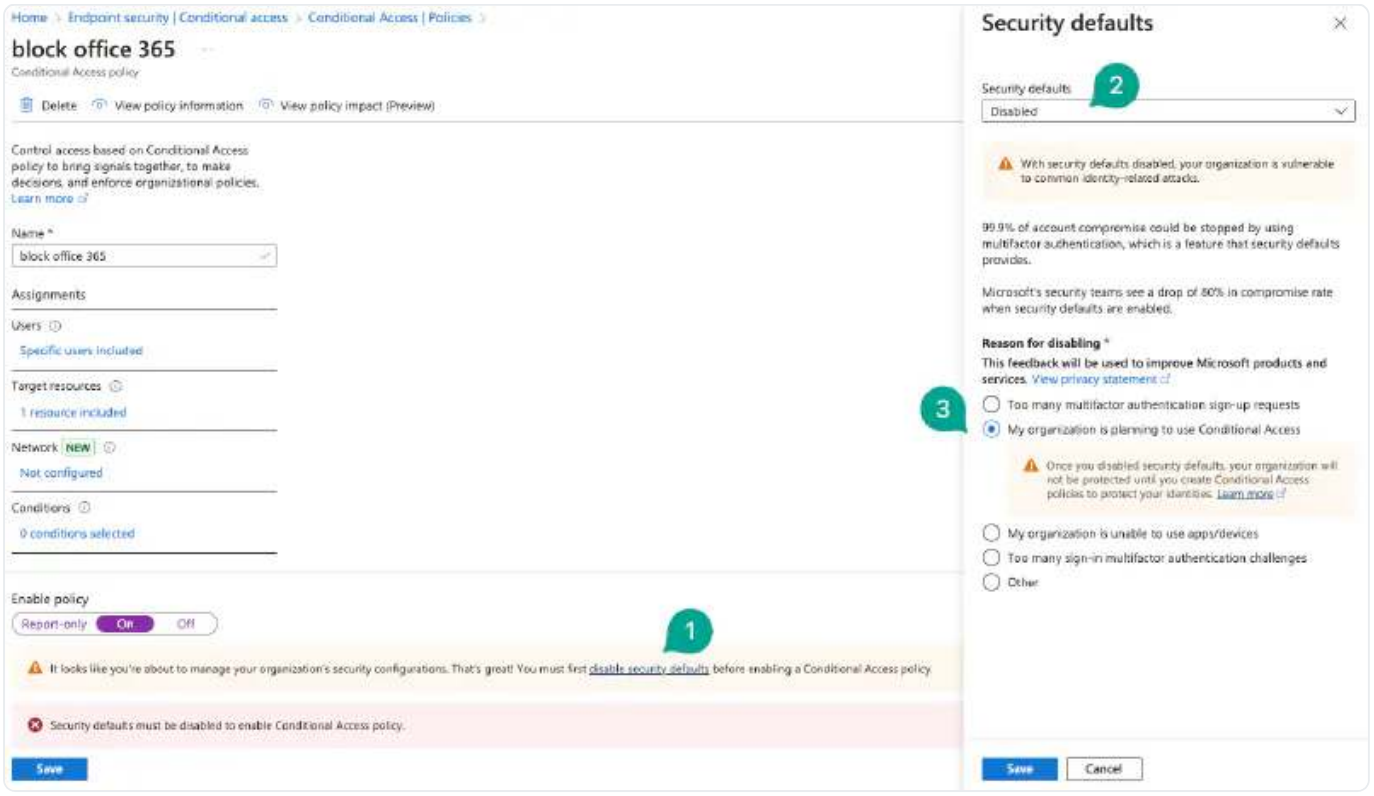
For version 26.4.0

Disable Security Defaults

If an error about security defaults is received, they must be disabled before Conditional Access policies can be used. More information can be found in the Microsoft documentation on security defaults →.

The security defaults are disabled as follows:

1. Disable security defaults is clicked.
2. Disabled is selected.
3. The selection is confirmed with My organization is planning to use Conditional Access.



Debugging and Policy Evaluation

PDF version 26.4.0

The Sign-in logs view in `Entra ID` or `Intune` shows whether and which Conditional Access policy was applied; the Conditional Access tab lists applied or evaluated policies.

Additionally, `Microsoft` offers a useful tool for troubleshooting and policy simulation: What If tool →. It simulates and analyzes the effect of policies before they are actually enabled.

Help with Conditional Access

- Where can I check if a device is compliant or non-compliant in Microsoft?
- The device is marked as N/A in Microsoft
- The device is marked as non-compliant in Microsoft, but the user can still access blocked apps
- The user can't register the device due to a Conditional Access block
- The device is blocked as non-compliant
- The device is not registered
- The user or device can't be registered

For version 26.4.0